# ACCORDO SUL TRATTAMENTO DEI DATI PERSONALI E DI RISERVATEZZA

**Data Processing Agreement (art. 28 GDPR) e Non-Disclosure Agreement**

**Versione 2.0 del 23/11/2026**

**Responsabile del trattamento:** Clanto Services S.r.l.s. a Socio Unico – Sede legale: Via delle Ginestre 16, 80017 Melito di Napoli (NA) – P.IVA e C.F.: IT07321581212 – Referente per la protezione dei dati: privacy@clanto.it – PEC: clanto.services.srls@pec.it; per le istituzioni scolastiche: scuole@pec.clanto.it (di seguito "**Responsabile**").

**Titolare del trattamento:** il soggetto identificato nel Modulo di adesione (di seguito "**Titolare**"); congiuntamente denominati "**Parti**" e singolarmente "**Parte**".

## PREMESSO CHE:

a) il Titolare ha affidato o potrà affidare al Responsabile uno o più dei Contratti di cui all'Art. 1 e, prima o indipendentemente da essi, gli richiede Attività Preliminari che comportano il trattamento di dati personali per suo conto;

b) l'esecuzione dei Contratti comporta il trattamento di dati personali riferiti al personale, ai collaboratori, agli utenti, ai clienti e ai fornitori del Titolare, ivi compresi, ove il Titolare sia un'istituzione scolastica o comunque tratti dati di soggetti di minore età, Dati dei Minori, ed eventualmente categorie particolari di dati;

c) il Responsabile presenta garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate ai sensi dell'art. 28, par. 1, GDPR, anche in ragione delle certificazioni ISO 9001, ISO/IEC 27001, 27017, 27018, 27701 e ISO 31700 di cui è in possesso, verificabili nella sezione Certificazioni del Compliance Center di cui all'Art. 1;

d) l'art. 28, par. 3, GDPR richiede che i trattamenti svolti dal Responsabile per conto del Titolare siano disciplinati da un contratto o da altro atto giuridico che vincoli il Responsabile al Titolare;

**tutto ciò premesso, il Titolare nomina il Responsabile quale Responsabile del trattamento e le Parti convengono quanto segue**

*Le premesse, gli Allegati e il Modulo di adesione costituiscono parte integrante e sostanziale del presente Accordo.*

## 1 – DEFINIZIONI

I termini utilizzati nel presente Accordo hanno il significato loro attribuito dall'art. 4 GDPR e dai Contratti. In particolare:

**Accordo (o DPA)**: il presente accordo, che disciplina il trattamento dei dati personali svolto dal Responsabile per conto del Titolare ai sensi dell'art. 28 GDPR e la riservatezza delle informazioni scambiate tra le Parti, comprensivo degli Allegati e del Modulo di adesione.

**Contratti**: il Contratto di Assistenza Tecnica Informatica e Servizi Gestiti per le imprese, il Contratto di Assistenza Tecnica Informatica e Servizi Gestiti Scolastici (singolarmente "Contratto di Assistenza"), il Contratto di Servizi di Gestione delle Piattaforme Didattiche ("Contratto Piattaforme"), il Contratto di Servizi DLP ("Contratto DLP"), i contratti o gli ordini di hosting, colocation e servizi cloud e gli Incarichi di Consulenza, ove stipulati o accettati dal Titolare.

**Modulo di adesione**: il documento con cui il Titolare, identificandosi, aderisce alla versione del presente Accordo ivi indicata e ne approva specificamente le clausole ai sensi degli artt. 1341 e 1342 c.c.

**Legale Rappresentante**: la persona fisica che rappresenta il Titolare; per le istituzioni scolastiche, il Dirigente Scolastico pro tempore.

**Atto di Affidamento**: il provvedimento con cui un Titolare soggetto alla normativa in materia di contratti pubblici affida i Contratti al Responsabile, unitamente all'offerta o al preventivo in esso richiamati.

**Richiesta di Attivazione**: la richiesta scritta con cui il Legale Rappresentante o il Referente, tramite i canali previsti dai Contratti, chiede l'attivazione di servizi a richiesta, integrazioni o ulteriori funzionalità, conservata dal Responsabile quale istruzione documentata.

**Incarico di Consulenza**: l'attività affidata al Responsabile mediante preventivo o offerta accettati dal Titolare, anche anteriore o indipendente dagli altri Contratti, quale a titolo esemplificativo audit e assessment dell'infrastruttura, sopralluoghi tecnici, verifiche di conformità, vulnerability assessment e penetration test, progettazione di architetture.

**Attività Preliminari**: le attività svolte dal Responsabile su richiesta del Titolare prima della stipula di un Contratto o dell'accettazione di un preventivo, al fine di valutare la situazione e formulare un'offerta o di contenere un'emergenza, quali a titolo esemplificativo sopralluoghi, censimento di postazioni e apparati, analisi dell'infrastruttura, primo contenimento e valutazione di incidenti di sicurezza.

**Servizi**: le prestazioni oggetto dei Contratti effettivamente attivate, come risultanti dai Contratti, dall'Atto di Affidamento, dal Portale Cliente, dalle conferme d'ordine e dalle Richieste di Attivazione.

**Fornitori del Cliente**: i soggetti con cui il Titolare intrattiene un rapporto contrattuale diretto (a titolo esemplificativo: fornitori di piattaforme cloud, di software gestionali, di connettività), che non sono Sub-responsabili del Responsabile.

**Fornitore della Piattaforma**: Google o Microsoft, in quanto fornitore di Google Workspace for Education o di Microsoft 365 Education in forza del contratto direttamente stipulato con il Titolare.

**Sub-responsabile**: il soggetto di cui il Responsabile si avvale per l'esecuzione di specifiche attività di trattamento per conto del Titolare, ai sensi dell'art. 28, par. 4, GDPR.

**Partner Tecnico**: il soggetto convenzionato con il Responsabile per gli interventi presso le sedi del Titolare, secondo quanto previsto dai Contratti.

**Amministratore di sistema**: la figura di cui al provvedimento dell'Autorità Garante per la protezione dei dati personali del 27 novembre 2008 e successive modificazioni.

**Referente**: la persona designata per iscritto dal Legale Rappresentante a interloquire con il Responsabile.

**Dati dei Minori**: i dati personali riferiti agli studenti e comunque a soggetti di minore età.

**Violazione**: la violazione dei dati personali di cui all'art. 4, n. 12, GDPR.

**Compliance Center**: la sezione del sito del Responsabile disponibile all'indirizzo https://clanto.it/compliance, che raccoglie la documentazione richiamata dal presente Accordo, organizzata nelle sezioni Certificazioni, Sub-responsabili, Informativa sul trattamento dei dati personali, Conservazione dei dati e Documentazione contrattuale. Il Responsabile mantiene disponibili tali sezioni per tutta la durata dell'Accordo e conserva lo storico datato delle versioni pubblicate, di cui fornisce copia al Titolare su richiesta.

**GDPR**: il Regolamento (UE) 2016/679, nonché il D.Lgs. 196/2003 come modificato dal D.Lgs. 101/2018.

## 2 – Oggetto e ambito

**2.1 — Nomina e oggetto.** Il Titolare nomina il Responsabile quale Responsabile del trattamento ai sensi dell'art. 28 GDPR per i trattamenti di dati personali necessari all'esecuzione dei Contratti e delle Attività Preliminari, descritti nell'Allegato A.

**2.2 — Applicabilità.** Le schede dell'Allegato A si applicano limitatamente ai Servizi attivati. L'Allegato D si applica se il Titolare ha stipulato il Contratto Piattaforme; l'Allegato F se il Titolare ha comunicato di essere soggetto alla disciplina NIS2 secondo il punto F.1; l'Allegato G se il Titolare è una pubblica amministrazione. Le schede e gli allegati non applicabili sono privi di effetto.

**2.3 — Fornitori del Cliente.** I Fornitori del Cliente, ivi compreso il Fornitore della Piattaforma, trattano i dati personali in forza dei rapporti diretti con il Titolare e non sono Sub-responsabili del Responsabile, anche ove i relativi servizi siano acquistati per il tramite del Responsabile quale rivenditore autorizzato. Il Responsabile non risponde dei trattamenti effettuati dai Fornitori del Cliente e dai fornitori di servizi e applicazioni di terze parti attivati dal Titolare.

**2.4 — Sostituzione di precedenti atti.** Il presente Accordo sostituisce ogni precedente atto di nomina, designazione o accordo relativo al trattamento dei dati personali per i medesimi Servizi, ivi comprese le nomine ad amministratore di sistema o di dominio riferite al Responsabile in quanto persona giuridica, la cui disciplina è assorbita dall'Art. 7.

**2.5 — Efficacia autonoma.** Il presente Accordo può essere sottoscritto anche in assenza di altri Contratti e disciplina in tal caso le Attività Preliminari. La richiesta scritta del Legale Rappresentante o del Referente, anche via email o tramite i canali del Responsabile, costituisce istruzione documentata ai sensi dell'Art. 5. Il presente Accordo non obbliga il Responsabile a eseguire prestazioni né il Titolare a corrisponderle: le condizioni economiche delle Attività Preliminari e dei servizi successivi sono disciplinate dal preventivo o dall'accordo scritto tra le Parti, anche via email, fermo quanto previsto dall'Allegato G per le pubbliche amministrazioni.

**2.6 — Responsabilità nelle Attività Preliminari.** Per le Attività Preliminari la responsabilità del Responsabile nei confronti del Titolare è limitata ai casi di dolo e colpa grave, salvi i limiti inderogabili di legge e la responsabilità verso gli interessati ai sensi dell'art. 82 GDPR.

