Lecce, 12 ottobre 2018

Spett.le
Agenzia per l'Italia Digitale
Via Liszt, 21
00144 Roma

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).**

Spett.le Agenzia,

la Coalizione dei conservatori accreditati, nata da un progetto interassociativo delle associazioni ANORC e AIFAG, che rappresenta 44 delle 73 imprese attualmente accreditate, ritiene necessario richiedere un parere al fine di chiarire il perimetro e le modalità di realizzazione dell'onere di comunicazione di eventuali incidenti di sicurezza che possano occorrere ai sistemi che realizzano servizi di conservazione ai sensi dell'art. 32-bis, comma 2, del Codice dell'Amministrazione Digitale (così come modificato dal Decreto Legislativo n.217/2017). Tale intervento risulterebbe un fondamentale chiarimento tutti gli enti e le imprese che hanno ottenuto l'accreditamento da parte di AgID per la conservazione dei documenti informatici.

PREMESSA

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].

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*".

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,*

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.

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.

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, un'indicazione dell'indirizzo presso l'Agenzia al quale recapitare le comunicazioni e un modulo per effettuare tali comunicazioni: 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.

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.

QUESITO

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

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

correttamente adempiere all'onere di comunicazione di cui all'art. 32-*bis*, comma 2, del CAD tenendo conto anche della minore "criticità" dei servizi di conservazione rispetto all'erogazione dei servizi fiduciari qualificati contemplati dal Regolamento eIDAS.

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.

Cordiali saluti

Il Direttore Generale

(dott. Alessandro Selam)