agid.AOO-AgID.REGISTRO UFFICIALE(U).0018595.03-12-2018

AGID
Agenzia per l'Italia Digitale
Direttore Generale

Spett.le ANORC
Associazione Nazionale per Operatori e
Responsabili Della Conservazione Digitale
anorc@pec.it

Spett.le AIFAG
Associazione Italiana Firma elettronica
Avanzata Biometrica e Grafometrica
aifag@sicuramail.it

Oggetto: richiesta di valutazione e parere sull'onere di comunicazione di eventuali incidenti di sicurezza che possano occorrere ai sistemi che realizzano servizi fiduciari ai sensi dell'art. 32-bis, comma 2, del Codice dell'Amministrazione Digitale (così come modificato dal D.Lgs 217/2017).

In riscontro alla vostra nota congiunta del 12 ottobre u.s., di pari oggetto, acquisita agli atti dell'Agenzia per l'Italia digitale con prot. 15930 in pari data, tramite la quale sono stati rappresentati alcuni quesiti inerenti il tema di cui in oggetto, si richiamano, nell'allegato alla presente nota, i singoli aspetti significativi sottoposti all'attenzione (riportati *in* corsivo),e si forniscono le relative osservazioni e valutazioni(riportate in grassetto) formulate dalla scrivente Agenzia.

Cordiamente

Teresa Alvaro

TERESA ALVARO
Firmato digitalmente da TERESA ALVARO
Data: 2018.11.30 18:44:09 +01'00'

Allegato

N.1

Q *Con le modifiche introdotte al Codice dell'Amministrazione Digitale (Decreto Legislativo n. 82/2005) con l'approvazione del Decreto Legislativo n. 217/2017, il Legislatore ha voluto dare concretezza a quanto previsto dall'art. 19 del regolamento eIDAS, intervenendo sugli artt. 32 e 32-bis del CAD e ridefinendo un onere di comunicazione di eventuali incidenti di sicurezza che possano occorrere ai sistemi che realizzano servizi fiduciari. La specifica previsione del Regolamento in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno impone, infatti, l'adozione di misure per prevenire e minimizzare l'impatto degli incidenti di sicurezza e informare le parti interessate degli effetti negativi di eventuali incidenti*[1]*.*

R. Ai sensi dell'art. 29 comma 1 del CAD è demandata a Linee Guida la nuova disciplina per i soggetti che intendono svolgere l'attività di conservatore di documenti informatici accreditati. Tale disciplina terrà conto delle previsioni sopra richiamate in materia di segnalazione incidenti di sicurezza, nonché dell'ulteriore previsione indicata allo stesso art. 29, comma 2, che estende ai conservatori le condizioni previste dall'articolo 24 (Requisiti per i prestatori di servizi fiduciari qualificati) del Regolamento eIDAS .

In attesa che si completi l'iter di emanazione delle Linee Guida, in virtù delle disposizioni transitorie (art. 65 del D.Lgs. 13/12/2017, n. 217 che ha introdotto Disposizioni transitorie in relazione al CAD.) rimangono in vigore le regole preesistenti che, nel caso dei conservatori, consistono nel DPCM 3 dicembre 2013, nella Circolare AgID n. 65/2014 emessa ai sensi dell'art. 13 di tale DPCM e nei documenti richiamati nella circolare stessa, in cui sono indicati i requisiti per i soggetti che operino come conservatori accreditati. In virtù di tali regole, la segnalazione e la gestione di incidenti di sicurezza e di eventi significativamente impattanti la regolarità del servizio deve essere effettuata secondo specifiche procedure, come previsto dai requisiti 20 e 21 del documento "Requisiti di qualità e sicurezza per l'accreditamento e la vigilanza". È richiesto, in particolare, che siano definite "… specifiche procedure per la gestione, mantenimento e segnalazione degli incidenti di sicurezza e delle azioni conseguenti, del relativo livello di priorità al quale associare l'intervento, degli strumenti utilizzati, ecc… ", che siano " …descritte le modalità attraverso le quali sono riportati tali eventi, …" , nonché che " …esiste ed è attuato il processo formalizzato per assicurare che gli eventi significativamente impattanti la normale e regolare erogazione del servizio sono segnalati, …".