## 3 – Durata

**3.1 — Efficacia e durata.** Il presente Accordo è efficace dal perfezionamento di cui all'Art. 21.6 e ha la medesima durata dei Contratti. Con riferimento a ciascun Servizio, cessa alla cessazione del relativo Contratto o alla disattivazione del Servizio; cessa integralmente alla cessazione dell'ultimo Contratto in essere, senza necessità di revoca. Per gli Incarichi di Consulenza, cessa con la conclusione dell'incarico e il completamento degli adempimenti di cui all'Art. 15. In assenza di Contratti, l'Accordo cessa decorsi 90 giorni dall'ultima Attività Preliminare senza che sia stato accettato un preventivo o stipulato un Contratto; in tal caso si applica l'Art. 15, con termine di 30 giorni dalla cessazione.

**3.2 — Obblighi successivi.** Gli obblighi di cui agli Artt. 13, 15, 16 e 20 permangono anche dopo la cessazione, per il tempo necessario al loro adempimento.

## 4 – Natura, finalità, dati e interessati

**4.1 — Descrizione dei trattamenti.** La natura e la finalità dei trattamenti, le operazioni, le categorie di interessati e di dati personali, i tempi di conservazione e la localizzazione sono descritti, per ciascun Servizio, nell'Allegato A.

**4.2 — Dati dei Minori e categorie particolari.** Nell'esecuzione dei Servizi il Responsabile può trattare Dati dei Minori e venire a conoscenza, anche incidentalmente, di dati appartenenti alle categorie particolari di cui all'art. 9 e di dati relativi a condanne penali e reati di cui all'art. 10 GDPR presenti nei sistemi del Titolare. Il Responsabile tratta tali dati esclusivamente nella misura strettamente necessaria all'esecuzione della singola attività e, per i Dati dei Minori, con le cautele di cui agli Artt. 14.4–14.6.

**4.3 — Divieto di finalità proprie.** Il Responsabile non tratta i dati personali per finalità proprie o di terzi, ivi comprese finalità di marketing e di profilazione e, salvo quanto previsto all'Art. 14.8, di addestramento di modelli di intelligenza artificiale.

## 5 – Istruzioni documentate

**5.1 — Trattamento su istruzione.** Il Responsabile tratta i dati personali soltanto su istruzione documentata del Titolare, anche in caso di trasferimento verso un paese terzo, salvo che lo richieda il diritto dell'Unione o nazionale; in tal caso ne informa il Titolare prima del trattamento, salvo che tale diritto lo vieti.

**5.2 — Fonti delle istruzioni.** Costituiscono istruzioni documentate del Titolare i Contratti, l'Atto di Affidamento, il presente Accordo, l'Allegato D, le Richieste di Attivazione e le istruzioni scritte impartite dal Legale Rappresentante o dal Referente tramite i canali previsti dai Contratti.

**5.3 — Istruzioni contrarie alla normativa o alla sicurezza.** Il Responsabile informa immediatamente il Titolare qualora, a suo parere, un'istruzione violi il GDPR o altre disposizioni in materia di protezione dei dati, e può sospenderne l'esecuzione fino alla conferma o alla modifica dell'istruzione. Si applicano le disposizioni dei Contratti in materia di richieste contrarie alla sicurezza o alla normativa, ove presenti. In assenza di analoghe disposizioni nei Contratti applicabili, il Responsabile può rifiutare le istruzioni che eliminino un controllo di sicurezza essenziale ai sensi

dell'art. 32 GDPR ed esegue quelle che riducono un controllo solo previa accettazione scritta dei rischi da parte del Titolare; il rifiuto, motivato per iscritto, non costituisce inadempimento.

**5.4 — Attività straordinarie.** Le istruzioni che richiedono attività non previste dai Contratti sono eseguite quali prestazioni accessorie secondo quanto previsto dai Contratti medesimi, previa accettazione del relativo preventivo da parte del Titolare.

## 6 – Personale autorizzato

**6.1 — Autorizzazione e riservatezza.** Il Responsabile garantisce che le persone autorizzate al trattamento dei dati personali siano autorizzate per iscritto, adeguatamente istruite e vincolate a un obbligo legale o contrattuale di riservatezza.

**6.2 — Formazione.** Il Responsabile assicura la formazione periodica del personale autorizzato in materia di protezione dei dati e di sicurezza delle informazioni.

**6.3 — Accesso minimo.** L'accesso del personale ai dati personali è limitato a quanto strettamente necessario all'esecuzione della singola attività.

## 7 – Amministratori di sistema

**7.1 — Designazione.** Il Responsabile designa individualmente quali Amministratori di sistema le persone fisiche del proprio personale preposte ai Servizi, previa valutazione delle caratteristiche di esperienza, capacità e affidabilità, ai sensi del provvedimento dell'Autorità Garante per la protezione dei dati personali del 27 novembre 2008 e successive modificazioni.

**7.2 — Conservazione e consegna.** Il Responsabile conserva gli atti di designazione e gli estremi identificativi degli Amministratori di sistema, con l'indicazione dei rispettivi ambiti di operatività, e li rende disponibili al Titolare su richiesta entro 5 giorni lavorativi, in forma di elenco aggiornato e, ove richiesto, in copia.

**7.3 — Registrazione degli accessi.** Gli accessi amministrativi sono registrati con modalità che ne garantiscono la completezza e l'inalterabilità, conservati per almeno sei mesi e resi disponibili al Titolare per la verifica annuale dell'operato degli Amministratori di sistema. L'analisi dei log è effettuata per sole finalità di sicurezza e non per il controllo dell'attività degli utenti.

## 8 – Misure di sicurezza

**8.1 — Misure adottate.** Il Responsabile adotta le misure tecniche e organizzative di cui all'art. 32 GDPR descritte nell'Allegato B, adeguate al rischio e, ove presenti, ai Dati dei Minori.

**8.2 — Certificazioni.** Il Responsabile mantiene le certificazioni di cui alle premesse, verificabili nella sezione Certificazioni del Compliance Center, e comunica senza ritardo al Titolare la perdita, la sospensione o la riduzione del campo di applicazione di ciascuna di esse.

**8.3 — Evoluzione delle misure.** Il Responsabile può aggiornare le misure di sicurezza in funzione dell'evoluzione tecnologica e dei rischi, a condizione che il livello di protezione complessivo non sia inferiore a quello descritto nell'Allegato B.

**8.4 — Documentazione.** La documentazione di dettaglio delle misure è resa disponibile al Titolare nell'ambito delle verifiche di cui all'Art. 16, nel rispetto degli obblighi di riservatezza e della tutela della sicurezza dei sistemi del Responsabile e degli altri clienti.

## 9 – Sub-responsabili

**9.1 — Autorizzazione generale.** Il Titolare autorizza in via generale il Responsabile ad avvalersi dei Sub-responsabili indicati nella sezione Sub-responsabili del Compliance Center, nella versione vigente alla data di adesione al presente Accordo.

**9.2 — Obblighi dei Sub-responsabili.** Il Responsabile impone ai Sub-responsabili, mediante contratto, i medesimi obblighi in materia di protezione dei dati previsti dal presente Accordo, con garanzie sufficienti in ordine alle misure tecniche e organizzative.

**9.3 — Modifiche.** Il Responsabile comunica al Titolare ogni aggiunta o sostituzione di Sub-responsabili con almeno 30 giorni di anticipo, mediante pubblicazione nella sezione Sub-responsabili del Compliance Center e contestuale comunicazione via email ai contatti indicati nel Modulo di adesione. Entro tale termine il Titolare può opporsi per motivi ragionevoli connessi alla protezione dei dati; decorso il termine senza opposizione, la modifica si intende autorizzata.

**9.4 — Opposizione.** In caso di opposizione fondata, qualora il Responsabile non sia in grado di proporre una soluzione alternativa, il Titolare può recedere dal Servizio interessato senza oneri ulteriori rispetto al corrispettivo delle prestazioni eseguite.

**9.5 — Responsabilità.** Il Responsabile conserva nei confronti del Titolare l'intera responsabilità dell'adempimento degli obblighi dei Sub-responsabili.

**9.6 — Partner Tecnici.** Il Responsabile può avvalersi dei Partner Tecnici pubblicati nella sezione Sub-responsabili del Compliance Center per gli interventi presso le sedi del Titolare esclusivamente previa autorizzazione specifica del Titolare per il singolo intervento, ai sensi dell'art. 28, par. 2, GDPR. Ciascun Partner Tecnico è vincolato dal Responsabile agli obblighi del presente Accordo mediante accordo ai sensi dell'art. 28, par. 4, GDPR. In mancanza di autorizzazione, l'intervento è eseguito da personale del Responsabile.

## 10 – Localizzazione e trasferimenti

**10.1 — Localizzazione.** I dati personali trattati dal Responsabile e dai Sub-responsabili sono trattati all'interno dello Spazio Economico Europeo, anche con riferimento agli accessi da remoto.

**10.2 — Trasferimenti.** Nessun trasferimento di dati personali verso paesi terzi od organizzazioni internazionali è effettuato senza la previa autorizzazione scritta del Titolare e senza il rispetto delle condizioni di cui al Capo V GDPR.

**10.3 — Trattamenti di terzi.** Restano esclusi dal presente articolo i trattamenti effettuati dai Fornitori del Cliente, ivi compreso il Fornitore della Piattaforma, e dai fornitori di servizi e applicazioni di terze parti attivati dal Titolare, disciplinati dai rapporti diretti tra questi e il Titolare.

**10.4 — Richieste delle autorità pubbliche.** Qualora riceva da un'autorità pubblica una richiesta di accesso o di comunicazione dei dati personali trattati per conto del Titolare, il Responsabile:

a) verifica la base giuridica e la competenza dell'autorità richiedente e comunica esclusivamente i dati strettamente necessari ad adempiere a un obbligo giuridico;
b) informa senza ritardo il Titolare, salvo che ciò sia vietato dalla legge;
c) contesta le richieste che ritenga illegittime o sproporzionate, nei limiti consentiti dall'ordinamento;
d) documenta la richiesta e la risposta fornita.

Le richieste di autorità di paesi terzi non sono eseguite se non nei limiti dell'art. 48 GDPR.

