pentha
Servizi Integrati per le Imprese
ANNO 15 NUMERO 274

Cuneo, 25/10/2022

In questo numero

Il focus di questo numero

Gentili Lettori,

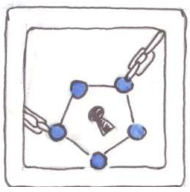
la premessa è doverosa: nulla è cambiato nel quadro attuale e il trasferimento dei dati verso gli Stati Uniti continua a essere illecito. L'ordine esecutivo emesso dal presidente americano Joe Biden il 7 ottobre, infatti, vuole sì essere un impegno in materia di protezione dei dati personali che possa garantire un livello di adeguatezza conforme alla normativa sulla protezione dei dati personali europea sufficiente a ripristinare il trasferimento dei dati verso gli Stati Uniti, tuttavia, questa determinazione di adeguatezza da parte dell'UE dovrebbe arrivare solamente nei primi mesi del 2023.

Dopo aver esaminato l'ordine esecutivo, abbiamo ascoltato le dichiarazioni di Guido Scorza (componente del Garante), letto anche le obiezioni di Max Schrems e prodotto l'elaborato che apre la nostra consueta rassegna e che vuole essere una sintesi di quanto accaduto e di quali possono essere gli scenari possibili.

Restando in territorio anglofono, è recente anche la notizia dell'inizio dei lavori relativamente a un sistema britannico per la protezione dei dati personali che intende sostituire il GDPR con una regolamentazione nazionale e che dovrà anch'essa essere sottoposta a valutazione di adeguatezza da parte dell'UE.

Segnaliamo infine, fra le notizie, quella relativa ai cookie wall delle testate giornalistiche che, da qualche giorno, compaiono all'apertura delle edizioni on line e che non sembrano in linea con il principio del libero consenso. Il caso, ancora al vaglio dello studio del Garante, non che è una fra le tante situazioni che stanno generando nelle persone una giustificata preoccupazione generale relativamente all'utilizzo e alla protezione dei propri dati e che, in futuro, potrebbe condizionare le loro scelte sui beni e sui servizi.

Lo staff di Pentha Vi augura una buona lettura e visione!



Il primo passo verso un impegno condiviso in attesa di un accordo definitivo

L'angolo della privacy

L'ordine esecutivo sulla privacy dei dati fra unione europea e stati uniti: un passo, ma non ancora la soluzione

Il 7 ottobre il presidente degli Sati Uniti, Joe Biden, ha firmato "l'ordine esecutivo per l'attuazione del quadro per la privacy dei dati tra l'Unione europea e gli Stati Uniti". Tuttavia, prima di gridare "Terra!" e impostare la rotta, conviene attendere che le acque si calmino e le nebbie di dissipino, onde evitare di disintegrare la nave sugli scogli.

L'ordine esecutivo è certamente una buona notizia, perché rappresenta un primo passo nella direzione della costruzione di un nuovo accordo fra Unione Europea e Stati Uniti in relazione al trasferimento dei dati dei cittadini europei verso quest'ultimo. Ma, appunto, si tratta di un passo verso la soluzione, non della soluzione.

Con l'ordine esecutivo, gli Stati Uniti dichiarano di voler mettere in campo «nuovi impegni di alto livello in materia di protezione dei dati personali» e di voler istituire un organismo indipendente che garantisca l'erogazione di un risarcimento nel caso in cui gli interessati ritengano da aver subito un illecito nella raccolta e nell'uso dei propri dati personali.

