

Accordo di designazione per il trattamento di dati personali

Il presente accordo costituisce allegato parte integrante e sostanziale del contratto "CONCESSIONE DEI SERVIZI EDUCATIVI PER LA PRIMA INFANZIA DEL COMUNE DI FORMIGINE - PERIODO 1/09/2023 – 31/08/2028", stipulato tra il Comune di Formigine (C.F. 00603990367), di seguito indicato, per brevità, anche "Ente" o "Titolare", ed il Soggetto esterno _____, quest'ultimo designato "Responsabile del trattamento di dati personali" di cui l'Ente è titolare, ai sensi dell'art. 28 del GDPR.

Si rinvia al sito internet comunale <https://www.comune.formigine.mo.it/footer/privacy> per quanto riguarda l'informativa in materia di privacy.

Le Parti convengono quanto segue:

1. Premesse

Il presente Accordo si compone delle clausole di seguito rappresentate e dall'Allegato 1 "Glossario", che ne forma parte integrante e sostanziale.

2. Trattamento dei dati nel rispetto delle istruzioni dell'Ente

2.1 Il Responsabile del trattamento, relativamente a tutti i Dati personali che tratta per conto dell'Ente, garantisce che:

2.1.1 tratta tali Dati personali solo ai fini dell'esecuzione dell'oggetto del contratto e, successivamente, solo nel rispetto di quanto eventualmente concordato dalle Parti per iscritto, agendo, pertanto, esclusivamente sulla base delle istruzioni documentate e fornite dall'Ente;

2.1.2 non trasferisce i Dati personali a soggetti terzi, se non nel rispetto delle condizioni di liceità assolute dall'Ente e a fronte di quanto disciplinato nel presente accordo;

2.1.3 non tratta o utilizza i Dati personali per finalità diverse da quelle per cui è stipulato il contratto dall'Ente, financo per trattamenti aventi finalità compatibili con quelle originarie;

2.1.4 prima di iniziare ogni trattamento e, ove occorra, in qualsiasi altro momento, informerà l'Ente se, a suo parere, una qualsiasi istruzione fornita dall'Ente stesso si ponga in violazione di Normativa applicabile.

2.2 Al fine di dare seguito alle eventuali richieste da parte di soggetti interessati, il Responsabile del trattamento si

obbliga:

2.2.1 ad adottare procedure idonee a garantire il rispetto dei diritti e delle richieste formulate all'Ente dagli interessati relativamente ai loro dati personali e/o a conformarsi alle istruzioni fornite dall'Ente in materia;

2.2.2 ad adottare procedure atte a garantire l'aggiornamento, la modifica e la correzione, su richiesta dell'Ente dei dati personali di ogni interessato e/o a conformarsi alle istruzioni fornite dall'Ente in materia;

2.2.3 ad adottare procedure atte a garantire la cancellazione o il blocco dell'accesso ai dati personali, a richiesta dall'Ente e/o a conformarsi alle istruzioni fornite dall'Ente in materia;

2.2.4 ad adottare procedure atte a garantire il diritto degli interessati alla limitazione di trattamento, su richiesta dell'Ente e/o a conformarsi alle istruzioni fornite dall'Ente in materia.

2.3 Il Responsabile del trattamento deve garantire e fornire all'Ente cooperazione, assistenza e le informazioni che potrebbero essere ragionevolmente richieste dallo stesso, per consentirgli di adempiere ai propri obblighi, ai sensi della normativa applicabile, ivi compresi i provvedimenti e le specifiche decisioni del Garante per la protezione dei dati personali.

2.4 Il Responsabile del trattamento, anche nel rispetto di quanto previsto all'art. 30 del Regolamento, deve mantenere, compilare e rendere disponibile a richiesta dell'Ente, un registro dei trattamenti dati personali che riporti tutte le informazioni richieste dalla norma.

2.5 Il Responsabile del trattamento assicura la massima collaborazione al fine dell'esperimento delle valutazioni di impatto ex art. 35 del GDPR che l'Ente intenderà esperire sui trattamenti che rivelino, a insindacabile giudizio dell'Ente stesso, un rischio elevato per i diritti e le libertà delle persone fisiche.

3. Le misure di sicurezza

3.1 Il Responsabile del trattamento deve adottare e mantenere appropriate misure di sicurezza, sia tecniche sia organizzative, per proteggere i dati personali da eventuali distruzioni o perdite di natura illecita o accidentale, danni, alterazioni, divulgazioni o accessi non autorizzati.