**10.5 — Giurisdizione.** Il Responsabile ha sede nello Spazio Economico Europeo e non è soggetto a normative di paesi terzi che impongano la comunicazione di dati ad autorità extra-UE. I Sub-responsabili sono selezionati tra soggetti che erogano i servizi tramite entità stabilite nello Spazio Economico Europeo.

## 11 – Diritti degli interessati

**11.1 — Richieste.** Il Responsabile inoltra al Titolare ogni richiesta di esercizio dei diritti di cui agli artt. 15–22 GDPR ricevuta direttamente dagli interessati entro 2 giorni lavorativi dalla ricezione, senza darvi riscontro, salvo diversa istruzione del Titolare.

**11.2 — Assistenza.** Tenendo conto della natura del trattamento, il Responsabile assiste il Titolare con misure tecniche e organizzative adeguate per dare seguito alle richieste degli interessati.

## 12 – Assistenza al Titolare

**12.1 — Ambito.** Tenendo conto della natura del trattamento e delle informazioni a sua disposizione, il Responsabile assiste il Titolare nel garantire il rispetto degli obblighi di cui agli artt. 32–36 GDPR, ivi compresa la valutazione d'impatto sulla protezione dei dati e l'eventuale consultazione preventiva dell'Autorità di controllo.

**12.2 — Modalità.** Il Responsabile fornisce senza costi aggiuntivi le informazioni relative ai Servizi necessarie alle valutazioni del Titolare, nella forma della documentazione standard del Responsabile. Le attività di redazione o di consulenza eccedenti sono prestazioni accessorie ai sensi dei Contratti.

## 13 – Violazioni dei dati personali

**13.1 — Comunicazione.** Il Responsabile comunica al Titolare ogni Violazione senza ingiustificato ritardo e comunque entro 48 ore dal momento in cui ne è venuto a conoscenza, a mezzo PEC al Titolare e con contestuale avviso al Referente o al Responsabile della Protezione dei Dati del Titolare, ai contatti indicati nel Modulo di adesione.

**13.2 — Contenuto.** La comunicazione contiene almeno le informazioni di cui all'art. 33, par. 3, GDPR: la natura della Violazione, le categorie e il numero approssimativo di interessati e di registrazioni coinvolti, le probabili conseguenze, le misure adottate o proposte e il punto di contatto del Responsabile. Qualora non sia possibile fornire tutte le informazioni contestualmente, esse sono fornite in fasi successive senza ulteriore ingiustificato ritardo.

**13.3 — Contenimento e cooperazione.** Il Responsabile adotta immediatamente le misure di contenimento ragionevolmente possibili e coopera con il Titolare per l'analisi della Violazione e per gli adempimenti di cui agli artt. 33 e 34 GDPR.

**13.4 — Comunicazioni a terzi.** Il Responsabile non effettua comunicazioni relative alla Violazione agli interessati, all'Autorità di controllo o a terzi senza istruzione del Titolare, salvo che vi sia tenuto per legge.

**13.5 — Documentazione.** Il Responsabile documenta le Violazioni in un registro interno, reso disponibile al Titolare per le Violazioni che lo riguardano.

## 14 – Lavoratori, minori e intelligenza artificiale

**14.1 — Controllo a distanza.** Gli strumenti utilizzati per i Servizi sono configurati per finalità di sicurezza, manutenzione e assistenza e non per il controllo dell'attività dei lavoratori del Titolare. Il Titolare, quale datore di lavoro, resta responsabile degli adempimenti di cui all'art. 4 della L. 300/1970 e dell'adeguata informazione ai lavoratori. Le funzionalità che consentono un controllo dell'attività dei lavoratori, ivi comprese quelle oggetto del Contratto DLP e dei servizi di Data Loss Prevention, sono attivate esclusivamente su istruzione scritta del Titolare, che dichiara di aver espletato tali adempimenti.

**14.2 — Metadati della posta elettronica.** I registri del server di posta del Responsabile, contenenti i metadati dei messaggi, sono conservati per 7 giorni per finalità di sicurezza e di funzionamento del servizio. Una conservazione più lunga è possibile solo su istruzione scritta del Titolare, che dichiara di aver espletato gli adempimenti di cui all'Art. 14.1.

**14.3 — Accesso ai contenuti.** L'accesso ai contenuti dei dispositivi, delle caselle di posta, delle piattaforme e degli archivi del Titolare è limitato a quanto strettamente necessario per la gestione della singola richiesta o attività ed è tracciato.

**14.4 — Dati dei Minori.** Ove il Titolare tratti Dati dei Minori, il loro trattamento da parte del Responsabile è improntato a cautele rafforzate, nel rispetto dei principi di minimizzazione e di protezione dei dati fin dalla progettazione e per impostazione predefinita.

**14.5 — Contatti con i minori.** I contatti tra il personale del Responsabile e gli studenti o altri soggetti di minore età avvengono esclusivamente tramite i canali tracciati previsti dai Contratti. Il personale del Responsabile non intrattiene contatti con i minori al di fuori di tali canali e non richiede dati personali ulteriori rispetto a quelli necessari alla gestione della richiesta. Tramite canali di comunicazione diversi dall'indirizzo email di supporto del Titolare non sono trasmessi documenti né dati personali dei minori.

**14.6 — Divieti.** È escluso qualsiasi trattamento dei Dati dei Minori per finalità di profilazione, di marketing o commerciali.

**14.7 — Intelligenza artificiale.** I sistemi di intelligenza artificiale utilizzati per i Servizi sono eseguiti esclusivamente su infrastruttura di proprietà del Responsabile ubicata nello Spazio Economico Europeo, senza ricorso a fornitori terzi di modelli, e operano sui dati telemetrici e di log, senza accesso al contenuto dei file del Titolare.

**14.8 — Addestramento di modelli di intelligenza artificiale.** È escluso l'utilizzo dei dati personali trattati per conto del Titolare per l'addestramento, l'affinamento o la valutazione di modelli di intelligenza artificiale. In deroga, tale utilizzo è ammesso esclusivamente su istruzione scritta del Legale Rappresentante, per progetti del Titolare, alle seguenti condizioni:

a) il modello è destinato all'uso esclusivo del Titolare e non è riutilizzato dal Responsabile per altri soggetti o finalità;
b) il progetto è disciplinato da specifico accordo scritto che ne definisce finalità, dati, durata e destinazione del modello al termine;
c) il Titolare ha effettuato la valutazione d'impatto ai sensi dell'art. 35 GDPR, ove necessaria, e adempiuto agli obblighi informativi;
d) i dati sono previamente pseudonimizzati o, ove possibile, anonimizzati e limitati a quanto necessario.

## 15 – Restituzione e cancellazione

**15.1 — Scelta del Titolare.** Alla cessazione di ciascun Servizio, il Titolare può richiedere per iscritto, entro 30 giorni, la restituzione dei dati personali in possesso del Responsabile. La restituzione avviene in formato strutturato, di uso comune e leggibile, entro 15 giorni dalla richiesta, e comprende in particolare le caselle di posta in formato standard, i file del cloud aziendale, l'esportazione cifrata degli archivi del password manager e i dati di backup; per i servizi di hosting e cloud, comprende l'esportazione dei siti, dei database e, ove tecnicamente possibile, delle immagini delle macchine virtuali in formati standard. I dati sono cancellati entro 7 giorni dalla consegna; in mancanza di richiesta, entro 7 giorni dalla scadenza del termine di 30 giorni.

**15.2 — Credenziali di amministrazione.** Le credenziali di amministrazione e le credenziali generiche dei sistemi del Titolare conservate nell'archivio dedicato al Cliente sono consegnate al Titolare, in forma cifrata, prima della cancellazione, indipendentemente dalla richiesta di cui al paragrafo 15.1.

**15.3 — Tabella di corrispondenza.** Ove attivo il servizio di pseudonimizzazione, la tabella di corrispondenza tra l'identità degli utenti e gli identificativi pseudonimi è trattata alla cessazione del servizio secondo la procedura di cui al punto D.7 dell'Allegato D.

**15.4 — Dati acquisiti per singole attività.** I dati acquisiti per singole attività di assistenza o manutenzione, quali copie temporanee ed estrazioni di database, sono cancellati al termine dell'attività, unitamente a tutte le relative copie.

**15.5 — Copie di backup.** Le copie conservate nell'ambito del servizio di backup seguono la politica di conservazione concordata con il Titolare e sono cancellate alla cessazione del servizio secondo il paragrafo 15.1. Le copie di sicurezza dei sistemi del Responsabile sono eliminate secondo i rispettivi cicli di rotazione, comunque entro 30 giorni dalla cancellazione, e nel frattempo restano protette e non utilizzate.

**15.6 — Obblighi di legge e attestazione.** Restano salvi gli obblighi di conservazione previsti dal diritto dell'Unione o nazionale. Su richiesta del Titolare, il Responsabile rilascia attestazione scritta dell'avvenuta cancellazione.

## 16 – Verifiche e audit

**16.1 — Informazioni e verifiche.** Il Responsabile mette a disposizione del Titolare tutte le informazioni necessarie a dimostrare il rispetto degli obblighi di cui all'art. 28 GDPR e consente e contribuisce alle attività di revisione, comprese le ispezioni, realizzate dal Titolare o da altro soggetto da questi incaricato.

**16.2 — Verifica documentale.** Le verifiche sono svolte in via prioritaria su base documentale, mediante esibizione delle certificazioni in corso di validità, risposta a questionari ed esibizione di estratti della documentazione del sistema di gestione.

**16.3 — Audit in loco.** Gli audit in loco sono concordati con un preavviso di almeno 15 giorni, si svolgono durante l'orario lavorativo e, salvo Violazioni, richieste dell'Autorità di controllo o fondati motivi, non più di una volta per anno contrattuale. Il soggetto incaricato è vincolato alla riservatezza e non accede ai dati di altri clienti né a informazioni la cui divulgazione comprometta la sicurezza dei sistemi. Ciascuna Parte sostiene i propri costi.

