DELIBERAZIONE 19 NOVEMBRE 2024
480/2024/S/COM

IRROGAZIONE DI UNA SANZIONE AMMINISTRATIVA PECUNIARIA PER VIOLAZIONE DI DISPOSIZIONI IN MATERIA DI FUNZIONAMENTO DEL SISTEMA INFORMATIVO INTEGRATO

L'AUTORITÀ DI REGOLAZIONE PER ENERGIA RETI E AMBIENTE

Nella 1317ª riunione del 19 novembre 2024

VISTI:

- la direttiva 2009/73/CE del Parlamento Europeo e del Consiglio del 13 luglio 2009 relativa a norme comuni per il mercato interno del gas naturale (di seguito: direttiva 2009/73/CE);
- la direttiva (UE) 2019/944 del Parlamento europeo e del Consiglio del 5 giugno 2019 (di seguito: direttiva (UE) 2019/944) relativa a norme comuni per il mercato interno dell'energia elettrica e che modifica la direttiva 2012/27/UE;
- la direttiva (UE) 2024/1788 del Parlamento europeo e del Consiglio del 13 giugno 2024;
- la legge 24 novembre 1981, n. 689 (di seguito: legge 689/81);
- l'articolo 2, comma 20, lettera c), della legge 14 novembre 1995, n. 481 e s.m.i. (di seguito: legge 481/95);
- il decreto legislativo 16 marzo 1999, n. 79;
- il decreto legislativo 23 maggio 2000, n. 164;
- il decreto del Presidente della Repubblica 9 maggio 2001, n. 244;
- l'articolo 11 *bis*, del decreto-legge 14 marzo 2005, n. 35 e s.m.i., introdotto dalla legge 14 maggio 2005, n. 80, come modificato dal decreto-legge 9 dicembre 2023, n. 181
- la legge 23 luglio 2009, n. 99;
- il decreto-legge 8 luglio 2010, n. 105 recante "Misure urgenti in materia di energia" convertito con legge 13 agosto 2010, n. 129 (di seguito: decreto-legge 105/10);
- l'articolo 45 del decreto legislativo 1 giugno 2011, n. 93 e s.m.i.;
- la deliberazione dell'Autorità di Regolazione per Energia Reti e Ambiente (di seguito: Autorità) 17 novembre 2010, ARG/com 201/10 (di seguito: deliberazione ARG/com 201/2010), recante le "Direttive per lo Sviluppo del Sistema informativo integrato per la gestione dei rapporti fra i diversi operatori dei mercati liberalizzati" e il relativo Allegato A come successivamente modificato e integrato (di seguito: Allegato A alla deliberazione ARG/com 201/10);

- la deliberazione dell'Autorità 8 marzo 2012, 79/2012/R/com di "Approvazione del regolamento di funzionamento del Sistema Informativo Integrato" (di seguito: deliberazione 79/2012/R/com);
- la deliberazione dell'Autorità 10 novembre 2020, 455/2020/R/com (di seguito: deliberazione 455/2020/R/com), recante "Approvazione del Regolamento di funzionamento del Sistema Informativo Integrato aggiornato";
- l'Allegato A alla deliberazione dell'Autorità 19 dicembre 2023, 598/2023/E/com recante "Modifiche al regolamento per la disciplina dei procedimenti sanzionatori e delle modalità procedurali per la valutazione degli impegni" (di seguito: o Regolamento Sanzioni e Impegni);
- il Regolamento del SII pro tempore vigente (di seguito: Regolamento del SII o anche Regolamento) e i relativi allegati, e in particolare l'allegato C recante "Regole e misure di sicurezza";
- le "Specifiche tecniche del Portale web" del SII del 4 dicembre 2013;
- la determinazione del Direttore della Direzione Sanzioni e Impegni dell'Autorità 17 aprile 2024, DSAI/15/2024/com (di seguito: determinazione DSAI/15/2024/com).

