Sintesi del parere del Garante europeo della protezione dei dati sulla proposta di regolamento relativo alla resilienza operativa digitale per il settore finanziario e che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014 e (UE) n. 909/2014

(Il testo integrale del parere è disponibile in inglese, francese e tedesco sul sito del GEPD www.edps.europa.eu)

(2021/C 229/05)

Il 24 settembre 2020 la Commissione europea ha adottato una proposta di regolamento relativo alla resilienza operativa digitale per il settore finanziario e che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014 e (UE) n. 909/2014 (la «proposta»). La proposta istituisce un quadro completo sulla resilienza operativa digitale per le entità finanziarie dell'UE, basato su cinque ambiti principali, ossia la gestione dei rischi relativi alle TIC (capo II), la gestione, la classificazione e la segnalazione degli incidenti (capo III), il test di resilienza operativa digitale (capo IV), la gestione dei rischi derivanti da terzi e la regolamentazione dei fornitori di servizi di TIC critici (capo V) nonché la condivisione delle informazioni (capo VI).

Il Garante europeo della protezione dei dati (GEPD) si compiace degli obiettivi della proposta e ritiene essenziale per la stabilità dei mercati finanziari dell'Unione europea il fatto che gli istituti finanziari contino su un quadro per la gestione dei rischi relativi alle TIC solido, esaustivo e adeguatamente documentato.

Il GEPD sottolinea l'importanza di garantire che qualsiasi attività di trattamento nel contesto delle operazioni delle entità finanziarie si fondi su una delle basi giuridiche previste dall'articolo 6 del RGPD ([1]). Il GEPD sottolinea inoltre l'importanza per le entità finanziarie di integrare nel loro quadro sulla resilienza operativa digitale un meccanismo solido di governance per la protezione dei dati, che identifichi chiaramente i ruoli e le responsabilità del titolare e del responsabile del trattamento, nonché le attività di trattamento che verranno svolte.

Per quanto concerne i trasferimenti internazionali verso fornitori terzi di servizi di TIC stabiliti in un paese terzo, il GEPD ricorda che qualsiasi trasferimento internazionale di dati personali deve soddisfare i requisiti di cui al capo V del RGPD secondo l'interpretazione data dalla giurisprudenza della CGUE, ivi compresa la sentenza nella causa *Schrems II*.

In merito ai meccanismi di condivisione delle informazioni e dei dati sulle minacce informatiche tra le entità finanziarie, il GEPD evidenzia che la protezione dei dati personali non costituisce un ostacolo alla condivisione di informazioni nel settore finanziario. Piuttosto, i requisiti in materia di protezione dei dati devono essere percepiti come un requisito di base cui conformarsi per garantire la salvaguardia dei diritti delle persone. In tale contesto, il GEPD incoraggia l'adozione, anche nel settore finanziario, di codici di condotta in conformità dell'articolo 40 del RGPD, in particolare per definire chiaramente i ruoli dei principali portatori di interessi nel trattamento dei dati personali e per garantire un trattamento corretto e trasparente.

Per quanto riguarda la pubblicazione di sanzioni amministrative, il GEPD raccomanda di includere, tra i criteri di cui deve tenere conto l'autorità competente, i rischi per la protezione dei dati di carattere personale. In aggiunta il GEPD ricorda che, in base al principio di limitazione della conservazione, i dati personali devono essere conservati per un periodo non superiore al tempo necessario per conseguire le finalità per le quali sono trattati.

In merito alla notifica della violazione dei dati, il GEPD sottolinea che la formulazione del considerando 42 della proposta è incompatibile con l'articolo 33 del RGPD e, pertanto, raccomanda di cancellare il riferimento alle autorità per la protezione dei dati dal considerando 42 della proposta e di modificare lievemente l'articolo 17 della stessa, conformemente alle raccomandazioni del presente parere.

1. **CONTESTO**

1. Il 24 settembre 2020 la Commissione europea ha adottato una proposta di regolamento relativo alla resilienza operativa digitale per il settore finanziario e che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014 e (UE) n. 909/2014 (la «**proposta**»). La proposta istituisce un quadro completo sulla resilienza operativa digitale per le entità finanziarie dell'UE, basato su cinque ambiti principali, ossia la gestione dei rischi relativi alle TIC (capo II), la gestione, la classificazione e la segnalazione degli incidenti (capo III), il test di resilienza operativa digitale (capo IV), la gestione dei rischi derivanti da terzi e la regolamentazione dei fornitori di servizi di TIC critici (capo V) nonché la condivisione delle informazioni (capo VI).

2. Tale proposta fa parte di un pacchetto che comprende una proposta di regolamento per la creazione di mercati delle cripto-attività ([2]) (il «**regolamento MICA**»), una proposta relativa a un regime pilota per le infrastrutture di mercato basate sulla DLT ([3]) e una proposta volta a chiarire o modificare determinate norme dell'UE in materia di servizi finanziari ([4]). Il GEPD è stato consultato in merito alla proposta relativa al regime pilota per le infrastrutture di mercato basate sulla DLT e ha presentato il suo parere il 23 aprile 2021 ([5]). Il 29 aprile 2021 è stato consultato anche in merito al regolamento MICA e presenterà il suo parere conformemente all'articolo 42, paragrafo 1, del regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio ([6]).