**16.4 — Autorità di controllo.** Il Responsabile coopera, su richiesta, con l'Autorità di controllo ai sensi dell'art. 31 GDPR, informandone il Titolare ove consentito.

## 17 – Registro delle attività di trattamento

Il Responsabile tiene il registro di tutte le categorie di attività relative al trattamento svolte per conto del Titolare ai sensi dell'art. 30, par. 2, GDPR e lo mette a disposizione dell'Autorità di controllo su richiesta.

## 18 – Responsabilità

**18.1 — Responsabilità verso gli interessati.** Il Responsabile risponde per il danno causato dal trattamento ai sensi dell'art. 82 GDPR se non ha adempiuto gli obblighi specificamente diretti ai responsabili del trattamento o ha agito in modo difforme o contrario rispetto alle legittime istruzioni del Titolare.

**18.2 — Rapporti tra le Parti.** Le limitazioni di responsabilità previste dai Contratti e dall'Art. 2.6 operano esclusivamente nei rapporti tra le Parti e nei limiti consentiti dalla legge, e non sono opponibili agli interessati. Resta fermo il diritto di regresso di cui all'art. 82, par. 5, GDPR.

## 19 – Coordinamento

**19.1 — Rapporto con i Contratti.** Il presente Accordo costituisce l'accordo ai sensi dell'art. 28 GDPR per tutti i Contratti e per le Attività Preliminari, ivi compreso l'accordo sul trattamento dei dati personali richiamato da ciascun Contratto. In caso di contrasto, per quanto attiene alla protezione dei dati personali prevale il presente Accordo.

**19.2 — Ulteriori istruzioni.** Le ulteriori istruzioni del Titolare, ivi comprese quelle contenute in modelli, regolamenti o procedure interne del Titolare, sono recepite nell'Allegato D o quali istruzioni scritte ai sensi dell'Art. 5, previa verifica della loro compatibilità con il presente Accordo e con la normativa, e non richiedono ulteriori atti di nomina o di designazione.

## 20 – Riservatezza delle informazioni (NDA)

**20.1 — Obbligo.** Ciascuna Parte mantiene riservate le informazioni dell'altra di cui venga a conoscenza in ragione del presente Accordo, delle Attività Preliminari, dei Contratti o di qualsiasi contatto finalizzato alla loro conclusione, anche in assenza di trattamenti di dati personali e anche se non costituiscono dati personali (a titolo esemplificativo: architettura e configurazioni dei sistemi, vulnerabilità, credenziali, informazioni commerciali); le utilizza esclusivamente per le finalità per cui sono state comunicate e non le divulga a terzi, salvo obbligo di legge o provvedimento dell'autorità.

**20.2 — Esclusioni.** Non sono soggette all'obbligo di riservatezza le informazioni che siano o divengano di pubblico dominio senza violazione del presente Accordo, che fossero già legittimamente note alla Parte ricevente, che siano sviluppate autonomamente senza utilizzo delle informazioni dell'altra Parte, che siano ricevute da terzi non vincolati da obblighi di riservatezza, ovvero la cui divulgazione sia imposta da un obbligo di legge o da un provvedimento dell'autorità; in quest'ultimo caso la Parte ricevente, ove consentito, ne informa preventivamente l'altra.

**20.3 — Personale e terzi.** Ciascuna Parte limita l'accesso alle informazioni riservate al proprio personale e ai terzi che ne abbiano necessità per le finalità del presente Accordo, vincolandoli a obblighi di riservatezza non meno stringenti, e risponde del loro operato.

**20.4 — Sistema di gestione.** Le informazioni sono trattate nell'ambito del sistema di gestione certificato del Responsabile ai sensi delle norme ISO/IEC 27001, 27017, 27018 e 27701, con le misure di cui all'Allegato B, anche quando le Attività Preliminari non sono seguite da un Contratto.

**20.5 — Restituzione.** Alla cessazione del presente Accordo, ovvero su richiesta scritta, ciascuna Parte restituisce o distrugge le informazioni riservate dell'altra in proprio possesso, fatti salvi gli obblighi di conservazione di legge, quanto previsto dall'Art. 15 e dall'Allegato A, e le copie conservate nei sistemi di backup fino alla loro rotazione.

**20.6 — Referenze.** Il Responsabile può indicare il Titolare come cliente o referenza commerciale solo previo consenso scritto del Titolare.

**20.7 — Durata.** L'obbligo di riservatezza permane per 5 anni dalla cessazione del presente Accordo; per le informazioni la cui divulgazione comprometterebbe la sicurezza dei sistemi del Titolare, permane finché esse mantengono carattere riservato.

## 21 – Disposizioni finali

**21.1 — Modifiche.** Le modifiche del presente Accordo sono pubblicate come nuova versione nella sezione Documentazione contrattuale del Compliance Center e notificate direttamente al Titolare via PEC o email ai contatti indicati nel Modulo di adesione. Le modifiche che ampliano i trattamenti o riducono le garanzie per gli interessati sono efficaci solo con la sottoscrizione di un nuovo Modulo di adesione. Le altre modifiche (adeguamenti normativi, rafforzamento delle garanzie, aggiornamento dei riferimenti) sono efficaci decorsi 30 giorni dalla notifica; entro tale termine il Titolare può opporsi e, in mancanza di accordo, recedere senza penali dai Servizi interessati. L'Allegato D è aggiornato mediante istruzione scritta del Titolare accettata dal Responsabile; l'elenco dei Sub-responsabili secondo l'Art. 9.3. Per le pubbliche amministrazioni si applica l'Allegato G.

**21.2 — Contatti.** Per il Titolare: il Legale Rappresentante, il Referente e l'eventuale Responsabile della Protezione dei Dati, ai recapiti indicati nel Modulo di adesione. Per il Responsabile: Referente per la protezione dei dati, email privacy@clanto.it; PEC clanto.services.srls@pec.it o, per le istituzioni scolastiche, scuole@pec.clanto.it.

**21.3 — Legge applicabile e foro.** Il presente Accordo è regolato dalla legge italiana. Si applicano le disposizioni dei Contratti in materia di mediazione e di foro competente; in assenza di Contratti, per i Titolari che non siano pubbliche amministrazioni è competente in via esclusiva il Foro di Napoli Nord. Per le pubbliche amministrazioni si applica l'Allegato G.

**21.4 — Sottoscrizione e versioni.** Il presente Accordo è sottoscritto con firma digitale dal Responsabile e pubblicato nella sezione Documentazione contrattuale del Compliance Center con indicazione della versione e della relativa impronta SHA-256. Ogni versione è conservata in forma immodificabile.

**21.5 — Informativa.** I dati personali del Legale Rappresentante, dei Referenti e del personale del Titolare che interagisce con il Responsabile sono trattati dal Responsabile, in qualità di titolare autonomo, per la gestione del rapporto contrattuale, l'assistenza, la fatturazione e gli adempimenti di legge, secondo l'informativa ai sensi degli artt. 13-14 GDPR pubblicata nella sezione Informativa sul trattamento dei dati personali del Compliance Center, di cui il Titolare dà atto di aver preso visione e che si impegna a portare a conoscenza dei propri Referenti.

**21.6 — Perfezionamento.** Il presente Accordo si perfeziona con la sottoscrizione del Modulo di adesione da parte del Titolare e la sua ricezione da parte del Responsabile; il Modulo di adesione ne costituisce parte integrante.

**Documento firmato digitalmente dal Responsabile. Il Titolare aderisce mediante il Modulo di adesione.**

# Allegato A – Schede dei trattamenti

Ciascuna scheda si applica alle condizioni indicate in testa alla stessa, ai sensi degli Artt. 2.2 e 2.5. Salvo diversa indicazione nella singola scheda, i ticket e le richieste di assistenza sono conservati per 6 mesi, i log e gli eventi per 6 mesi, i log degli accessi amministrativi per almeno 6 mesi. I tempi di conservazione di dettaglio per tipologia di dato sono pubblicati nella sezione Conservazione dei dati del Compliance Center. Salvo diversa indicazione, i dati sono trattati su infrastruttura del Responsabile ubicata nello Spazio Economico Europeo.

## A.1 – Assistenza tecnica, RMM e teleassistenza

**Si applica se:** il Titolare ha stipulato un Contratto di Assistenza.

**Finalità:** monitoraggio, manutenzione, aggiornamento e gestione remota di Postazioni, Server e apparati di rete; assistenza software e hardware; telegestione e teleassistenza.

**Operazioni:** raccolta di dati tecnici e di inventario, consultazione, estrazione occasionale, conservazione temporanea; sessioni di teleassistenza interattive avviate solo con il consenso dell'utente della Postazione e registrate localmente sulla Postazione; operazioni di manutenzione automatizzate dell'RMM eseguite senza sessione interattiva.

**Interessati:** personale, collaboratori e, per le istituzioni scolastiche, studenti del Titolare, nonché altri soggetti i cui dati sono presenti sui Dispositivi.

**Categorie di dati:** dati identificativi degli utenti dei Dispositivi; indirizzi IP, identificativi e inventario dei Dispositivi e del software; log delle sessioni di teleassistenza (operatore, data e ora, Dispositivo, attività svolta); contenuti presenti sui Dispositivi, compresi incidentalmente dati di cui agli artt. 9 e 10 GDPR, cui il Responsabile accede solo se strettamente necessario all'intervento.

**Conservazione:** log delle connessioni su log server non modificabile per 6 mesi; i contenuti non sono conservati oltre l'intervento.

## A.2 – Suite di Sicurezza

**Si applica se:** il Titolare ha stipulato un Contratto di Assistenza.

**Finalità:** protezione degli endpoint e rilevazione di minacce informatiche.

**Operazioni:** raccolta di telemetria di sicurezza, analisi dei file sospetti, gestione degli eventi e delle quarantene.

**Interessati:** utenti dei Dispositivi.

**Categorie di dati:** telemetria di sicurezza, nomi e percorsi dei file, file sospetti inviati ad analisi, eventi di sicurezza, identificativi dei Dispositivi.