FATTO:

1. Con nota 25 ottobre 2023 (acquisita con prot. Autorità 66961) successivamente integrata con nota 21 marzo 2024 (acquisita con prot. Autorità 21089) Acquirente Unico S.p.A., in qualità di Gestore del Sistema Informativo Integrato (di seguito anche Gestore del SII o AU), ha segnalato all'Autorità la potenziale violazione del Regolamento del SII da parte di alcuni Utenti, tra cui Egogreen S.r.l. (di seguito Egogreen o società), che risultavano avere divulgato le proprie credenziali di accesso al SII a persone fisiche diverse dall'utente finale cui erano intestate in via esclusiva e/o averle utilizzate tramite c.d. BOTNET.
2. Segnatamente, in data 12 settembre 2023 AU disabilitava un'utenza di Egogreen a causa del rilevamento di un'attività sospetta: da diversi indirizzi IP mediante le medesime credenziali assegnate ad un utente finale (persona fisica) – avente congiuntamente il ruolo di Responsabile del SII, Responsabile della Sicurezza, Referente tecnico e operatore – erano stati effettuati oltre 200 (duecento) "*tentativi di consultazione non concessa*" ai dati del SII caratterizzati da automatismi robotici. In data 19 settembre 2023, nel corso dell'interlocuzione con l'Help Desk di AU, il titolare delle credenziali dichiarava che "*attualmente non sono presenti software automatici di interrogazione se non l'utilizzo della PDC integrata con il nostro ERP. Altresì, vi informiamo che purtroppo tramite la medesima user più utenti, dislocati fisicamente in diverse regioni d'Italia, hanno utilizzato i servizi del SIIPortal*".
3. Dagli approfondimenti svolti dal Gestore del SII in esito alle interlocuzioni con Egogreen, veniva altresì rilevato l'utilizzo della predetta UserID, personale e relativa a persona fisica, tramite BOTNET, nonché l'effettuazione di "*richieste sistemiche verso pagine e file non disponibili*", quindi non concessi per ragioni di sicurezza; al contempo, alla data del 22 febbraio 2024, non risultavano ulteriori condotte anomale (nota di AU prot. 21089 del 21 marzo 2024).

4. Pertanto, in esito all'esame della documentazione trasmessa, con determinazione DSAI/15/2024/com l'Autorità ha avviato nei confronti di Egogreen un procedimento sanzionatorio ai sensi dell'articolo 2, comma 20, lettera c), della legge n. 481/95 per l'accertamento della violazione di alcune disposizioni in materia di funzionamento del SII.
5. In particolare, con la determinazione di avvio del presente procedimento è stata contestata alla società la violazione degli articoli 6, comma 1, lettera d) dell'Allegato A alla deliberazione ARG/com 201/10, 6 comma 1 lettera c) e 15, comma 3, del Regolamento del SII, nonché delle sezioni 2.2 e 2.4 dell'allegato C al medesimo Regolamento, dal momento che le credenziali di accesso assegnate dal Gestore del SII ad un utente finale (persona fisica) di Egogreen erano state illegittimamente divulgate e utilizzate da altre persone fisiche nonché tramite BOTNET.
6. Il 28 giugno 2024 la società ha presentato istanza di accesso ai documenti (acquisita con prot. Autorità 45655 e 48006), accolta dal Responsabile del procedimento in data 8 luglio 2024 (prot. Autorità 48508), previa comunicazione ai sensi dell'articolo 3 del d.P.R. 184/2006 e dell'articolo 17 dell'Allegato A alla deliberazione dell'Autorità 412/2021/A ad Acquirente Unico S.p.A. (con prot. Autorità 46335 del 1° luglio 2024) e relativo riscontro (acquisito con prot. Autorità 47159 del 4 luglio 2024).
7. In data 10 luglio 2024, la società ha trasmesso una memoria difensiva (acquisita con prot. Autorità 50032).
8. Nel corso della fase decisoria non sono state prodotte memorie difensive.