3.2 Nei casi in cui il Responsabile effettui trattamenti di conservazione dei dati personali del Titolare nel proprio

sistema informativo, garantisce la separazione di tipo logico di tali dati da quelli trattati per conto di terze parti o per proprio conto.

3.3. Il Responsabile del trattamento conserva, nel caso siano allo stesso affidati servizi di amministrazione di sistema, direttamente e specificamente, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema.

3.4 Nell'ipotesi di cui al precedente comma, l'Ente attribuisce al Responsabile del trattamento il compito di dare attuazione alla prescrizione di cui al punto 2 lettera e) "Verifica delle attività" del Provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008 "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema".

3.5 Il Responsabile del trattamento deve adottare misure tecniche ed organizzative adeguate per salvaguardare la sicurezza di qualsiasi rete di comunicazione elettronica o dei servizi forniti al Titolare, con specifico riferimento alle misure intese a prevenire l'intercettazione di comunicazioni o l'accesso non autorizzato a qualsiasi computer o sistema.

3.6 Conformemente alla disposizione di cui all'art. 28 comma 1 del Regolamento e alla valutazione delle garanzie che il Responsabile del trattamento deve presentare, lo stesso Responsabile attesta, a mezzo della sottoscrizione del presente accordo, la conformità della propria organizzazione almeno ai parametri di livello minimo di cui alle misure di sicurezza individuate da Agid con la circolare n. 2/2017¹.

3.7 Il Responsabile del trattamento dà esecuzione al contratto in aderenza al GDPR.

4. Analisi dei rischi, privacy by design e privacy by default

4.1 Con riferimento agli esiti dell'analisi dei rischi effettuata dall'Ente sui trattamenti di dati personali cui concorre il Responsabile del trattamento, lo stesso assicura massima cooperazione e assistenza al fine di dare effettività alle azioni di mitigazione previste dall'Ente per affrontare eventuali rischi identificati.

4.2 Il Responsabile del trattamento dovrà consentire all'Ente, tenuto conto dello stato della tecnica, dei costi, della natura, dell'ambito e della finalità del relativo trattamento, di adottare, sia nella fase iniziale di determinazione dei

¹ http://www.gazzettaufficiale.it/do/atto/serie_generale/caricaPdf?cdimg=17A0239900200010110001&dgu=2017-04-04&art.dataPubblicazioneGazzetta=2017-04-04&art.codiceRedazionale=17A02399&art.num=1&art.tiposerie=SG

mezzi di trattamento, sia durante il trattamento stesso, ogni misura tecnica ed organizzativa che si riterrà opportuna per garantire ed attuare i principi previsti in materia di protezione dati e a tutelare i diritti degli interessati.

4.3 In linea con i principi di privacy by default, dovranno essere trattati, per impostazione predefinita, esclusivamente quei dati personali necessari per ogni specifica finalità del trattamento e che, in particolare, non siano accessibili dati personali ad un numero indefinito di soggetti senza l'intervento di una persona fisica.

4.4 Il Responsabile del trattamento dà esecuzione al contratto in aderenza alle policy di privacy by design e by default adottate dall'Ente e specificatamente comunicate.

5. Soggetti autorizzati ad effettuare i trattamenti - Designazione

5.1 Il Responsabile del trattamento garantisce competenze ed affidabilità dei propri dipendenti e collaboratori autorizzati al trattamento dei dati personali (di seguito anche incaricati) effettuati per conto dell'Ente.

5.2 Il Responsabile del trattamento garantisce che gli incaricati abbiano ricevuto adeguata formazione in materia di protezione dei dati personali e sicurezza informatica.

5.3 Il Responsabile del trattamento, con riferimento alla protezione ed alla gestione dei dati personali, impone ai propri incaricati obblighi di riservatezza non meno onerosi di quelli previsti nel Contratto di cui il presente documento costituisce parte integrante. In ogni caso il Responsabile del trattamento è ritenuto direttamente responsabile per qualsiasi divulgazione di dati personali che dovesse realizzarsi ad opera di tali soggetti.

6. Sub-Responsabili del trattamento di dati personali

6.1 Nell'ambito dell'esecuzione del contratto, il Responsabile del trattamento è autorizzato, sin d'ora, alla designazione di altri responsabili del trattamento (d'ora in poi, anche, "sub-responsabili"), previa informazione all'Ente ed imponendo agli stessi condizioni vincolanti in materia di trattamento dei dati personali non meno onerose di quelle contenute nel presente Accordo.