**Conservazione:** 6 mesi per eventi e telemetria, salvo i tempi del Sub-responsabile indicato nell'elenco di cui all'Art. 9.1.

**Localizzazione:** Spazio Economico Europeo, anche tramite il Sub-responsabile ESET indicato nell'elenco di cui all'Art. 9.1.

## A.3 – Firewall e filtro DNS

**Si applica se:** il Titolare ha richiesto la gestione del firewall o il firewall in comodato.

**Finalità:** protezione della rete, gestione delle VPN, applicazione di Indicatori di Compromissione e blacklist DNS.

**Operazioni:** registrazione delle connessioni e delle risoluzioni DNS, analisi per finalità di sicurezza.

**Interessati:** utenti della rete del Titolare.

**Categorie di dati:** indirizzi IP, log di connessione e di navigazione, account VPN.

**Conservazione:** log di navigazione per 30 giorni; conservazione più lunga solo su istruzione scritta del Titolare ai sensi dell'Art. 14.1.

## A.4 – Password manager e credenziali

**Si applica se:** il Servizio è attivato; per l'archivio dedicato al Cliente, sempre in presenza di un Contratto di Assistenza.

**Finalità:** conservazione delle credenziali di amministrazione e delle credenziali generiche dei sistemi del Titolare utilizzate dal Responsabile, in archivio dedicato al Cliente; password manager per il personale del Titolare, ove attivato.

**Operazioni:** conservazione cifrata, condivisione controllata, registrazione degli accessi. Il password manager adotta la cifratura lato client: il Responsabile non può accedere in chiaro alle credenziali del personale del Titolare, salvo quelle che il Titolare condivide espressamente con il personale del Responsabile all'interno del password manager.

**Interessati:** personale del Titolare titolare di account.

**Categorie di dati:** account utente, credenziali cifrate, credenziali di amministrazione e generiche comprese quelle deprecate, log degli accessi alle credenziali con indicazione di chi e quando vi ha avuto accesso.

**Conservazione:** per la durata del Servizio. Le credenziali personali degli utenti non sono conservate dal Responsabile; le password provvisorie sono eliminate dopo l'invio. Alla cessazione si applica l'Art. 15.2.

## A.5 – Backup in cloud

**Si applica se:** il Titolare ha richiesto il servizio di backup.

**Finalità:** copia di sicurezza e ripristino dei dati indicati dal Titolare.

**Operazioni:** copia, conservazione cifrata, verifica e ripristino.

**Interessati e categorie di dati:** quelli contenuti nei dati e nei sistemi inclusi dal Titolare nel perimetro di backup.

**Conservazione:** secondo la politica di frequenza e conservazione concordata con il Titolare.

### A.6 – Posta elettronica e cloud

**Si applica se:** il Titolare ha richiesto il servizio.

**Finalità:** erogazione di caselle di posta elettronica, rubrica e archiviazione condivisa; protezione antispam, antivirus e antiphishing.

**Operazioni:** ospitalità, ricezione, invio e conservazione dei messaggi e dei file; analisi automatizzata dei messaggi per finalità di sicurezza.

**Interessati:** utenti del Titolare, mittenti e destinatari dei messaggi, soggetti presenti nelle rubriche e nei file.

**Categorie di dati:** contenuti e metadati dei messaggi, rubriche, file archiviati.

**Conservazione:** contenuti per la durata del servizio secondo le scelte degli utenti; registri del server di posta per 7 giorni ai sensi dell'Art. 14.2; messaggi in quarantena per i tempi pubblicati nella sezione Conservazione dei dati del Compliance Center.

### A.7 – Analisi dei log mediante intelligenza artificiale

**Si applica se:** il Titolare ha stipulato un Contratto di Assistenza.

**Finalità:** classificazione degli alert, rilevazione di anomalie tecniche e minacce, esecuzione di azioni di risposta automatizzate predefinite.

**Operazioni:** analisi automatizzata dei dati delle schede A.1, A.2 e A.3 su infrastruttura propria del Responsabile, ai sensi dell'Art. 14.7. I dati non sono utilizzati per l'addestramento di modelli, salvo quanto previsto all'Art. 14.8.

**Categorie di dati:** log e telemetria; nessun contenuto dei file del Titolare.

**Conservazione:** quella delle schede da cui provengono i dati.

### A.8 – Ticketing e canali di supporto

**Si applica se:** sempre.

**Finalità:** gestione delle richieste di assistenza e delle comunicazioni operative.

**Operazioni:** registrazione, classificazione e tracciamento delle richieste; invio via SMS del collegamento di accesso al canale di supporto.

**Interessati:** Legale Rappresentante, Referenti, personale del Titolare e, ove previsto dai Contratti, studenti e genitori che richiedono assistenza.

**Categorie di dati:** dati identificativi e di contatto dei richiedenti, numero di cellulare, contenuto delle richieste e degli allegati.

**Conservazione:** ticket e allegati per 6 mesi dalla chiusura, salvo quanto previsto al punto D.8 dell'Allegato D.

### A.9 – Data Loss Prevention

**Si applica se:** il Titolare ha stipulato il Contratto DLP.

**Finalità:** prevenzione della perdita di dati secondo le regole stabilite dal Titolare.

**Operazioni:** analisi automatizzata dei contenuti e delle operazioni sui Dispositivi, blocco o segnalazione degli eventi ai soggetti designati dal Titolare; attivazione subordinata all'Art. 14.1.

**Interessati:** personale del Titolare che utilizza i Dispositivi protetti.

**Categorie di dati:** eventi di rilevazione, metadati delle operazioni, contenuti sottoposti ad analisi.

**Conservazione:** 6 mesi per gli eventi, salvo diversa istruzione scritta del Titolare.

**Localizzazione:** console e dati su server del Responsabile nello Spazio Economico Europeo.

### A.10 – Hosting

**Si applica se:** il Titolare ha attivato servizi di hosting (siti web, applicazioni, database, caselle di posta su domini del Titolare).

**Finalità:** ospitalità ed erogazione dei siti, delle applicazioni e dei database del Titolare; gestione dei sistemi sottostanti, backup, sicurezza e monitoraggio.

**Operazioni:** conservazione, elaborazione automatizzata richiesta dalle applicazioni del Titolare, copia di sicurezza, analisi dei log per finalità di sicurezza. Il Responsabile non accede ai contenuti ospitati, salvo quanto necessario alla singola richiesta di assistenza o alla gestione di un incidente.

**Interessati:** utenti, clienti e visitatori dei siti e delle applicazioni del Titolare, personale del Titolare.

**Categorie di dati:** quelli caricati o generati dalle applicazioni del Titolare, la cui determinazione resta in capo al Titolare; log di accesso dei server web (indirizzo IP, data e ora, risorsa richiesta, user agent).

**Conservazione:** contenuti per la durata del servizio; log di accesso per 6 mesi; backup secondo la politica concordata.

### A.11 – Colocation

**Si applica se:** il Titolare ospita propri apparati tramite il servizio di colocation del Responsabile.

**Natura del trattamento:** gli apparati del Titolare sono ospitati presso il data center partner indicato nel contratto di colocation, che disciplina anche i soggetti autorizzati all'accesso fisico e le relative modalità. Il Responsabile e il gestore del data center forniscono spazio, alimentazione,

connettività e custodia fisica e non accedono logicamente agli apparati del Titolare; per i dati contenuti negli apparati il Responsabile non effettua trattamenti, salvo quanto previsto per gli interventi su richiesta.

**Interventi su richiesta:** operazioni fisiche eseguite su istruzione scritta del Titolare (a titolo esemplificativo: riavvii, sostituzione di dischi, collegamenti). I supporti rimossi sono consegnati al Titolare o distrutti su sua istruzione, con verbale.

**Categorie di dati trattati dal Responsabile:** dati identificativi del personale del Titolare autorizzato all'accesso, registri degli accessi fisici, eventuali riprese di videosorveglianza del data center secondo le politiche del gestore del sito.

**Conservazione:** registri degli accessi fisici per 6 mesi; videosorveglianza secondo le politiche del gestore del data center.

## A.12 – Servizi cloud

**Si applica se:** il Titolare ha attivato servizi cloud del Responsabile, quali macchine virtuali, storage, database gestiti, applicazioni di collaborazione o di videoconferenza.

**Finalità:** erogazione dell'infrastruttura e delle applicazioni cloud richieste.

**Operazioni:** per i servizi infrastrutturali (macchine virtuali e storage gestiti dal Titolare), il Responsabile si limita all'ospitalità e non accede ai sistemi operativi e ai dati del Titolare; per i servizi gestiti (database gestiti, applicazioni), il Responsabile amministra il servizio con le limitazioni di cui all'Art. 14.3.

**Interessati e categorie di dati:** quelli inseriti dal Titolare e dai suoi utenti; dati degli account e log di utilizzo dei servizi gestiti.

**Conservazione:** contenuti per la durata del servizio; log per 6 mesi; backup secondo la politica concordata.

## A.13 – Consulenza, audit e assessment

**Si applica se:** il Titolare ha affidato un Incarico di Consulenza.

**Finalità:** esecuzione dell'incarico, compresi analisi dell'infrastruttura esistente, sopralluoghi, interviste, verifiche di configurazione, scansioni di rete e test di sicurezza, redazione del rapporto finale.

**Operazioni:** raccolta di inventari, configurazioni, estratti di log ed esiti delle scansioni; consultazione di documenti e sistemi messi a disposizione dal Titolare; fotografie degli apparati durante i sopralluoghi. Le credenziali eventualmente fornite sono conservate esclusivamente nel password manager del Responsabile e revocate al termine dell'incarico. I test di sicurezza attivi sono eseguiti solo nel perimetro, nelle finestre temporali e con le modalità autorizzati per iscritto dal Titolare.

**Interessati:** personale del Titolare e soggetti i cui dati sono presenti nei sistemi o nei documenti esaminati.

**Categorie di dati:** dati identificativi e di contatto del personale intervistato; account, indirizzi IP e identificativi dei dispositivi; contenuti incidentalmente visibili durante le verifiche, cui il Responsabile non accede oltre quanto necessario.

