DETERMINAZIONE DSAI/16/2024/COM

AVVIO DI PROCEDIMENTO SANZIONATORIO PER VIOLAZIONE DI DISPOSIZIONI IN MATERIA DI FUNZIONAMENTO DEL SISTEMA INFORMATIVO INTEGRATO

IL DIRETTORE DELLA DIREZIONE SANZIONI E IMPEGNI DELL'AUTORITÀ DI REGOLAZIONE PER ENERGIA RETI E AMBIENTE

Il giorno 17 aprile 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 legge 24 novembre 1981, n. 689;
- l'articolo 2, comma 20, lettera c), della legge 14 novembre 1995, n. 481 e s.m.i. (di seguito: legge 481/95);
- la legge 23 luglio 2009, n. 99 (di seguito legge 99/09);
- il decreto legislativo 16 marzo 1999, n. 79;
- il decreto legislativo 23 maggio 2000, n. 164;
- l'articolo 11 *bis*, del decreto-legge 14 marzo 2005, n. 35 e s.m.i., introdotto dalla legge 14 maggio 2005, n. 80;
- il decreto legislativo 1° giugno 2011, n. 93 e s.m.i. (di seguito: decreto legislativo 93/11);
- il decreto del Presidente della Repubblica 9 maggio 2001, n. 244;
- 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);
- la deliberazione dell'Autorità di Regolazione per Energia Reti e Ambiente (di seguito: Autorità) 17 novembre 2010, ARG/com 201/2010 (di seguito: deliberazione 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 201/2010);
- 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);
- il Regolamento del SII 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;
- 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: deliberazione 598/2023/E/com);
- gli Allegati A e B alla deliberazione dell'Autorità 12 maggio 2023, 201/2023/A (di seguito: deliberazione 201/2023/A);
- la deliberazione dell'Autorità 12 maggio 2023, 202/2023/A (di seguito: deliberazione 202/2023/A);
- la deliberazione dell'Autorità 13 giugno 2023, 266/2023/A (di seguito: deliberazione 266/2023/A).

CONSIDERATO CHE:

- la legge 481/95 assegna all'Autorità, tra le altre, la funzione di garantire la promozione della concorrenza e dell'efficienza nel settore energetico;
- la legge 99/09 prevede che l'Autorità si avvalga di Acquirente Unico S.p.A. (di seguito anche AU) per il rafforzamento delle attività di tutela dei consumatori di energia;
- la molteplicità di soggetti dei settori energetici e il crescente numero delle interazioni fra questi a seguito dell'avvio della liberalizzazione dei mercati energetici ha reso necessaria una modifica dell'architettura dei loro rapporti mediante la progettazione e realizzazione di un sistema informatico centralizzato in grado di migliorare le modalità di erogazione dei servizi, a tutela dei consumatori;
- per sostenere la competitività e la funzionalità delle imprese operanti nei mercati dell'energia elettrica e del gas naturale, l'articolo 1-bis, primo comma, del decreto-legge 105/10 ha istituito presso l'Acquirente unico S.p.A. un "*Sistema informatico integrato per la gestione dei flussi informativi*" relativi a detti mercati, basato su una "*banca dati dei punti di prelievo e dei dati identificativi dei clienti finali*" affidando all'Autorità il compito di emanare i criteri generali per il suo funzionamento;

- il secondo comma del citato articolo 1-bis attribuisce all'Autorità la competenza a stabilire le modalità di gestione dei flussi informativi che devono essere realizzati nell'ambito del Sistema informativo integrato (di seguito anche SII), mentre il quarto comma riconosce all'Autorità la competenza a quantificare il corrispettivo dovuto all'Acquirente Unico "*a remunerazione dei costi relativi alle attività svolte*";
- il SII 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 fondamentali per garantire uno svolgimento dei servizi regolati continuativo, trasparente e sicuro;
- in attuazione del predetto articolo 1-bis, l'Autorità con la deliberazione 201/10 ha dettato le prime direttive per lo sviluppo del SII;
- segnatamente, con l'Allegato A alla citata deliberazione, recante "*Criteri generali, modello di funzionamento e modello organizzativo del SII*", ha stabilito che:
  i) sulla base dei criteri generali ivi indicati, il Gestore del SII, ovvero Acquirente Unico S.p.A., 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);
  ii) il Gestore 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);
  iii) "*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);
- conformemente alle predette disposizioni, Acquirente Unico S.p.A. 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 Acquirente Unico S.p.A.; 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", ovvero ad esempio le società di vendita e le imprese di distribuzione, mentre "*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;
- ai sensi del successivo articolo 6, gli Utenti, in quanto operatori che svolgono attività soggette a regolazione, devono osservare quanto indicato nel Regolamento, tra cui "*il rispetto delle misure di sicurezza e dei livelli di servizio secondo quanto indicato (…) nell'allegato C (…) del Regolamento*" (comma 1 lettera 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*";
- 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:
  a. il Responsabile del SII nomina il Referente del Processo, il quale a sua volta nomina e coordina le 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);
  b. 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);
  c. 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);
- ai sensi degli articoli 8, comma 2, e 10 del Regolamento del SII, ciascun Utente per operare con il SII mediante gli strumenti di comunicazione evoluta previsti

dal modello tecnologico di cui all'allegato A è tenuto ad 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; gli strumenti di comunicazione evoluta previsti sono unicamente la Porta di Comunicazione e il servizio di Cloud Storage (sezione 3 dell'allegato A);

