CYBERSECURITY360

04/11/2020 11:58
Sito Web

cybersecurity360.it

Trasferimenti dati extra UE: la strategia dell'EDPS e gli impatti pratici per le aziende

LINK: https://www.cybersecurity360.it/legal/privacy-dati-personali/trasferimenti-di-dati-extra-ue-la-strategia-delledps/

Nicola Sandon Associate, Tonucci & Partners
Alessandro Vasta Partner, Tonucci & Partners

Il provvedimento del 29 ottobre scorso con cui il Garante Europeo per la protezione dei dati ha riacceso i riflettori sui colossali impatti pratici derivanti dalla sentenza Schrems II e dall'abolizione del Privacy Shield, delinea la strategia d'azione dell'EDPS e individua principi di carattere generale applicabili a tutte le organizzazioni, pubbliche o private, che effettuano trasferimenti di dati extra UE Adistanza di quasi quattro mesi dalla storica sentenza della Corte di Giustizia dell'Unione europea ("CGUE") nel caso Data Protection Commissioner v. Facebook Ireland e Maximillian Schrems, causa C-311/18 ("sentenza Schrems II"), che ha invalidato il "Privacy Shield" e minato le fondamenta dell'intera pratica dei trasferimenti di dati personali extra UE, cioè al di fuori del territorio dell'Unione Europea, è il Garante Europeo per la Protezione dei Dati (European Data Protection Supervisor, o, in breve, "EDPS") a rompere ufficialmente il silenzio che regnava incontrastato tra le istituzioni europee, con un sintetico ma al contempo denso provvedimento pubblicato lo scorso 29 ottobre. Se fino ad oggi in molti avevano sottovalutato la portata degli effetti della sentenza Schrems II dello scorso 16 luglio, anche a causa del torpore istituzionale seguito alla pronuncia, è giunto il momento di ricredersi (e correre quanto prima ai ripari): il documento intitolato "Strategy for Union institutions, offices, bodies and agencies to comply with the 'Schrems II' Ruling", ad oggi disponibile unicamente in lingua inglese sul sito istituzionale del Garante Europeo, è un segnale d'allarme per gli operatori che riaccende i riflettori sui colossali impatti pratici che l'arresto del supremo giudice dell'Unione è destinato ad avere sulla gestione dei trasferimenti di dati personali verso paesi non ritenuti "adeguati" dalla Commissione ai sensi dell'art. 45 del Regolamento UE 2016/679 (il "GDPR"). Il provvedimento che andremo ad analizzare nel dettaglio si rivolge espressamente alle istituzioni ed agli enti europei sulla base della normativa ad essi applicabile[1], tuttavia è lecito presumere che buona parte dei principi contenuti nello stesso assumeranno carattere generale, trovando applicazione a tutte le organizzazioni, pubbliche o private, che effettuino trasferimenti di dati al di fuori dell'Unione, in particolar modo qualora il paese di importazione dei dati siano gli Stati Uniti d'America. L'EDPS, infatti, autorità di controllo indipendente incaricata di garantire il rispetto del diritto alla protezione dei dati da parte delle istituzioni e gli organi dell'UE, è anche uno dei membri del Comitato Europeo per la Protezione dei Dati, organo di vertice a livello unionale per quanto riguarda la protezione dei dati personali, ad oggi impegnato a redigere apposite linee guida per aiutare gli operatori a comprendere le attività da porre in essere e le misure supplementari da applicare per adeguarsi al dicutm della CGUE. Indice degli argomenti Trasferimenti di dati extra UE: il provvedimento dell'EDPS Trasferimento dati extra