**Conservazione:** i dati di lavoro (configurazioni, log, esiti delle scansioni, fotografie) sono cancellati entro 30 giorni dalla consegna del rapporto finale. Il rapporto finale è conservato per 2 anni dalla consegna, pseudonimizzato ove possibile, a supporto di eventuali contestazioni e quale evidenza del sistema di gestione certificato, ed è quindi cancellato.

## A.14 – Attività Preliminari

**Si applica se:** il Titolare richiede Attività Preliminari ai sensi dell'Art. 2.5.

**Finalità:** valutazione della situazione del Titolare per la formulazione di un'offerta; contenimento e prima valutazione di incidenti di sicurezza.

**Operazioni:** censimento di dispositivi, postazioni e apparati; raccolta di configurazioni e log; fotografie durante i sopralluoghi. In caso di incidente: isolamento dei sistemi compromessi, acquisizione di copie e campioni per l'analisi, individuazione del perimetro della compromissione.

**Interessati e categorie di dati:** come la scheda A.13; in caso di incidente, anche i dati coinvolti dalla compromissione, cui il Responsabile accede nei limiti dell'Art. 14.3.

**Incidenti di sicurezza:** il Responsabile assiste il Titolare negli adempimenti di cui agli artt. 33 e 34 GDPR, compreso il termine di 72 ore per la notifica all'Autorità di controllo; preserva le evidenze con modalità che ne consentano l'utilizzo nei confronti delle autorità; non comunica con gli autori dell'attacco né con terzi senza istruzione del Titolare.

**Conservazione:** i dati sono cancellati entro 30 giorni dalla consegna dell'offerta o della relazione, ovvero dalla cessazione di cui all'Art. 3.1; le copie forensi sono conservate fino alla consegna al Titolare o all'autorità competente, o fino a diversa istruzione scritta del Titolare.

## A.15 – Gestione della Piattaforma didattica

**Si applica se:** il Titolare ha stipulato il Contratto Piattaforme.

**Finalità:** amministrazione, configurazione e monitoraggio della Piattaforma; gestione di utenti e gruppi; supporto agli utenti e al Team Digitale.

**Operazioni:** creazione, modifica, sospensione e cancellazione degli account; configurazione dei criteri; consultazione dei log di audit; accesso ai contenuti solo su richiesta e nei limiti dell'Art. 14.3.

**Interessati:** personale del Titolare, studenti e genitori, anche in quanto richiedenti il ripristino delle credenziali.

**Categorie di dati:** dati anagrafici e scolastici trasmessi negli elenchi (nome, cognome, data di nascita, classe, sezione, plesso, tipo di liberatoria sottoscritta); account e dati di autenticazione; log di audit; contenuti delle richieste di supporto; fotografie dei documenti trasmessi per il ripristino delle credenziali, con i relativi metadati; storico dei ripristini; indirizzi email per l'invio delle credenziali, ivi compresi quelli dei genitori; dati di

contatto del Legale Rappresentante, dei membri del Team Digitale e del Responsabile della Protezione dei Dati del Titolare; contenuti della Piattaforma limitatamente a quanto necessario alla singola richiesta.

**Conservazione:** elenchi cancellati al termine delle operazioni di creazione o aggiornamento degli account; fotografie e allegati cancellati 72 ore dopo la chiusura della richiesta; storico dei ripristini per la durata dell'account; dati di contatto per la durata del Contratto; registri tecnici del server di posta secondo il ciclo di rotazione; richieste di supporto per i tempi pubblicati nella sezione Conservazione dei dati del Compliance Center; log secondo le impostazioni della Piattaforma.

**Localizzazione:** dati trattati dal Responsabile nello Spazio Economico Europeo; i dati presenti sulla Piattaforma sono ospitati dal Fornitore della Piattaforma secondo i propri termini.

### A.16 – Pseudonimizzazione (Identity Provider, Email Security Gateway, Data Loss Prevention)

**Si applica se:** il servizio è attivato mediante Richiesta di Attivazione ai sensi del Contratto Piattaforme.

**Finalità:** autenticazione degli utenti mediante identificativi pseudonimi; protezione della posta da malware, spam e phishing; prevenzione del caricamento sulla Piattaforma di dati personali non consentiti.

**Operazioni:** conservazione cifrata della tabella di corrispondenza; autenticazione; analisi automatizzata dei messaggi; analisi automatizzata dei contenuti caricati e segnalazione degli eventi ai soggetti designati dal Titolare; registrazione del consenso degli utenti maggiorenni al primo accesso; rimozione automatica di dati personali dai messaggi prima della consegna; rotazione periodica degli identificativi pseudonimi e ricreazione automatica degli account compromessi.

**Interessati:** utenti della Piattaforma; mittenti e destinatari della posta del dominio del Titolare.

**Categorie di dati:** identità e identificativi pseudonimi; credenziali; metadati e contenuti dei messaggi sottoposti ad analisi automatizzata; contenuti caricati sottoposti a rilevazione ed eventi rilevati; registro dei consensi.

**Conservazione:** tabella di corrispondenza per la durata del servizio e, alla cessazione, secondo la procedura di cui al punto D.7 dell'Allegato D; messaggi in quarantena ed eventi per i tempi pubblicati nella sezione Conservazione dei dati del Compliance Center.

### A.17 – Browser Protetto

**Si applica se:** il servizio è attivato mediante Richiesta di Attivazione.

**Finalità:** accesso protetto alla Piattaforma tramite VPN gestita dal Responsabile, con protezione anti-traccianti.

**Operazioni:** instradamento del traffico; registrazione dei dati di connessione per finalità di sicurezza. Il contenuto del traffico cifrato non è oggetto di ispezione.

**Interessati:** utenti che utilizzano il Browser Protetto.

**Categorie di dati:** indirizzi IP, identificativi e orari di connessione, volumi di traffico.

**Conservazione:** per i tempi pubblicati nella sezione Conservazione dei dati del Compliance Center.

### A.18 – Integrazioni e servizi scuola.org

**Si applica se:** le Integrazioni sono attivate ai sensi del Contratto Piattaforme.

**Finalità:** configurazione di Servizi Aggiuntivi e Applicazioni di Terze Parti; erogazione dei servizi scuola.org (a titolo esemplificativo: Jitsi Meet, Excalidraw, Matrix).

**Operazioni:** configurazione delle abilitazioni per utenti e unità organizzative; per i servizi scuola.org, ospitalità ed erogazione del servizio.

**Interessati:** utenti abilitati.

**Categorie di dati:** elenco degli utenti e delle unità organizzative abilitate; per i servizi scuola.org, dati dell'account e contenuti delle comunicazioni e delle attività di collaborazione generati dagli utenti.

**Conservazione:** secondo le condizioni d'uso dei servizi scuola.org pubblicate nella sezione Documentazione contrattuale del Compliance Center.

**Localizzazione:** infrastruttura del Responsabile nello Spazio Economico Europeo. I trattamenti dei Servizi Aggiuntivi e delle Applicazioni di Terze Parti sono effettuati dai rispettivi fornitori ai sensi dell'Art. 10.3.

### Riepilogo dei tempi di conservazione

| Dato | Conservazione |
|---|---|
| Ticket e allegati | 6 mesi dalla chiusura |
| Log, eventi di sicurezza, telemetria, eventi DLP | 6 mesi |
| Log degli accessi amministrativi | Almeno 6 mesi |
| Log delle sessioni di teleassistenza e di accesso hosting | 6 mesi |
| Registri degli accessi fisici (colocation) | 6 mesi |
| Registri del server di posta (metadati) | 7 giorni, estendibili su istruzione |
| Log di navigazione firewall e DNS | 30 giorni, estendibili su istruzione |
| Contenuti di posta, cloud e hosting | Durata del servizio |

| Dato | Conservazione |
|---|---|
| Backup | Secondo la retention concordata |
| Credenziali dell'archivio dedicato | Durata del servizio, poi consegna e cancellazione |
| Elenchi per la creazione degli account (Piattaforma) | Fino al termine delle operazioni |
| Fotografie per il ripristino delle credenziali | 72 ore dalla chiusura della richiesta |
| Storico dei ripristini delle credenziali | Durata dell'account |
| Tabella di corrispondenza (pseudonimizzazione) | Durata del servizio, poi punto D.7 |
| Dati di lavoro di consulenze e Attività Preliminari | 30 giorni dalla consegna |
| Rapporto finale di consulenza | 2 anni, pseudonimizzato ove possibile |
| Copie forensi | Fino alla consegna o a diversa istruzione |
| Copie di sicurezza dei sistemi del Responsabile | Entro 30 giorni dalla cancellazione |

# Allegato B – Misure tecniche e organizzative

Il Responsabile adotta le seguenti misure, la cui documentazione di dettaglio è disponibile per le verifiche di cui all'Art. 16.

**Governance:** sistema di gestione certificato ISO/IEC 27001, 27017, 27018 e 27701, con analisi dei rischi e riesame periodico.

**Controllo degli accessi:** account nominativi, autenticazione multifattore, chiavi hardware FIDO o passkey per gli accessi sensibili del personale, minimo privilegio, revoca tempestiva alla cessazione dell'incarico.

**Credenziali:** password manager di proprietà del Responsabile con cifratura lato client e algoritmi conformi alle indicazioni di ACN e del Garante; credenziali di amministrazione di almeno 32 caratteri casuali ove supportato; verifica delle password contro gli archivi di password compromesse; credenziali monouso per gli accessi amministrativi ai client; registrazione di chi e quando accede alle credenziali dell'archivio dedicato al Cliente; credenziali iniziali degli utenti generate casualmente, con modifica obbligatoria al primo accesso, inviate dai server di posta del Responsabile nello Spazio Economico Europeo ed eliminate dai sistemi di invio dopo la consegna.