---

[1] *Il comma 2 del citato art. 19 prevede che senza indugio, ma in ogni caso entro 24 ore dall'esserne venuti a conoscenza, i prestatori di servizi fiduciari qualificati e non qualificati debbano notificare all'organismo di vigilanza (in Italia questo ruolo è stato affidato ad AgID) e, ove applicabile, ad altri organismi interessati, quali l'ente nazionale competente per la sicurezza delle informazioni o l'autorità di protezione dei dati, tutte le violazioni della sicurezza o le perdite di integrità che abbiano un impatto significativo sui servizi fiduciari prestati o sui dati personali ivi custoditi. L'obbligo di notifica viene esteso anche alle persone fisiche o giuridiche che possano aver subito effetti negativi dalla violazione di sicurezza.*

N.2

Q *In particolare l'art. 32-bis, comma 2, (così come modificato dal D.Lgs. n. 217/2017) prevede che: "Fatti salvi i casi di forza maggiore o di caso fortuito, qualora si verifichi un malfunzionamento nei servizi forniti dai soggetti di cui al comma 1 che determini l'interruzione del servizio, ovvero in caso di mancata o intempestiva comunicazione dello stesso disservizio a AgID o agli utenti, ai sensi dell'articolo 32, comma 3, lettera m-bis), AgID, ferma restando l'irrogazione delle sanzioni amministrative, diffida altresì i soggetti di cui al comma 1 a ripristinare la regolarità del servizio o ad effettuare le comunicazioni previste".*

L'effetto è quello di imporre anche ai gestori del Servizio Pubblico d'Identità Digitale, di Posta Elettronica Certificata e ai Conservatori Accreditati il dovere, già previsto dal richiamato art. 32, comma 3 lett. m-bis, per i fornitori di servizi di firma elettronica qualificata, di "garantire il corretto funzionamento e la continuità del sistema e comunicare immediatamente a AgID e agli utenti eventuali malfunzionamenti che determinano disservizio, sospensione o interruzione del servizio stesso".

R. Per effetto di tali disposizioni intervenute, i soggetti già accreditati devono aver adeguato le procedure in uso per prevedere la segnalazione "tempestiva":

- **ad AgID o agli utenti nel caso di malfunzionamenti che determinino interruzioni di servizio**
- **solamente ad agID nel caso di incidenti di sicurezza.**

Più conservatori accreditati, infatti, sin dall'entrata in vigore delle suddette disposizioni stanno provvedendo ad inviare le segnalazioni di incidenti e disservizi coerentemente con le procedure ed i sistemi in uso.

La "tempestività", quando non sono definiti specifici valori limiti, sta ad indicare che la comunicazione deve pervenire "in tempo utile", per consentire ad AgID o all'utente di adottare le contromisure o le azioni possibili per limitare l'impatto sui servizi, evitare o contenere potenziali danni all'utente stesso o ai terzi. Il conservatore, pertanto, a quadro normativo e regolamentare attuale è tenuto a definire e ad adottare un sistema di classificazione degli incidenti di sicurezza e dei disservizi in ragione di ciò che conserva o dei contratti in essere con i propri clienti.

N.3

Q *Tale dovere si affianca a quello principale di garantire la continua e regolare erogazione dei servizi di conservazione e viene prevista, in caso di malfunzionamento o mancata o intempestiva comunicazione, oltre ad una sanzione amministrativa (che a seguito delle ultime modifiche è stata decuplicata rispetto alla precedente versione del CAD) anche una diffida da parte di AgID a regolarizzare il servizio o ad effettuare le dovute comunicazioni. Inoltre, qualora un'interruzione del servizio o la mancata o intempestiva comunicazione sia reiterata nel corso di un biennio, AgID è tenuta ad applicare l'ulteriore sanzione della cancellazione del conservatore dall'elenco pubblico dei conservatori accreditati.*