- 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 definisce regole tecniche, specifiche tecniche e linee guida che l'Utente ha l'obbligo di rispettare; segnatamente il Gestore definisce:
  i. "*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);
  ii. "*le specifiche tecniche e di sicurezza (…) necessarie all'utilizzo del Portale WEB del SII*" (punto 2);
  iii. "*le specifiche tecniche e di sicurezza (…) necessarie all'utilizzo degli strumenti di comunicazione evoluta, comprese le procedure di qualificazione*" (punto 3);
- ai sensi del citato allegato C:
  i) gli Utenti sono responsabili della corretta gestione degli strumenti di comunicazione evoluta installati all'interno del proprio dominio applicativo e del corretto utilizzo del Portale web; la politica di sicurezza del SII si basa su una chiara separazione delle responsabilità del Gestore del SII e dei singoli Utenti, i quali "*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);
  ii) ogni accesso ai dati contenuti nel SII deve essere tracciabile e univocamente riferibile alle entità *autorizzate*, siano esse utenti finali o strumenti di comunicazione evoluta (sezione 2.2 dell'allegato C);
  iii) 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) che partecipano allo scambio di messaggi, alla erogazione ed alla fruizione dei servizi, e di *autenticazione* delle medesime entità 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, ciascuno con profili di autorizzazione uguali o gerarchicamente inferiori rispetto a quelli associati all'Utente stesso (sezione 4 dell'allegato C), in relazione al numero di POD/PDR

movimentati in ragione dei Processi ai quali sono registrati; i requisiti di *autorizzazione* all'effettuazione delle operazioni riguardano i *singoli* fruitori di ciascun servizio applicativo (utenti finali e sistemi) (sezione 2.4.3 dell'allegato C);

- 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*" come stabilito da Acquirente Unico S.p.A. nella sezione 2.4.2 dell'allegato C al Regolamento del SII (enfasi aggiunta) e ribadito nel paragrafo 9.2.7 delle Specifiche tecniche del Portale web;
- ai sensi dell'articolo 12 comma 2 del Regolamento del SII, "*il Gestore notifica all'Autorità il verificarsi di gravi e reiterate anomalie riscontrate nell'esecuzione dei processi e nel rispetto del Regolamento*";
- il rispetto delle regole relative al SII, fin da quelle che ne disciplinano l'accesso, è essenziale per il buon funzionamento dei mercati energetici; affinché tutti i servizi regolati che confluiscono nel SII siano svolti in modo sicuro e corretto è evidentemente necessario, in primo luogo, che tutte le interazioni con il SII siano riconducibili ad una filiera di agenti identificabili e perciò responsabili;
- ciò è tanto più importante in considerazione del riverbero di quelle attività sul rapporto contrattuale con il cliente finale nell'attuale e delicato contesto di transizione dal mercato tutelato al mercato libero, in cui è ancora più urgente che i vari processi – di *switching*, di voltura, di attivazione/disattivazione della fornitura – gestiti esclusivamente attraverso il SII, siano svolti nel pieno rispetto delle prescrizioni vigenti.

CONSIDERATO, INOLTRE, CHE:

- con nota datata 25 ottobre 2023 (prot. Autorità 66961) e successivamente integrata con nota 21 marzo 2024 (acquisita con prot. Autorità 21089) Acquirente Unico S.p.A. ha segnalato all'Autorità la potenziale violazione del Regolamento del SII da parte di alcuni Utenti, tra cui Olimpia S.r.l. (di seguito Olimpia o società), che risulterebbero avere divulgato le proprie credenziali di accesso al SII a persone fisiche diverse dall'utente finale cui sono intestate in via esclusiva e/o di averle utilizzate tramite c.d. BOTNET;
- segnatamente, in data 17 luglio 2023 il Gestore del SII disabilitava un'utenza di Olimpia a causa del rilevamento di un'attività sospetta: con le credenziali di un'unica utenza, da diversi indirizzi IP, venivano fatti migliaia di tentativi di accesso ai dati del SII, caratterizzati da automatismi robotici indicativi dell'uso di un BOTNET, nonostante il portale fosse in manutenzione;
- successivamente, la società chiedeva lo sblocco della predetta utenza – assegnata all'Amministratore unico di Olimpia – e veniva aperto un ticket dall'*Help Desk* di AU che domandava quale fosse l'IP sorgente utilizzato dall'utenza in questione;
- la società in data 19 luglio chiariva che l'utenza bloccata era "*associata ad un software per la gestione delle pratiche dei Reseller che tramite un BOT dialoga*

sia in upload che download col SII ma è un'utenza che viene anche utilizzata da un ristrettissimo numero di utenti interno all'azienda per interrogazioni e attività spot" e che "*(…) c'è un ulteriore applicativo che accede solo al SII cloud tramite token e non direttamente con la login (…)*";