**Interventi in sede:** le operazioni sono svolte in presenza dell'utente della Postazione; le credenziali necessarie sono condivise tramite il password manager o inserite da remoto da altro operatore, senza comunicazione in chiaro.

**Accesso remoto:** sessioni interattive solo con il consenso dell'utente della Postazione e registrate localmente sulla Postazione; operazioni RMM automatizzate tracciate; log delle connessioni su log server non modificabile; accesso agli apparati con inserimento automatico delle credenziali e limitazione alle sole funzioni necessarie.

**Tracciamento:** registrazione degli accessi amministrativi con garanzia di integrità e conservazione per almeno sei mesi.

**Cifratura:** dati cifrati in transito e a riposo sull'infrastruttura del Responsabile.

**Continuità operativa:** backup cifrati, test periodici di ripristino, infrastruttura ospitata in data center certificati.

**Gestione delle vulnerabilità:** aggiornamenti e gestione delle vulnerabilità secondo priorità di rischio.

**Monitoraggio e incidenti:** SOC/NOC con monitoraggio continuativo e procedura di gestione degli incidenti e delle Violazioni.

**Personale:** formazione periodica e vincolo di riservatezza del personale autorizzato.

**Ubicazione del personale:** il personale del Responsabile e dei Partner Tecnici accede ai sistemi e ai dati del Titolare esclusivamente dal territorio dello Spazio Economico Europeo, salvo autorizzazione scritta del Titolare.

**Fornitori:** valutazione dei fornitori e imposizione di obblighi contrattuali equivalenti ai Sub-responsabili e ai Partner Tecnici.

**Supporti di memoria:** i supporti di proprietà del Responsabile contenenti dati non escono dal suo controllo e sono cancellati in modo sicuro o distrutti al termine del loro utilizzo; per i server forniti dai Sub-responsabili di infrastruttura, i dati sono cifrati a riposo e la dismissione dei supporti avviene secondo le procedure di cancellazione sicura del fornitore.

# Allegato C – Ripartizione degli adempimenti

La tabella riepiloga la ripartizione dei principali adempimenti tra le Parti; in caso di contrasto prevalgono gli articoli dell'Accordo richiamati.

| Adempimento | Titolare | Responsabile |
|---|---|---|
| Base giuridica e informativa a personale, utenti, famiglie e clienti | ✔ | Supporto documentale (Art. 12) |
| Adempimenti art. 4 L. 300/1970 | ✔ | Descrizione tecnica degli strumenti (Art. 14.1) |
| Liberatorie per Servizi Aggiuntivi e Applicazioni di Terze Parti | ✔ | Attivazione solo in loro presenza (Allegato D) |
| Registro dei trattamenti | Art. 30, par. 1 | Art. 30, par. 2 (Art. 17) |
| Valutazione d'impatto e consultazione preventiva | ✔ | Informazioni sui Servizi (Art. 12) |
| Notifica al Garante e comunicazione agli interessati | ✔ | Comunicazione entro 48 ore e assistenza (Art. 13) |
| Riscontro alle richieste degli interessati | ✔ | Inoltro entro 2 giorni e assistenza (Art. 11) |
| Misure di sicurezza sui sistemi gestiti | Definizione delle policy e approvazione delle deroghe | Attuazione e mantenimento (Art. 8, Allegato B) |
| Regole DLP e filtri di navigazione | Definizione | Configurazione |
| Verifica annuale dell'operato degli Amministratori di sistema | ✔ | Elenco e log (Art. 7) |
| Scelta dei Fornitori del Cliente e relativi accordi | ✔ | — |
| Conservazione documentale a norma | ✔ | — |

# Allegato D – Istruzioni per la gestione della Piattaforma didattica

**Si applica se:** il Titolare ha stipulato il Contratto Piattaforme. Nel presente Allegato il Titolare è indicato come "Istituto". Le presenti istruzioni costituiscono la configurazione predefinita della Piattaforma; restano ferme le misure minime e le misure non derogabili previste dal Contratto Piattaforme.

**D.1 — Account e minimizzazione.** Gli account sono creati sulla base degli elenchi trasmessi dall'Istituto, contenenti nome, cognome, data di nascita, classe, sezione, plesso e tipo di liberatoria sottoscritta. Il nome utente segue lo schema nome.cognome.sXX, dove XX è un suffisso numerico di unicità generato dal Responsabile a partire dai dati anagrafici, con modalità che non consentono di ricostruire la data di nascita. La data di nascita è utilizzata esclusivamente per la generazione del suffisso e per l'individuazione degli utenti minori di 18 anni e non è registrata nella Piattaforma; classe, sezione e plesso sono utilizzati per l'assegnazione alle unità organizzative e ai gruppi. Gli elenchi sono cancellati dal Responsabile al termine delle operazioni di creazione o aggiornamento degli account. Gli elenchi contengono inoltre gli indirizzi email cui inviare le credenziali di primo accesso, per gli studenti quelli dei genitori. Gli account per utenti esterni sono creati sulla base di nome, cognome, data di nascita, indirizzo email e tipo di liberatoria sottoscritta, e non sono creati in assenza di liberatoria. Il Responsabile non conserva copia dei messaggi di invio massivo delle credenziali di primo accesso; gli indirizzi email utilizzati per l'invio sono cancellati unitamente agli elenchi e permangono esclusivamente nei registri tecnici del server di posta, cancellati secondo il relativo ciclo di rotazione entro i tempi pubblicati nella sezione Conservazione dei dati del Compliance Center. Il personale e gli studenti sono collocati in unità organizzative distinte, con criteri di sicurezza differenziati. Le unità organizzative degli studenti sono contrassegnate, ove la Piattaforma lo preveda, come contenenti utenti minori di 18 anni.

**D.2 — Autenticazione.** Gli account con privilegi amministrativi utilizzano l'autenticazione a due fattori mediante app di autenticazione o chiave di sicurezza. Agli studenti non è richiesto il numero di telefono.

**D.3 — Servizi.** Sono attivi per impostazione predefinita i Servizi Principali della Piattaforma. I Servizi Aggiuntivi sono disattivati per impostazione predefinita e attivati esclusivamente secondo le disposizioni del Contratto Piattaforme in materia di Servizi Aggiuntivi e Liberatorie, previa acquisizione delle Liberatorie. L'indicazione del tipo di liberatoria sottoscritta, riportata negli elenchi di cui al punto D.1, costituisce la dichiarazione dell'Istituto ai sensi del presente punto. Ove l'Istituto non acquisisca la liberatoria per i Servizi Principali, ne assume la relativa responsabilità. Agli utenti di età inferiore a 14 anni i Servizi Aggiuntivi e le Applicazioni di Terze Parti non sono attivati, anche in presenza di liberatoria.

**D.4 — Applicazioni di terze parti.** L'accesso degli studenti alle applicazioni di terze parti non configurate è bloccato per impostazione predefinita. I servizi della Piattaforma sono impostati, ove previsto, in modalità con restrizioni rispetto alle applicazioni di terze parti. Ciascuna applicazione è classificata come bloccata, con restrizioni o attendibile su richiesta scritta del Titolare, previa valutazione del Responsabile secondo le disposizioni del Contratto Piattaforme in materia di funzionalità e integrazioni a rischio elevato e, per gli studenti, previa acquisizione delle Liberatorie. L'accesso al marketplace della Piattaforma è limitato alle applicazioni autorizzate.

**D.5 — Condivisione.** La condivisione esterna e la condivisione pubblica tramite collegamento sono disattivate per gli account degli studenti, salvo domini esterni espressamente autorizzati dal Titolare per finalità didattiche.

**D.6 — Funzionalità di intelligenza artificiale.** Gli assistenti basati su intelligenza artificiale con accesso ai contenuti della Piattaforma sono disattivati per impostazione predefinita e attivabili esclusivamente secondo le disposizioni del Contratto Piattaforme in materia di funzionalità e integrazioni a rischio elevato.

**D.7 — Account amministrativi.** Gli account di super amministratore sono nominativi, in numero limitato e protetti da autenticazione a due fattori. L'Istituto dispone di almeno un proprio account amministrativo nominativo, assegnato a personale dell'Istituto designato dal Dirigente Scolastico quale amministratore della Piattaforma. Le credenziali degli Amministratori di sistema del Responsabile sono personali e non sono comunicate a terzi, ivi compreso il Titolare.

Ove attiva la Pseudonimizzazione, l'Istituto non dispone di account amministrativi, in quanto l'operatività amministrativa di soggetti diversi dal Responsabile comprometterebbe, per i vincoli tecnici del sistema di pseudonimizzazione del Responsabile, la sincronizzazione con l'Identity Provider e l'integrità del servizio. Tale effetto è comunicato all'Istituto prima dell'attivazione secondo il Contratto Piattaforme. Il Responsabile rende disponibili al Titolare, su richiesta, i log di audit della Piattaforma ai fini delle verifiche di cui all'Art. 7.3 dell'Accordo.

In caso di cessazione del servizio di Pseudonimizzazione, per qualsiasi causa, il Dirigente Scolastico comunica per iscritto, entro 30 giorni dalla cessazione, la scelta tra le seguenti opzioni:

a) reversione: il Responsabile converte gli account pseudonimizzati in account nominativi della Piattaforma sulla base della tabella di corrispondenza, disattiva l'Identity Provider e crea account di super amministratore nominativi per il Dirigente Scolastico e per i soggetti da questi designati, ai quali trasferisce l'amministrazione della Piattaforma. Il ripristino delle credenziali degli utenti è a cura dell'Istituto;
b) cancellazione integrale: il Responsabile mette a disposizione dell'Istituto l'esportazione dei contenuti della Piattaforma unitamente alla tabella di corrispondenza. Su attestazione scritta del Dirigente Scolastico dell'avvenuta acquisizione dei dati da conservare e del rispetto degli obblighi di conservazione documentale, procede alla cancellazione integrale degli account e dei contenuti e crea gli account di super amministratore di cui alla lettera a).

