altrabolletta.it®
energie a confronto

Risposta al DCO 316/2024/R/com

Cogliamo volentieri l'occasione di questa consultazione per esprimere le nostre visioni sul tema.

Riteniamo imprescindibile mettere i consumatori nelle condizioni di fruire al meglio dei propri dati di consumo e poterli condividere con terze parti, bilanciando le esigenze di fruibilità del dato e di garanzia della riservatezza dello stesso, al fine di poter sfruttare al meglio le opportunità che la tecnologia odierna offre e ancor più offrirà in futuro.

Pur condividendo e apprezzando le intenzioni sottostanti alla proposta dell'Autorità, delineate in maniera più che adeguata in merito al processo di qualifica delle terze parti autorizzate, non riteniamo invece idonee le proposte sulle modalità di condivisione dei dati con le terze parti autorizzate. Il processo delineato nel documento di consultazione risulta inutilmente burocratico e pesante, e non tiene conto degli standard e best practice esistenti e collaudati per esigenze analoghe.

La proposta che emerge dal documento rispecchia una visione burocratica e anacronistica della condivisione delle informazioni, introducendo un processo che seppur innovativo per il settore energetico italiano non ha alcun bisogno di essere progettato o inventato da zero: in situazioni analoghe in tutti i settori lo standard consolidato è quello denominato OAuth 2.0, che riteniamo essere il più adatto anche per lo scopo di condivisione delle informazioni del Portale Consumi sostituendo in toto la proposta delineata nel DCO.

Una volta autorizzata, la terza parte dovrebbe avere la possibilità di registrare, sul Portale consumi o sul Sistema Informativo Integrato, le proprie applicazioni per l'accesso ai dati di consumo dei clienti. La registrazione delle applicazioni potrebbe essere soggetta a limiti quantitativi e/o a verifiche, anche con intervento umano, prima dell'approvazione, purché siano garantite tempistiche certe di evasione e un meccanismo di feedback adeguato per consentire agli sviluppatori di correggere i problemi che non consentono l'approvazione.

L'applicazione registrata e approvata potrebbe quindi essere esposta e integrata nei sistemi della terza parte autorizzata, creando un layer di autenticazione e autorizzazione analogo a quello utilizzato sul Portale consumi per l'accesso tramite SPID o CIE.

In un ipotetico funnel di un servizio che potrebbe richiedere l'accesso ai dati di consumo, il cliente si troverebbe a questo punto l'opzione di consentire l'accesso alla terza parte ai propri dati. Selezionando tale opzione, il cliente verrebbe reindirizzato dall'applicazione precedentemente registrata verso un endpoint del Portale consumi dedicato alla verifica dell'accesso: il cliente effettuerebbe quindi il login sul Portale consumi, prenderebbe visione dei dati richiesti dall'applicazione e fornirebbe o negherebbe il consenso.

In questo modo, una volta prestato il consenso tutto il processo di condivisione dei dati potrebbe avvenire in automatico senza la necessità di ulteriori passaggi né da parte del cliente né della terza parte autorizzata. I dati ovviamente dovrebbero poi essere messi a disposizione in modalità pressoché immediata e non tramite aree di scambio in cui verrebbero depositati con ritardi più o meno elevati creando un'esperienza utente molto più snervante.

Invitiamo quindi l'Autorità e il Gestore del SII ad approfondire le modalità di gestione dello scambio dati tramite protocollo OAuth 2.0 e l'utilizzo di API REST al fine di consentire un'esperienza di sviluppo e di

fruizione del dato il più possibile snella e immediata sia da parte delle terze parti autorizzate che da parte dei consumatori.

Q.1 Si condivide di prevedere fasi successive per la progressiva estensione dei soggetti autorizzabili e iscrivibili all'ETP?

Comprendiamo le esigenze sottostanti all'esigenza e la condividiamo in quanto ridurrebbe il rischio, specie nella fase iniziale dell'avvio del processo, di una "corsa all'iscrizione" con conseguente elevata mole di richieste da valutare da parte del Gestore del SII e conseguenti ritardi nell'evasione.

Si ritiene che tutto il processo di accreditamento debba comunque prevedere tempistiche di evasione certa e modalità e canali di contatto chiari e pubblici per poter gestire l'iter ed evitare inutili rallentamenti o blocchi delle pratiche per ragioni non chiare.

Q.2 Si condividono le tipologie di soggetti individuate per l'ammissione all'ETP nella Fase 2? Motivare eventuali proposte di integrazione dei soggetti precisando se sia possibile fare riferimento a un'identificazione pregressa presso enti terzi, albi o simili.

Sì.

Q.3 Si ritiene opportuno identificare come ammissibili all'ETP altre tipologie di soggetti, oltre a quelle già delineate per la Fase 3? Illustrare le motivazioni per ciascuna categoria ulteriore

Si ritiene opportuno prevedere che a regime, anche in una eventuale fase 4, non ci sia alcun restringimento del perimetro di soggetti ammissibili, purché garantiscano opportuni requisiti minimi di affidabilità e sicurezza.