VALUTAZIONE GIURIDICA:

9. Il Sistema informativo integrato (di seguito: SII) è stato istituito presso AU con l'articolo 1-bis, primo comma, del decreto-legge 105/10 per sostenere la competitività e la funzionalità delle imprese operanti nei mercati dell'energia elettrica e del gas naturale, ed all'Autorità è stato affidato il compito di emanare i criteri generali per il suo funzionamento. Il SII, basato su una "*banca dati dei punti di prelievo e dei dati identificativi dei clienti finali*", costituisce un'infrastruttura giuridica essenziale poiché è la sede esclusiva, che progressivamente sostituisce tutti i precedenti sistemi informatici, ove i diversi operatori dei mercati energetici interagiscono, secondo la regolazione dell'Autorità, per lo svolgimento delle attività della filiera del settore dell'energia e, in particolare, allo scopo di dare esecuzione ai rapporti contrattuali con i clienti finali. La disciplina che definisce i processi, ossia le prestazioni rese attraverso il SII, nonché quella che stabilisce le modalità di funzionamento del SII stesso e che concerne in particolare le modalità di interazione tra il Gestore del SII e i suoi utenti, sono pertanto fondamentali per garantire uno svolgimento dei servizi regolati continuativo, trasparente e sicuro.
10. In attuazione del predetto articolo 1-bis, l'Autorità con la deliberazione ARG/com 201/10 ha dettato le prime direttive per lo sviluppo del SII e, segnatamente con l'Allegato A alla citata deliberazione, recante "*Criteri generali, modello di funzionamento e modello organizzativo del SII*", ha stabilito che:

- sulla base dei criteri generali ivi indicati, il Gestore del SII, ovvero AU, predispone un Regolamento che disciplini il funzionamento del SII, inclusi i rapporti tra il SII e gli Utenti, le modalità di trattamento dei dati personali e sensibili e i requisiti e le condizioni di accesso al sistema; detto Regolamento deve essere approvato dall'Autorità (articolo 2 commi 6 e 8);
- AU garantisce la sicurezza, la riservatezza delle informazioni e la loro salvaguardia nel tempo e a tal fine si dota di adeguate procedure per garantire che ogni accesso ai dati contenuti nel SII sia tracciabile e sia univocamente riferibile agli Utenti autorizzati (articolo 5 comma 1);
- "*ciascun Utente è autonomo nella gestione dei propri sistemi, nella definizione e nella attuazione delle politiche di sicurezza del proprio sistema informativo, fermo restando l'obbligo di rispettare le disposizioni del regolamento di cui al comma 2.6 e in particolare i requisiti minimi di sicurezza previsti*" (articolo 6 comma 1, lettera d).

11. Conformemente alle predette disposizioni, AU ha predisposto il Regolamento del SII e i relativi allegati, che sono stati approvati dall'Autorità con deliberazione 79/2012/R/com e con deliberazione 455/2020/R/com, e sono pubblicati sul sito internet di AU. Quest'ultimo, poi, in attuazione dell'articolo 14 comma 1 punto 2) del citato Regolamento, ha adottato – tra l'altro – le "Specifiche tecniche del Portale web" del SII ovvero dell'interfaccia standardizzata per l'interazione sicura, certificata e controllata, tra gli utenti finali e l'infrastruttura centrale del SII. Ai sensi dell'articolo 1 del predetto Regolamento:
    - "*Utente*" è il "*soggetto giuridico che partecipa al SII*", come ad esempio le società di vendita e le imprese di distribuzione;
    - - "*Utente finale*" è "*la persona fisica autorizzata dall'Utente ad operare con il SII*";
    - - gli "*Strumenti di Comunicazione Evoluta*" (di seguito anche applicazioni o sistemi) sono le componenti standardizzate, previste nel modello tecnologico del SII, per l'interazione tra il sistema informatico dell'Utente e l'infrastruttura centrale
12. Ai sensi dell'articolo 6 del Regolamento gli Utenti, in quanto operatori che svolgono attività soggette a regolazione, devono – tra gli altri – assicurare "*il rispetto delle misure di sicurezza e dei livelli di servizio secondo quanto indicato (…) nell'allegato C (…) del Regolamento*" (articolo 6, comma 1, lettera c e articolo 15, comma 3), il quale allegato C a sua volta ribadisce che gli Utenti "*sono responsabili (…) del corretto utilizzo del Portale web*" e "*sono direttamente responsabili anche nel caso in cui la gestione dei servizi informatici sia affidata a terzi*" (sezioni 1 e 2.1 dell'allegato C). In particolare, ciascun Utente al momento dell'accreditamento presso il SII (articolo 9 comma 1 del Regolamento del SII e paragrafo 5 delle "Specifiche tecniche del Portale web") deve indicare:
    - il Responsabile del SII, cioè la persona fisica che rappresenta l'Utente nei confronti del SII;

