

Cassina

Il nuovo regolamento europeo entrato in vigore il 25 maggio 2018 ha introdotto delle importanti novità in tema di principi e modalità di gestione dei dati personali.

Questa scheda ha l'obiettivo di raccogliere alcune informazioni relative al sistema informativo, alle procedure e policy inerenti il trattamento delle banche dati oggetto del contratto sottoscritto tra le parti.

L'obiettivo dell'Ente è acquisire delle evidenze in ottemperanza i principi di Accountability, Risk Analysis, privacy by design e by default contenuti nel R.U.E 679/2016. Sicuri della Vostra collaborazione chiediamo di fornirci le informazioni richieste e documenti a supporto di quanto l'Azienda ha attuato per ottemperare alle prescrizioni della normativa in vigore e le buone prassi implementate per la gestione delle banche dati di cui il comune è Titolare.

<b>Ragione sociale:</b>		
<b>Sede legale:</b>		
<b>Persona di riferimento:</b>		
<b>Eventuale riferimento del DPO: Data Protection officer:</b>		
<b>Attività e procedure attuate</b>	<b>Si/No</b>	<b>Documenti da allegare e trasmettere</b>
L'azienda ha predisposto un piano di sicurezza inerente il trattamento dei dati?		Piani di sicurezza, procedure, analisi dei rischi
Sono state definite le procedure per la gestione delle attività oggetto del contratto di servizio sottoscritto con il Comune?		Procedure, buone prassi attuate e documentate
L'azienda ha un sistema di gestione certificato secondo lo standard di Qualità ISO 9001		Fornire attestato di certificazione
L'azienda ha un sistema di gestione certificato secondo lo standard di sicurezza ISO 27001		Fornire attestato di certificazione
È stato predisposto il registro dei trattamenti in ottemperanza all'art. 30 del GDPR?		Registro dei trattamenti inerenti le banche dati del Comune
I dipendenti sono stati formati attraverso la partecipazione a corsi e seminari inerenti la normativa sul trattamento dei dati (RUE 679/2016)?		Registro dei corsi/seminari e/o Attestato di partecipazione e/o Documenti contabili che diano evidenza della partecipazione a corsi e seminari (fatture)
Sono state adottate misure di sicurezza informatica per la protezione delle banche dati che l'azienda tratta nell'ambito del contratto di servizio sottoscritto con il Comune?		Descrizione delle policy attuate, piano o procedure di sicurezza informatiche, misure di sicurezza attuate
Nel caso in cui il soggetto esterno sia un ente pubblico		Fornire l'evidenza delle misure minime di sicurezza adottate dall'ente e previste dalla

		circolare AGID 2/2017
<b>Acquisizione di informazioni nel caso di gestione presso propria struttura di una banca dati dell'ente</b>		
L'azienda tratta (presso le proprie strutture) dati personali di cui il Comune è titolare?		In caso affermativo descrizione delle policy di backup tempi di conservazione, attivazione di servizi di backup geografico
L'azienda tratta (presso le proprie strutture) dati personali di cui il Comune è titolare?		In caso affermativo descrizione delle policy e soluzioni di disaster recovery attuate
<b>Caratteristiche delle applicazioni software fornite</b>		
L'Azienda fornisce applicazioni software che gestiscono banche dati personali?		Fornire un documento o una procedura operativa che descriva come vengono gestiti le procedure di autenticazione e profilazione degli utenti (possibilità di impostare complessità e scadenza dei codici di accesso, modalità di salvataggio delle chiavi di autenticazione)
L'Azienda fornisce all'ente applicazioni software che gestiscono banche dati personali particolari?		Fornire un documento o una procedura che illustri le misure di sicurezza implementate dalla soluzione applicativa (cifatura dati particolari ecc., regole di profilazione per funzione ecc.)
L'Azienda fornisce applicazioni software che gestiscono banche dati personali?		Descrivere come la procedura gestisce la cancellazione di dati ed informazioni che esauriscono il ciclo di vita. (procedure di cancellazione o storicizzazione dei dati con la possibilità di attivare dei filtri per data /tipologia di documento ecc.) Possibilità di associare a documenti mandati in conservazione dei tempi di obsolescenza del dato Sui tempi di conservazione dei documenti fare riferimento al massimario di scarto allegato al piano di gestione documentale <a href="https://www.google.it/search?q=agid+massimario+scarto&amp;oq=agid+massimario+scarto&amp;aqs=chrome..69i57.4824j0j7&amp;sourceid=chrome&amp;ie=UTF-8">https://www.google.it/search?q=agid+massimario+scarto&amp;oq=agid+massimario+scarto&amp;aqs=chrome..69i57.4824j0j7&amp;sourceid=chrome&amp;ie=UTF-8</a>
Funzionalità di logging del software fornito		Il software consente di gestire il logging degli utenti dell'applicativo
L'azienda fornisce servizi di assistenza / manutenzione applicativa		Descrivere modalità e strumenti che vengono usati per fornire assistenza remota, l'uso di protocolli sicuri ecc.