6.2 Il Responsabile del trattamento dovrà provvedere a che ogni Sub-responsabile sottoscriva un accordo di trattamento dei dati che, a meno di ulteriori e specifiche esigenze, preveda sostanzialmente almeno gli stessi termini del presente Accordo. Copia del suddetto Accordo dovrà essere inviata all'Ente.

6.3 In tutti i casi, il Responsabile del trattamento si assume la responsabilità nei confronti dell'Ente per qualsiasi violazione od omissione realizzate da un Sub-responsabile, sia lo stesso formalmente incaricato o meno o da altri terzi soggetti incaricati dallo stesso, ivi comprese le conseguenze patrimoniali derivanti da tali violazioni od omissioni.

7. Trattamento dei dati personali fuori dall'area economica europea

7.1 L'Ente non autorizza il trasferimento dei dati personali oggetto di trattamento al di fuori dell'Unione Europea.

8. Cancellazione dei dati personali

8.1 Il Responsabile del trattamento provvede, a richiesta del Titolare, alla restituzione o alla cancellazione dei dati personali trattati per l'esecuzione del contratto, di cui il presente accordo è parte integrante, al termine dell'affidamento o del periodo di conservazione e in qualsiasi circostanza in cui sia richiesto dall'Ente, compresa l'ipotesi in cui la stessa debba avvenire per dare seguito a specifica richiesta da parte di interessati.

9. Audit

9.1 Il Responsabile del trattamento si rende disponibile a specifici audit in tema di privacy e sicurezza informatica, previo preavviso di almeno 5 giorni lavorativi, da parte dell'Ente.

9.2 Il Responsabile del trattamento consente, pertanto, all'Ente - a seguito di sottoscrizione di opportuni impegni alla riservatezza - l'accesso ai propri locali, ai computer e ad altri sistemi informativi, ad atti, documenti e a quanto ragionevolmente richiesto per verificare che il Responsabile del trattamento rispetti gli obblighi derivanti dalla normativa in materia di protezione dei dati personali e, quindi, da questo Accordo.

9.3 L'Ente può esperire specifici audit anche richiedendo al Responsabile del trattamento di attestare la conformità della propria organizzazione agli oneri di cui alla Normativa applicabile e al presente Accordo.

9.4 L'esperimento di tali audit non deve avere ad oggetto dati di terze parti, informazioni sottoposte ad obblighi di riservatezza degli interessi commerciali.

9.5 Il rifiuto del Responsabile del trattamento di consentire l'audit all'Ente comporta la risoluzione del contratto.

10. Indagini dell'Autorità e reclami

10.1 Nei limiti della normativa applicabile, il Responsabile del trattamento o qualsiasi Sub-responsabile informa

senza alcun indugio l'Ente di qualsiasi:

- a) richiesta o comunicazione promanante dal Garante per la protezione dei dati personali o da forze dell'ordine;
- b) istanza ricevuta da soggetti interessati.

Il Responsabile del trattamento fornisce, in esecuzione del contratto e, quindi, gratuitamente, tutta la dovuta assistenza all'Ente per garantire che lo stesso possa rispondere a tali istanze o comunicazioni nei termini temporali previsti dalla normativa e dai regolamentari applicabili.

11. Violazione dei dati personali e obblighi di notifica

11.1 In virtù di quanto previsto dall'art. 33 del Regolamento e nei limiti di cui al perimetro delle attività affidate, il Responsabile del trattamento deve comunicare a mezzo di posta elettronica certificata all'Ente nel minor tempo possibile e, comunque, non oltre 24 (ventiquattro) ore da quando ne abbia avuto notizia, qualsiasi violazione di sicurezza che abbia comportato, accidentalmente o in modo illecito, la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati, ivi incluse le violazioni che abbiano riguardato i propri Sub-responsabili. Tale comunicazione deve contenere ogni informazione disponibile utile alla gestione del *data breach*, tra le quali:

- a) la descrizione della natura della violazione dei dati personali;
- b) le categorie ed il numero approssimativo di interessati in questione nonché le categorie ed il numero approssimativo di registrazioni dei dati personali in questione;
- c) i recapiti del DPO nominato o del soggetto competente alla gestione del data breach;
- d) la descrizione delle probabili conseguenze della violazione dei dati personali;
- e) una descrizione delle misure adottate, o che si intenderanno adottare, per affrontare la Violazione della sicurezza, comprese, ove opportuno, misure per mitigarne i possibili effetti negativi.

