

ALLEGATO 5

Designazione quale responsabile del trattamento dei dati personali ai sensi del Regolamento U.E. 679/2016

La ditta Hera S.p.A, Gestore del servizio rifiuti urbani ed assimilati (SGRUA) nel territorio comunale, effettua trattamenti di dati personali di titolarità del Comune di Bologna in esecuzione della *"Convenzione per la gestione dei flussi dati nell'ambito del progetto di riorganizzazione dei servizi di raccolta rifiuti urbani finalizzato all'applicazione della Tariffa puntuale denominato progetto TARIP"* stipulata in data _____ fra la stessa ditta e il Comune di Bologna.

In virtù di tale trattamento e a seguito dell'entrata in vigore del Regolamento UE n. 2016/679 (di seguito, anche "GDPR") e del D.lgs 101/2018 di armonizzazione, le Parti stipulano il presente accordo al fine di disciplinare oneri e responsabilità in aderenza alla normativa.

Hera S.p.A è, pertanto, designata dal Comune di Bologna quale Responsabile del trattamento dei dati personali ai sensi e per gli effetti dell'art. 28 del Regolamento EU n. 2016/679 per il seguente trattamento di dati personali:

- Titolo trattamento: Pagamenti, pignoramenti, riscossioni, sanzioni – Entrate
- Titolo del procedimento: Gestione e riscossione dei tributi comunali e altre entrate comunali
- Finalità trattamento: gestione dell'attività di applicazione e riscossione dei tributi comunali e altre entrate comunali

Hera S.p.A si obbliga quindi a dare esecuzione alla Convenzione suindica conformemente a quanto previsto dal presente Accordo che costituisce parte integrante e sostanziale della Convenzione stessa.

Le Parti riconoscono e convengono che il rispetto delle istruzioni di cui al presente accordo, nonché alle prescrizioni della normativa applicabile, non producono l'insorgere di un diritto in capo al Responsabile del trattamento al rimborso delle eventuali spese che lo stesso potrebbe dover sostenere per conformarsi.

Accordo per il trattamento di dati personali

1. Premesse

Il presente Accordo si compone delle clausole di seguito rappresentate e dall'Allegato 1 Glossario

Le categorie di dati personali trattati possono essere:

Dati identificativi della persona Cognome, Nome, data di nascita, luogo di nascita, codice fiscale, residenza, domicilio. In relazione a :telefono, email, PEC, i dati saranno trattati per le sole esigenze di servizio, con particolare riferimento ai sopralluoghi delle utenze target

Le categorie di interessati sono: soggetti passivi d'imposta, persone fisiche e ditte, rappresentanti legali delle ditte.

Le Parti convengono quanto segue:

2. Trattamento dei dati nel rispetto delle istruzioni del Comune di Bologna

2.1 Hera S.p.A , relativamente a tutti i Dati personali che tratta per conto del Comune di Bologna, garantisce che:

- tratta tali Dati personali solo ai fini dell'esecuzione dell'oggetto della Convenzione, e, successivamente, solo nel rispetto di quanto eventualmente concordato dalle Parti per iscritto, agendo pertanto, esclusivamente sulla base delle istruzioni documentate e fornite dal Comune di Bologna;

- non trasferisce i Dati personali a soggetti terzi, se non nel rispetto delle condizioni di liceità assolute dal Comune di Bologna e a fronte di quanto disciplinato nel presente accordo;
- non tratta o utilizza i Dati personali per finalità diverse dall'esecuzione della Convenzione, financo per trattamenti aventi finalità compatibili con quelle originarie;
- prima di iniziare ogni trattamento e, ove occorra, in qualsiasi altro momento, informerà il Comune di Bologna se, a suo parere, una qualsiasi istruzione fornita dall'Ente si ponga in violazione di Normativa applicabile;

2.2. Al fine di dare seguito alle eventuali richieste da parte di soggetti interessati, Hera S.p.A si obbliga ad adottare:

- procedure idonee a garantire il rispetto dei diritti e delle richieste formulate al Comune di Bologna dagli interessati relativamente ai loro dati personali e/o a conformarsi alle istruzioni fornite dall'Ente;
- procedure atte a garantire l'aggiornamento, la modifica e la correzione, su richiesta del Comune di Bologna dei dati personali di ogni interessato e/o a conformarsi alle istruzioni fornite dall'Ente;
- procedure atte a garantire la cancellazione o il blocco dell'accesso ai dati personali a richiesta del Comune di Bologna e/o a conformarsi alle istruzioni fornite dall'Ente;
- procedure atte a garantire il diritto degli interessati alla limitazione di trattamento, su richiesta del Comune di Bologna e/o a conformarsi alle istruzioni fornite dall'Ente.

2.3 Il Responsabile del trattamento deve garantire e fornire al Comune di Bologna 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 della stessa, 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 il Comune di Bologna intenderà esperire sui trattamenti che rivelano, a Suo insindacabile giudizio, 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 che organizzative, per proteggere i dati personali da eventuali distruzioni o perdite di natura illecita o accidentale, danni, alterazioni, divulgazioni o accessi non autorizzati, ed in particolare, laddove il trattamento comporti trasmissioni di dati su una rete, da qualsiasi altra forma illecita di trattamento.

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 comunica al Titolare, 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 con le relative istruzioni per consentire allo stesso le eventuali attività di vigilanza;

3.4 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 all'Ente, 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. 2/2017

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 Hera S.p.A, la stessa assicura massima cooperazione e assistenza al fine di dare effettività alle azioni di mitigazione previste dall'Ente per affrontare eventuali rischi identificati.