- il Referente tecnico, cioè la persona fisica a cui è assegnato il compito di sovrintendere alla realizzazione ed al funzionamento delle componenti tecniche necessarie alla corretta gestione dei processi;
- il Responsabile della sicurezza, cioè la persona fisica a cui è assegnata la responsabilità relativa alla gestione della sicurezza e che "*Gestisce ed è garante delle credenziali di accesso degli utenti finali e dei certificati necessari all'interazione con il SII*".

13. Inoltre, per ciascun Processo (cioè servizio o prestazione) del SII (come *switching*, voltura, *pre-check*, consultazione puntuale o massiva), il Regolamento del SII e le Specifiche tecniche del Portale web prevedono che: il Responsabile del SII nomina il Referente del Processo, il quale a sua volta nomina e coordina persone fisiche che per conto dell'Utente sono autorizzate a svolgere le attività operative sul SII (operatori di Processo), definendo anche il profilo di abilitazione da associare a ciascuna di esse (articolo 11, comma 3 del Regolamento del SII e paragrafi 5 e 7.2 delle Specifiche tecniche). Tutte le modifiche alle predette informazioni, inclusa la revoca dell'abilitazione alle persone fisiche indicate, devono essere tempestivamente comunicate dall'Utente al Gestore del SII (articolo 11, comma 4 del Regolamento del SII e paragrafi 7.2.1 e 7.2.3 delle Specifiche tecniche). Sulla base dei nominativi comunicati dal Referente del Processo, il Gestore del SII gestisce le autorizzazioni, individuando per ciascuno di essi le modalità di accesso personali corrispondenti al ruolo e al profilo di accesso indicato (quali ad esempio accesso in sola lettura, lettura e scrittura, annullamento) (articolo 11, comma 6 del Regolamento del SII).
14. Ciascun Utente può operare con il SII anche mediante gli strumenti di comunicazione evoluta previsti dal modello tecnologico di cui all'Allegato A al Regolamento (articoli 8, comma 2, e 10 del Regolamento del SII), cioè la Porta di Comunicazione e il servizio di *Cloud Storage* (sezione 3 dell'allegato A), e in questo caso deve effettuare le procedure di qualificazione di cui al successivo articolo 14, finalizzate a verificare, tra l'altro, il rispetto delle misure di sicurezza e dei livelli di servizio di cui al medesimo articolo.
15. Ai sensi del predetto articolo 14 comma 1 del Regolamento del SII, al fine della corretta ed efficace realizzazione del SII e del successivo funzionamento, il Gestore del SII definisce regole tecniche, specifiche tecniche e linee guida che l'Utente ha l'obbligo di rispettare; segnatamente:
    - "*le regole tecniche per l'accreditamento al SII, contenenti almeno le regole e le misure di sicurezza*" di cui all'allegato C al Regolamento del SII (il cui rispetto è richiamato anche dal successivo articolo 15 comma 3) (punto 1);
    - "*le specifiche tecniche e di sicurezza (…) necessarie all'utilizzo del Portale WEB del SII*" (punto 2);
    - "*le specifiche tecniche e di sicurezza (…) necessarie all'utilizzo degli strumenti di comunicazione evoluta, comprese le procedure di qualificazione*" (punto 3).
16. La sezione 2.2 dell'Allegato C prevede, tra gli obiettivi di sicurezza del SII che ogni accesso ai dati contenuti nel SII debba essere tracciabile e univocamente riferibile alle entità autorizzate, siano esse utenti finali (cioè persone fisiche) o strumenti di comunicazione evoluta secondo le definizioni di cui al citato articolo 1 del

