Contratto di individuazione del Responsabile del Trattamento dei Dati ai sensi e per gli effetti dell'art. 28 del Regolamento Europeo 27 aprile 2016, n.679 ("GDPR").

ISTITUTO COMPRENSIVO FOLIGNO 4 (P.IVA: 82001640547), con sede legale in VIA MONTE SORATTE 47 - 06034 FOLIGNO (PG), in qualità di Titolare del trattamento dati, ai sensi dell'art. 4 del Regolamento UE 2016/679 (GDPR), di seguito anche Data Controller/ Titolare

e

BANCA DI CREDITO COOPERATIVA DI SPELLO E BETTONA, P. IVA 00228700548, con sede in Piazza della Pace 1 - Spello (PG), rappresentata del proprio Legale rappresentante _____ , in forza dei poteri al medesimo conferiti, di seguito anche Data Processor Esterno/Responsabile

PREMESSO CHE:

- in forza del rapporto esistente tra le Parti, il **Responsabile** svolge per conto del **Titolare** operazioni di trattamento di dati personali e/o di categorie particolari di dati personali;

> - per trattamento si intende *"qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate ai dati personali o insieme di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l' adattamento o la modifica, l' estrazione, la consultazione, l' uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione"*;

- alla luce delle verifiche documentali effettuate, possiede l'esperienza, la capacità, l'affidabilità e fornisce idonee garanzie del pieno rispetto delle disposizioni vigenti in materia di trattamento dati, ivi compreso il profilo della sicurezza in relazione alle finalità e alle modalità delle operazioni di trattamento nonché alle garanzie di tutela dei diritti dell'interessato;

- le Parti intendono regolare, con il presente atto, i loro reciproci rapporti in tema di disciplina del trattamento dei dati personali ed in particolare per il/i trattamento/i dati riferito ai seguenti punti:

DI SEGUITO LA LISTA DEI TRATTAMENTI:

TRATTAMENTO: GESTIONE DEL SERVIZIO DI CASSA - L'Istituto bancario BCC Spello e Bettona si occupa dei seguenti servizi: riscossione delle entrate e pagamento delle spese facenti capo all'Istituto e dallo stesso ordinate

- **QUESTE LE CATEGORIE INTERESSATI:**
  Consulenti e liberi professionisti, anche in forma associata, Lavoratori autonomi, Studenti, familiari/ tutori, Personale ATA, Insegnanti, Fornitori

- **QUESTI I CAMPI TRATTATI:**
  DB CARTELLA COMUNE - ALUNNI (Dati personali), DIPENDENTI (Dati personali), FAMIGLIE (Dati personali), FORNITORI (Dati personali)

- **LE FINALITÀ DEL TRATTAMENTO:**

L’Istituto Comprensivo Foligno 4, tramite il trattamento ”GESTIONE DEL SERVIZIO DI CASSA”, tratta i sotto indicati dati secondo le seguenti finalità:

DATI COMUNI

- Dati anagrafici

- Dati contabili, fiscali e finanziari

I dati sono di natura comune e vengono trattati per consentire la riscossione delle entrate e il pagamento delle spese, facenti capo all'Istituto e dallo stesso ordinate, per anticipazioni di cassa e apertura di credito finalizzate alla realizzazione di progetti formativi:

- Svolgere le attività finanziarie connesse alle procedure di solvenza per acquisizione di beni e servizi, anche tramite fatturazione elettronica;

- Svolgete attività di servizio di cassa per la gestione dei viaggi di istruzione e uscite didattiche, dei contributi finalizzati alla copertura assicurativa e volontari per l'ampliamento dell'offerta formativa

Il Data Processor e il Data Controller vigilano per garantire agli interessati che i dati saranno trattati solo per la finalità dichiarata e solo per la parte strettamente necessaria al trattamento. Si impegnano inoltre, entro i limiti della ragionevolezza, a modificare correggere tutti i dati che risultano nel frattempo diversi dagli originali, a tenerli sempre aggiornati e a cancellare tutti quei dati che risultano eccedenti al trattamento dichiarato.