Il Responsabile del trattamento si impegna ad inviare tempestivamente l'eventuale ulteriore informazione/documentazione utile alla gestione del *data breach*, non appena disponibile.

11.2 Il Responsabile del trattamento deve fornire tutto il supporto necessario all'Ente ai fini delle indagini e sulle

valutazioni in ordine alla violazione di dati, anche al fine di individuare, prevenire e limitare gli effetti negativi della stessa, conformemente ai suoi obblighi ai sensi del presente articolo e, previo accordo con l'Ente, per svolgere qualsiasi azione che si renda necessaria per porre rimedio alla violazione stessa. Il Responsabile del trattamento non deve né rilasciare, né pubblicare alcun comunicato stampa o relazione riguardante eventuali data breach o violazioni di trattamento senza aver ottenuto il previo consenso scritto dell'Ente.

12. Responsabilità e manleve

12.1 Il Responsabile del trattamento sarà responsabile nei confronti dell'Ente per ogni perdita, costo, sanzione, danno e responsabilità di qualsiasi natura derivante o in connessione con una qualsiasi violazione da parte del Responsabile del trattamento delle disposizioni contenute nel presente Accordo.

12.2 Nel caso in cui il Responsabile del trattamento commetta violazioni alla normativa in materia di protezione dei dati personali e al presente Accordo, quali, a titolo esemplificativo, quelle indicate all'art. 83 commi 4 e 5 del Regolamento, l'Ente può risolvere il contratto o applicare una penale, come disciplinato all'art. 36 "Penali" del capitolato.

12.3 A fronte della ricezione di un reclamo relativo alle attività oggetto del presente Accordo, e nei limiti di eventuali indicazioni e/o disposizioni da parte delle Autorità, il Responsabile del trattamento:

- avverte, prontamente ed in forma scritta, l'Ente del Reclamo;
- non fornisce dettagli al reclamante senza la preventiva interazione con l'Ente;
- non transige la controversia senza il previo consenso scritto dell'Ente;
- fornisce all'Ente tutta l'assistenza che potrebbe ragionevolmente richiedere nella gestione del reclamo.

Il Comune di Formigine - Il Dirigente - _____

La ditta _____ - Il Presidente e Legale Rappresentante - _____

Allegato 1

GLOSSARIO

"Dati personali ": si intende una qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»). Si considera identificabile la persona fisica che può essere identificata, direttamente o

indirettamente, con particolare riferimento o a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o ad uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale; per le finalità di cui al presente Accordo, è possibile che vengano raccolti e trattati dati personali qualificabili come "categorie particolari", tra cui i dati degli utenti che rivelano l'origine razziale od etnica e/o relativi alla salute.

"Garante per la protezione dei dati personali": è l'autorità di controllo responsabile per la protezione dei dati personali in Italia;

"GDPR" o "Regolamento": si intende il Regolamento UE 2016/679 sulla protezione delle persone fisiche relativamente al trattamento dei dati personali e della loro libera circolazione (General Data Protection Regulation);

"Normativa Applicabile": si intende l'insieme delle norme rilevanti in materia di protezione dei dati personali, incluso il Regolamento Privacy UE 2016/679 (GDPR) ed ogni provvedimento del Garante per la protezione dei dati personali e del WP Art. 29;

"Pseudonimizzazione": si intende il trattamento dei dati personali in modo tale che i tali dati non possano più essere attribuiti ad un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;

"Reclamo": si intende ogni azione, reclamo, segnalazione presentata nei confronti del Titolare o di un Suo Responsabile del trattamento;

"Responsabile del trattamento": si intende la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

"Titolare del Trattamento": si intende la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità ed i mezzi del trattamento di dati personali. Quando le finalità ed i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

"Trattamento": si intende qualsiasi operazione o insieme di operazioni, compiute, con o senza l'ausilio di processi automatizzati, ed applicate a dati personali o insiemi di dati personali, quali 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.

Il presente atto, composto da n. 9 (nove) pagine a video, viene sottoscritto con firma digitale, in corso di validità.

Il Comune di Formigine - Il Dirigente - _____

La ditta _____ - Il Presidente e Legale Rappresentante - _____