UE: il piano d'azione dell'EDPS La strategia dell'EDPS sul medio periodo Conclusioni Trasferimenti di dati extra UE: il provvedimento dell'EDPS L'EDPS, con il proprio provvedimento "Strategy for Union institutions, offices, bodies and agencies to comply with the 'Schrems II' Ruling", intende delineare un piano d'azione a breve e medio termine per garantire e monitorare la conformità delle autorità europee ai principi stabiliti dalla sentenza Schrems II, in particolar modo per quanto riguarda l'inedito (ed incredibilmente oneroso) obbligo di preventiva verifica, da parte dell'esportatore, in merito alla capacità del paese verso cui si intendono trasferire i dati di assicurare effettivamente, in considerazione della sua legislazione nazionale o dei suoi impegni internazionali, un livello di protezione delle libertà e dei diritti fondamentali sostanzialmente equivalente a quello garantito all'interno dell'Unione in forza del GDPR, letto alla luce della Carta dei diritti fondamentali dell'Unione Europea. Il Garante Europeo riconosce che un peso di assoluto rilievo nell'applicazione della propria strategia rivestono i principi di responsabilizzazione degli enti coinvolti e della collaborazione con l'autorità di vigilanza: questo perché l'intero sistema di garanzie posto a base dei trasferimenti di dati personali extra U.E., ereditato in forma pressoché invariata dalla previgente Direttiva 95/46/CE, è stato improvvisamente svuotato di significato a seguito della pronuncia della CGUE, lasciando gli operatori pericolosamente privi di riferimenti normativi in un periodo storico in cui lo sviluppo tecnologico procede di pari passo con l'interconnessione e la circolazione delle informazioni, finendo per scaricare su di essi una buona fetta di responsabilità. L'EDPS premette alla descrizione della propria strategia l'identificazione dei criteri di priorità da adottare ai fini dell'analisi dei trasferimenti di dati personali posti in essere dalle istituzioni europee. Nel fare questo, il Garante riconosce - richiamando a tal fine anche le risultanze di una propria analisi[2] condotta nel 2017 - come un numero sempre più elevato di servizi, soprattutto in campo informatico, connessi all'espletamento delle attività istituzionali sia stato nel corso degli ultimi anni esternalizzato affidandosi a providers con sede negli States, ovvero a fornitori europei che a sua volta ricorrono agli (irrinunciabili) servizi offerti da compagnie americane. Per dare un'idea della magnitudine del fenomeno, si pensi al mondo dei servizi Microsoft (es. Office365, Dynamics, Azure, ecc.), riguardo al quale l'EDPS ha peraltro svolto un'apposita indagine[3] le cui risultanze sono state rese pubbliche proprio nel luglio di quest'anno. Idem dicasi per qualsiasi piattaforma o funzionalità offerta in modalità Software-as-a-Service: anche in tal caso è altamente probabile che almeno una parte del trattamento si svolga negli Stati Uniti. Ne consegue - continua il Garante - che al giorno d'oggi la mole maggiore di trasferimenti di dati personali al di fuori del territorio dell'Unione effettuata, direttamente o indirettamente, da parte delle autorità europee avviene in stretta connessione alla fruizione di tali servizi: saranno dunque questi i trasferimenti che dovranno essere analizzati dalle autorità europee con il massimo grado di priorità. Tralasciando le possibili ricadute in ambito concorrenziale, l'EDPS fotografa con questo paragrafo introduttivo l'incredibile balzo