- **DURATA DEL TRATTAMENTO:**
  Il trattamento "GESTIONE DEL SERVIZIO DI CASSA" termina il 30/06/2022.

- **PERMESSI RELATIVI AL TRATTAMENTO:**

Trattamento	Raccolta	Inserimento	Registrazione	Modifica	Cancellazione	Distruzione	Lettura	Consultazione	Creazione	Stampa	Comunicazione
GESTIONE DEL SERVIZIO DI CASSA	NO	NO	NO	NO	NO	NO	SI	SI	NO	SI	NO

CONTRATTO di NOMINA del RESPONSABILE ESTERNO DEL TRATTAMENTO DEI DATI

OGGETTO| MATERIA: Con la stipula del presente atto, ai sensi dell'articolo 28 del Regolamento UE 2016/679 (GDPR), il Titolare designa **BANCA DI CREDITO COOPERATIVA DI SPELLO E BETTONA** Responsabile delle operazioni di trattamento dei dati personali affidati. In virtù di tale nomina e del rapporto contrattuale intercorrente tra le Parti, il Responsabile è autorizzato al trattamento dei dati individuati per natura, finalità, tipologia e per categorie di interessati a cui si riferiscono e strettamente pertinenti alle attività svolte per conto del **Titolare.**

OBBLIGHI DEL RESPONSABILE: La sottoscrizione del presente atto vincola il Responsabile del trattamento al Titolare del trattamento e fa sorgere in capo al Responsabile una serie di obblighi specificamente individuati in apposita e separata clausola che segue il presente documento (**Allegato A**).

MISURE DI SICUREZZA E VIOLAZIONE DEI DATI: Il Responsabile è tenuto a mettere in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio in merito al trattamento dei dati effettuato (art. 32 GDPR) meglio precisate nell' **Allegato B** del presente documento.

DECORRENZA – DURATA - CESSAZIONE DEL TRATTAMENTO:

Dopo il completamento del trattamento per conto del Titolare, il Responsabile deve, su istruzioni del Titolare del trattamento, restituire o cancellare i dati personali, e le relative copie esistenti, salvo che non siano previste specifiche e differenti politiche di conservazione dei dati (anche in relazione alle categorie di dati trattati) a norma del diritto dell'Unione o degli Stati membri cui è soggetto il Responsabile del trattamento. In entrambi i casi il Responsabile deve rilasciare contestualmente un'attestazione scritta che presso lo stesso non esiste alcuna copia dei dati personali trattati in nome e per conto del Titolare del trattamento.

Nel caso in cui il Responsabile si serva di sub-fornitori per svolgere attività strettamente necessarie all'esecuzione dei servizi richiesti dal Titolare che comportino trattamento di dati personali del Titolare, il Responsabile si impegna a selezionare sub-fornitori tra soggetti che per esperienza, capacità e affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento di dati personali, ivi compreso il profilo relativo alla sicurezza; nonché a stipulare specifici accordi scritti con i sub-fornitori a mezzo dei quali il Responsabile specifichi analiticamente i loro compiti e imponga a tali soggetti di rispettare i medesimi obblighi, con riferimento alla disciplina sulla protezione dei dati personali imposta dal Titolare sul Responsabile. A ciò si aggiunga che il Responsabile comunque si impegna a garantire circa il rispetto da parte degli eventuali sub-fornitori di tutti gli obblighi con riferimento alla disciplina sulla protezione dei dati personali, imposti dal Titolare sul Responsabile, manlevare e tenere indenne il Titolare da qualsiasi danno, pretesa e/o sanzione possa derivare al Titolare medesimo dalla mancata osservanza di tali obblighi e più in generale dall'applicabile normativa sulla tutela dei dati personali da parte dei sub-fornitori.

