Sintesi del parere del Garante europeo della protezione dei dati sulla proposta della Commissione di regolamento del Parlamento europeo e del Consiglio relativa alla fiducia e alla sicurezza nelle transazioni elettroniche nel mercato interno (regolamento sui servizi fiduciari elettronici)

(Il testo completo del presente parere è reperibile in EN, FR e DE sul sito web del GEPD http://www.edps.europa.eu)

(2013/C 28/04)

I. Introduzione

I.1. *La proposta*

1. Il 4 giugno 2012 la Commissione ha adottato una proposta di regolamento del Parlamento europeo e del Consiglio che modifica la direttiva 1999/93/CE del Parlamento europeo e del Consiglio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno («la proposta») ([1]).

2. La proposta si inserisce nel quadro delle misure presentate dalla Commissione per rafforzare la diffusione delle transazioni elettroniche nell'Unione europea. Fa seguito alle azioni previste nell'Agenda digitale europea ([2]) relative al miglioramento della normativa sulla firma elettronica (Azione fondamentale 3) e volte a fornire un quadro coerente per il riconoscimento reciproco dell'identificazione e dell'autenticazione elettronica (Azione fondamentale 16).

3. La proposta è destinata a migliorare la fiducia nelle transazioni elettroniche paneuropee e garantire il riconoscimento legale transfrontaliero dell'identificazione elettronica, dell'autenticazione elettronica, delle firme elettroniche e dei servizi fiduciari connessi, nonché un livello elevato di protezione dei dati e di responsabilizzazione degli utilizzatori nel mercato interno.

4. Un livello elevato di protezione dei dati è essenziale per l'utilizzo dei regimi di identificazione elettronica e dei servizi fiduciari. Lo sviluppo e l'uso di tali mezzi elettronici deve fare affidamento sul trattamento adeguato dei dati personali da parte dei prestatori di servizi fiduciari e dei soggetti che rilasciano le identità elettroniche. Ciò è tanto più importante in quanto si farà affidamento su tale trattamento, tra l'altro, per identificare e autenticare persone fisiche (o giuridiche) nel modo più affidabile.

I.2. *Consultazione del GEPD*

5. Prima dell'adozione della proposta, è stata data al GEPD la possibilità di formulare osservazioni informali. Molte di queste osservazioni sono state prese in considerazione nella proposta, rafforzando di conseguenza le garanzie di protezione dei dati.

6. Il GEPD si compiace di essere stato altresì consultato formalmente dalla Commissione ai sensi dell'articolo 28, paragrafo 2, del regolamento (CE) n. 45/2001.

I.3. *Contesto della proposta*

7. La proposta si basa sull'articolo 114 del trattato sul funzionamento dell'Unione europea e stabilisce le condizioni e i meccanismi per il riconoscimento e l'accettazione reciproci dell'identificazione elettronica e dei servizi fiduciari tra gli Stati membri. In particolare, essa stabilisce i principi connessi alla prestazione di servizi di identificazione e di servizi fiduciari elettronici, comprese le norme applicabili al riconoscimento e all'accettazione. Fissa inoltre i requisiti per la creazione, la verifica, la convalida, la gestione e la conservazione di firme elettroniche, sigilli elettronici, validazioni temporali elettroniche, documenti elettronici, servizi elettronici di recapito, autenticazione dei siti web e certificati elettronici.

8. Inoltre, la proposta di regolamento stabilisce le norme per la vigilanza della prestazione di servizi fiduciari e impone agli Stati membri di istituire a tale scopo organismi di vigilanza. Tali organismi, tra gli altri compiti, valuteranno la conformità delle misure tecniche e organizzative attuate dai prestatori di servizi fiduciari elettronici.

([1]) COM(2012) 238 final.
([2]) COM(2010) 245 del 19.5.2010.

9. Il capo II tratta i servizi di identificazione elettronica, mentre il capo III è dedicato ad altri servizi fiduciari elettronici quali la firma elettronica, i sigilli elettronici, la validazione temporale elettronica, i documenti elettronici, i servizi elettronici di recapito, i certificati e l'autenticazione dei siti web. I servizi di identificazione elettronica sono collegati a schede di identificazione nazionali e possono essere utilizzati nell'accesso ai servizi digitali e, in particolare, ai servizi di *e-government*; ciò significa che un ente che emette l'identificazione elettronica agisce per conto di uno Stato membro e tale Stato membro è responsabile per stabilire in modo corretto la correlazione tra un individuo concreto e i suoi mezzi di identificazione elettronica. Per quanto riguarda altri servizi fiduciari elettronici, il prestatore/soggetto rilasciante è una persona fisica o giuridica che è responsabile per la prestazione corretta e sicura di questi servizi.

I.4. *Questioni relative alla protezione dei dati sollevate dalla proposta*

10. Il trattamento dei dati personali è inerente all'utilizzo di regimi di identificazione e in qualche misura anche alla prestazione di altri servizi fiduciari (ad esempio, nel caso delle firme elettroniche). Il trattamento dei dati personali sarà necessario al fine di stabilire un collegamento affidabile tra l'identificazione elettronica e i mezzi di autenticazione utilizzati da una persona fisica (o giuridica) e tale persona, al fine di certificare che la persona dietro il certificato elettronico è veramente chi sostiene di essere. Per esempio, le identificazioni elettroniche o i certificati elettronici si riferiscono a persone fisiche e comprenderanno una serie di dati che rappresentano in modo inequivocabile tali individui. In altre parole, la creazione, la verifica, la convalida e la gestione dei mezzi elettronici di cui all'articolo 3, punto 12, della proposta comporteranno, in molti casi, il trattamento di dati personali e, pertanto, la protezione dei dati diventa rilevante.