tecnologico compiuto dal mondo nell'ultimo decennio e al tempo stesso riconosce implicitamente l'incapacità del legislatore di offrire strumenti adeguati ad affrontare le sfide da esso poste: la fragilità dei meccanismi a suo tempo pensati in materia di trasferimento di dati personali extra U.E. - e fatti colpevolmente salvi dal GDPR - ne è un esempio lampante. Si rileva poi come l'Autorità europea non celi il proprio atteggiamento critico nei confronti dei provider di servizi informatici americani, contribuendo ad alimentare la sensazione che forti interessi politici siano alla base di quest'ultimo capitolo nel confronto tra Unione ed il mondo delle Big Tech. Trasferimento dati extra UE: il piano d'azione dell'EDPS Terminata l'introduzione, il provvedimento entra nel vivo, delineando il piano d'azione ideato dal Garante Europeo per garantire il rispetto della normativa da parte delle istituzioni unionali, che si prevede essenzialmente due tipologie di operazioni: nel breve termine, mappatura dei trasferimenti dati extra UE; nel medio termine, analisi degli stessi ed implementazione dei correttivi in base ai rischi rilevati. L'EDPS ha imposto alle autorità europee di avviare un'approfondita opera di mappatura dei trattamenti in essere che implichino un trasferimento di dati personali al di fuori del territorio dell'Unione, indicando nel dettaglio una serie di informazioni, tra cui gli estremi dei trattamenti in questione, i destinatari dei dati, il paese di destinazione, gli strumenti impiegati per il trasferimento, le categorie di dati trasferiti e le categorie di interessati (informazioni che in linea di principio dovrebbero essere già rinvenibili nei registri delle attività di trattamento tenuti dalle singole autorità). Esaustiva reportistica della suddetta attività dovrà essere fornita dalle singole istituzioni all'EDPS entro il prossimo 15 novembre. EVENTO Da emergenza a strategia: Sicurezza, Dati, AI e Cloud. La sfida è proprio ora Big Data Cloud Inizia tra: 12 19 31 10 Iscriviti all'Evento La mappatura dovrà però accompagnarsi anche ad una prima attività valutativa: adottando un approccio basato sul rischio, gli enti europei soggetti alla vigilanza dell'EDPS saranno infatti tenuti ad evidenziare le principali criticità rilevate in merito ai trattamenti mappati. Le autorità dovranno prestare particolare attenzione alle categorie di trasferimenti classificate più ad alto rischio dal provvedimento, e cioè quelli: posti in essere in assenza di una delle condizioni di liceità del trasferimento individuate dalla normativa; basati sulle deroghe specifiche al divieto di trasferimento in assenza di garanzie adeguate; verso entità americane espressamente soggette all'art. 702 del FISA[4] e all'E.O. 12333[5] - ovverosia le disposizioni di diritto statunitense a fondamento delle attività di intelligence (quali i programmi PRISM e UPSTREAM) che hanno in primis determinato l'invalidazione del Privacy Shield da parte della CGUE - a maggior ragione ove queste prevedano il trasferimento di dati su larga scala, il trattamento di dati sensibili o operazioni complesse di trattamento (tra cui spiccano quelle che implichino l'analisi o l'elaborazione di big data, l'impiego di nuove tecnologie o di tecniche complesse di profilazione o processi decisionali automatizzati ecc.). Se la puntualizzazione in merito ai trasferimenti posti in essere in assenza di un meccanismo di trasferimento potrebbe sembrare del tutto superflua, è il caso di ricordare che in questa categoria rientrano anche i trasferimenti di dati tra un responsabile del

trattamento con sede nell'UE ed eventuali sub-responsabili da questo ingaggiati che non siano vincolati da clausole contrattuali standard o misure equiparabili: questione piuttosto spinosa se consideriamo che ad oggi non esistono clausole standard dedicate ai trasferimenti tra responsabili e sub-responsabili, e quelle elaborate dalla Commissione nel 2010 non risultano applicabili a tale fattispecie per espressa previsione del Gruppo di Lavoro art. 29[6]. Per quanto riguarda invece l'eventuale avvio di nuovi trattamenti e/o esternalizzazione di nuovi servizi, il Garante Europeo è lapidario e mette nero su bianco esattamente lo scenario che gli operatori temevano di più a valle della pubblicazione della sentenza Schrems II: l'EDPS, infatti, "raccomanda fermamente alle autorità europee di evitare che qualsiasi nuova operazione di trattamento o nuovo contratto con fornitori di servizi comporti il trasferimento di dati personali verso Stati Uniti". Sarebbe superfluo aprire qui un dibattito sull'effettiva portata della raccomandazione contenuta nel provvedimento da un punto di vista giuridico: dopotutto, il documento costituisce uno strumento di c.d. "soft law", per sua natura non strettamente vincolante. Tuttavia, il monito avanzato dal Garante è piuttosto chiaro ed appare idoneo a travalicare i confini del proprio ridotto ambito di competenza, invitando gli operatori a diffidare dei provider statunitensi ed a tenere ben in considerazione i profili di rischio ad essi connessi ove si dovesse ritenere indispensabile ricorrervi. La strategia dell'EDPS sul medio periodo Passando poi alla descrizione delle azioni di medio periodo previste dalla propria strategia, l'EDPS specifica che le autorità dovranno impiegare i documenti di mappatura (e le relative valutazioni) elaborati nel corso della prima fase per identificare le misure da porre in essere qualora emerga che, a causa del trasferimento, non sia possibile assicurare agli interessati i cui dati trasferiti si riferiscono un livello di protezione sostanzialmente equivalente a quello garantito all'interno dell'Unione. A tal fine, il Garante elabora un nuovo strumento di compliance, figlio del principio di responsabilizzazione: le autorità europee saranno infatti tenute a condurre apposite valutazioni d'impatto sul trasferimento dei dati (c.d. "Transfer Impact Assessment", o "TIA"). La forma ed il contenuto di tale strumento non appaiono però ad oggi chiaramente definiti: l'EDPS informa infatti i destinatari che una lista di domande preliminari da rivolgere ai fornitori di servizi che si qualifichino come importatori - e che costituirà molto probabilmente il corpo centrale del TIA - sarà elaborata solo a seguito della pubblicazione delle linee guida del Comitato Europeo in merito alle garanzie supplementari da adottare per la protezione dei dati, ad oggi ancora in fase di redazione. Il risultato delle TIA avrà valore dirimente in merito al futuro dei trasferimenti in essere, secondo un meccanismo equiparabile a quello dell'altra valutazione d'impatto, quella sulla protezione dei dati personali descritta all'art. 35 del GDPR: ove a seguito dell'assessment risultino presenti le condizioni per proseguire il trasferimento, sarà necessario individuare le misure supplementari da adottare per garantire un livello di protezione dei dati equiparabile a quello offerto all'interno dell'U.E.; mentre se, anche a valle di tali accorgimenti aggiuntivi, ciò non sia possibile, si renderà necessario interrompere il