Le comunicazioni tra le parti, ai fini del presente incarico, dovranno avvenire:

- per il Data Controller, a **ISTITUTO COMPRENSIVO FOLIGNO 4**

- per il Data Processor, a **BANCA DI CREDITO COOPERATIVA DI SPELLO E BETTONA**

Il corrispettivo per il presente incarico di Responsabile Esterno del trattamento rimane ad ogni effetto ricompreso nel compenso complessivo pattuito per la fornitura dei servizi già in essere e disciplinati nel contratto.
Per tutto quanto non espressamente previsto nel presente atto, si rinvia alle disposizioni generali vigenti in materia di protezione dei dati personali.
Con l'occasione, il **Titolare** ricorda l'importanza delle prescrizioni di legge in materia di trattamento dei dati personali, nonché il fatto che la violazione di dette normative può comportare responsabilità sia civili che penali per il Titolare e per il Responsabile, con possibile applicazione di sanzioni amministrative e pecuniarie, ai sensi degli artt. 82, 83 e 84 GDPR.

Si prega, dunque, di voler cortesemente restituire copia della presente sottoscritta per accettazione.

Luogo e data: FOLIGNO, 19/03/2019

Il titolare

ACCETTAZIONE NOMINA

Il sottoscritto BANCA DI CREDITO COOPERATIVA DI SPELLO E BETTONA accetta la presente nomina nei contenuti, limiti, obblighi ed istruzioni in essa indicati.

Luogo e data: _____

Firma per visione e accettazione

ALLEGATI:

- **Allegato A -** Obblighi del Responsabile del trattamento designato.
- **Allegato B -** Misure di Sicurezza e Violazione dei dati.

ALLEGATO A. Obblighi del Responsabile del trattamento designato. (art. 28 e Considerando 81 e ss del Regolamento EU 2016/679)

In virtù dell'atto che vincola il Responsabile designato al Titolare del trattamento, sorgono in capo al Responsabile una serie di obblighi.

1. Rispetto delle istruzioni impartite dal/i Titolare/i: Il Responsabile deve assistere e coadiuvare il Titolare nella corretta gestione delle operazioni di trattamento che dovranno esser effettuate nel pieno rispetto degli obblighi previsti dal GDPR. A tale proposito, il Responsabile deve trattare i dati personali soltanto su istruzione documentata del Titolare del trattamento, anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il Responsabile del trattamento; in tal caso, il Responsabile deve informare il Titolare circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico.

2. Riservatezza: Il Responsabile deve assicurare per se stesso e per le persone, da lui o dal Titolare del trattamento autorizzate al trattamento dei dati personali, piena riservatezza rispetto alle operazioni di trattamento effettuate.
Sarà cura del Responsabile, qualora lo reputasse opportuno, vincolare le persone autorizzate al trattamento dei dati al segreto mediante un adeguato obbligo legale di riservatezza, anche per il periodo successivo all'estinzione del rapporto di lavoro intrattenuto con il Responsabile, in relazione alle operazioni di Trattamento da essi eseguite.

3. Conformità a leggi e regolamenti applicabili: Il Responsabile è tenuto ad uniformarsi alle disposizioni del GDPR e più in generale, di ogni altra disposizione normativa, nazionale e sovranazionale, in materia di trattamento dei dati personali attualmente in vigore o che in futuro vengano a modificare, integrare o sostituire l'attuale disciplina, nonché dei provvedimenti dell'Autorità Garante competente e delle linee guida adottate dall'European Data Protection Board.

4. Misure di sicurezza: Il Responsabile è tenuto a mettere in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio in merito al trattamento dei dati effettuato (art. 32 GDPR). Si veda Allegato B. Misure di sicurezza e Violazione dei dati.

5. Audit: Il Responsabile del trattamento dovrà consentire al Titolare del trattamento, dandogli piena collaborazione, periodiche verifiche circa l'adeguatezza delle misure di sicurezza adottate e il rispetto della Normativa Privacy e delle disposizioni del Titolare del trattamento stesso.

Ogni attività di audit da parte del Titolare dovrà essere convenuta con il Responsabile del trattamento. Qualora tali attività comportino oneri e spese non previste dal presente contratto tutte le richieste del Titolare dovranno essere gestite a livello progettuale con una stima dei costi necessari per la loro attuazione (siano esse attività di "penetration test", "vulnerability assessment", altro).