Ai fini della corretta irrogazione delle sanzioni citate, AgID ha adottato, lo scorso 5 giugno, un "Regolamento relativo alla Vigilanza sui soggetti iscritti negli elenchi pubblici ai sensi dell'art. 14-bis, comma 2, lettera i) del Codice dell'amministrazione digitale" recante le "modalità per la vigilanza e per l'esercizio del potere sanzionatorio ai sensi dell'art. 32-bis del decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni". Tale Regolamento, unitamente ad un precedente "Regolamento riportante le modalità di esecuzione delle verifiche sui soggetti qualificati e accreditati", adottato nel maggio del 2017, stabilisce le modalità di esercizio dei poteri di vigilanza - e il correlato potere sanzionatorio dell'Agenzia per l'Italia Digitale - sui fornitori di servizi fiduciari, sui gestori PEC e SPID e sui conservatori accreditati.

R. Si fa qui riferimento ad un documento superato (quello adottato nel maggio 2017). Con la pubblicazione del "Regolamento recante le modalità per la vigilanza e per l'esercizio del potere sanzionatorio ai sensi dell'art.32-bis del d.lgs. 7 marzo 2005, n.82 e successive modificazioni" (Avviso su GU 141 del 20/06/2018) è stato aggiornato anche il documento che descrive le modalità per l'esecuzione delle verifiche sui soggetti qualificati e accreditati, che costituisce un allegato allo stesso Regolamento. Determina di adozione, Regolamento e allegato sono pubblicati sia sul sito, che nella Sezione trasparenza ed è stato dato avviso sulla GU.

N.4

***Q** Il Regolamento AgID del 5 giugno 2018, si limita a ribadire, al suo paragrafo 13, che nei casi di interruzioni di servizio o mancata o intempestiva comunicazione di disservizio, previsti all'articolo 32- bis, comma 2, del CAD, l'Agenzia nella persona del Responsabile del procedimento, con apposito atto da notificarsi tramite PEC, diffida il gestore a ripristinare la regolarità del servizio o ad effettuare le comunicazioni previste.*

Se da un lato, quindi, non vi sono indicazioni sufficientemente chiare in merito alla corretta gestione delle comunicazioni relative agli incidenti, dall'altro, come abbiamo visto, ci sono chiare e precise sanzioni che vanno da 40000 a 400000 euro e che possono essere accompagnate dall'ulteriore sanzione della cancellazione dall'elenco dei conservatori accreditati.

In considerazione dei possibili effetti di tale situazione, riteniamo che, in ottica collaborativa e al fine di garantire la piena e corretta esecuzione degli obblighi derivanti dalla normativa citata, sia necessario prevedere un'indicazione più precisa dei casi nei quali effettuare le dovute comunicazioni all'Agenzia per l'Italia Digitale e agli utenti coinvolti,

R. Come già detto, le indicazioni di dettaglio sono oggetto di Linee guida. Nel transitorio le comunicazioni devono essere effettuate secondo le procedure definite in base ai requisiti indicati nel documento "Requisiti di qualità e sicurezza per l'accreditamento e la vigilanza" già richiamato in precedenza, prevedendo la segnalazione ad AgID o agli utenti quando ricorrono le condizioni che il conservatore stesso ha definito nelle procedure, in ragione di ciò che conserva e dell'impatto che eventuali incidenti o malfunzionamenti possono avere sugli utenti.