trasferimento, pena l'illiceità dello stesso. Una volta portata a termine anche tale seconda fase del piano d'azione, le istituzioni europee saranno nuovamente chiamate a rendicontare l'EDPS in merito al proprio operato, stavolta con termini più ampi, con scadenza prevista per la primavera del 2021. Costituiranno oggetto specifico di tale seconda attività relazionale i trasferimenti caratterizzati dal grado di rischio più elevato, sempre da individuarsi sulla base delle indicazioni dell'Autorità. In particolare, sarà necessario prestare attenzione ai trasferimenti: verso paesi terzi che, a valle dell'attività di TIA, non garantiscano un livello di protezione adeguato; cessati o sospesi sulla base delle valutazioni effettuate dalla singola autorità; che si basino sulle deroghe alle limitazioni ai trasferimenti specificamente previste dalla normativa di riferimento. Sulla base dei report ricevuti, l'EDPS studierà ulteriori attività di compliance a medio e lungo termine e valuterà l'opportunità di procedere a valutazioni congiunte sul livello di protezione offerto dai paesi terzi. Conclusioni Pur rappresentando un gradito strumento e spunto di riflessione in attesa dell'anticipato intervento del Comitato Europeo per la Protezione dei Dati, molti sono i dubbi che esso lascia dietro di sé, nonostante i più previdenti avessero ben compreso il percorso impresso dall'Unione Europea al tema dei trasferimenti di dati personali al di fuori dell'Unione Europea all'indomani della pubblicazione della sentenza Schrems II. Le perplessità per lo più riconducibili a due distinti ambiti. In primo luogo, il documento sembra mancare ancora di specificità nell'individuazione delle possibili soluzioni ad un problema così terribilmente concreto come quello posto dalla necessità di sottoporre a revisione tutti i trasferimenti di dati personali posti in essere all'interno di un'organizzazione, a prescindere dal fatto che esso avvenga in maniera diretta o indiretta (i.e. mediante sub-responsabili). Certo, viene identificata in maniera espressa la necessità di provvedere quanto prima ad una dettagliata ricognizione dei trasferimenti posti in essere, ma tale opera è solamente propedeutica alle azioni di compliance, non ancora delineate, come del tutto sconosciuto risulta lo strumento cui ci si dovrebbe affidare per l'individuazione delle stesse. E mentre il Garante Europeo diluisce nel tempo l'impatto della sentenza, concedendo alle istituzioni europee di effettuare le proprie valutazioni entro la primavera del 2021, un simile termine non viene ad oggi riconosciuto in favore degli altri operatori, cui anzi è stato negato qualsivoglia periodo di grazia per espressa previsione del Comitato Europeo[7]. A ciò si aggiunga che se le autorità europee potranno contare sulla guida e la puntuale verifica da parte dell'EDPS, lo stesso non potrà dirsi per gli altri operatori, pubblici o privati che siano. In secondo luogo, non si può non riscontrare come le autorità europee sembrino manifestare nel proprio agire un certo distacco dalla realtà, per lo meno in merito allo specifico fenomeno dei trasferimenti extra UE di dati personali. È giusto infatti ricordare come attualmente un eventuale blocco dei trasferimenti di dati verso gli States risulterebbe disastroso per una pletora di aziende ed enti europei, appartenenti ai settori più disparati: eppure, in un già complesso quadro normativo, viene introdotta quella che ha tutto l'aspetto di essere l'ennesima complicazione "burocratica", complicazione che, in assenza di indicazioni chiare e precise