6. Persone autorizzate al trattamento: Il Responsabile si avvale di persone autorizzate al trattamento dei dati che operano sotto la sua responsabilità, in quanto deputati alle operazioni di Trattamento, e alle quali fornisce specifiche istruzioni scritte (salvo che il diritto dell'Unione o degli Stati membri non richieda diversamente, art. 29 GDPR). È compito del Responsabile designato vigilare sulla corretta esecuzione delle istruzioni impartite (art. 4.10 GDPR).

7. Sub-responsabile: Il Titolare del trattamento autorizza il Responsabile del trattamento a ricorrere ad un altro Responsabile (di seguito "Sub- responsabile") per l'esecuzione di specifiche attività di trattamento. Il Responsabile inoltra al Titolare l'atto di nomina del "Subresponsabile" e lo informa di eventuali modifiche riguardanti l'aggiunta o la sostituzione di altri Responsabili, alle quali il Titolare del trattamento conserva il diritto di opporsi. Al "Sub-responsabile" sono imposti, con specifico atto sottoscritto, gli stessi obblighi in materia di protezione dei dati contenuti nel contratto che lega il Titolare e il Responsabile del trattamento. Il "Sub- responsabile" è tenuto ad: osservare, valutare e organizzare la gestione del trattamento dei dati personali e la loro protezione (mettendo in atto tutte le misure tecniche ed organizzative adeguate per assicurare un livello di sicurezza adeguato al rischio derivante dal trattamento dati effettuato) affinché questi siano trattati in modo lecito e pertinente e nel rispetto della normativa vigente. Qualora il "Sub- responsabile" del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il Responsabile conserva nei confronti del Titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi del "Sub-responsabile" anche ai fini del risarcimento di eventuali danni causati dal trattamento, salvo dimostri che l'evento dannoso "non gli è in alcun modo imputabile" (art. 82. 1 e 82. 3 GDPR).

8. Registro dei Trattamenti: Ove applicabile, il Responsabile deve tenere un Registro delle attività di trattamento svolte sotto la propria responsabilità in nome e per conto del Titolare del trattamento (art. 30 GDPR). Il Registro, anche in formato elettronico, deve contenere tutta una serie di informazioni, che il Responsabile raccoglie anche interfacciandosi con i vari uffici o unità interne e/o esterne all'azienda, che trattano dati personali per conto del Titolare. In particolare:

- il nome e i dati di contatto del Responsabile del trattamento;
- le categorie dei trattamenti effettuati per conto di ogni Titolare;
- i trasferimenti di dati personali verso un Paese terzo o un'organizzazione internazionale;
- una descrizione delle misure tecniche adottate.

Il Responsabile del trattamento deve mettere il Registro a disposizione dell'Autorità di controllo, se questa ne fa richiesta, affinché possa fungere da strumento per il monitoraggio dei trattamenti effettuati (Considerando 82 GDPR).

9. Esercizio dei diritti dell'interessato: Il Responsabile, dovrà informare tempestivamente e per iscritto il Titolare del trattamento, della ricezione di eventuali richieste degli interessati, avanzate ai sensi degli artt. da 15 a 22 del GDPR, in merito, tra l'altro, alle finalità e alle modalità del trattamento, all'origine dei dati, all'aggiornamento, alla rettificazione, cancellazione, alla portabilità e limitazione dei dati od opposizione al trattamento (compresa la profilazion e), o al fine di revocare il consenso prestato e/o proporre reclamo al Garante per la protezione dei dati personali.
In particolare, il Responsabile è tenuto a:

- coordinarsi a tal fine con le funzioni aziendali preposte dal Titolare alle relazioni con i soggetti interessati;
- darne tempestiva comunicazione scritta al Titolare allegando copia della richiesta;
- accertare l'identità del richiedente per verificare la legittimità della richiesta;
- attivare le dovute procedure atte a dare seguito alle richieste per l'esercizio dei diritti degli interessati, senza ingiustificato ritardo, e comunque, al più tardi entro un mese dal ricevimento delle richiesta stesse, ai sensi dell'art. 12 GDPR.

10. Altri adempimenti: il Responsabile del trattamento è tenuto altresì a:

- cooperare con l'Autorità di Controllo quando richiesto;
- supportare l'attività svolta dal DPO (Data Protection Officer – Responsabile della Protezione dei Dati) per conto del Titolare del trattamento, se nominato (artt. 37,38 GDPR);
- designare per iscritto un Rappresentante che lo rappresenti nell'Unione, se il Responsabile non è stabilito nell'UE e ricorrano i presupposti di cui all'art. 27 GDPR.