In mancanza di scelta entro il termine, si applica l'opzione a). Al termine delle operazioni la tabella di corrispondenza è cancellata dal Responsabile.

**D.8 — Recupero delle credenziali.** Il ripristino delle credenziali non può essere effettuato in autonomia dall'utente ed è eseguito dal Responsabile su richiesta inviata all'indirizzo di supporto dell'Istituto, ospitato sui server di posta del Responsabile nello Spazio Economico Europeo, previa verifica del richiedente:

a) per gli studenti, mediante fotografia scattata al momento della tessera sanitaria o del tesserino del codice fiscale dello studente, anche se scaduti; non sono accettate fotografie degli studenti;

b) per il personale, mediante richiesta inviata dalla propria casella istituzionale del dominio istruzione.it ovvero mediante fotografia del documento d'identità.

L'operatore verifica l'autenticità della fotografia anche attraverso i relativi metadati, senza possibilità di salvarla sulla propria postazione. I metadati non necessari alla verifica, ivi compresi quelli di geolocalizzazione, non sono utilizzati. Le fotografie e gli allegati sono cancellati automaticamente 72 ore dopo la chiusura della richiesta, al fine di consentire eventuali correzioni senza nuova verifica. Il Responsabile conserva esclusivamente lo storico dei ripristini (identificativo dell'utente, data e ora) per la durata dell'account, per finalità di sicurezza. Entro un'ora dal ripristino tutte le sessioni attive sono disconnesse ed è richiesta la modifica della password al primo accesso.

**D.9 — Dispositivi gestiti.** Ove l'Istituto disponga delle relative licenze di gestione, ai dispositivi forniti in comodato agli studenti sono applicati criteri di sicurezza definiti con il Titolare.

**D.10 — Fine dell'anno scolastico e uscite.** Salvo diversa istruzione scritta del Titolare, al ricevimento degli elenchi aggiornati degli utenti trasmessi dall'Istituto, il Responsabile:

a) comunica agli utenti non più presenti negli elenchi, tramite il rispettivo account, che dispongono di 15 giorni per esportare i propri dati, anche al fine del loro trasferimento verso l'account di un altro istituto scolastico. Per tale periodo, in deroga al punto D.5, il Responsabile abilita per tali account gli strumenti di esportazione e di trasferimento dei contenuti della Piattaforma;
b) decorso tale termine, sospende l'account;
c) decorsi ulteriori 45 giorni dalla sospensione, elimina l'account e i relativi dati.

La Piattaforma non costituisce sistema di archiviazione o di conservazione documentale né è destinata alla conservazione di categorie particolari di dati. La conservazione dei documenti soggetti a obblighi di legge resta in capo all'Istituto, che vi provvede mediante i propri sistemi di gestione documentale. Il Responsabile non accede ai contenuti degli account né li trasferisce ad altri account o a terzi, ivi compreso il Titolare, fatte salve le operazioni di cui al punto D.12. L'eliminazione è sospesa per gli account oggetto di specifica istruzione del Titolare, anche in relazione a contenziosi, procedimenti o richieste dell'Autorità. Ove attiva la Pseudonimizzazione, con l'eliminazione dell'account è cancellata la relativa voce della tabella di corrispondenza.

**D.11 — Attivazione della Pseudonimizzazione.** All'attivazione del servizio di Pseudonimizzazione gli account preesistenti sono eliminati, alla data indicata per iscritto dal Dirigente Scolastico, e sostituiti da account pseudonimizzati. L'Istituto comunica preventivamente agli utenti l'invito a esportare i propri dati entro tale data; gli account eliminati non sono recuperabili. In caso di elenchi non conformi, il Responsabile può eliminare gli account creati in modo errato e ricrearli alla ricezione di elenchi corretti.

**D.12 — Operazioni massive.** Le operazioni che incidono contemporaneamente sugli account di più utenti, quali la rimozione da tutte le caselle di un messaggio inviato per errore, sono eseguite esclusivamente su istruzione del Dirigente Scolastico, confermata direttamente dal Responsabile, mediante gli strumenti della Piattaforma e senza accesso al contenuto di altri messaggi.

**D.13 — Aggiornamento.** Il presente Allegato è aggiornato ai sensi dell'Art. 21.1. Le istruzioni del Titolare contenute in modelli o regolamenti dell'Istituto sono recepite nel presente Allegato ai sensi dell'Art. 19.2.

# Allegato E – Corrispondenza con l'art. 28 GDPR

La tabella indica, per ciascun obbligo previsto dal GDPR, l'articolo del presente Accordo che lo disciplina.

| **Obbligo GDPR** | **Articolo del DPA** |
|---|---|
| Art. 28, par. 1 – garanzie sufficienti | Premessa c), Artt. 8.2, 9.2 |
| Art. 28, par. 2 e 4 – sub-responsabili | Art. 9 |
| Art. 28, par. 3, lett. a) – istruzioni documentate, anche per i trasferimenti | Artt. 5, 10 |
| Art. 28, par. 3, lett. b) – riservatezza del personale | Artt. 6.1, 20 |
| Art. 28, par. 3, lett. c) – misure di sicurezza (art. 32) | Art. 8, Allegato B |
| Art. 28, par. 3, lett. d) – condizioni per i sub-responsabili | Art. 9 |
| Art. 28, par. 3, lett. e) – assistenza per i diritti degli interessati | Art. 11 |
| Art. 28, par. 3, lett. f) – assistenza per gli artt. 32-36 | Artt. 12, 13 |
| Art. 28, par. 3, lett. g) – restituzione e cancellazione | Art. 15 |
| Art. 28, par. 3, lett. h) – informazioni e audit; istruzioni illecite | Artt. 16, 5.3 |
| Art. 28, par. 9 – forma scritta, anche elettronica | Artt. 21.4, 21.6 |
| Art. 28, par. 10 – divieto di finalità proprie | Artt. 4.3, 14.8 |
| Art. 30, par. 2 – registro del responsabile | Art. 17 |
| Art. 33, par. 2 – notifica delle violazioni al titolare | Art. 13 |
| Art. 82 – responsabilità | Art. 18 |

# Allegato F – Clausole NIS2 (opzionale)

**F.1 — Applicabilità.** Il presente Allegato si applica ai Titolari che comunicano formalmente al Responsabile, a mezzo PEC, di essere soggetti essenziali o importanti ai sensi del D.Lgs. 138/2024. L'Allegato si applica dal giorno lavorativo successivo alla ricezione della comunicazione, senza necessità di ulteriore sottoscrizione; il Responsabile ne conferma la ricezione. Il Titolare comunica con le stesse modalità la perdita di tale qualifica, dalla quale l'Allegato cessa di applicarsi.

**F.2 — Notifica degli incidenti.** Il Responsabile notifica al Titolare ogni incidente che abbia o possa avere un impatto significativo sui Servizi entro 24 ore dalla conoscenza, fornisce un aggiornamento entro 72 ore e una relazione finale entro un mese, al fine di consentire al Titolare di adempiere agli obblighi di notifica verso il CSIRT Italia. Resta fermo, per le Violazioni, quanto previsto all'Art. 13.

**F.3 — Sicurezza della catena di approvvigionamento.** Il Responsabile fornisce le informazioni necessarie alle misure di gestione dei rischi del Titolare, ivi compresa la risposta a questionari di valutazione dei fornitori una volta per anno contrattuale.

**F.4 — Vulnerabilità.** Il Responsabile comunica senza ritardo al Titolare le vulnerabilità rilevanti individuate sui sistemi gestiti, con le misure di mitigazione proposte.

**F.5 — Verifiche.** Si applica l'Art. 16. Le attività eccedenti la documentazione standard del Responsabile costituiscono prestazioni accessorie ai sensi dei Contratti.

# Allegato G – Pubbliche amministrazioni

**G.1 — Applicabilità.** Il presente Allegato si applica se il Titolare è una pubblica amministrazione, ivi comprese le istituzioni scolastiche statali, e integra o deroga l'Accordo nei limiti di seguito indicati.

**G.2 — Contratti pubblici.** Per gli aspetti diversi dalla protezione dei dati personali prevalgono le condizioni della procedura di affidamento e la normativa in materia di contratti pubblici (D.Lgs. 36/2023). Per la protezione dei dati personali prevale l'Accordo, ai sensi dell'Art. 19.1.

**G.3 — Modifiche.** In deroga all'Art. 21.1, le modifiche dell'Accordo sono efficaci solo con la sottoscrizione di un nuovo Modulo di adesione da parte del Legale Rappresentante. Resta ferma la procedura di cui all'Art. 9.3 per i Sub-responsabili.

**G.4 — Attività Preliminari.** Le Attività Preliminari svolte in favore di una pubblica amministrazione sono rese a titolo gratuito e senza impegno di spesa; nessun corrispettivo è dovuto in assenza di Atto di Affidamento. Esse non costituiscono affidamento né attribuiscono al Responsabile alcun titolo preferenziale nelle successive procedure, restando in capo al Titolare il rispetto dei principi della normativa sui contratti pubblici.

**G.5 — Responsabilità.** La limitazione di cui all'Art. 2.6 opera nei limiti consentiti dalla normativa in materia di contratti pubblici.

**G.6 — Foro.** In deroga all'Art. 21.3, per le controversie è competente il foro previsto dai Contratti o, in mancanza, quello determinato dalla legge, ivi compresi i fori inderogabili.

**G.7 — Accesso agli atti.** L'obbligo di riservatezza di cui all'Art. 20 opera nei limiti della disciplina sull'accesso documentale, civico e agli atti di gara. Il Responsabile indica le parti della documentazione tecnica che costituiscono segreto tecnico o commerciale, la cui ostensione comprometterebbe la sicurezza dei sistemi.

**G.8 — Codice di comportamento.** Il personale del Responsabile che opera per il Titolare rispetta, in quanto compatibili, gli obblighi di condotta del D.P.R. 62/2013 e del codice di comportamento del Titolare.

Firmato digitalmente da:
Antonio Esposito
Data: 23/11/2026 01:43:54