I diversi punti dell'ordine esecutivo, dunque, riguarderebbero:

- La limitazione dell'attività di intelligence in ragione del solo perseguimento di obiettivi di sicurezza nazionale e effettuata solamente nella misura necessaria a tale scopo ("proporzionata"), salvaguardando la privacy e la libertà civile di tutte le persone, a prescindere dalla nazionalità e dal paese di residenza;
- •L'estensione delle responsabilità dei funzionari legali affinché possano supervisionare la conformità di tali attività e rimediare, ove necessario, a eventuali non conformità;
- La creazione di un meccanismo multilivello per l'esame delle denunce di violazione delle norme sul trattamento dei dati che prevede, tra le altre, l'istituzione di una commissione di giudici nominati al di fuori del governo degli Stati Uniti (Corte di riesame della protezione dei dati), che abbiano esperienza nel settore della privacy e della sicurezza dei dati e che, in modo indipendente, esamineranno i casi sottoposti alla loro attenzione e stabilendo, nel caso di una effettiva violazione della legge, un'adeguata riparazione al danno cagionato (risarcimento);
- La revisione delle politiche e delle procedure di intelligence affinché siano conformi a quanto stabilito dall'ordine esecutivo.

Tutto ciò premesso, questo ordine esecutivo (che ancora non è legge), come già detto, rappresenta esclusivamente un primo passo, dal momento che esso dovrà ora essere sottoposto al vaglio della Commissione europea la quale dovrà stabilire se queste

clausole possano essere sufficienti per «adottare una nuova determinazione di adeguatezza» e quindi ripristinare il trasferimento dei dati verso gli Stati Uniti, offrendo, al contempo, anche maggiori certezze alle società che «utilizzano clausole contrattuali standard e regole vincolanti per trasferire i dati personali dell'UE negli Stati Uniti».

La determinazione di adeguatezza, potrebbe arrivare nei primi mesi del 2023 e, se effettivamente stabilita e per un tempo che sia durevole, risolverebbe certamente molti grattacapi che attualmente le aziende si trovano ad affrontare, senza, tuttavia, garantire che una nuova sentenza "Schrems" torni a invalidare gli accordi, dal momento che due sono gli importanti incagli che rendono difficoltosa la strada della soluzione definitiva: il primo è il concetto di "proporzionalità" che viene interpretato diversamente dall'Europa e dagli Stati Uniti; il secondo è che, nonostante entrambi gli ordinamenti politici concordino sui principi della privacy, mentre per l'Europa si tratta di un diritto fondamentale che deve essere applicato a ogni essere umano, per gli Stati Uniti, e in base al quarto emendamento, hanno accesso a tale diritto solamente i cittadini statunitensi o i suoi residenti permanenti. Il che, di fatto, esclude automaticamente i cittadini europei.

Concludendo: qualcosa si sta muovendo, ma ancora non conosciamo quale sia la direzione, né l'approdo. Frattanto, quindi, il consiglio è quello di continuare sulla rotta della ricerca e dell'utilizzo strumenti alternativi che evitino tout court il trasferimento dei dati verso gli Stati Uniti per evitare attività sanzionatorie da parte delle autorità dei diversi paesi europei. Se nel 2023 questo primo passo si trasformerà in accordo, si potrà tornare indietro, mentre, in caso contrario, si starà già comunque navigando in acque sicure.

Fonte: Pentha s.r.l.

Per i cookie wall c'è uno spiraglio: non sono illegittimi in assoluto

Editori sotto la lente del Garante

Per i cookie wall c'è uno spiraglio: non sono illegittimi in assoluto. Dipende. Lo hanno detto il Garante privacy, il Garante della concorrenza del mercato, la Cassazione. L'illegittimità scatta quando la volontà è calpestata. Ma il "prendere o lasciare" (o consenso per farsi tracciare e profilare con i cookie o niente accesso a un sito) e cioè scambio dati contro contenuti digitali è stato sdoganato anche dalla legge.

L'argomento è salito alla ribalta per l'indagine aperta dal Garante privacy sui cookie wall di alcuni quotidiani on line. Alcune testate giornalistiche, siti web e aziende operanti sul web nel settore televisivo, hanno cominciato a usare sistemi e filtri, che condizionano l'accesso ai contenuti alla sottoscrizione di un abbonamento (il cosiddetto paywall) o, in alternativa, al rilascio del consenso da parte degli utenti all'installazione di cookie e altri strumenti di tracciamento dei dati personali (il cosiddetto cookie wall). Ma dati contro un servizio, ad alcune condizioni, si può. Si può essere in disaccordo con questa regola, ma si tratta di una regola che affonda le sue radici nelle pronunce dei Garanti italiani, trova conferma nella giurisprudenza e nella legislazione relativa al mercato digitale.