3. Il 15 marzo 2021 la Commissione europea ha richiesto al Garante europeo della protezione dei dati (il «GEPD») di emettere un parere sulla proposta, ai sensi dell'articolo 42, paragrafo 1, del regolamento (UE) 2018/1725. Le presenti osservazioni sono limitate alle disposizioni della proposta che sono pertinenti dal punto di vista della protezione dei dati.

4. **CONCLUSIONI**

Alla luce di quanto precede:

— il GEPD sottolinea l'importanza di garantire che **qualsiasi attività di trattamento** nel contesto delle operazioni delle entità finanziarie **si fondi su una delle basi giuridiche di cui all'articolo 6 del RGPD** e indica l'articolo 6, paragrafo 1, lettere c), e) ed f), del RGPD, come possibile base giuridica di cui devono tenere conto le entità finanziarie.

— Il GEPD sottolinea inoltre l'importanza per le entità finanziarie di integrare nel loro quadro per la resilienza operativa digitale un **meccanismo solido di governance per la protezione dei dati**, che identifichi chiaramente i ruoli e le responsabilità del titolare e del responsabile del trattamento, nonché le attività di trattamento che verranno svolte.

— Il GEPD ricorda che **qualsiasi trasferimento internazionale di dati personali da parte di entità finanziarie** verso un fornitore terzo di servizi di TIC stabilito in un paese terzo **deve soddisfare i requisiti di cui al capo V del RGPD** e, qualora venga effettuato, deve essere soggetto a garanzie adeguate, conformemente al quadro sulla protezione dei dati e alla giurisprudenza della CGUE, in particolare alla causa Schrems II. Tali entità finanziarie possono ricorrere alle clausole contrattuali standard, poiché sembrerebbero essere lo strumento di trasferimento più pertinente.

— Il GEPD sottolinea che la **protezione dei dati personali non costituisce un ostacolo alla condivisione di informazioni nel settore finanziario**. Piuttosto, i requisiti in materia di protezione dei dati devono essere percepiti come un requisito di base cui conformarsi per garantire la salvaguardia dei diritti delle persone nell'ambito del quadro per la resilienza operativa digitale delle entità finanziarie.

— Il GEPD incoraggia l'**adozione, anche nel settore finanziario, di codici di condotta** in conformità dell'articolo 40 del RGPD, in particolare per definire chiaramente i ruoli dei principali portatori di interessi nel trattamento dei dati personali e per garantire un trattamento corretto e trasparente.

— Per quanto riguarda la **pubblicazione di sanzioni amministrative**, il GEPD raccomanda di includere, tra i criteri di cui deve tenere conto l'autorità competente, **i rischi per la protezione dei dati di carattere personale**.

— In base al principio di limitazione della conservazione, il GEPD raccomanda alle entità finanziarie di adottare misure per garantire che le **informazioni sulle sanzioni amministrative siano cancellate dal loro sito web dopo che siano trascorsi cinque anni o prima**, se non sono più necessarie.

— Il GEPD sottolinea che la formulazione del **considerando 42 della proposta è incompatibile con l'articolo 33 del RGPD**. Perciò il GEPD raccomanda di cancellare il riferimento alle autorità per la protezione dei dati dal considerando 42 della proposta e di modificare l'articolo 17 della stessa affinché sia incluso un riferimento all'obbligo di notificare le violazioni dei dati alle competenti autorità per la protezione dei dati.

— Il GEPD raccomanda di modificare l'articolo 23, paragrafo 2, della proposta per garantire che i test, lo sviluppo dei prodotti o la ricerca relativamente a sistemi TIC non possano essere effettuati su reali sistemi di produzione contenenti dati personali dei clienti.

Bruxelles, 10 maggio 2021.

Wojciech Rafał WIEWIÓROWSKI

([1]) Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) (GU L 119 del 4.5.2016, pag. 1).

([2]) *Proposta di regolamento del Parlamento europeo e del Consiglio relativo ai mercati delle cripto-attività e che modifica la direttiva (UE) 2019/1937, COM/2020/593 final. Consultabile all'indirizzo EUR-Lex - 52020PC0593 - IT - EUR-Lex (europa.eu)*

([3]) *Proposta di regolamento del Parlamento europeo e del Consiglio relativo ad un regime pilota per le infrastrutture di mercato basate sulla tecnologia di registro distribuito COM/2020/594 final, consultabile all'indirizzo EUR-Lex - 52020PC0594 - IT - EUR-Lex (europa.eu)*

([4]) *Proposta di direttiva del Parlamento europeo e del Consiglio che modifica le direttive 2006/43/CE, 2009/65/CE, 2009/138/UE, 2011/61/UE, UE/2013/36, 2014/65/UE, (UE) 2015/2366 e UE/2016/2341, COM/2020/596 final. Consultabile all'indirizzo EUR-Lex - 52020PC0596 - IT - EUR-Lex (europa.eu)*

([5]) *Parere 6/2021 sulla proposta di un regime pilota per le infrastrutture di mercato basate sulla tecnologia di registro distribuito, consultabile all'indirizzo 2021-0219_d0912_opinion_6_2021_en_0.pdf (europa.eu)*

([6]) Regolamento (UE) 2018/1727 del Parlamento europeo e del Consiglio, del 14 novembre 2018, che istituisce l'Agenzia dell'Unione europea per la cooperazione giudiziaria penale (Eurojust) e che sostituisce e abroga la decisione 2002/187/GAI del Consiglio (GU L 295 del 21.11.2018, pag. 138).