PROCEDURA DI GARA APERTA TELEMATICA, SOPRA SOGLIA DI RILEVANZA EUROPEA, FINALIZZATA ALL'AFFIDAMENTO DEI SERVIZI APPLICATIVI E INFRASTRUTTURALI RELATIVI AI SISTEMI WEB-BASED DELL'AUTORITÀ DI REGOLAZIONE PER ENERGIA RETI E AMBIENTE.

PROCEDURA DI GARA APERTA TELEMATICA

CIG B8B3485154

ALLEGATO 5 AL CAPITOLATO TECNICO

INFORMATION SECURITY POLICY PER I FORNITORI

SOMMARIO

1 INTRODUZIONE

L'Autorità di Regolazione per Energia Reti e Ambiente (di seguito: l'Autorità o ARERA) è un organismo indipendente istituito con la legge 14 novembre 1995, n. 481 con il compito di tutelare gli interessi dei consumatori e di promuovere la concorrenza, l'efficienza e la diffusione di servizi con adeguati livelli di qualità, attraverso l'attività di regolazione e di controllo. L'azione dell'Autorità, inizialmente limitata ai settori dell'energia elettrica e del gas naturale, è stata in seguito estesa, attraverso più interventi normativi, ai servizi idrici (dl n.201/11,convertito nella legge n. 214/11), al teleriscaldamento e tele raffrescamento (decreto legislativo 4 luglio 2014 n. 102).

Da ultimo, con la legge 27 dicembre 2017, n. 205, sono state attribuite all'Autorità funzioni di regolazione e controllo del ciclo dei rifiuti, anche differenziati, urbani e assimilati.

In tutti i settori, oltre a garantire la promozione della concorrenza e dell'efficienza nei settori energetici, l'azione dell'Autorità è diretta ad assicurare la fruibilità e la diffusione dei servizi in modo omogeneo sull'intero territorio nazionale, a definirne adeguati livelli di qualità, a predisporre sistemi tariffari certi, trasparenti e basati su criteri predefiniti e a promuovere la tutela degli interessi di utenti e consumatori. Tali funzioni sono svolte armonizzando gli obiettivi economico-finanziari dei soggetti esercenti i servizi con gli obiettivi generali di carattere sociale, di tutela ambientale e di uso efficiente delle risorse.

Ai fini dello svolgimento della propria missione L'Autorità ha la necessità di raccogliere dati e informazioni dagli operatori e da altri soggetti operanti nei settori di competenza; ulteriori informazioni pervengono dai consumatori, dalle associazioni di categoria e dai diversi soggetti, anche istituzionali, che interagiscono con l'Autorità per i settori di competenza.

L'Autorità coopera inoltre con alcuni organismi internazionali (Commissione Europea, ACER, CEER, ecc.) con scambi di informazioni e dati che richiedono procedure di trattamento idonee a garantirne la riservatezza.

Infine l'Autorità tratta anche dati e informazioni che possono assumere caratteristiche di riservatezza oltre a dati riguardanti il personale della propria struttura, collaboratori, fornitori e consulenti.

Con la deliberazione 17 marzo 2016 108/2016/A (di seguito: deliberazione 108/2016) l'Autorità ha adottato le *Policy* di alto livello per la gestione della sicurezza delle informazioni e dei dati ricevuti trattati e gestiti.

L'entrata in vigore del Regolamento generale sulla protezione dei dati (GDPR) che ha introdotto rilevanti novità in materia di protezione dei dati personali impone la necessità di garantire un approccio sistematico, omogeneo e coerente in materia di sicurezza dei dati trattati.

Con la deliberazione 17 settembre 2024 362/2024/A l'Autorità ha, altresì, adottato il "Regolamento dell'Autorità di Regolazione per Energia Reti e Ambiente relativo agli adempimenti in materia di trattamento dei dati personali ai sensi dell'articolo 29 del Regolamento (UE) n. 2016/679 e dell'articolo 2-*quaterdecies* del decreto legislativo 30 giugno 2003, n. 196" (di seguito: deliberazione Regolamento Privacy) che pone specifici obblighi sui soggetti chiamati a trattare i dati personali per conto dell'Autorità in qualità di responsabili del trattamento.

Il presente documento costituisce una *policy* specificatamente dedicata ai fornitori dell'Autorità anche in attuazione della deliberazione 108/2016 e del Regolamento Privacy e descrive procedure, regole e requisiti da applicare al trattamento delle informazioni gestite dall'Autorità alle quali i fornitori tutti dovranno conformarsi.

2 LE POLICY DI ALTO LIVELLO

Si riportano alcuni degli elementi che caratterizzano l'approccio scelto dall'Autorità con la deliberazione 108/2016/A.

Politiche di sicurezza dei dati e delle informazioni dell'Autorità per l'energia elettrica il gas e il sistema idrico - Princìpi Fondamentali.

1. L'approccio alla sicurezza dei dati e delle informazioni dell'Autorità è orientato alla **riduzione del rischio ed è conforme agli standard internazionali nonché alle buone pratiche consolidate**. Le informazioni dell'Autorità, in qualsiasi forma ne sia in possesso, sono protette in modo **coerente e proporzionato**.

2. L'Autorità sviluppa e gestisce il **Sistema di Gestione della Sicurezza delle Informazioni (SGSI)** costituito da un insieme di politiche, procedure, linee guida, risorse e attività associate che l'Autorità mette in atto, attraverso un sistema coerente e proporzionato, allo scopo di proteggere le proprie informazioni.

3. Il Sistema di Gestione della Sicurezza delle Informazioni dell'Autorità (SGSI) **si conforma all'insieme di standard ISO/IEC 27000**, e in particolare:

- ISO/IEC 27001 per i requisiti della sicurezza delle informazioni;
- ISO/IEC 27002 come linee guida e buone pratiche per la selezione, l'implementazione e la gestione dei controlli di sicurezza delle informazioni;
- ISO/IEC 27005 per la gestione del rischio della sicurezza delle informazioni;
- ISO/IEC 27010 per le comunicazioni intersettoriali e inter-organizzative.

4. Le misure di sicurezza devono essere **efficaci e coerenti**. La loro efficacia e coerenza sono valutate prendendo in considerazione **l'analisi dei rischi e gli obiettivi di riduzione del rischio** individuati relativamente a ciascuna tipologia di informazione trattata.

