HERA S.p.A.
Holding Energia Risorse Ambiente
Viale C. Berti Pichat 2/4 40127 Bologna
tel. 051.287111 fax 051.287525
www.gruppohera.it

Al Comune di Bologna
P.zza Maggiore, n. 6
40124 BOLOGNA

p.c. Simone Rossi
Via C. Diana 34
44124 FERRARA
(Responsabile Unità Organizzativa di competenza)

Oggetto: Reg. UE 679/2016 - Nomina a Responsabile "esterno" del trattamento dei dati personali

La società Hera S.p.A., Viale Carlo Berti Pichat 2/4 - 40127 Bologna, in persona del legale rappresentante pro-tempore (d'ora in avanti "il committente")

PREMESSO

a) che a seguito dell'entrata in vigore del Reg. UE n. 679 del 24 maggio 2016 (GDPR), sono state introdotte all'interno del quadro normativo europeo sulla protezione dei dati personali alcune novità di rilievo;
b) che il ***committente*** (identificato in **Hera S.p.A.**) ha commissionato al ***fornitore*** (il **Comune** in indirizzo) la prestazione di servizi - di cui alla **Convenzione tra il comune di Bologna e Hera S.p.A**. per la gestione delle domande di bonus da parte di clienti domestici economicamente svantaggiati del servizio teleriscaldamento - che ha come finalità la raccolta iniziale e il trattamento di dati personali dei clienti richiedenti il bonus a compensazione della spesa per il teleriscaldamento (d'ora in avanti "i dati"), verso cui il committente stesso assume la veste di Titolare del trattamento.
c) che la convenzione di cui al punto b), cui questo documento si allega, disciplina la materia, la durata, la natura e le finalità del trattamento, il tipo di dati personali, le categorie di interessati, gli obblighi e i diritti del titolare del trattamento, per i dettagli si rinvia alla citata convenzione;
d) che il *fornitore* tratta tali dati per conto del *committente* unicamente al fine di dare esecuzione ai servizi oggetto degli accordi suddetti;
e) che il fornitore dichiara di rispettare e conformarsi a tutte le Norme e i Provvedimenti del Garante applicabili;

tutto ciò premesso e considerato, preso atto che il *fornitore* presenta garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del Reg. UE 679/2016 e garantisca la tutela dei diritti dell'interessato,

NOMINA

il *Comune,* ai sensi dell'art.28 GDPR*,* quale **Responsabile del trattamento** dei dati personali oggetto dei servizi di cui in premessa, per tutta la durata degli stessi (altrimenti detto anche*: Responsabile Privacy Esterno)*.

Nella veste di Responsabile Privacy, il *fornitore* si impegna a trattare i dati in modo lecito, secondo correttezza e nel pieno rispetto di tutte le disposizioni emesse in materia di trattamento dei dati personali, nonché delle seguenti specifiche istruzioni.