Al riguardo, poiché ai conservatori sono estese dal CAD (art. 29, comma 2) le condizioni dell'art. 24 del Regolamento eIDAS, già in occasione delle verifiche ispettive svolte sino ad oggi si è raccomandato, attraverso formulazione nei rapporti di verifica di apposita osservazione, di prendere a riferimento quanto previsto per i prestatori di servizi fiduciari qualificati, per i quali sono state adottate le indicazioni da Linee Guida ENISA (https://www.enisa.europa.eu/publications/article19-incident-reporting-framework), prevedendo uno schema di classificazione degli incidenti e dei malfunzionamenti secondo 5 livelli di severity:

1. Nessun impatto;

2. Impatto non significativo: le risorse del provider sono state interessate ma non hanno avuto alcun impatto sui servizi di base;

3. Impatto significativo: parte dei clienti o dei servizi è stata interessata;

4. Impatto grave: gran parte dei clienti / servizi è interessato;

5. Disastroso: l'intera organizzazione, tutti i servizi sono interessati

e prevedendo quindi la notifica entro 24 ore degli eventi di severity 3, 4, 5 ad AgID e agli utenti interessati.

In tal modo, se un evento è classificabile secondo i livelli 1 e 2, nessuna comunicazione è dovuta ad AgID o agli utenti, fermi restando gli obblighi di registrazione e gestione di tutti gli eventi (incidenti e malfunzionamenti) a carico dei conservatori. In altri termini, è il conservatore che stabilisce cosa e in che tempi comunicare ad AgID o agli utenti, attribuendo un livello di severity piuttosto che un altro secondo quanto codificato nelle procedure sulla base delle valutazioni di impatto. Tutti questi aspetti, la coerenza degli eventi registrati e segnalati con le procedure definite sono oggetto di verifica nel corso delle ispezioni svolte da AgID in ambito vigilanza e dagli organismi di certificazione ai fini del rilascio delle relazioni di conformità biennali.

N.5

Q *[Si chiede] un'indicazione dell'indirizzo presso l'Agenzia al quale recapitare le comunicazioni*

R. Come da indicazioni nel Regolamento sopra richiamato, tutte le comunicazioni sono da effettuare a mezzo PEC, all'unico indirizzo rilevabile dal sito web protocollo@pec.agid.gov.it , usato per tutte le comunicazioni da/verso i conservatori accreditati.

N.6

Q *E [si chiede altresì] un modulo per effettuare tali comunicazioni*:

R. Non essendo prevista dal quadro regolatorio attuale una modalità standard di classificazione e notifica ad AgID di incidenti e malfunzionamenti, non è stato richiesto l'utilizzo di un modulo standard, potendo le modalità variare da conservatore a conservatore. Ad ogni modo, prendendo spunto dalle sollecitazioni di codeste associazioni, si provvederà a rendere disponibile sul sito un

modulo che ripropone le modalità di segnalazione previste per i prestatori di servizi fiduciari qualificati, , il cui utilizzo presuppone comunque che il conservatore adegui le procedure in uso.

N.7

Q *indicazioni che dovranno tenere ben presente il contesto nel quale gli obblighi e le sanzioni viste vanno ad operare.*

Mentre, infatti, l'obbligo di comunicazione tempestiva è facilmente comprensibile in relazione a servizi "critici" come quelli relativi alle firme qualificate e alle marche temporali, alla PEC o allo SPID, la cui interruzione anche di poche ore può comportare disservizi e danni anche gravi agli utenti, non risulta giustificata la sua rigida applicazione ai servizi di conservazione che, in caso di lievi interruzioni comunque al di sotto delle 24 ore[2], difficilmente possono causare danni apprezzabili agli utenti.

R. La criticità per i servizi erogati dai conservatori dipende dagli oggetti che si conservano e dalle obbligazioni che sono state assunte nei rapporti contrattuali con i clienti (pubbliche amministrazioni e privati). Sulla base di tali aspetti è definito dal conservatore il sistema di classificazione e, per esempio con riferimento ai 5 livelli sopra indicati, sono attribuite le severity 1 o 2 agli eventi che non hanno nessun impatto e che non occorre segnalare ad AgID o agli utenti. Eventi che, invece, possono causare danni agli utenti, ancorché non apprezzabili, devono essere classificati almeno a livello 3 e segnalati ad AgID e all'utente nelle 24 ore, affinché questi soggetti siano messi in grado di definire e mettere in atto le contromisure necessarie o le azioni che riterranno più opportune.