NEL SEGUITO SI RIPORTANO LE POLICY CHE I FORNITORI DEVONO SEGUIRE PER SVILUPPARE LE POLICY DI DETTAGLIO E LE PROCEDURE OPERATIVE ATTE A GARANTIRE IL RAGGIUNGIMENTO DEGLI OBIETTIVI DI SICUREZZA DELLE INFORMAZIONI QUI DEFINITI.

3 POLICY DI SICUREZZA DELLE INFORMAZIONI PER I FORNITORI

Le policy qui descritte sono da considerarsi requisiti della fornitura e il Fornitore dovrà produrre le evidenze che ne dimostrino il soddisfacimento. L'Autorità potrà richiedere specifiche evidenze laddove non siano sufficienti quelle fornite.

Policy ID	Descrizione
Sec001	**Security Policy** Il Fornitore deve garantire la conformità al Regolamento Privacy e alle Politiche per la sicurezza indicate dall'Autorità (di cui questo documento costituisce parte fondamentale), assicurandone la diffusione dei principi presso tutto il personale che si trova ad interagire con il sistema informativo legato al servizio e più in generale con gli aspetti organizzativi del servizio erogato per l'Autorità. Inoltre, è compito del Fornitore diffondere i requisiti di sicurezza e di gestione dei dati personali dell'Autorità lungo la filiera di fornitura in caso di subappalto di parti del servizio fornito. Nel corso del contratto le policy inserite in questo documento e le istruzioni sul trattamento dei dati personali possono essere aggiornate, modificate, migliorate sia per mutate condizioni, sia a fronte dell'analisi dei rischi, sia per il modello di "miglioramento continuo" previsto da ISO 27001. Gli aggiornamenti dovranno essere recepiti ed implementati dal Fornitore.
Sec002	**Conformità normativa** Il servizio, l'infrastruttura ed il contesto tecnico-organizzativo circostante dovranno essere conformi alla normativa e mantenuti conformi nel tempo. A titolo di esempio si citano alcune delle normative su cui è richiesta conformità: - D.lgs. 138/2024 di recepimento della direttiva (UE) 2022/2555 (c.d. NIS 2), relativa a misure per i soggetti **essenziali** per un livello comune elevato di cibersicurezza nell'Unione. - Legge 28 giugno 2024, n. 90, Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici. - Decreto del Presidente del Consiglio Dei Ministri 30 aprile 2025 che deve essere applicato anche agli eventuali subfornitori. - Regolamento (UE) 2016/679 recante il Regolamento generale sulla protezione dei dati (GDPR) - D.lgs. 196/2003 Codice in materia di protezione dei dati personali. - Provvedimento del Garante sulla privacy per gli amministratori di sistema del 27 novembre 2008. - Il codice dell'amministrazione digitale (CAD) - D.Lgs 7 marzo 2005, n. 82 e successive modifiche. - Legge 48 del 18 marzo 2008 sul crimine informatico. - Dipartimento per l'Innovazione e le Tecnologie pubblicata sulla G.U. n.69 del 22 marzo 2002 "Sicurezza Informatica e delle Telecomunicazioni nelle Pubbliche Amministrazioni Statali". - Legge 633/41 e D. Lgs 518/92 Titolarità diritti sul software (legge diritto d'autore).
Sec003	**Privacy** Il GDPR stabilisce norme relative alla protezione dei dati personali delle persone fisiche e pone in capo al titolare del trattamento l'obbligo di regolare contrattualmente i rapporti con i soggetti che trattano i dati per suo conto da nominarsi responsabili del trattamento, ai sensi dell'art. 28 del GDPR, previa verifica in ordine all'adozione di misure, tecniche e organizzative, adeguate a garantire e a dimostrare che il trattamento stesso è effettuato in conformità della norma. Il soggetto nominato responsabile del trattamento che effettui trattamenti di dati personali per conto dell'Autorità dovrà farlo in ottemperanza al GDPR e al Regolamento Privacy che declina le norme in materia di trattamento dei dati nell'Autorità, declinando procedure e istruzioni per il corretto trattamento. *L'Annesso A al presente documento presenta il modello di "Accordo di nomina del Responsabile del trattamento dei dati personali" per il Fornitore che verrà indicato come Responsabile dei trattamenti afferenti al contratto, in ossequio alla Decisione di Esecuzione (UE) 2021/915 della*

	Commissione Europea del 4 giugno 2021 relativa alle clausole contrattuali tipo tra titolari del trattamento e responsabili del trattamento e al Regolamento Privacy.
Sec004	**Conformità ai principali standard di sicurezza internazionali** Il Fornitore deve adeguare le proprie procedure, anche in termini di Ciclo di vita dello sviluppo dei sistemi, ai principali standard internazionali in tema di sicurezza delle informazioni, alle linee guida, ai framework e alle buone pratiche maggiormente diffuse; a titolo esemplificativo si fa riferimento a ISO 27001, OWASP NIST CSF, ecc. L'Autorità segue un approccio alla sicurezza orientato al rischio. Ogni misura di sicurezza deve essere quindi orientata alla riduzione del rischio e alla verifica della sua l'efficacia nel tempo.
Sec005	**Gestione del rischio relativo alla sicurezza delle informazioni** Il Fornitore deve assicurarsi che siano poste in atto tutte le necessarie azioni al fine di ridurre i rischi connessi ai trattamenti di informazioni affidatigli. In particolare, il Fornitore deve avere un processo di gestione del rischio che includa: - la valutazione del rischio relativo alla sicurezza delle informazioni (risk assessment); - il trattamento del rischio relativo alla sicurezza delle informazioni (risk treatment). Il processo di gestione dei rischi deve essere iterativo: la valutazione del rischio e il suo trattamento devono essere ripetuti regolarmente almeno una volta l'anno o in caso di cambiamenti importanti nei servizi, nelle applicazioni o nell'infrastruttura interessata. La valutazione del rischio deve prevedere la classificazione delle informazioni trattate e l'impatto che il concretizzarsi di eventuali minacce ha sulle attività dell'Autorità. Il Fornitore deve effettuare quest'attività coinvolgendo il personale dell'Autorità (data owner) e richiedendo le informazioni utili a tale valutazione.
Sec006	**Riservatezza, Integrità e Disponibilità** I tre fattori critici che devono essere considerati dal Fornitore vanno esaminati in dettaglio durante l'analisi dei rischi e la definizione delle contromisure per ridurre il rischio tenendo conto dei seguenti principi generali: **Riservatezza**: i dati trattati dall'Autorità hanno spesso un livello di riservatezza elevato (dal punto di vista normativo e/o commerciale); il livello di riservatezza può cambiare nel tempo (un'informazione può diventare pubblica in alcuni casi, si pensi ad una deliberazione) o può mantenere lo stesso livello nel tempo (si pensi ai dati personali); il Fornitore deve garantire la corretta riservatezza delle informazioni trattate. **Integrità**: l'integrità delle informazioni è un fattore determinante per una Pubblica Amministrazione in quanto tutti gli atti amministrativi si basano sulla "qualità" del dato (correttezza, completezza, precisione, veridicità, ecc.); di norma l'integrità deve essere mantenuta per tutto il ciclo di vita del dato; il Fornitore deve garantire la corretta elaborazione e la protezione delle informazioni e dei dati presenti nel patrimonio informativo dell'Autorità. **Disponibilità**: la disponibilità delle informazioni ha impatto sui tempi dei processi che permettono all'Autorità di svolgere i propri funzioni istituzionali; i parametri relativi a questo fattore sono in genere definiti nei capitolati di gara in termini di indici di qualità e livelli di servizio; in questo caso il Fornitore deve prendere in considerazione aspetti relativi alla tempestività delle risposte alle esigenze dell'Autorità (change request, incident, problem, ecc.) attuando opportune strategie tecniche e organizzative (ITIL, DR, BC, Backup&Restore, ecc.). Se un incidente informatico impatta su uno dei tre fattori descritti verrà classificato come incidente di sicurezza delle informazioni.
Sec007	**Controllo degli Accessi** Il Fornitore deve controllare e regolamentare l'accesso al patrimonio informativo dell'Autorità, effettuato dal personale dell'Autorità, dal proprio personale e dagli utenti esterni, nell'ambito delle attività previste dal rapporto contrattuale con l'Autorità.