4.2 Hera S.p.A 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 mezzi di trattamento, che 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 alla Convenzione 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, consegnando all'Ente le evidenze di tale formazione.

5.3 Il Responsabile del trattamento, con riferimento alla protezione e gestione dei dati personali, impone ai propri incaricati obblighi di riservatezza non meno onerosi di quelli previsti nella Convenzione di cui il presente documento costituisce parte integrante. In ogni caso Hera S.p.A sarà direttamente ritenuto responsabile per qualsiasi divulgazione di dati personali dovesse realizzarsi ad opera di tali soggetti.

6. Sub-Responsabili del trattamento di dati personali

6.1 Nell'ambito dell'esecuzione della Convenzione, Hera S.p.A è autorizzata sin d'ora, alla designazione di altri responsabili del trattamento (d'ora in poi anche "subresponsabili"), previa informazione dell'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 Su specifica richiesta dell'Ente, Hera S.p.A dovrà provvedere a che ogni Sub-Responsabile sottoscriva direttamente con l'Ente un accordo di trattamento dei dati che, a meno di ulteriori e specifiche esigenze, preveda sostanzialmente gli stessi termini del presente Accordo.

6.3 In tutti i casi, Hera S.p.A si assume la responsabilità nei confronti dell'Ente per qualsiasi violazione od omissione realizzati da un Sub-Responsabile o da altri terzi soggetti incaricati dallo stesso, indipendentemente dal fatto che Hera S.p.A abbia o meno rispettato i propri obblighi contrattuali, ivi comprese le conseguenze patrimoniali derivanti da tali violazioni od omissioni.

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

7.1 Il Comune di Bologna non autorizza il trasferimento dei dati personali oggetto di trattamento al di fuori dell'Unione Europea.

8. Cancellazione dei dati personali

8.1 Hera S.p.A provvede alla cancellazione dei dati personali trattati per l'esecuzione della Convenzione al termine del periodo di conservazione e in qualsiasi circostanza in cui sia richiesto dal Comune di Bologna, compresa l'ipotesi in cui la stessa debba avvenire per dare seguito a specifica richiesta da parte di interessati.

8.2 Alla cessazione della Convenzione e, conseguentemente del presente Accordo, per qualsiasi causa avvenga, i dati personali dovranno, a discrezione dell'Ente, essere distrutti o restituiti allo stesso, unitamente a qualsiasi supporto fisico o documento contenente dati personali di proprietà dell'Ente.

9. Audit

9.1 Hera S.p.A si rende disponibile a specifici audit in tema di privacy e sicurezza informatica da parte del Comune di Bologna .

9.2 Hera S.p.A consente, pertanto, all'Ente l'accesso ai propri locali e ai locali di qualsiasi Sub-Responsabile, ai computer e altri sistemi informativi, ad atti, documenti e a quanto ragionevolmente richiesto per verificare che Hera S.p.A, e/o i suoi Sub-fornitori, rispettino 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 di Hera S.p.A di consentire l'audit all'Ente comporta la risoluzione della Convenzione.

10. Indagini dell'Autorità e reclami

Nei limiti della normativa applicabile, Hera S.p.A o qualsiasi Sub-Responsabile informa senza alcun indugio l'Ente di qualsiasi:

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

Hera S.p.A fornisce, in esecuzione della Convenzione e, quindi, gratuitamente, tutta la dovuta assistenza all'Ente per garantire che la stessa 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 Hera S.p.A, in virtù di quanto previsto dall'art. 33 del Regolamento, dovrà 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 quelle che abbiano riguardato i propri sub-Fornitori. Tale comunicazione deve contenere ogni informazione utile alla gestione del *data breach*, oltre a:

- descrivere la natura della violazione dei dati personali;
- le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
- i recapiti del DPO nominato o del soggetto competente alla gestione del data breach ;
- la descrizione delle probabili conseguenze della violazione dei dati personali;
- una descrizione delle misure adottate o che si intende adottare per affrontare la Violazione della sicurezza, compreso, ove opportuno, misure per mitigare i suoi possibili effetti negativi.

Tutti i potenziali incidenti devono essere comunicati all'indirizzo **serverfarm@comune.bologna.it**,

11.2 Hera S.p.A 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. Hera S.p.A non deve 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 Hera S.p.A tiene indenne e manleva l'Ente da ogni perdita, costo, sanzione, danno e da ogni responsabilità di qualsiasi natura derivante o in connessione con una qualsiasi violazione da parte di Hera S.p.A 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 ad esempio quelle indicate all'art. 83 commi 4 e 5, l'Ente può risolvere la Convenzione o chiedere una cospicua riduzione del prezzo.

12.3 A fronte della ricezione di un reclamo relativo alle attività oggetto del presente Accordo, Hera S.p.A:

- 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.

Firmato digitalmente da:

COMUNE DI BOLOGNA – Dott. Mauro Cammarata (documento firmato digitalmente)

Hera S.p.A - Dott. Stefano Venier (documento firmato digitalmente)

Allegato 1

GLOSSARIO

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

“ **Dati personali** ”: 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 a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

“ **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) che sarà direttamente applicabile dal 25 maggio 2018;

“ **Normativa Applicabile** ”: si intende l'insieme delle norme rilevanti in materia 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.

“ **Appendice Security** ”: consiste nelle misure di sicurezza che il Titolare determina assicurando un livello minimo di sicurezza, e che possono essere aggiornate ed implementate dal Titolare, di volta in volta, in conformità alle previsioni del presente Accordo;

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

“ **Titolare del Trattamento** ”: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e 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** ”: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi 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;

“ **Responsabile del trattamento** ” : la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento

“ **Pseudonimizzazione** ”: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a 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.