Regolamento del SII. Per tale ragione, l'erogazione e la fruizione di un servizio applicativo del SII richiede che siano *preliminarmente* effettuate operazioni di *identificazione* univoca delle entità (basate su UserID per gli utenti finali e su URI, *Uniform Resource Identifier*, per i sistemi) e di *autenticazione* delle medesime mediante meccanismi anch'essi individuali (Password e/o meccanismi di autenticazione forte, cioè il certificato digitale su dispositivo elettronico fisico, ad esempio Smartcard, o virtuale, ad esempio il Token virtuale, ed il PIN, per gli utenti finali e certificati digitali "*emessi dalla Autorità di Certificazione (CA) della Infrastruttura a Chiave Pubblica (PKI) del SII o da un Certificatore accreditato secondo la normativa vigente*" per gli strumenti di comunicazione evoluta) (sezione 2.4 e sezioni 3 e 4 dell'allegato C nonché paragrafo 9 delle Specifiche tecniche). Gli Utenti possono disporre di uno o più account di accesso, (sezione 4 dell'allegato C) ma in ogni caso, "*Le credenziali associate agli utenti finali sono strettamente personali, non possono essere cedute a terzi ed il possessore si assume la responsabilità della loro custodia garantendo la confidenzialità delle stesse*" (sezione 2.4.2 dell'allegato C al Regolamento del SII e paragrafo 9.2.7 delle Specifiche tecniche del Portale web).

ARGOMENTAZIONI DIFENSIVE DI EGOGREEN E RELATIVE VALUTAZIONI

17. Con la memoria del 10 luglio 2024, la società ha fornito chiarimenti in merito all'accaduto rilevato dal Gestore del SII che, come concluso dal Responsabile del procedimento, confermano la fondatezza delle contestazioni e consentono di ritenere accertati gli illeciti in argomento.
18. Egogreen, infatti, ha ammesso sia l'utilizzo di un software e quindi dei meccanismi e automatismi di cui si caratterizza, per svolgere e gestire le attività di propria competenza sul SII, sia l'utilizzo da parte di terzi, ovvero a due collaboratori, delle credenziali strettamente personali rilasciate dal SII all'Amministratore unico della società.
19. Tanto basta per integrare gli illeciti in contestazione, dal momento che le credenziali personali possono essere usate esclusivamente dalla persona fisica a cui sono intestate e non possono essere utilizzate né da parte di altre persone fisiche, risultando al riguardo del tutto indifferente agli scopi di sicurezza perseguiti dalle disposizioni violate che si tratti di soggetti dipendenti o meno dell'azienda, né, tantomeno, mediante software di alcun genere.
20. In merito alla cessione delle credenziali, la società ha dichiarato nella memoria difensiva di aver provveduto a richiedere il rilascio di nuove credenziali individuali intestate a propri collaboratori già in data 19 settembre 2023, dopo le interlocuzioni con AU conseguenti al blocco dell'utenza.
21. In merito, invece, all'utilizzo delle credenziali personali per il tramite del *software*, non vale a giustificare la condotta tenuta la spiegazione fornita dalla società, e a sua volta ricevuta dal produttore del *software* medesimo, ovvero che lo strumento informatico in questione non conterrebbe "*sistemi robotici per l'interrogazione e compilazione automatica*", poiché "*l'unico sistema integrato nel software automatico*