	Il controllo degli accessi dovrà essere commisurato al tipo di dato a cui si ha accesso (personale, sensibile, riservato ecc.). L'uso della crittografia, di *audit log*, ecc. dovrà essere implementato laddove l'analisi dei rischi lo renda opportuno o dove questi sia un obbligo normativo. La *strong authentication* è di norma usata per tutti gli accessi ai dati non pubblici dell'Autorità. Per le applicazioni interne gli accessi avvengono in SSO con Multi-Factor Authentication (MFA). Dovranno essere implementate particolari misure di sicurezza atte a minimizzare il rischio legato alle utenze privilegiate (amministratori di sistema e affini) anche in conformità alle disposizioni del Garante della Privacy. L'accesso agli ambienti di test deve essere comunque sottoposto a SSO e strong authentication ma per permettere la simulazione di vari profili utente devono essere implementati meccanismi di "impersonamento/cambio profilo".
Sec008	**Separazione degli ambienti e dei ruoli** La separazione dei ruoli fra chi utilizza il sistema, chi lo esercisce (sistemisti, DBA) e chi lo progetta (programmatori, ecc.), deve corrispondere ad una profilazione opportuna degli accessi e dei "privilegi" che ogni utente ha sul sistema. Al riguardo si rimanda alla normativa in materia e, in particolare, al "Provvedimento del Garante della Privacy - 27 Novembre 2008 – relativo alle misure per le attribuzioni delle funzioni di amministratore di sistema" come richiamato nel Regolamento Privacy. Deve essere inoltre prevista la separazione funzionale e logica degli ambienti di sviluppo, test, collaudo e produzione.
Sec009	**Business Continuity e Disater Recovery** Il Fornitore deve produrre, mantenere e sottoporre a prove periodiche i piani per la continuità dei servizi informatici erogati (BCP – Business Continuity Plan). Laddove richiesto e/o in funzione dei parametri di *recovery point objective* (RPO) e il *recovery time objective* (RTO), dovranno essere assicurate le attività di predisposizione e gestione di un'architettura di Disaster Recovery attraverso la quale erogare i servizi agli utenti in caso di disastro, garantendo la fornitura e la gestione di tutte le risorse hardware software e di connettività, necessarie a garantire il funzionamento e l'erogazione dei servizi agli utenti in caso di disastro (DRP – Disaster Recovery Plan). Il Disaster Recovery Plan deve essere testato con frequenza annuale.
Sec010	**Backup e restore** Dovrà essere assicurata la gestione del salvataggio, l'archiviazione ed il ripristino dei dati di sistema e utente presenti sui server dedicati all'esercizio delle applicazioni dell'Autorità. Il servizio dovrà essere effettuato nel rispetto della normativa vigente in merito alla gestione e conservazione dei dati, con particolare riferimento ai dati gestiti e al periodo di conservazione degli stessi. Dovrà essere assicurata altresì: - la gestione del salvataggio dei dati; - la gestione dei cicli di *backup* dei dati secondo un piano concordato con l'Autorità; - il ripristino dei dati a seguito di danneggiamento o perdita di integrità; - il metodo di validazione dei supporti di salvataggio; - il luogo dove depositare i supporti, la loro identificazione e i cicli di rotazione; - frequenza e modalità dei test di *restore.* I test di backup e restore dovranno essere svolti **con una frequenza minima di uno ogni tre mesi** e dovranno comprendere tutti gli elementi che erogano il servizio (es. applicazione, codice, file system, database, ecc.). Laddove vi siano istanze di database che contengono più schemi dovranno essere effettuati test di ripristino mirati anche a un solo schema.