Garante Privacy - Risale al 2000 il provvedimento datato 13 gennaio, nel quale il Garante, trattando di un caso di un quotidiano on line, scriveva che rimane nella disponibilità degli interessati l'acconsentire a servizi che subordinano una prestazione - quale l'accesso ad Internet - alla cessione di dati identificativi o attinenti a gusti, preferenze ed interessi. Ovviamente aggiungeva che la persona deve essere messa in grado di capire a cosa va incontro e bisogna darle tutte le informazioni per esprimere le proprie scelte liberamente e consapevolmente.

Peraltro, è scontato che non bisogna mentire o ingannare, ma questo non pregiudica la legittimità dell'operazione. Il Garante ha trattato i cookie wall anche nel provvedimento 231 del 10 giugno 2021, nel quale li ha bocciati, ma con molte possibilità di ripescaggio: va verificato caso per caso se il cookie wall è compatibile con un libero consenso.

Non a caso, in un comunicato del 21 ottobre 2022, lo stesso Garante ha rilevato che la normativa europea sulla privacy non esclude in linea di principio che il titolare di un sito subordini l'accesso ai contenuti, da parte degli utenti, al consenso prestato dai medesimi per finalità di profilazione (attraverso cookie o altri strumenti di tracciamento) o, in alternativa, al pagamento di una somma di denaro.

Antitrust - È del 2000 (17 febbraio) il parere dell'Antitrust, reso nel procedimento n.8051, nel quale l'autorità scriveva a proposito del "diritto di non essere destinatario di comunicazioni d'impresa veicolate attraverso talune tecniche di comunicazione a distanza"

che si tratta di "un diritto disponibile, con consenso esplicito e preventivo" e aggiungeva che questo diritto è "sicuramente negoziabile". In altre parole, si può scambiare il cookie con un servizio. Ribadiamolo, con l'ovvio rispetto della volontà e senza inganni (ma questo vale per tutti i contratti).

Cassazione - Più recente, del 2 luglio 2018, è la sentenza n. 17278 della Cassazione, nelle cui motivazioni è spiegato che un gestore di un sito Internet, nel somministrare un servizio fungibile, cui l'utente possa rinunciare senza gravoso sacrificio, può legittimamente condizionare la fornitura del servizio al trattamento dei dati per finalità pubblicitarie. Anche qui c'era la precisazione delle ovvie condizioni a proposito della libertà del consenso e, a questo proposito, la cassazione ha ritenuto necessario che l'interessato sia informato sui settori merceologici o dei servizi oggetto dei messaggi pubblicitari. Tra l'altro la sentenza ha riguardato il caso di una newsletter su tematiche legate alla finanza, al fisco, al diritto e al lavoro.

Direttive Ue - La direttiva UE 2019/770 e il decreto legislativo di recepimento n. 173/2021 hanno sdoganato, con apposite modifiche al codice del consumo, i contratti in cui un'impresa fornisce o si obbliga a fornire un contenuto digitale o un servizio digitale al consumatore e il consumatore fornisce o si obbliga a fornire dati personali al professionista. I dati personali son la valuta con cui si paga il contenuto o il servizio digitale.

Fonte: Italia Oggi (Antonio Ciccio Messina)

Il Regno Unito è pronto a dire addio al Gdpr per sostituirlo con una propria regolamentazione nazionale

La riforma britannica sulla protezione dei dati personali

Il Regno Unito è pronto a uno "strappo" con l'Europa sulla protezione dei dati personali: il nuovo governo di Liz Truss sta infatti spingendo su una riforma per sostituire il Gdpr con una regolamentazione nazionale. Parlando alla conferenza annuale del Partito Conservatore, Michelle Donelan, nominata dalla Truss nel ruolo di Secretary of State for Digital, culture, media and sport, ha annunciato che il governo «sostituirà il Gdpr con un proprio sistema britannico per la protezione dei dati che meglio tutelerà gli interessi di imprese e consumatori».