da parte delle autorità, si trasformerà immancabilmente in un nuovo costo a carico degli operatori, a tutto svantaggio delle realtà emergenti o di dimensioni medio-piccole, per le quali il ricorso a nuovi servizi tecnologici rappresenta uno strumento di crescita ed internazionalizzazione, nonché un volano per la crescita. Per non parlare del fatto il buon esito delle TIAs rimarrebbe inestricabilmente connesso alla collaborazione dei fornitori, soggetti solitamente dotati di un enorme potere contrattuale e presumibilmente ben poco inclini a scendere a patti con migliaia di operatori sulla base di valutazioni d'impatto prive di qualsivoglia oggettività. Per quanto sia appezzabile lo sforzo europeo volto alla tutela dei diritti inviolabili degli esseri umani, tra cui spicca il diritto alla riservatezza, e sia senz'altro da riconoscere che è indispensabile sensibilizzare gli attori presenti sul mercato in merito alle possibili conseguenze di un trattamento non adeguato di dati personali, è forse opportuno valutare un approccio alternativo in grado di tutelare adeguatamente un altro diritto fondamentale: quello della libertà di iniziativa economica. Risulta ormai evidente come l'Unione Europea stia facendo leva sugli aspetti inerenti alla protezione dei dati personali per fare breccia nel primato dei colossi americani del tech, nel tentativo di limitarne il potere distorsivo sull'economia (e, con l'occasione, di ritagliare per le aziende europee una fetta di un mercato caratterizzato da barriere all'ingresso pressoché insormontabili). Appare però discutibile la scelta del campo di battaglia: mentre, ad esempio, adottando contromisure in ambito fiscale o antitrust lo scontro si sarebbe svolto sullo stesso piano, vedendo imprese miliardarie confrontarsi con autorità di vigilanza nazionali o sovranazionali, ad oggi vi è il concreto rischio che a pagare il prezzo più elevato siano le imprese e i consumatori europei, stritolati tra incertezza normativa, totale assenza di potere contrattuale e stringenti esigenze di business. NOTE Il Regolamento UE 2018/1725 del Parlamento europeo e del Consiglio, del 23 ottobre 2018, sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati, e che abroga il regolamento (CE) n. 45/2001 e la decisione n. 1247/2002/CE. EDPS, "Measuring compliance with data protection rules in EU institutions", 2017, disponibile qui. EDPS, "Public Paper on Outcome of own-initiative investigation into EU institutions' use of Microsoft products and services", 2 luglio 2020, disponibile qui. Foreign Intelligence Surveillance Act. Executive Order 12333. Gruppo di Lavoro art. 29, WP176 "FAQs in order to address some issues raised by the entry into force of the EU Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC" del 12 luglio 2010, domande n. 2 e 3. V. Comitato Europeo per la Protezione dei Dati "Domande frequenti sulla sentenza della Corte di giustizia dell'Unione europea nella causa C-311/18 - Data Protection Commissioner/Facebook Ireland Ltd e Maximillian Schrems" del 23 luglio 2020.