Sec011	**Formazione e Consapevolezza** Il Fornitore deve rendere disponibile a tutto il personale dell'Autorità, ed in particolare ai referenti tecnici e agli utenti del sistema informativo, adeguata formazione sulla sicurezza delle informazioni e sulle procedure messe in atto, senza onere aggiuntivo per l'Autorità. Il Fornitore inoltre deve attivare un programma di formazione continuo interno alla propria azienda che abbia come obbiettivo la diffusione di una cultura della sicurezza delle informazioni e la conoscenza delle procedure per ridurre al minimo i rischi per le informazioni gestite.
Sec012	**Security Incident Management** È richiesta una efficace e adeguata gestione degli incidenti informatici relativi alla sicurezza che abbia come obiettivo primario la riduzione dell'impatto e il continuo miglioramento (ISO 27001). Tutti gli eventi riguardanti la sicurezza delle informazioni devono essere tracciati e opportunamente gestiti per ridurne l'eventuale impatto sulle attività dell'Autorità. A tale proposito ci si aspetta che il fornitore implementi sistemi di Gestione degli Eventi di Sicurezza (SIEM) e di Orchestrazione e Automazione della Risposta (SOAR) avanzati che includano funzionalità di Intelligenza Artificiale e Machine Learning (a titolo di esempio Next Gen SIEM e UEBA). Si raccomanda in particolare l'utilizzo di processi di gestione strutturati (es. sul modello delle best practice ITIL), che possono migliorare la gestione del *Security Incident Management.* A tale proposito il fornitore deve avere una propria procedura di Security Incident Management integrata con la corrispondente procedura dell'Autorità e di altri attori che potrebbero essere coinvolti nell'erogazione del servizio. Tale procedura deve essere conosciuta d tutto il personale del fornitore che lavora per l'Autorità. Il Fornitore dovrà in ogni caso raccogliere segnalazioni di incidenti e formalizzare tempestivi rapporti su tutte le infrazioni della sicurezza, vere o presunte, fornendo ove richiesto supporto per la conduzione di indagini da parte dell'Autorità, degli organismi di sicurezza preposti o di soggetti terzi da essa incaricati. Le violazioni di dati personali (Art. 33 del GDPR) sono soggette all'obbligo di notifica all'Autorità Garante per la protezione dei dati personali, secondo la procedura di cui al Regolamento Privacy. Si ricordano inoltre gli obblighi di notifica previsti dal Decreto Legislativo 4 settembre 2024, n. 138, art.5. Particolare attenzione deve essere posta ai tempi massimi previsti nella normativa.
Sec013	**Procedure di sicurezza** Il Fornitore deve realizzare e mantenere aggiornate procedure a sostegno della politica di sicurezza in conformità alle esigenze dell'Autorità. Tali procedure devono comprendere, a titolo esemplificativo e non esaustivo: - classificazione e controllo degli asset; - protezione fisica delle risorse; - protezione logica delle informazioni; - gestione degli incidenti e dei malfunzionamenti inerenti alla sicurezza; - regolamentazione dell'accesso al sistema informativo dell'Autorità; - sviluppo e manutenzione dei sistemi; - test periodici di sicurezza, VA e PT; - Business Continuity e Disaster Recovery. Dovrà inoltre essere previsto un meccanismo di verifica periodica dell'efficacia e della validità nel tempo delle contromisure adottate, mediante la definizione di opportune metriche e l'implementazione di sistemi di monitoraggio e controllo.
Sec014	**Infrastrutture e tool di sicurezza** Il fornitore deve implementare un'infrastruttura e gli strumenti necessari a garantire la sicurezza delle informazioni trattate. A titolo esemplificativo e non esaustivo si elencano alcuni degli elementi ritenuti mandatori:

	• Protezioni perimetrali (Firewall, Web Application Firewall, ecc.); • Sistemi anti-malware; • Monitoraggio degli eventi di sicurezza (SIEM); • Log collection and log analysis; • sistemi di Privileged Access Management (es. Oracle Database Vault); • VPN access per attività da remoto; • Sistemi di end-point security
Sec015	**Sicurezza degli sviluppi** Il fornitore deve garantire che i requisiti di sicurezza siano considerati e implementati durante il ciclo di sviluppo del software e dei sistemi attraverso: • l'applicazione di standard e buone pratiche (OWASP, NIST, ecc.) • opportune sessioni di test focalizzate sugli aspetti di sicurezza • sessioni di code review che individuino eventuali vulnerabilità • sessioni di training specifico del personale dei team di sviluppo (analisti, programmatori, tester, …)
Sec016	**Test di vulnerabilità e penetration test** Il Fornitore è tenuto a effettuare, con cadenza almeno semestrale, test di vulnerabilità sia a livello applicativo che a livello sistemistico e infrastrutturale, che prevedano almeno: - la scansione dei sistemi fisici, alla ricerca di configurazioni del software di base e applicativo ritenute non sicure e vulnerabili ad attacchi (*vulnerability assessment*); - test di penetrazione (*penetration testing*) che consentono di valutare la resistenza dei sistemi a determinati attacchi informatici simulati e a verificare la possibilità di sfruttare eventuali vulnerabilità evidenziate durante il vulnerability assessment. I test di vulnerabilità dovranno essere eseguiti dal Fornitore previa informazione all'Autorità che si riserva di designare eventuali terze parti per la supervisione dei test durante la loro effettuazione. I risultati dei test saranno oggetto di analisi da parte dell'Autorità, che potrà avvalersi di parti terze per individuare le eventuali criticità e le azioni correttive necessarie alla loro rimozione. L'attuazione delle eventuali azioni correttive avverrà mediante uno specifico piano di rientro *(Remediation plan)*; le attività richieste ai fornitori per l'implementazione del *remediation plan* non comporteranno oneri aggiuntivi all'Amministrazione. Fanno eccezioni eventuali variazioni delle Politiche di Sicurezza dell'Autorità.
Sec017	**Audit da parte dell'Autorità e di terzi designati** L'Autorità si riserva il diritto di richiedere evidenze o effettuare Audit, anche con l'ausilio di terze parti, presso le sedi del Fornitore o dei subfornitori dei servizi ICT per verificare l'effettivo rispetto delle policy di sicurezza delle informazioni, dei requisiti contrattuali corrispondenti e delle norme italiane ed internazionali che regolano la materia. Il Fornitore deve fornire tutti gli accessi ad eventuali sistemi e applicazioni che permettono di verificare la corretta gestione della sicurezza delle informazioni da parte del Fornitore. L'Autorità si riserva inoltre di effettuare, anche senza preavviso, propri test di sicurezza (VA o PT) o di farli eseguire da parti terze; in tal caso il Fornitore è tenuto a fornire il supporto richiesto mediante attività coordinate tra risorse dedicate ai servizi applicativi e risorse dedicate ai servizi infrastrutturali, sotto la supervisione dell'Autorità.