è quello relativo alla Porta Di Comunicazione (PDC)". Difatti, che il software in discussione sia stato ammesso all'interazione con il SII per il tramite della Porta di Comunicazione dimostra, semmai, che la società era edotta del fatto che per interagire con il SII mediante strumenti di comunicazione evoluta (qual è il software automatico in questione) esiste una procedura di autorizzazione ed autenticazione appositamente prevista dal Regolamento del SII, che genera delle credenziali univoche e relative esclusivamente a quello specifico strumento informatico. Pertanto, il *software* così autorizzato e di cui la società intende avvalersi per la gestione delle attività di propria competenza sul SII può essere utilizzato unicamente mediante la Porta di Comunicazione e l'impiego delle specifiche credenziali assegnategli. Le credenziali personali relative ad un Utente finale – delle quali nel presente procedimento si contesta l'illegittimo utilizzo – possono, invece, essere utilizzate esclusivamente dalla persona fisica cui sono intestate, la quale opera nel sistema attraverso un'interfaccia distinta (portale web del SII) e secondo il profilo di abilitazione riconosciuto esclusivamente a quello specifico soggetto al momento del rilascio delle credenziali medesime. Al riguardo, si osserva che gli Utenti del SII, e nel caso di specie Egogreen, sono direttamente responsabili anche nel caso in cui la gestione dei servizi informatici sia affidata a un terzo (sezioni 1 e 2.1 dell'allegato C al Regolamento del SII). La società, inoltre, non ha espressamente dichiarato di aver smesso di utilizzare le credenziali personali, cioè rilasciate a persona fisica, mediante applicativi non autorizzati.

22. In definitiva, le circostanze dedotte dalla società non sono idonee ad escluderne la responsabilità per la violazione degli articoli 6, comma 1, lettera d) dell'Allegato A alla deliberazione ARG/com 201/10, 6 comma 1 lettera c) e 15, comma 3, del Regolamento del SII, nonché delle sezioni 2.2 e 2.4 dell'allegato C al medesimo Regolamento, integrata dalla illegittima divulgazione delle credenziali di accesso assegnate dal Gestore del SII ad un Utente finale (persona fisica) e dalla utilizzazione delle stesse tramite BOTNET.

QUANTIFICAZIONE DELLA SANZIONE:

23. L'articolo 11 della legge 689/81 dispone che la quantificazione della sanzione sia compiuta in applicazione dei seguenti criteri:
    a) gravità della violazione;
    b) opera svolta dall'agente per la eliminazione o attenuazione delle conseguenze della violazione;
    c) personalità dell'agente;
    d) condizioni economiche dell'agente.
24. L'Autorità applica i criteri di cui al sopra citato articolo 11 alla luce di quanto previsto dagli articoli 29 e ss. del Regolamento Sanzioni e Impegni.
25. Sotto il criterio della *gravità della violazione*, la cessione delle credenziali e l'utilizzazione delle stesse tramite BOTNET sono illeciti di pericolo e si pongono in contrasto con le primarie regole di funzionamento del SII, poste a tutela dell'integrità dello stesso ovvero dei dati gestiti da un sistema informativo essenziale per il buon