ALLEGATO B. Misure di Sicurezza e Violazione dei dati (artt.32 e ss e Considerando 74-77, 83 e ss del Regolamento EU 2016/679 – GDPR)

Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il Responsabile del trattamento deve mettere in atto misure tecniche e organizzative adeguate per assicurare un livello di sicurezza adeguato al rischio, previste dall'art. 32 GDPR, che comprendono, tra le altre, se del caso:

- la pseudonimizzazione e la cifratura dei dati personali;
- la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
- la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
- una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Tali misure devono assicurare un elevato livello di sicurezza. Nella valutazione del rischio per la sicurezza dei dati il Responsabile del trattamento deve tenere in considerazione i rischi presentati dal trattamento dei dati personali come la distruzione accidentale o illegale, la perdita, la modifica, la rivelazione o l'accesso non autorizzati a dati personali trasmessi, conservati o comunque elaborati, che potrebbero cagionare in particolare un danno fisico, materiale o immateriale. Il Responsabile del trattamento, se necessario e su richiesta, dovrà altresì assistere il Titolare del trattamento nella redazione del "DPIA" (Data Protection Impact Assessment), contenente la valutazione sulla particolare probabilità e gravità del rischio inerente alle operazioni di trattamento da effettuare (tenuto conto della natura, dell'ambito di applicazione, del contesto, delle finalità e delle fonti di rischio) e sulle misure tecniche ed organizzative da adottare al fine di attenuare tale rischio assicurando la protezione dei dati personali e la conformità al GDPR. Se del caso, il Responsabile dovrà richiedere in merito un parere al DPO (Data Protection Officer), se nominato (art.35 e C.90 GDPR).

Violazione dei dati. Se dovesse venire a conoscenza di una violazione dei dati personali (Data Breach), il Responsabile, senza ingiustificato ritardo, deve informare per iscritto il Titolare del trattamento affinché possa procedere, se del caso, a notificare la violazione all'autorità di controllo competente (art.33 GDPR) e, qualora la violazione dei dati personali in questione dovesse essere suscettibile di presentare un elevato rischio per i diritti e le libertà delle persone fisiche, il Titolare del trattamento provvederà a darne comunicazione all'interessato (art.34 GDPR).

Il Responsabile deve coadiuvare il Titolare del trattamento nella redazione di specifiche procedure che consentono di individuare prontamente le violazioni dei dati subite (Data Breach) e le relative procedure di risposta attraverso l'elaborazione di una specifica policy. La suddetta policy deve includere, tra le altre cose:

- le linee guida per valutare le violazioni di dati subite al fine individuare quelle che sono suscettibili di presentare un elevato rischio per i diritti e le libertà delle persone;
- fisiche e che dunque dovranno essere notificate all'Autorità di controllo competente;
- le linee guida sulla scelta delle informazioni che saranno rese disponibili all'interessato dal Titolare del trattamento attraverso la comunicazione della violazione, se dalla valutazione precedentemente effettuata, fosse risultata suscettibile di presentare rischi elevati per i diritti e le libertà dell'interessato;
- il Responsabile dovrà documentare per iscritto qualsiasi violazione di dati subita, le circostanze ad essa relative, le conseguenze e i provvedimenti adottati per porvi rimedio.

Nello specifico dovranno essere documentati:

- la natura della violazione 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;
- il nome e i dati di contatto del DPO (se nominato) o di altro punto di contatto presso cui l'Autorità di controllo competente potrà ottenere maggiori informazioni;
- la descrizione delle probabili conseguenze della violazione dei dati personali;
- la descrizioni delle misure adottate per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuare i possibili effetti negativi.

Tale documentazione dovrà essere resa disponibile all'Autorità di controllo competente attraverso la procedura di notifica della violazione dei dati (Data breach) prevista dall'art. 33 comma 3.

Luogo e data: _____

Firma per accettazione degli allegati A e B