Spett.le Fornitore  
Via

## **OGGETTO: Nomina Quale Responsabile Esterno del Trattamento dei Dati**

Il Comune di Cassina de Pecchi con sede in P.za De Gasperi, 1, nella persona del proprio legale rappresentante pro-tempore (qui di seguito "Titolare")

e

\_\_\_\_\_ nella persona del proprio legale rappresentante (di seguito il "Mandatario" o il "Responsabile")

Premesso che:

- I. Il comune ed il Mandatario hanno stipulato un contratto/accordo (di seguito il "Contratto") di cui il presente atto di nomina costituisce una parte integrante;
- II. Per l'esecuzione di detto Contratto il Mandatario svolgerà, per conto dell'Ente determinate attività di trattamento di dati personali di interessati di cui è l'ente è Titolare;
- III. L'ente svolge il ruolo di Titolare del trattamento di dati personali, come previsto dal R.UE 679/2016 (in seguito "Regolamento europeo sulla protezione dei dati") in quanto decide autonomamente sulle finalità e modalità dello stesso;
- IV. il Mandatario gode di competenza e conoscenze tecniche in relazione alle finalità e modalità del trattamento, alle misure di sicurezza da adottare a garanzia della riservatezza, completezza ed integrità dei dati trattati, nonché della normativa in materia di tutela dei dati personali;
- V. Il Comune di Cassina de' Pecchi, nella sua qualità di Titolare, intende nominare il Mandatario quale Responsabile del trattamento di cui all' Accordo, e quest'ultimo intende accettare la nomina;
- VI. le Parti, in relazione a tale nomina, intendono regolare con il presente documento i loro reciproci rapporti in tema di disciplina del trattamento dei dati personali effettuato dal Mandatario per conto dell'Ente.

Tutto ciò premesso:

Con la stipula del presente mandato, ai sensi dell'art. 28 del R.UE 679/2016, Regolamento in materia di Protezione dei Dati Personali, il Comune di Cassina de' Pecchi designa il Mandatario quale soggetto Responsabile, secondo la definizione degli articoli 4, punto 8) e 28 del R.UE 679/2016, del trattamento dei dati personali contenuti nelle banche dati digitali di seguito identificate:

Anagrafica utenti  
Dati sullo stato di salute  
Dati relativi alle diete per motivi religioso

### **1. Finalità del Trattamento**

Il trattamento dei dati personali è realizzato dal Responsabile esclusivamente nell'adempimento degli obblighi assunti nei confronti dell'Ente ed in particolare per dare esecuzione al Contratto tra le Parti. Nell'esercizio delle sue funzioni il Responsabile potrà raccogliere e trattare, elaborare e gestire dati personali necessari e strumentali all'esecuzione del Contratto intercorrente tra le Parti **esclusivamente per le finalità di competenza** sotto riportate:

Servizio di Pre-Post scuola settembre 2019- giugno 2022

Il Responsabile è tenuto ad utilizzare i dati personali oggetto del trattamento solo per le finalità indicate nel presente documento; in nessun caso potrà utilizzare i dati per fini propri.

## **2. Interessati e dati ad essi relativi**

I soggetti i cui dati personali saranno trattati dal Responsabile Esterno, sono **identificati come** "Interessati del trattamento".

## **3. Obblighi del Responsabile**

Il Responsabile Esterno, per quanto di propria competenza, è tenuto, per sé, per i propri dipendenti e per chiunque collabori con la sua attività, al rispetto della normativa in materia di trattamento dei dati personali. In particolare il Responsabile deve adempiere a quanto di seguito specificato.