funzionamento dei mercati energetici, ossia affinché tutti i servizi regolati che confluiscono nel SII siano svolti in modo sicuro. La quantificazione della sanzione tiene conto del fatto che la violazione delle regole di sicurezza anche da parte di un operatore di modeste dimensioni costituisce di per sé un *vulnus* per la sicurezza di un sistema informativo che rappresenta una infrastruttura essenziale per il buon funzionamento dei mercati energetici. Inoltre, ai fini della valutazione della gravità della violazione rilevano le seguenti circostanze: a) che l'esercente abbia *ceduto* a terzi le credenziali assegnate ad un Utente finale, persona fisica, e le abbia altresì *utilizzate* per il tramite di BOTNET, laddove tanto la cessione quanto l'utilizzazione delle credenziali sono da sole idonee ad integrare la violazione delle disposizioni sopra richiamate; b) che l'offensività della condotta risulta comunque contenuta in considerazione della dimensione dell'operatore; c) che le credenziali illegittimamente utilizzate siano quelle del Responsabile della sicurezza, cioè della persona fisica a cui è assegnata la responsabilità relativa alla gestione della sicurezza e che "*Gestisce ed è garante delle credenziali di accesso degli utenti finali e dei certificati necessari all'interazione con il SII*" (cfr. Specifiche tecniche del Portale web). Si dà atto che il Gestore del SII ha rilevato che alla data del 22 febbraio 2024 non risultavano ulteriori condotte anomale, sebbene la società non abbia dato evidenza di aver cessato l'utilizzo mediante *software* delle credenziali personali rilasciate dal SII.

26. Con riferimento al criterio dell'*opera svolta dall'agente per la eliminazione o attenuazione delle conseguenze delle violazioni* e della *personalità*, non risultano circostanze rilevanti.
27. Per quanto attiene alle *condizioni economiche dell'agente*, si rileva che dall'ultimo bilancio depositato, relativo all'anno 2023, i ricavi ammontano a euro 6.583.699.
28. Per tutto quanto sopra, la sanzione è determinata nella misura complessiva di euro 185.000,00 (centottantacinque)

DELIBERA

1. di accertare la violazione, da parte di Egogreen S.r.l., nei termini di cui in motivazione, degli articoli 6, comma 1, lettera d) dell'Allegato A alla deliberazione ARG/com 201/10, 6 comma 1 lettera c) e 15, comma 3, del Regolamento del SII, nonché delle sezioni 2.2 e 2.4 dell'allegato C al medesimo Regolamento recante "Regole e misure di sicurezza";
2. di irrogare, nei confronti di Egogreen S.r.l., ai sensi dell'articolo 2, comma 20, lettera c), della legge 481/95, la sanzione amministrativa pecuniaria nella misura complessiva di euro 185.000,00 (centottantacinquemila/00);
3. di ordinare a Egogreen S.r.l. di pagare le sanzioni irrogate entro il termine di 30 giorni dalla data di comunicazione del presente provvedimento, con versamento diretto al concessionario del servizio di riscossione, oppure mediante delega ad una banca o alla Poste Italiane S.p.A., presentando il modello "F23" (recante codice ente QAE e codice tributo "787T"), come previsto dal decreto legislativo 237/97;

4. di avvisare che, decorso il termine di cui al precedente punto 3, per il periodo di ritardo inferiore ad un semestre, devono essere corrisposti gli interessi di mora nella misura del tasso legale a decorrere dal giorno successivo alla scadenza del termine del pagamento e sino alla data del pagamento (codice tributo "788T"); in caso di ulteriore ritardo nell'adempimento, saranno applicate le maggiorazioni di cui all'articolo 27, comma 6, della legge 689/81 (codice tributo "789T");
5. di ordinare a Egogreen S.r.l. di comunicare l'avvenuto pagamento della sanzione amministrativa irrogata all'Autorità, mediante l'invio di copia del documento attestante il versamento effettuato via mail all'indirizzo protocollo@pec.arera.it entro cinque giorni dalla sua effettuazione;
6. di comunicare il presente provvedimento a Egogreen S.r.l. (P.IVA 11484710964) mediante pec agli indirizzi egogreen@legalmail.it e di pubblicarlo sul sito internet dell'Autorità www.arera.it.

Avverso il presente provvedimento può essere proposto ricorso dinanzi al competente Tribunale Amministrativo Regionale della Lombardia, sede di Milano, entro il termine di 60 giorni dalla data di notifica dello stesso oppure ricorso straordinario al Capo dello Stato, entro il termine di 120 giorni.

19 novembre 2024

IL PRESIDENTE
Stefano Besseghini