ANNESSO A: Accordo di nomina del Responsabile del trattamento dei dati personali

Accordo di nomina del Responsabile del trattamento dei dati personali
ai sensi e per gli effetti dell'articolo 28 del Regolamento (UE) 2016/679

VISTO il contratto [●] (di seguito: Contratto), stipulato in data [●] con decorrenza da [●], OPPURE la deliberazione n. [●] (di seguito: Delibera), del [●], con cui l'Autorità di Regolazione per Energia Reti e Ambiente (di seguito: l'Autorità o ARERA o Titolare) ha affidato le attività ivi descritte alla società [●], codice fiscale e partita IVA n. [●], con sede legale in [●], via/piazza [●] n. [●], cap. [●], in persona del Legale Rappresentante [●] (di seguito: Società/Responsabile);

CONSIDERATO che le attività oggetto del Contratto/Delibera comportano o possono comportare il trattamento di dati personali, ai sensi del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 (di seguito: GDPR) nonché del D. Lgs. 196/2003 e ss.mm.ii. recante il Codice in materia di protezione dei dati personali (di seguito: Codice Privacy);

VISTO, in particolare, l'articolo 4, paragrafo 1, n. 7) del GDPR, che individua il Titolare del trattamento ne «*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* […]» e visto altresì l'articolo 4, paragrafo 1, n. 8) del GDPR, che identifica il responsabile del trattamento ne «*la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento*»;

VISTO l'articolo 28, paragrafo 1 del GDPR, secondo cui «*qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato*»;

VISTA la Decisione di Esecuzione (UE) 2021/915 della Commissione Europea del 4 giugno 2021 relativa alle clausole contrattuali tipo tra titolari del trattamento e responsabili del trattamento a norma dell'articolo 28, paragrafo 7, del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, le cui "clausole" sono riportate e integrate nel presente accordo di nomina (di seguito: Accordo);

VISTO il Provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008, ss.mm.ii. relativo alle "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" (di seguito: "Provvedimento");

VISTO il vigente Regolamento di organizzazione e funzionamento dell'Autorità di Regolazione per Energia Reti e Ambiente;

VISTA la deliberazione 362/2024/A del 17 settembre 2024 e l'allegato "Regolamento dell'Autorità di Regolazione per Energia Reti e Ambiente relativo agli adempimenti in materia di trattamento dei dati personali ai sensi dell'articolo 29 del Regolamento (UE) n. 2016/679 e dell'articolo 2-*quaterdecies* del decreto legislativo 30 giugno 2003, n. 196" (di seguito: Regolamento Privacy), nonché gli ulteriori atti allegati al Regolamento Privacy che qui si intendono espressamente richiamati quali procedure e istruzioni impartite al Responsabile e che sottoscrivendo il presente Accordo dichiara di conoscere e accettare incondizionatamente;

VISTI gli articoli 5 e 6 del Regolamento Privacy che attribuiscono ai dirigenti responsabili della macrostruttura dell'Autorità (Segretario Generale, Direttori di Divisione, Direttori di Direzione, Responsabili di Ufficio speciale), quali Designati al trattamento, ciascuno per i procedimenti e le attività di competenza, il potere di sottoscrivere gli accordi di designazione con i responsabili del trattamento;

CONSIDERATA l'idoneità, alla luce dell'attività istruttoria già svolta in sede istruttoria, della Società aggiudicatrice del Contratto/individuata con la Delibera al rispetto delle garanzie richieste dal GDPR, dal Codice Privacy e dai provvedimenti amministrativi attuativi con riferimento all'adeguatezza delle misure tecniche e organizzative per la tutela dei diritti dell'interessato;

L'AUTORITÀ

nella persona del dott./della dott.ssa [●] nella sua qualità di Designato al trattamento dal Titolare per le materie di competenza e domiciliato per la funzione presso la sede in Milano, Piazza Cavour 5

NOMINA

ai sensi e per gli effetti di cui all'articolo 28 del GDPR, la Società, che accetta,

RESPONSABILE DEL TRATTAMENTO DEI DATI PERSONALI

con riferimento alle attività di cui al Contratto/Delibera, che qui si intende integralmente richiamato/a.

Articolo 1
Scopo e ambito di applicazione

1.1. Il Titolare e il Responsabile del trattamento accettano le premesse di cui al presente Accordo e tutti gli articoli al fine di garantire il rispetto dell'articolo 28, paragrafi 3 e 4, del GDPR.
1.2. I presenti articoli si applicano al trattamento dei dati personali specificato all'allegato II.
1.3. Gli allegati da I a III costituiscono parte integrante dell'Accordo.
1.4. I presenti articoli lasciano impregiudicati gli obblighi cui è soggetto il Titolare a norma del GDPR.
1.5. I presenti articoli non garantiscono, di per sé, il rispetto degli obblighi connessi ai trasferimenti internazionali conformemente al capo V del GDPR.
1.6. Le parti si impegnano ad effettuare ogni notifica e/o comunicazione prevista o rilevante ai fini dell'Accordo a mezzo PEC e via mail agli indirizzi dei rispettivi Responsabili della Protezione dei Dati (di seguito: RPD)
Per il Titolare
PEC: protocollo@pec.arera.it
RPD: Avv. Davide Mula, tel. 0265565536, mail: rpd@arera.it
Per il Responsabile
PEC: [●]
RPD: Nome Cognome, tel. [●], mail: [●].
Le parti si impegnano a comunicare tempestivamente ogni variazione dei predetti recapiti.

Articolo 2
Interpretazione

2.1. Quando i presenti articoli utilizzano i termini definiti nel GDPR tali termini hanno lo stesso significato di cui al regolamento interessato.
2.2. I presenti articoli vanno letti e interpretati alla luce delle disposizioni del GDPR.
2.3. I presenti articoli non devono essere interpretati in un senso che non sia conforme ai diritti e agli obblighi previsti dal GDPR, o che pregiudichi i diritti o le libertà fondamentali degli interessati.

Articolo 3
Gerarchia

3.1. In caso di contraddizione tra i presenti articoli e le disposizioni di accordi correlati, vigenti tra le parti al momento dell'accettazione deli presenti articoli, o conclusi successivamente, prevalgono i presenti articoli.

SEZIONE II
OBBLIGHI DELLE PARTI

Articolo 4
Descrizione del trattamento

4.1. I dettagli dei trattamenti, in particolare le categorie di dati personali e le finalità del trattamento per le quali i dati personali sono trattati per conto del titolare del trattamento, sono specificati nell'allegato I.

Articolo 5
Obblighi delle parti

5.1. Istruzioni
5.1.1. Il Responsabile tratta i dati personali soltanto su istruzione documentata del Titolare, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il Responsabile. In tal caso, il Responsabile informa il Titolare circa tale obbligo giuridico prima del trattamento, a meno che il diritto lo vieti per rilevanti motivi di interesse pubblico. Il Titolare, oltre a quanto previsto nel Regolamento Privacy, può anche impartire ulteriori istruzioni successive per tutta la durata del trattamento dei dati personali. Tali istruzioni sono sempre documentate.

5.1.2. Il Responsabile informa immediatamente il Titolare qualora, a suo parere, le istruzioni impartite violino il GDPR o le disposizioni applicabili, nazionali o dell'Unione, relative alla protezione dei dati.

5.2. Limitazione delle finalità

5.2.1. Il Responsabile tratta i dati personali soltanto per le finalità specifiche del trattamento di cui all'allegato I, salvo ulteriori istruzioni del titolare del trattamento.

