Nomina di Hera S.p.A a Responsabile privacy esterno da parte di terzi

DEFINIZIONI utili alla comprensione delle istruzioni e del modello:

Amministratore di Sistema (AS). *La persona fisica, con capacità tipicamente tecniche, i cui compiti siano finalizzati alla gestione e alla manutenzione di un impianto di elaborazione con cui vengono effettuati trattamenti di dati personali, compresi i sistemi di gestione delle basi di dati, all'amministrazione di sistemi software complessi quali i sistemi ERP (Enterprise Resource Planning) utilizzati. Sono inoltre incluse nella definizione di AS anche le figure equiparabili sotto il profilo dei rischi relativi alla protezione dei dati personali. Le attività tecniche assegnate agli AS comportano, in molti casi, un'effettiva capacità di azione su informazioni che va considerata a tutti gli effetti alla stregua di un trattamento di dati personali; ciò, anche quando l'amministratore non consulti «in chiaro» le informazioni medesime. Esclusione dalla definizione: non rientrano nella definizione di AS quei soggetti che solo occasionalmente intervengono (per es.: per scopi di manutenzione a seguito di guasti o malfunzioni) sui sistemi di elaborazione e sui sistemi software.*

Clausola: *è un elemento del contratto. Essa rappresenta una delle disposizioni attraverso cui si concretizza la convenzione/accordo tra le parti.*

Convenzione: *accordo organizzativo con il quale due o più enti/soggetti fanno fronte ad esigenze di collaborazione grazie al coordinamento di funzioni/servizi/attività.*

Ente: *ai fini della presente istruzione si intendono le seguenti categorie di soggetti: Enti Pubblici , Associazioni, Altri Soggetti diversi dai Fornitori*

EELL: *acronimo di Enti Locali. Sono un sottoinsieme degli Enti Pubblici*

Ente Pubblico: *persona giuridica creata secondo norme di diritto pubblico, detta anche persona giuridica di diritto pubblico, attraverso la quale la Pubblica Amministrazione svolge la propria funzione amministrativa. La definizione include gli Enti Locali. L'art. 4 della L. 70/1975 dispone che nessun Ente Pubblico possa essere riconosciuto o istituito se non per legge.*

Per gli enti istituiti prima di tale legge si pone il problema di individuare a quali debba essere riconosciuta tale natura. Il criterio più seguito è quello del regime giuridico, caratterizzato da un sistema di controlli pubblici, dall'ingerenza dello Stato tramite direttive nel raggiungimento degli obiettivi, ecc.

Nomina di Hera S.p.A a Responsabile privacy esterno da parte di terzi

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

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 Comune di…….* ha commissionato al *fornitore* (identificato in Hera spa – Direzione Servizi Ambientali) la prestazione di servizi - di cui alla presente Convenzione - che presuppongono per la loro esecuzione il trattamento di dati personali di interessati (d'ora in avanti "*i dati")*
c) che la convenzione di cui al punto b) 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;
d) che Hera spa tratta tali dati per conto del committente unicamente al fine di dare esecuzione ai servizi commissionatigli;

tutto ciò premesso e considerato, preso atto che Hera spa 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 Hera spa quale **Responsabile del trattamento** dei dati relativi e connessi all'oggetto dei servizi in questione e per tutta la durata degli stessi (altrimenti detto anche*: Responsabile Privacy esterno)*.

Tale nomina verrà registrata nell'apposito elenco disponibile presso il Comune e resa conoscibile in modo agevole da chi ne faccia richiesta.

Nella veste di Responsabile Privacy, il Hera spa s'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.

COMPITI E ISTRUZIONI

1. **Persone autorizzate al trattamento**. Prima di iniziare qualsiasi trattamento di dati, Hera deve garantire che le persone autorizzate al trattamento dei dati personali 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 al Comune immediatamente, su semplice richiesta.
1. **Clausola di riservatezza.** I dati sono da considerarsi quali informazioni riservate del Comune su questa base:
    - Hera spa 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;
    - nel caso in cui Hera spa 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 Hera spa. Fuori da questi casi e fatto salvo il successivo punto 14, Hera è tenuta a chiedere specifica autorizzazione al Comune;

Nomina di Hera S.p.A a Responsabile privacy esterno da parte di terzi

2. **Finalità.** Il trattamento dei dati deve essere effettuato da HERA spa ai soli fini di dare esecuzione ai servizi commissionati. Esso si dovrà configurare, quindi, come strettamente necessario per effettuare il servizio.
3. **Privacy by design & Privacy by default.** Hera spa 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).
4. **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. Hera spa deve supportare il Comune con ogni mezzo adeguato per garantire la conformità alle disposizioni relative ai diritti dell'interessato; deve inoltre assistere il Comune 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.
5. **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, Hera spa 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.
6. **Assistenza del committente.** Hera spa deve assistere il Comune 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.
7. **Violazione di dati personali (data breach).** Hera spa 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. Hera spa s'impegna, altresì, a collaborare attivamente con il Comune 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.
8. **Verifiche del *Fornitore*.** Hera spa 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. Hera spa si impegna inoltre a informare immediatamente il Comune segnalando ogni situazione di cui venga a conoscenza che possa esporre il Comune a violazioni di legge o possa generare un trattamento illecito o porre in pericolo la riservatezza e l'integrità dei dati.
9. **Verifiche del *Committente***. Hera spa 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.
10. **Restituzione di dati**. Al termine del servizio oggetto del contratto Hera spa deve restituire tutti i dati personali al committente e cancellare le eventuali copie esistenti in suo possesso.
11. **Dovere di informazione.** Hera spa deve informare immediatamente il Comune qualora, a suo parere, un'istruzione violi il regolamento europeo o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati.
12. **Valutazione d'impatto sulla protezione dei dati personali (DPIA).** Hera spa deve assistere il Comune 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.
13. **Sub-responsabile.** Hera spa può ricorrere a un altro responsabile solo previa autorizzazione scritta, specifica o generale, del committente. La presente vale quale autorizzazione scritta generale. Hera spa

è comunque sempre tenuto ad informare il Comune 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 Hera spa 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, Hera spa 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, Hera spa conserva l'intera responsabilità dell'adempimento degli obblighi del sub-responsabile.

14. **Registro delle attività dei trattamenti.** Hera spa deve tenere un registro delle attività dei trattamenti ai sensi dell'art. 30 c.2 del GDPR.

15. **Responsabile della protezione dei dati (DPO).** Hera spa deve procedere, se del caso, alla designazione del responsabile della protezione dei dati (DPO) ai sensi dell'art. 37 del GDPR. Qualora Hera spa ritenga di non doversi dotare di tale figura ne fornisce autodichiarazione al committente.

Qualora Hera spa 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 Comune ed Hera spa*) 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.