- in data 21 luglio 2023 l'*Help Desk* di AU comunicava all'Utente che l'evento che aveva condotto al blocco dell'utenza era in contrasto con l'allegato C al Regolamento del SII in quanto "*l'utenza è nominativa, non ad uso applicativo, automatico, continuativo, robotico e permanente*";
- la società successivamente reiterava la richiesta di sblocco evidenziando che la UserID in esame era associata a plurimi ruoli: Responsabile del SII, Responsabile Sicurezza, Referente Tecnico e Referente di processo, nonché l'unica per lo scarico dal *Cloud*;
- con e-mail del 3 agosto 2023 l'*Help Desk* di AU comunicava che tramite Procedura di *Reset* sarebbe stata ripristinata la UserID bloccata, fermo restando che sarebbe stata costantemente monitorata;
- dagli approfondimenti svolti dal Gestore del SII veniva rilevato l'utilizzo della predetta UserID, relativa a persona fisica e strettamente personale, tramite BOTNET (nota AU prot. 21089 del 21 marzo 2024);
- alla data del 22 febbraio 2024 non risultavano ad AU ulteriori condotte anomale (relazione allegata alla nota di AU prot. 21089 del 21 marzo 2024);
- dalla documentazione acquisita e dalle dichiarazioni della società risulta, pertanto, che le credenziali di accesso assegnate dal Gestore del SII ad un utente finale (persona fisica) di Olimpia S.r.l. – dunque strettamente personali e non cedibili ad altra persona fisica (neppure interna all'azienda), né tantomeno utilizzabili tramite strumenti informatici –, sono state illegittimamente divulgate e utilizzate da altre persone fisiche nonché tramite BOTNET, in violazione degli articoli 6, comma 1, lettera d) dell'Allegato A alla deliberazione 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.

RITENUTO CHE:

- gli elementi acquisiti costituiscono presupposto per l'avvio, nei confronti di Olimpia S.r.l., in qualità di Utente del SII, di un procedimento sanzionatorio ai sensi dell'art. 2, comma 20, lettera c) della legge 481/95.

DETERMINA

1. di avviare un procedimento nei confronti di Olimpia S.r.l. per l'accertamento, nei termini di cui in motivazione, della violazione di disposizioni in materia di funzionamento del Sistema Informativo Integrato e per l'adozione del relativo provvedimento sanzionatorio, ai sensi dell'art. 2, comma 20, lett. c), della legge 481/95;

2. di designare, ai sensi dell'articolo 5 dell'Allegato A alla deliberazione 598/2023/E/com e degli articoli 13, comma 3, lettera b) e 16, comma 2, lettera b) dell'Allegato A alla deliberazione 201/2023/A, quale responsabile del procedimento l'avv. Veronica Olmari, nella sua qualità di Responsabile dell'Unità Violazioni della Regolazione nei Mercati Energetici della Direzione Sanzioni e Impegni;
3. di comunicare che, ai sensi dell'articolo 3, comma 2, dell'Allegato A alla deliberazione 598/2023/E/com, il termine di durata dell'istruttoria è di 140 (centoquaranta) giorni, decorrenti dalla comunicazione del presente provvedimento;
4. di comunicare che, ai sensi dell'articolo 3, comma 1, dell'Allegato A alla deliberazione 598/2023/E/com, il termine per l'adozione del provvedimento finale è di 250 (duecentocinquanta) giorni, decorrenti dalla comunicazione del presente provvedimento;
5. di avvisare che le comunicazioni, di cui all'articolo 9 dell'Allegato A alla deliberazione 598/2023/E/com, possono essere inviate tramite posta elettronica certificata (PEC) all'indirizzo protocollo@pec.arera.it all'attenzione del Responsabile del procedimento e di invitare, altresì, i partecipanti al presente procedimento a comunicare, nel primo atto utile, l'eventuale casella di PEC o altro indirizzo (nel solo caso di assenza di indirizzo PEC) presso cui ricevere le comunicazioni relative al procedimento sanzionatorio avviato col presente provvedimento;
6. di avvisare che i soggetti che hanno titolo per partecipare al procedimento, ai sensi dell'articolo 6 dell'Allegato A della deliberazione 598/2023/E/com, possono presentare al Responsabile del procedimento richiesta di accesso agli atti del procedimento, secondo le modalità di cui al precedente punto 5;
7. di comunicare il presente provvedimento a Olimpia S.r.l. (P. IVA 03589630239) mediante PEC all'indirizzo olimpiavr@pec.it e di pubblicarlo sul sito *internet* dell'Autorità www.arera.it.

Milano, 17 aprile 2024

Il Direttore

avv. Michele Passaro

Michele Passaro
Autorità di Regolazione per Energia Reti e Ambiente
17.04.2024 13:21:43 GMT+01:00