5.3. Durata del trattamento dei dati personali

5.3.1. Il Responsabile tratta i dati personali soltanto per la durata specificata nell'allegato I.

5.4. Sicurezza del trattamento

5.4.1. Il Responsabile mette in atto almeno le misure tecniche e organizzative specificate nell'allegato II per garantire la sicurezza dei dati personali. Ciò include la protezione da ogni violazione di sicurezza che comporti accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati (violazione dei dati personali). Nel valutare l'adeguato livello di sicurezza, le parti tengono debitamente conto dello stato dell'arte, dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi per gli interessati.

5.4.2. Il Responsabile concede l'accesso ai dati personali oggetto di trattamento ai membri del suo personale soltanto nella misura strettamente necessaria per l'attuazione, la gestione e il controllo del contratto. Il Responsabile garantisce che le persone autorizzate al trattamento dei dati personali ricevuti si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza.

5.5. Dati sensibili

5.5.1. Se il trattamento riguarda dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale, dati genetici o dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona, o dati relativi a condanne penali e a reati («dati sensibili»), il Responsabile applica limitazioni specifiche e/o garanzie supplementari.

5.6. Documentazione e rispetto

5.6.1. Le parti devono essere in grado di dimostrare il rispetto deli presenti articoli.

5.6.2. Il Responsabile risponde prontamente e adeguatamente alle richieste di informazioni del Titolare relative al trattamento dei dati conformemente ali presenti articoli.

5.6.3. Il Responsabile mette a disposizione del Titolare tutte le informazioni necessarie a dimostrare il rispetto degli obblighi stabiliti nei presenti articoli e che derivano direttamente dal GDPR. Su richiesta del titolare del Trattamento, il Responsabile consente e contribuisce alle attività di revisione delle attività di trattamento di cui ali presenti articoli, a intervalli ragionevoli o se vi sono indicazioni di inosservanza. Nel decidere in merito a un riesame o a un'attività di revisione, il Titolare può tenere conto delle pertinenti certificazioni in possesso del Responsabile.

5.6.4. Il Titolare può scegliere di condurre l'attività di revisione autonomamente o incaricare un revisore indipendente. Le attività di revisione possono comprendere anche ispezioni nei locali o nelle strutture fisiche del Responsabile e, se del caso, sono effettuate con un preavviso ragionevole.

5.6.5. Su richiesta, le parti mettono a disposizione della o delle autorità di controllo competenti le informazioni di cui al presente articolo, compresi i risultati di eventuali attività di revisione.

5.7. Ricorso a sub-responsabili del trattamento

5.7.1. Fatti salvi gli eventuali sub-responsabili già autorizzati dal Titolare di cui all'allegato III, il Responsabile non può subcontrattare a un sub-responsabile del trattamento i trattamenti da effettuare per conto del Titolare conformemente ai presenti articoli, senza la previa autorizzazione specifica scritta del Titolare. Il Responsabile presenta la richiesta di autorizzazione specifica almeno 20 giorni lavorativi prima di ricorrere al sub-responsabile del trattamento in questione, unitamente alle informazioni necessarie per consentire al Titolare di decidere in merito all'autorizzazione. L'elenco dei sub-responsabili del trattamento autorizzati dal Titolare del trattamento figura nell'allegato III. Le parti tengono aggiornato tale allegato.

5.7.2. Qualora il Responsabile ricorra a un sub-responsabile del trattamento per l'esecuzione di specifiche attività di trattamento, stipula un contratto che impone al sub-responsabile del trattamento, nella sostanza, gli stessi obblighi in materia di protezione dei dati imposti al Responsabile conformemente ai presenti articoli. Il Responsabile si assicura che il sub-responsabile del trattamento rispetti gli obblighi cui il Responsabile è soggetto a norma dei presenti articoli, del Regolamento Privacy e del GDPR.

5.7.3. Su richiesta del Titolare, il Responsabile gli fornisce copia del contratto stipulato con il sub-responsabile del trattamento e di ogni successiva modifica. Nella misura necessaria a proteggere segreti aziendali o altre informazioni riservate, compresi i dati personali, il Responsabile può espungere informazioni dal contratto prima di trasmetterne una copia.

5.7.4. Il Responsabile rimane pienamente responsabile nei confronti del Titolare dell'adempimento degli obblighi del sub-responsabile del trattamento derivanti dal contratto che questi ha stipulato con il Responsabile. Il Responsabile notifica tempestivamente al Titolare qualunque inadempimento, da parte del sub-responsabile del trattamento, degli obblighi contrattuali.

5.7.5. Il Responsabile concorda con il sub-responsabile del trattamento un articolo del terzo beneficiario secondo il quale, qualora il Responsabile sia scomparso di fatto, abbia giuridicamente cessato di esistere o sia divenuto insolvente, il Titolare ha diritto di risolvere il contratto con il sub-responsabile del trattamento e di imporre a quest'ultimo di cancellare o restituire i dati personali.

5.8. Trasferimenti internazionali

5.8.1. Qualunque trasferimento di dati verso un paese terzo o un'organizzazione internazionale da parte del Responsabile è effettuato soltanto su istruzione documentata del Titolare o per adempiere a un requisito specifico a norma del diritto dell'Unione o degli Stati membri cui è soggetto il Responsabile, e nel rispetto del capo V del GDPR.
5.8.2. Il Titolare conviene che, qualora il Responsabile ricorra a un sub-responsabile del trattamento conformemente alla articolo 5.7 per l'esecuzione di specifiche attività di trattamento (per conto del Titolare) e tali attività di trattamento comportino il trasferimento di dati personali ai sensi del capo V del GDPR, il Responsabile e il sub-responsabile del trattamento possono garantire il rispetto del capo V del GDPR utilizzando le clausole contrattuali tipo adottate dalla Commissione conformemente all'articolo 46, paragrafo 2, del GDPR, purché le condizioni per l'uso di tali clausole contrattuali tipo siano soddisfatte.