### **3.1 Misure di sicurezza (MDS)**

Il responsabile dichiara di aver adottato idonee regole di sicurezza inerenti i dati, derivante da un'attività di analisi dei rischi sul trattamento delle informazioni, policy che devono essere comunicate in forma scritta al Comune di Cassina de Pecchi.

Il Responsabile, anche in relazione alle conoscenze acquisite in base al progresso tecnico e tecnologico, alla natura dei dati, alle caratteristiche delle operazioni di trattamento svolte sulle banche dati oggetto del contratto in essere deve assicurare che le misure di sicurezza predisposte ed adottate siano idonee a ridurre al minimo i rischi di distruzione o perdita intenzionale o accidentale dei dati; accesso non autorizzato; trattamento non consentito; trattamento non conforme alle finalità delle operazioni di trattamento.

Il responsabile deve inoltre implementare misure che garantiscano:

- la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi utilizzati per la gestione delle banche dati;
- la capacità di ripristinare la disponibilità dei dati oggetto del contratto in caso di danno grave ai sistemi e strumenti utilizzati dal trattamento;
- la verifica e valutazione periodica dell'efficacia delle misure tecniche e organizzative;

### **3.2 Valutazione d'impatto**

Se si rende necessaria una Valutazione d'impatto sulla protezione dei dati, in merito alle attività di trattamento oggetto del presente Accordo, il Responsabile supporta il Titolare nella redazione della Valutazione d'impatto sulla protezione dei dati;

### **3.3 Consultazione preventiva**

Se si rende necessaria la Consultazione preventiva dell'autorità Garante, in merito alle attività di trattamento oggetto del presente accordo, il Responsabile assiste il Titolare fornendogli tutte le informazioni necessarie per la Redazione della Consultazione preventiva;

### **3.4 Informativa e Consenso**

Il Responsabile, per quanto di propria competenza e nei limiti del presente mandato, opera con il presupposto di legittimità che il Titolare abbia inoltrato il testo dell'informativa ai soggetti interessati nonché che sia stato richiesto il relativo consenso, se richiesto dal Regolamento Europeo.

### **3.5 Istanze degli interessati e procedure dinanzi al Garante**

Nel caso in cui il Responsabile riceva istanze dagli interessati per l'esercizio dei diritti degli interessati, questi dovrà:

- darne tempestiva comunicazione scritta al Titolare allegando copia della richiesta,
- coordinarsi, per quanto di propria competenza, con le funzioni aziendali preposte dal Titolare alle relazioni con i soggetti interessati.
- Il Responsabile, su richiesta del Titolare, è tenuto a coadiuvare quest'ultimo nelle procedure davanti al Garante o all'Autorità giudiziaria in relazione alle attività rientranti nella sua competenza.

### 3.6 Incaricati

Il Responsabile deve individuare i propri incaricati, in quanto deputati alle operazioni di trattamento. Contestualmente, il Responsabile si fa carico di fornire adeguate istruzioni agli Incaricati circa le modalità del trattamento ed in particolare in relazione alla natura dei dati trattati per conto del Titolare.

#### Subappalto dei servizi e comunicazione di dati a terzi

Il Responsabile si impegna a non comunicare i dati a terzi a meno che non sia espressamente autorizzato a farlo dal Titolare.

Nel caso in cui il responsabile si avvalga di altri soggetti per il trattamento dei dati, deve sottoscrivere con questi un contratto nel quale vengano definite le istruzioni per il trattamento delle informazioni e le misure di sicurezza che devono essere adottate.

Il Mandante deve comunicare all'ente i soggetti esterni che a vario titolo trattano le banche dati fornite dal titolare.

Nel caso di trasferimento/comunicazione dei dati ad altro soggetto deve essere richiesta preventiva autorizzazione se il trattamento dei dati venga fatto in stati non appartenenti all'Unione Europea.