N.8

Q *Infine, andrebbe tenuto presente che uno specifico ulteriore obbligo di comunicazione di eventuali incidenti che possano compromettere l'integrità, l'accessibilità e la riservatezza dei dati personali trattati dai sistemi di conservazione (cd. "data breach") è già previsto e regolato dal Regolamento europeo n. 679/2016 e da successive indicazioni del Garante italiano.*

R. Si tratta di obblighi *ex lege*: anche il Regolamento eIDAS, art. 19, comma 2, come evidenziato nella Nota 1 riportata da codeste Associazioni, prevede obblighi di notifica dei cd. data breach ad AgID ed al Garante, sebbene ciò sia previsto e regolato dal Regolamento europeo n. 679/2016.

N.9

Q *Tenuto conto dell'attuale panorama normativo e regolamentare, si chiede all'Agenzia per l'Italia Digitale di indicare quali siano le modalità e le tempistiche con le quali i conservatori accreditati possano correttamente adempiere all'onere di comunicazione di cui all'art. 32-bis, comma 2, del*

---

[2] *Si fa riferimento a disservizi e/o interruzioni del servizio che non abbiano comportato una perdita di dati e/o informazioni conservate.*

CAD tenendo conto anche della minore "criticità" dei servizi di conservazione rispetto all'erogazione dei servizi fiduciari qualificati contemplati dal Regolamento eIDAS.

R. Si è già risposto sopra. Tenuto conto dell'attuale panorama normativo e regolamentare, la comunicazione e la gestione delle interruzioni di servizio e degli incidenti va effettuata secondo procedura, adottando un sistema di classificazione che preveda la segnalazione tempestiva ad AgID e agli utenti di eventi valutati critici in ragione della tipologia degli oggetti che si conservano e dei contratti in essere. La procedura, ai sensi del requisito 20, evidenzierà come sono attribuiti i livelli di priorità ed a quali livelli corrisponde la notifica ad AgID ed agli utenti ai sensi del sopravvenuto art. 32-bis del CAD, nonché entro quali tempi la comunicazione è inviata per poter risultare "tempestiva", Come da raccomandazioni fornite ai conservatori sin qui visitati, si possono prendere a riferimento, adeguando le procedure in uso, le modalità definite per i prestatori di servizi fiduciari qualificati e sopra richiamate. Ciò consente anche, agli operatori che sono qualificati o accreditati per più ambiti, di uniformare le modalità di gestione e segnalazione di tali eventi.

N.10

Q *Si chiede, inoltre, se nelle more dell'individuazione di tali specifiche modalità di comunicazione, l'onere di comunicazione in capo al conservatore accreditato, in caso di incidenti di sicurezza, possa ritenersi assolto con la creazione e conservazione di uno specifico rapporto d'intervento che contenga:*

- *la descrizione dell'evento,*
- *la data di occorrenza,*
- *la data di segnalazione interna,*
- *l'indicazione delle azioni eseguite,*
- *l'indicazione degli elementi che hanno consentito di considerare l'evento risolto,*
- *la data di chiusura della segnalazione così come previsto dal punto 20 della Lista di riscontro AgID per la valutazione di conformità dei sistemi di conservazione.*

R. Per incidenti o malfunzionamenti che, in ragione delle valutazioni di impatto, sono classificabili nel sistema adottato dal conservatore secondo livelli equiparabili ai livelli 3, 4 e 5 sopra indicati, non basta solo la creazione e la conservazione, ma occorre anche la comunicazione ad AgID e agli utenti entro i tempi definiti nella procedura dallo stesso conservatore. Per eventi (incidenti o malfunzionamenti che comportino interruzioni) classificabili secondo i livelli 1 e 2 dell'esempio, ovvero che non abbiano impatto o risultino di impatto poco significativo, è sufficiente la sola gestione dell'evento e la relativa registrazione.

AGID | via Liszt, 21 – 00144 Roma | protocollo@pec.agid.gov.it | www.agid.gov.it | tel. 06 85264.1