ISTRUZIONI

1. **Persone autorizzate al trattamento**. Prima di iniziare qualsiasi trattamento di dati, il fornitore deve garantire che le persone autorizzate al trattamento dei dati personali, tramite apposite lettere di incarico, si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza che include altresì il rispetto di eventuali ulteriori istruzioni ricevute ai sensi degli artt. 29 e 32 c.4 del GDPR; tali istruzioni dovranno, ovviamente, essere anche coerenti con quelle indicate nel presente documento. Nei confronti di ciascuna persona dovrà essere effettuato un adeguato piano di formazione. L'elenco aggiornato di tutti i nominativi delle persone autorizzate al trattamento dovrà essere sempre disponibile e dovrà essere fornito alla committente immediatamente, su semplice richiesta.
2. **Clausola di riservatezza.** I dati sono da considerarsi quali informazioni riservate del committente. Su questa base:
    - il fornitore non potrà in alcun caso comunicare i dati a terzi, a meno che ciò sia necessario per l'assolvimento di un obbligo derivante da una legge o abbia ottenuto il consenso scritto del committente;
    - nel caso in cui il fornitore riceva richiesta o intimazione di comunicare informazioni personali o particolari del processo di trattamento di dati qui regolato, da parte di una pubblica autorità o da parte dell'autorità giudiziaria, dovrà provvedere a dare di ciò pronta notizia al committente e si impegna a seguire le istruzioni del committente;
    - non deve in alcun modo trasferire dati personali verso soggetti terzi o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il fornitore. Fuori da questi casi e fatto salvo il successivo punto 15, il fornitore è tenuto a chiedere specifica autorizzazione al committente;
3. **Finalità.** Il trattamento dei dati deve essere effettuato dal fornitore ai soli fini di dare esecuzione ai servizi commissionatigli. Esso si dovrà configurare, quindi, come strettamente necessario per effettuare il servizio.
4. **Privacy by design & Privacy by default.** Il fornitore deve rispettare i principi di protezione dei dati fin dalla progettazione (*privacy by design*) e protezione dei dati per impostazione predefinita (*privacy by default*) di cui all'art. 25 GDPR comunicando al committente le soluzioni individuate ed adottate per rispettare tali principi (vedi successivo punto 6).
5. **Diritto di accesso**. Deve essere garantito agli interessati l'effettivo esercizio dei diritti loro riconosciuti dal GDPR, con particolare riguardo al diritto di accesso ai dati a cui occorrerà dare riscontro nelle modalità ed entro i termini di legge anche in conformità alle procedure emesse al riguardo dal committente. Il fornitore deve supportare il committente con ogni

mezzo adeguato per garantire la conformità alle disposizioni relative ai diritti dell'interessato; deve inoltre assistere il committente con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo dei titolari del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato.

6. **Misure di sicurezza**. 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 fornitore deve adottare idonee ed adeguate misure necessarie ai fini della sicurezza dei dati personali ai sensi dell'articolo 32 del GDPR, fra le quali, ad esempio:
    a. la pseudonimizzazione e la cifratura dei dati personali;
    b. la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
    c. la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
    d. una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento;

    comunicando al committente le soluzioni individuate ed adottate per rispettare tale obbligo.
    In particolare, la comunicazione verso l'esterno deve essere sottoposta, prima del trasferimento, a cifratura a chiave pubblica (leggibile solo dagli effettivi destinatari) o analogo sistema di protezione. La password per decifrare i dati deve essere scambiata con un canale di comunicazione diverso da quello di invio dei dati.
    Nel caso in cui il Comune si avvalga di un fornitore per l'esecuzione del servizio, questi dovrà adottare le misure di sicurezza concordate.
7. **Assistenza al committente.** Il fornitore deve assistere il committente ai fini del rispetto degli obblighi di cui agli articoli da 32 a 36 del GDPR, tenendo conto della natura del trattamento e delle informazioni a sua disposizione.
8. **Violazione di dati personali (data breach).** Il fornitore deve implementare soluzioni atte a rilevare eventuali violazioni dei dati personali (ossia le violazioni di sicurezza che comportano 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) e, al verificarsi di tali violazioni, comunicarle tempestivamente al committente. Il fornitore s'impegna, altresì, a collaborare attivamente con il committente ai fini delle conseguenti comunicazioni all'Autorità Garante per la protezione dei dati personali e, eventualmente, agli interessati ai sensi degli artt. 33 e 34 del GDPR.
9. **Verifiche del *Fornitore*.** Il fornitore dovrà mantenere un costante controllo in merito al fatto che i dati siano trattati in modo lecito, secondo correttezza e comunque nel rispetto delle leggi, delle disposizioni in materia di trattamento compreso il profilo relativo alla sicurezza oltre che delle istruzioni impartite. A tale proposito dovrà anche condurre verifiche periodiche da effettuare in conformità alla normativa e nel rispetto minimo delle scadenze di legge. Il fornitore si impegna inoltre a informare immediatamente il committente segnalando ogni situazione di cui venga a conoscenza che possa esporre il committente a violazioni di legge o possa generare un trattamento illecito o porre in pericolo la riservatezza e l'integrità dei dati.
10. **Verifiche del *Committente***. Il fornitore deve mettere a disposizione del committente tutte le informazioni necessarie per dimostrare la conformità con il GDPR e contribuire alle attività di revisione, comprese le verifiche realizzate dal committente o da un altro soggetto da questi incaricato.