5.9 Nomina degli Amministratori di Sistema

5.9.1. Qualora nell'ambito dell'erogazione del servizio il Responsabile debba selezionare, nominare, fornire istruzioni e curare l'aggiornamento dei dipendenti propri o dei propri sub-responsabili che assumeranno il ruolo di Amministratore di Sistema di applicativi e/o di sistemi informativi gestiti in esecuzione del Contratto/della Delibera ai sensi del Provvedimento, il Responsabile dichiara di possedere garanzie sufficienti rispetto all'obbligo di selezione nomina, istruzione e aggiornamento degli Amministratori di Sistema ai sensi del richiamato Provvedimento sia per mettere in atto misure tecniche e organizzative adeguate, che per implementare le stesse, in modo tale che il trattamento soddisfi i requisiti del GDPR e garantisca la tutela dei diritti degli interessati.
5.9.2. Il Responsabile si impegna ad individuare tra i propri dipendenti coloro che in concreto saranno preposti allo svolgimento della funzione di amministratore di sistema, verificando il rispetto, in capo a tali soggetti, dei requisiti di cui al Provvedimento e provvedendo alla formazione continua dei medesimi; tali ruoli ed oneri permangono in capo al Responsabile.
5.9.3. Con riferimento agli Amministratori di Sistema il Responsabile si impegna a:
1) designare con atto scritto quali amministratori di sistema dipendenti propri o dei sub-fornitori previa valutazione delle caratteristiche di esperienza, capacità e affidabilità dei soggetti che si intende designare in materia di trattamento, ivi compreso il profilo relativo alla sicurezza e del possesso di ogni altro requisito soggettivo definito nel Provvedimento;
2) predisporre e conservare l'elenco contenente gli estremi identificativi delle persone fisiche qualificate quali amministratori di sistema e le specifiche funzioni ad essi attribuite e a comunicare con cadenza trimestrale l'elenco al Titolare e, comunque, ogni qual volta ne faccia richiesta;
3) curare la formazione di aggiornamento degli amministratori di sistema e dar prova di averla svolta;
4) verificare annualmente l'operato degli amministratori di sistema, anche in ordine al mantenimento dei requisiti soggettivi per ricoprire tale ruolo;
5) prevedere l'uso di sistemi di autenticazione a più fattori per le utenze degli Amministratori di Sistema, imporre che siano modificate ogni tre mesi e le stesse credenziali non possano essere riutilizzate prima di sei mesi;
6) mantenere i file di log in conformità a quanto previsto nel suddetto Provvedimento.

5.10. Obblighi aggiuntivi

5.10.1. Il Responsabile manleva e tiene indenne il Titolare da ogni perdita subita, da ogni contestazione mossagli e da ogni responsabilità addebitatagli in ragione del trattamento effettuato dal Responsabile stesso; è obbligato a rimborsare al Titolare le spese sostenute nonché i costi subiti, anche a titolo di sanzioni amministrative pecuniarie e risarcimento degli interessati, e a risarcirgli tutti i danni (anche reputazionali) derivanti anche da una sola violazione della normativa in materia di trattamento dei dati personali e/o del Regolamento Privacy e/o dell'Accordo (inclusi gli allegati), comunque derivata dalla condotta (attiva e/o omissiva) sua e/o delle persone da lui autorizzate e/o dai sub-Responsabili (ove autorizzati dal Titolare).

Articolo 6

Assistenza al titolare del trattamento

6.1. Il Responsabile notifica prontamente al Titolare qualunque richiesta ricevuta dall'interessato entro e non oltre 2 giorni solari. Non risponde egli stesso alla richiesta, a meno che sia stato autorizzato in tal senso dal Titolare.
6.2. Il Responsabile assiste il Titolare nell'adempimento degli obblighi di rispondere alle richieste degli interessati per l'esercizio dei loro diritti, tenuto conto della natura del trattamento. Nell'adempiere agli obblighi di cui al presente articolo, il Responsabile si attiene al Regolamento Privacy e alle istruzioni del titolare del trattamento.
6.3. Oltre all'obbligo di assistere il Titolare ai sensi del presente articolo, il Responsabile assiste il Titolare anche nel garantire il rispetto dei seguenti obblighi, tenuto conto della natura del trattamento dei dati e delle informazioni a disposizione del Responsabile:

1) l'obbligo di effettuare una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali ai sensi dell'articolo 35 del GDPR qualora un tipo di trattamento possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche;
2) l'obbligo, prima di procedere al trattamento, di consultare la o le autorità di controllo competenti qualora la valutazione d'impatto sulla protezione dei dati indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal Titolare per attenuare il rischio;
3) l'obbligo di garantire che i dati personali siano esatti e aggiornati, informando senza indugio il Titolare qualora il Responsabile venga a conoscenza del fatto che i dati personali che sta trattando sono inesatti o obsoleti;
4) gli obblighi di cui all'articolo 32 del GDPR.
6.4 Le parti stabiliscono nell'allegato II le misure tecniche e organizzative adeguate con cui il Responsabile è tenuto ad assistere il Titolare nell'applicazione del presente articolo, nonché l'ambito di applicazione e la portata dell'assistenza richiesta.

Articolo 7

Notifica di una violazione dei dati personali

7.1. In caso di violazione dei dati personali, il Responsabile coopera con il Titolare e lo assiste nell'adempimento degli obblighi che incombono a quest'ultimo a norma degli articoli 33 e 34 del GDPR, ove applicabile, tenuto conto della natura del trattamento e delle informazioni a disposizione del Responsabile.

7.2. Violazione riguardante dati trattati dal Titolare

7.2.1. In caso di una violazione dei dati personali trattati dal Titolare, il Responsabile assiste il Titolare:
a) nel notificare la violazione dei dati personali alla o alle autorità di controllo competenti, senza ingiustificato ritardo dopo che il titolare del trattamento ne è venuto a conoscenza, se del caso (a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche);
b) nell'ottenere le seguenti informazioni che, in conformità dell'articolo 33, paragrafo 3, del GDPR, devono essere indicate nella notifica del titolare del trattamento e includere almeno:
1) la natura dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
2) le probabili conseguenze della violazione dei dati personali;
3) le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali, se del caso anche per attenuarne i possibili effetti negativi.
7.2.2. Qualora, e nella misura in cui, non sia possibile fornire tutte le informazioni contemporaneamente, la notifica iniziale contiene le informazioni disponibili in quel momento, e le altre informazioni sono fornite successivamente, non appena disponibili, senza ingiustificato ritardo.
c) nell'adempiere, in conformità dell'articolo 34 del GDPR, all'obbligo di comunicare senza ingiustificato ritardo la violazione dei dati personali all'interessato, qualora la violazione dei dati personali sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