## 4. Tenuta del registro delle attività di trattamento

Il Responsabile si impegna predisporre, se dovuto, il registro delle attività di trattamento effettuate per conto del Titolare, come previsto dalla normativa, che contenga almeno le seguenti informazioni:

- nome e i dati di contatto dei Responsabili del trattamento, di ogni Titolare del trattamento per conto del quale il Responsabile agisce, e, ove applicabile, del responsabile della protezione dei dati;
- categorie delle attività di trattamento effettuate per conto di ogni Titolare del trattamento;
- ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale corredata dalla documentazione che legittima tale trasferimento;
- una descrizione generale delle misure di sicurezza tecniche e organizzative adottate;

## 5. Controlli ed Ispezioni

- Il Responsabile consente la periodica verifica dell'adempimento del presente mandato al Titolare, anche attraverso l'invio di adeguata reportistica. Lo stesso si impegna a mettere a disposizione del titolare tutte le informazioni necessarie per verificare il rispetto delle presenti prescrizioni.
- Il Responsabile si impegna inoltre ad esercitare una adeguata attività di supervisione e controllo diretto sugli incaricati del trattamento, relativamente alla corretta osservanza delle istruzioni impartite dal Titolare e dal Responsabile stesso circa il compiuto e corretto trattamento dei dati e alla puntuale osservanza delle misure di sicurezza adottate a tutela dei dati stessi.
- Il responsabile a tal fine si impegna a garantire un idoneo livello di conoscenza e consapevolezza in materia di privacy e misure di sicurezza, anche effettuando programmi di addestramento e formazione.
- La valutazione circa l'adeguatezza del livello di sicurezza deve tenere conto, in particolare, dei rischi del trattamento derivanti da: distruzione o perdita anche accidentale, modifica, divulgazione non autorizzata, nonché accesso non autorizzato, anche accidentale o illegale, o trattamento non consentito o non conforme alle finalità del trattamento dei dati personali conservati o comunque trattati.

Il Responsabile del trattamento deve mettere a disposizione del Titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al Regolamento UE, oltre a contribuire e consentire al Titolare - anche tramite soggetti terzi dal medesimo autorizzati, dandogli piena collaborazione - verifiche periodiche circa l'adeguatezza e l'efficacia delle misure di sicurezza adottate ed il pieno e scrupoloso rispetto delle norme in materia di trattamento dei dati personali.

A tal fine, il Titolare informa preventivamente il Responsabile del trattamento con un preavviso minimo di tre o diverso termine indicato dalla PA giorni lavorativi; nel caso in cui all'esito di tali verifiche periodiche, ispezioni e audit le misure di sicurezza dovessero risultare inadeguate rispetto al rischio del trattamento o, comunque, inadeguate ad assicurare l'applicazione del Regolamento, o risulti che l'appaltatore agisca in modo difforme o contrario alle istruzioni fornite dal Comune, quest'ultimo applicherà le penali previste nel contratto e diffonderà l'appaltatore ad adottare tutte le misure più opportune o a tenere una condotta conforme alle istruzioni entro un termine congruo che sarà all'occorrenza fissato.

In caso di mancato adeguamento a seguito della diffida, resa anche ai sensi dell'art. 1454 cc, il Comune, in ragione della gravità dell'inadempimento, potrà risolvere il contratto ed escutere la

garanzia definitiva, salvo il risarcimento del maggior danno.

#### **1) (Autorizzazione generale)**

Il Responsabile del trattamento può ricorrere ad un altro Responsabile del trattamento (di seguito, "sub-Responsabile del trattamento") per gestire attività di trattamento specifiche, informando, periodicamente \_\_\_\_\_ (la PA deve specificare la periodicità), il Titolare del trattamento delle nomine e delle sostituzioni dei Responsabili. Nella comunicazione andranno specificate le attività di trattamento delegate, i dati identificativi dei sub-Responsabili nominati e i dati del contratto di esternalizzazione.

Oppure

#### **2) (Autorizzazione specifica)**

Il Responsabile del trattamento può avvalersi di ulteriori Responsabili per delegargli attività specifiche, previa autorizzazione scritta del Titolare del trattamento. Il sub-Responsabile del trattamento deve rispettare obblighi analoghi a quelli forniti dal Titolare al Responsabile Iniziale del trattamento, riportate in uno specifico contratto o atto di nomina. Spetta al Responsabile Iniziale del trattamento assicurare che il sub-Responsabile del trattamento presenti garanzie sufficienti in termini di conoscenza specialistica, affidabilità e risorse, per l'adozione di misure tecniche ed organizzative appropriate di modo che il trattamento risponda ai principi e alle esigenze del Regolamento UE.