11. **Restituzione di dati**. Al termine del servizio oggetto del contratto il fornitore deve restituire tutti i dati personali al committente e cancellare le eventuali copie esistenti in suo possesso.
12. **Dovere di informazione.** Il fornitore deve informare immediatamente il committente qualora, a suo parere, un'istruzione violi il regolamento europeo o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati.
13. **Valutazione d'impatto sulla protezione dei dati personali (DPIA).** Il fornitore deve assistere il committente con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di agevolare la realizzazione di valutazioni d'impatto sulla protezione dei dati personali, ai sensi dell'art. 35 del GDPR, per il trattamento in questione.
14. **Trasferimento dei dati personali al di fuori dello SEE.**
    E' vietato il trasferimento dei dati personali al di fuori dello Spazio Economico Europeo.
15. **Sub-responsabile.** Il fornitore può ricorrere a un altro responsabile solo previa autorizzazione scritta, specifica o generale, del committente. La presente vale quale autorizzazione scritta generale. Il fornitore è comunque sempre tenuto ad informare il committente in merito alla scelta, aggiunta o sostituzione di qualsiasi responsabile del trattamento, dando così al committente l'opportunità di valutarla, e se del caso opporvisi. Se il fornitore ricorre a un altro responsabile (sub-responsabile) per l'esecuzione di specifiche attività di trattamento per conto del committente, deve imporgli, mediante un contratto o un altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, gli stessi obblighi in materia di protezione dei dati contenuti nel presente contratto. In particolare, il fornitore deve prevedere in quest'ultimo caso garanzie sufficienti affinché il sub-responsabile metta in atto misure tecniche e organizzative adeguate al fine di soddisfare i requisiti normativi previsti. Qualora il sub-responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il fornitore conserva l'intera responsabilità dell'adempimento degli obblighi del sub-responsabile.
16. **Registro delle attività dei trattamenti.** Il fornitore deve tenere un registro delle attività dei trattamenti ai sensi dell'art. 30 c.2 del GDPR.
17. **Responsabile della protezione dei dati (DPO).** Il fornitore indicherà al committente, se richiesto, il nome del responsabile della protezione dei dati (DPO) designato ai sensi dell'art. 37 del GDPR.
18. **Rapporti con le Autorità** Il fornitore, su richiesta del committente, deve coadiuvare quest'ultima nella difesa, in caso di procedimenti dinanzi al Garante per la protezione dei dati personali o all'Autorità Giudiziaria ordinaria, anche consentendogli la tempestiva esibizione della modulistica privacy e dei documenti probatori rientranti nella competenza del fornitore stesso.
19. **Estinzione e revoca** Resta inteso che la nomina a Responsabile del trattamento decadrà in qualunque caso di cessazione della prestazione di servizi, con effetto dalla data di tale cessazione.

Qualora il fornitore determini autonomamente le finalità e i mezzi di trattamento, in violazione delle precedenti istruzioni, si assume i conseguenti oneri, rischi e responsabilità come se fosse un autonomo titolare relativamente al trattamento in questione.
Ciascuna delle parti (*il committente e il fornitore*) non sarà ritenuta responsabile delle eventuali violazioni delle disposizioni di legge in materia di trattamento dei dati personali riferibili ad azioni od omissioni dell'altra parte. Ciascuna parte sarà manlevata e indennizzata da qualsiasi conseguenza, sia civile che amministrativa, responsabilità, perdita, danno o costo sopportato per effetto della

violazione delle presenti istruzioni o di una qualsiasi disposizione di legge in materia di trattamento dei dati personali riferibile ad azioni od omissioni dell'altra parte.
In ogni caso di dubbio in materia o per eventuali necessità aggiuntive vi preghiamo di contattare il Responsabile privacy dell'Unità Organizzativa di Hera S.p.A., indicato in copia nella presente.

Cordiali Saluti

Per il Titolare di HERA S.p.A.
Ing. Marcello Guerrini

Per conferma e accettazione

Timbro del Comune……