Prevedere a priori un insieme ristretto di soggetti ammissibili, in un mondo in rapida evoluzione come quello odierno, non porrebbe al riparo da comportamenti non conformi che non possono essere certo bloccati da meri controlli burocratici ex ante, ma avrebbe certamente l'effetto di frenare la possibile innovazione del settore non tenendo in considerazione possibili soggetti emergenti che sarebbero tagliati fuori dall'accesso ai dati.

La predisposizione di una procedura di ammissione robusta, che debba essere periodicamente rinnovata e che preveda opportuni controlli e verifiche consentirebbe di raggiungere in maniera molto migliore gli obiettivi di tutela della privacy proposti senza tarpare le ali all'innovazione.

Q.4 Si ritengono opportune ulteriori considerazioni in merito alla fase di definizione dell'ammissibilità delle diverse tipologie di soggetti all'ETP? Se sì, specificare

Si ritiene che la procedura di ammissione dovrebbe prevedere, per tutti i soggetti e in tutte le fasi, oltre alla verifica documentale il superamento di idonei test tecnici per verificare la robustezza dei processi. Tali test dovrebbero essere noti ex ante e prevedere opportune piattaforme di simulazione per poter valutare e adeguare i sistemi ai requisiti, e dovrebbero essere ripetuti periodicamente, almeno una volta ogni biennio, per poter mantenere l'accreditamento.

Inoltre, sia in fase di iscrizione che in fase di revisione periodica la terza parte autorizzata dovrebbe fornire gli esiti positivi di security test conformi agli standard OWASP effettuate da società specializzate dotate di idonea professionalità.

Q.5 Si ritiene siano stati identificati in modo corretto i dati messi a disposizione delle parti terze? Motivare la risposta.

Le informazioni fornite nella consultazione sono troppo vaghe per fornire un parere sulla proposta. Si ritiene che i dati debbano includere anche tutti gli elementi tecnici necessari alla loro corretta interpretazione, come i coefficienti K di trasformazione delle letture, e che eventuali dati di consumo siano già messi a disposizione convertiti nell'idonea unità di misura, senza necessità di ulteriori trasformazioni come, ad esempio, la moltiplicazione per i coefficienti K come avviene ora per alcuni flussi di misura elettrici sul SII.

Non si condivide affatto, come già discusso in premessa, che la messa a disposizione dei dati avvenga tramite un ambiente da cui i dati vengano scaricati. I dati dovrebbero essere forniti immediatamente a valle della richiesta tramite un endpoint API REST in formato JSON, o in alternativa tramite API SOAP in formato XML, senza prevederne lo stoccaggio in alcun "SII Cloud" dedicato.

Q.6 Si condivide l'orientamento secondo cui i dati di misura messi a disposizione prevedano diverse profondità temporali e, nel caso di finalità dell'erogazione dei servizi energetici, l'approccio dinamico che consente di mettere a disposizione anche i dati di misura relativi a un periodo successivo all'autorizzazione? In caso di approccio dinamico, quale dovrebbe essere la durata prestabilita del periodo di messa a disposizione successiva alla data del consenso espresso dal cliente? Motivare le risposte.

Si condividono le due tipologie di approccio di fornitura dei dati richiesti.

Nel caso di approccio dinamico, al fine di consentire la miglior fruibilità per l'utente, la durata del consenso dovrebbe essere indeterminata, facilitando l'esercizio della revoca da parte del cliente tramite l'invio periodico, ad esempio ogni 6 o 12 mesi dall'autorizzazione, di un promemoria delle autorizzazioni fornite che consenta l'esercizio immediato o quasi della revoca, ad esempio con la presenza di un link dedicato per la revoca di una singola parte precedentemente autorizzata.

Qualora si ritenga preferibile una durata determinata da rinnovare, allora è indispensabile lo sviluppo di un approccio il più possibile automatizzato come proposto in premessa al fine di facilitare le terze parti autorizzate alla raccolta del rinnovo dei consensi. In questo caso, si ritiene congrua una durata di 12 mesi.

Durante il periodo di validità del consenso, nessun dato dovrebbe essere automaticamente messo a disposizione delle parti autorizzate, ma dovrebbero essere queste a richiederlo per i clienti di loro interesse. Anche per questo motivo si ritiene preferibile prevedere la messa a disposizione del dato tramite API REST, prevedendo opportuni vincoli sulla frequenza delle richieste congruentemente allo scopo del loro utilizzo.

Q.7 Quale tra le due procedure di autorizzazione della delega si ritiene più opportuna ed efficiente? Motivare le risposte. Si individuano possibilità alternative?

Entrambe le procedure sono inutilmente complicate, burocratizzate, inefficienti e scarsamente automatizzabili e se dovessero essere implementate limiterebbero fortemente le potenzialità della condivisione dei dati di consumo, per cui si invita a ripensarle completamente prevedendo una procedura che implementi lo standard OAuth 2.0.

Q.8 Ci sono ulteriori aspetti relativi alla revoca da considerare? Motivare la risposta.

Non ci sono ulteriori considerazioni in merito oltre a quanto già esposto in risposta al precedente quesito 6.