11. È quindi essenziale che il trattamento dei dati nel contesto della prestazione di regimi di identificazione elettronica o di servizi fiduciari elettronici avvenga in conformità con il quadro dell'UE per la protezione dei dati, in particolare con le disposizioni nazionali di attuazione della direttiva 95/46/CE.

12. Nel presente parere, il GEPD concentrerà la sua analisi su tre questioni principali:

a) come viene affrontata nella proposta la protezione dei dati;

b) gli aspetti relativi alla protezione dei dati dei regimi di identificazione elettronica da riconoscere e accettare a livello transfrontaliero; e

c) gli aspetti relativi alla protezione dei dati dei servizi fiduciari elettronici da riconoscere e accettare a livello transfrontaliero.

III. **Conclusioni**

50. Il GEPD accoglie con favore la proposta, in quanto può contribuire al riconoscimento reciproco (e all'accettazione) dei servizi fiduciari elettronici e dei regimi di identificazione a livello europeo. Si compiace inoltre della creazione di un insieme comune di requisiti che devono essere soddisfatti dai soggetti che rilasciano mezzi di identificazione elettronica e dai prestatori di servizi fiduciari. Nonostante il suo sostegno generale della proposta, il GEPD desidera fornire le seguenti raccomandazioni generali:

— le disposizioni di protezione dei dati contenute nella proposta non dovrebbero essere limitate ai prestatori di servizi fiduciari e dovrebbero essere applicabili anche al trattamento dei dati personali nei regimi di identificazione elettronica di cui al capo II della proposta,

— la proposta di regolamento dovrebbe stabilire un insieme comune di requisiti di sicurezza per i prestatori di servizi fiduciari e i soggetti che rilasciano l'identificazione elettronica. In alternativa, potrebbe consentire alla Commissione di definire, ove necessario, attraverso un uso selettivo di atti delegati o misure di esecuzione, i criteri, le condizioni e i requisiti per la sicurezza nei servizi fiduciari elettronici e nei regimi di identificazione elettronica,

— i prestatori di servizi fiduciari elettronici e i soggetti che rilasciano l'identificazione elettronica dovrebbero essere tenuti a fornire agli utilizzatori dei loro servizi: i) informazioni adeguate sulla raccolta, la comunicazione e la conservazione dei dati, nonché ii) un mezzo per controllare i loro dati personali ed esercitare i loro diritti alla protezione dei dati,

— il GEPD raccomanda un inserimento più selettivo nella proposta delle disposizioni che conferiscono alla Commissione il potere di specificare o precisare, con atti delegati o di esecuzione, disposizioni concrete dopo l'adozione della proposta di regolamento.

51. Alcune disposizioni specifiche relative al riconoscimento reciproco dei regimi di identificazione elettronica dovrebbero altresì essere migliorate:

— la proposta di regolamento dovrebbe specificare quali dati o categorie di dati personali saranno trattati per l'identificazione transfrontaliera degli individui. Tale specificazione dovrebbe contenere almeno lo stesso livello di dettaglio fornito negli allegati per altri servizi fiduciari e dovrebbe tener conto del rispetto del principio di proporzionalità,

— le garanzie richieste per la fornitura di regimi di identificazione dovrebbero essere almeno conformi ai requisiti previsti per i prestatori di servizi fiduciari qualificati,

— la proposta dovrebbe istituire meccanismi appropriati al fine di stabilire un quadro per l'interoperabilità dei regimi nazionali di identificazione.

52. Infine, il GEPD esprime altresì le seguenti raccomandazioni in relazione ai requisiti per la prestazione e il riconoscimento dei servizi fiduciari elettronici:

— è opportuno precisare, in relazione a tutti i servizi elettronici, se saranno trattati dati personali e, nei casi in cui avvenga tale trattamento, i dati o le categorie di dati che saranno elaborati,

— il regolamento dovrebbe includere adeguate misure di salvaguardia al fine di evitare sovrapposizioni tra le competenze degli organismi di vigilanza per i servizi fiduciari elettronici e quelle delle autorità garanti per la protezione dei dati,

— gli obblighi imposti ai prestatori di servizi fiduciari elettronici in materia di violazioni dei dati e incidenti di sicurezza devono essere coerenti con i requisiti stabiliti nella direttiva riveduta sulla *e-privacy* e nella proposta di regolamento sulla protezione dei dati,

— maggiore chiarezza andrebbe conferita alla definizione degli organismi pubblici o privati che possono agire come terzi incaricati di effettuare le verifiche ai sensi degli articoli 16 e 17 o abilitati a certificare i dispositivi elettronici per la creazione di una firma elettronica ai sensi dell'articolo 23, nonché riguardo ai criteri in base ai quali sarà valutata l'indipendenza di tali organismi,

— il regolamento dovrebbe essere più preciso nel fissare un limite di tempo per la conservazione dei dati di cui all'articolo 19, paragrafi 2 e 4 ([1]).

Fatto a Bruxelles, il 27 settembre 2012

Giovanni BUTTARELLI

Garante europeo aggiunto della protezione dei dati

([1]) Ai sensi dell'articolo 19, paragrafo 2, lettera g), i prestatori di servizi fiduciari qualificati registrano per un congruo periodo di tempo tutte le informazioni pertinenti relative a dati da essi rilasciati e ricevuti. Ai sensi dell'articolo 19, paragrafo 4, i prestatori di servizi fiduciari qualificati trasmettono alle parti facenti affidamento sulla certificazione informazioni sulla situazione di validità o revoca dei certificati qualificati da essi rilasciati.