In caso di mancato adempimento da parte del sub-Responsabile del trattamento degli obblighi in materia di protezione dei dati, il Responsabile Iniziale del trattamento è interamente responsabile nei confronti del Titolare del trattamento di tali inadempimenti; il Comune potrà in qualsiasi momento verificare le garanzie e le misure tecniche ed organizzative del sub-Responsabile, tramite audit e ispezioni anche avvalendosi di soggetti terzi. Nel caso in cui tali garanzie risultassero insussistenti o inadeguate il Comune potrà chiedere la presentazione di garanzie sufficienti entro un termine congruo ed in caso di mancato riscontro risolvere il contratto con il Responsabile iniziale.

Nel caso in cui all'esito delle verifiche, ispezioni e audit le misure di sicurezza dovessero risultare inapplicabili o inadeguate rispetto al rischio del trattamento o, comunque, inadeguate ad assicurare l'applicazione del Regolamento o risulti che il sub responsabile agisca in modo difforme o contrario alle istruzioni fornite dal Comune, quest'ultimo applicherà all'appaltatore /Responsabile Iniziale del trattamento le penali previste nel contratto e diffiderà lo stesso a far adottare al sub-Responsabile del trattamento tutte le misure più opportune o a tenere una condotta conforme alle istruzioni entro un termine congruo che sarà all'occorrenza fissato. In caso di mancato adeguamento a tale diffida, resa anche ai sensi dell'art. 1454 cc, il Comune potrà, in ragione della gravità dell'inadempimento, risolvere il contratto attuativo con il Responsabile iniziale ed escutere la garanzia definitiva, salvo il risarcimento del maggior danno.

### **6. Cessazione del trattamento e restituzione delle banche dati**

All'atto di cessazione per qualsiasi causa del trattamento da parte del Responsabile o del rapporto contrattuale sottostante, il Responsabile sarà tenuto: a restituire al Titolare qualsiasi banca dati oggetto del trattamento di cui il Comune è Titolare in un formato standard aperto che sia interpretabile dall'ente e a provvedere alla loro integrale distruzione entro un anno dandone comunicazione in forma scritta al titolare, salvi solo i casi in cui la conservazione dei dati sia richiesta da norme di legge ad altri fini.

### **7. Responsabilità**

- Il Mandante solleva da ogni responsabilità il Titolare per qualsiasi danno, incluse le spese legali, che possa derivare dall'eventuale illiceità o non correttezza delle operazioni di trattamento che sia imputabile a fatto, comportamento o omissione dello stesso o di chiunque collabori con lui.
- Se il Responsabile del trattamento viola i contenuti dell'Accordo determinando le finalità e modalità di trattamento, è considerato Titolare delle attività di trattamento per le quali ha determinato in autonomia finalità e mezzi del trattamento.

### **8. Decorrenza**

La presente nomina ha la medesima durata ed efficacia dell'Accordo intercorrente tra le Parti e pertanto cesserà al momento del completo adempimento o del venir meno per qualsiasi causa dell'Accordo stesso.

## **9. Sopravvivenza delle clausole**

Alla cessazione, per qualsiasi causa, dell'Accordo continueranno ad avere efficacia quelle clausole che per la loro natura sopravvivono all'estinzione del rapporto giuridico.

Il Responsabile accetta la nomina e conferma la sua conoscenza degli obblighi che si assume in relazione ai dettami del R.U.E 679/2016 e si impegna a procedere al trattamento dei dati personali attenendosi a comportamenti rispettosi dalla normativa vigente.

Cassina de Pecchi, \_\_\_\_\_

\_\_\_\_\_  
Il Comune di Cassina de Pecchi (nella persona del legale rappresentante protempore)

Accettazione dell'Incarico  
\_\_\_\_\_ nella persona del legale rappresentante protempore)

Preso atto di quanto esposto nella lettera di nomina di cui sopra, dichiara di accettare l'incarico di Responsabile Esterno del trattamento dei dati personali per la Società alle condizioni contenute nella nomina medesima.

\_\_\_\_\_  
Per accettazione:  
Il Responsabile del trattamento