7.3. Violazione riguardante dati trattati dal Responsabile

7.3.1. In caso di una violazione dei dati personali trattati dal Responsabile, quest'ultimo ne dà notifica al Titolare senza ingiustificato ritardo e comunque entro e non oltre 24 ore dopo esserne venuto a conoscenza, anche ove questa sia generica e non circostanziata. La notifica contiene almeno:
a) una descrizione della natura della violazione (compresi, ove possibile, le categorie e il numero approssimativo di interessati e di registrazioni dei dati in questione);
b) i recapiti di un punto di contatto presso il quale possono essere ottenute maggiori informazioni sulla violazione dei dati personali;
c) le probabili conseguenze della violazione dei dati personali e le misure adottate o di cui si propone l'adozione per porre rimedio alla violazione, anche per attenuarne i possibili effetti negativi.
7.3.2. Qualora, e nella misura in cui, non sia possibile fornire tutte le informazioni contemporaneamente, la notifica iniziale contiene le informazioni disponibili in quel momento, e le altre informazioni sono fornite successivamente, non appena disponibili, senza ingiustificato ritardo.
7.3.3. Le parti stabiliscono nell'allegato II tutti gli altri elementi che il Responsabile è tenuto a fornire quando assiste il Titolare nell'adempimento degli obblighi che incombono a norma degli articoli 33 e 34 del GDPR.

SEZIONE III
DISPOSIZIONI FINALI

Articolo 8

Inosservanza delle clausole e risoluzione

8.1. Fatte salve le disposizioni del GDPR, qualora il Responsabile violi gli obblighi che gli incombono a norma dei presenti articoli, il Titolare del trattamento può dare istruzione al Responsabile di sospendere il trattamento dei dati

personali fino a quando quest'ultimo non rispetti i presenti articoli o non sia risolto il contratto. Il Responsabile informa prontamente il Titolare qualora, per qualunque motivo, non sia in grado di rispettare i presenti articoli.
8.2. Il Titolare ha diritto di risolvere il contratto per quanto riguarda il trattamento dei dati personali conformemente ali presenti articoli, fatto salvo il diritto al risarcimento, qualora:
1) il trattamento dei dati personali da parte del Responsabile sia stato sospeso dal Titolare in conformità al presente articolo e non sia ripristinato entro un termine ragionevole e in ogni caso entro un mese dalla sospensione;
2) il Responsabile violi in modo sostanziale o persistente i presenti articoli o gli obblighi che gli incombono a norma del GDPR;
3) il Responsabile non rispetti una decisione vincolante di un organo giurisdizionale competente o della o delle autorità di controllo competenti per quanto riguarda i suoi obblighi in conformità deli presenti articoli o del GDPR.
8.3. Il Responsabile ha diritto di risolvere il contratto per quanto riguarda il trattamento dei dati personali a norma dei presenti articoli qualora, dopo aver informato il Titolare che le sue istruzioni violano i requisiti giuridici applicabili in conformità dell'articolo 5.1.2., il Titolare insista sul rispetto delle istruzioni.
8.4. Dopo la risoluzione del contratto il Responsabile cancella tutti i dati personali trattati per conto del titolare del trattamento e certifica a quest'ultimo di averlo fatto, oppure restituisce al titolare del trattamento tutti i dati personali e cancella le copie esistenti, a meno che il diritto dell'Unione o dello Stato membro non richieda la conservazione dei dati personali. Finché i dati non sono cancellati o restituiti, il Responsabile continua ad assicurare il rispetto deli presenti articoli.

Documento sottoscritto digitalmente da

Ragione sociale della Società **Il Legale Rappresentante** **[●]**	**Autorità di Regolazione** **per Energia Reti e Ambiente** **Il Designato al trattamento** **[●]**

ALLEGATO I

Descrizione del trattamento
…
Categorie di interessati i cui dati personali sono trattati
…
Categorie di dati personali trattati
…
NOTA: in caso di trattamento di dati sensibili trattati indicare nell'allegato II le limitazioni o garanzie applicate che tengono pienamente conto della natura dei dati e dei rischi connessi, ad esempio una rigorosa limitazione delle finalità, limitazioni all'accesso (tra cui accesso solo per il personale che ha seguito una formazione specializzata), tenuta di un registro degli accessi ai dati, limitazioni ai trasferimenti successivi o misure di sicurezza supplementari.
…
Natura del trattamento
…
Finalità per le quali i dati personali sono trattati per conto del titolare del trattamento
…
Durata del trattamento
…
…
Specificare i trattamenti svolti da parte dei sub-responsabili del trattamento, specificare anche la materia disciplinata, la natura e la durata del trattamento

---

ALLEGATO II

Misure tecniche e organizzative, comprese misure tecniche e organizzative per garantire la sicurezza dei dati
NOTA ESPLICATIVA:
Le misure tecniche e organizzative devono essere descritte in modo concreto e non genericamente.
Descrizione delle misure di sicurezza tecniche e organizzative messe in atto dal o dai responsabili del trattamento (comprese le eventuali certificazioni pertinenti) per garantire un adeguato livello di sicurezza, tenuto conto della natura, dell'ambito di applicazione, del contesto e della finalità del trattamento, nonché dei rischi per i diritti e le libertà delle persone fisiche. Esempi di possibili misure:
misure di pseudonimizzazione e cifratura dei dati personali

misure per assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento
misure per assicurare la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
procedure per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento
misure di identificazione e autorizzazione dell'utente
misure di protezione dei dati durante la trasmissione
misure di protezione dei dati durante la conservazione
misure per garantire la sicurezza fisica dei luoghi in cui i dati personali sono trattati
misure per garantire la registrazione degli eventi
misure per garantire la configurazione del sistema, compresa la configurazione per impostazione predefinita
misure di informatica interna e di gestione e governance della sicurezza informatica
misure di certificazione/garanzia di processi e prodotti
misure per garantire la minimizzazione dei dati
misure per garantire la qualità dei dati
misure per garantire la conservazione limitata dei dati
misure per garantire la responsabilità
misure per consentire la portabilità dei dati e garantire la cancellazione]

Per i trasferimenti a sub-responsabili del trattamento, descrivere anche le misure tecniche e organizzative specifiche che il sub-responsabile del trattamento deve prendere per essere in grado di fornire assistenza al Titolare.
Descrizione delle misure tecniche e organizzative specifiche che il Responsabile deve prendere per essere in grado di fornire assistenza al Titolare.

ALLEGATO III

Elenco dei sub-responsabili del trattamento

Il Titolare ha autorizzato il ricorso ai seguenti sub-responsabili del trattamento:
1. Nome: …
Indirizzo: …
Nome, qualifica e dati di contatto del referente: …
Descrizione del trattamento (compresa una chiara delimitazione delle responsabilità qualora siano autorizzati più sub-responsabili del trattamento): …
2. …

___