Come riporta The Guardan, la Donelan ha affermato che il Regno Unito può essere "il ponte sull'Atlantico e operare come hub di dati del mondo", dando particolare enfasi sulla riduzione degli adempimenti burocratici, considerati un fardello dell'Ue per le imprese.

Il nuovo sistema britannico per la data protection mirerà alla semplificazione delle regole e dei requisiti esistenti, ha proseguito il ministro, e attingerà ai sistemi di altri paesi ritenuti adeguati dall'Ue anche senza il Gdpr, come Giappone, Corea del Sud, Israele, Canada e Nuova Zelanda, "per formare un sistema di protezione dei dati che sia veramente su misura".

La Gran Bretagna aveva già intrapreso una riforma delle regole sulla privacy, infatti a inizio anno il governo di Boris Johnson aveva proposto un emendamento alla versione del Gdpr che Londra ha adottato dopo la Brexit, mettendo sul tavolo la bozza di una legge chiamata "Data Reform Bill".

Il nuovo esecutivo inglese vuole andare oltre per dare risalto ai flussi di dati con altri paesi esterni all'Ue, in particolare Stati Uniti, Australia, Corea del Sud e Singapore. Londra non ha fornito dettagli sulle ulteriori modifiche legislative e ciò non permette di capire al momento se manterrà comunque l'adequacy ruling (decisione di adeguatezza) dell'Ue, che permette lo scambio di dati personali tra l'Unione Europea e il Regno Unito.

In seguito alla Brexit, infatti, i trasferimenti di dati tra le due parti sono stati approvati dalla Commissione perché Londra aveva ancora una normativa allineata al Gdpr. In questa decisione era inclusa anche una "sunset clause", che ne assicurava la scadenza automatica e, quindi, la necessaria revisione e rinnovo ci sarebbero state in ogni caso nel 2024.

Fonte: Federprivacy

Il 76% dei consumatori non comprerebbe da un'azienda di cui non si fida riguardo al rispetto della privacy

La via per l'affermazione di un diritto centrale passa attraverso il rischio commerciale e reputazionale

Il 76% dei consumatori non comprerebbe prodotti o servizi da un'azienda che non ispirasse fiducia circa il rispetto della loro privacy e l'81% si dice convinto che il modo in cui un'azienda è trasparente in relazione al trattamento dei dati personali è sintomatico del rispetto che ha per i consumatori. Sono alcuni dei risultati della quarta edizione della CISCO customer privacy survey appena pubblicati.

E sono risultati che per quanto difficili da conciliare con l'osservazione empirica di un universo nel quale utenti e consumatori, specie nella dimensione digitale, sembrano davvero poco preoccupati della loro privacy, lasciano intravedere un timido lumicino in fondo al tunnel perché raccontano di un mercato che, prima o poi, premierà chi rispetterà di più la privacy di utenti e consumatori e punirà chi, al contrario, la rispetterà di meno.

La survey, infatti, suggerisce che utenti e consumatori esigano dai loro interlocutori commerciali più rispetto per la loro privacy di quanto accaduto sin qui. Si tratta, forse, dell'unica reale speranza di affermazione di un diritto tanto centrale nella nostra società quanto dimenticato, bistrattato e offeso: se i consumatori iniziano a chiedere più rispetto per la loro privacy, ai fornitori di prodotti e servizi non resterà altra alternativa che accontentarli e, a quel punto, il piano potrebbe inclinarsi e le regole, sin qui troppo spesso tradite, ignorate e violate cominceranno a essere rispettate non tanto per paura delle sanzioni ma, invece, per paura di perdere utenti e clienti.

In fondo si tratta di un processo analogo, con i distinguo del caso, a quello registratosi in relazione all'ecologia, al green, alla sostenibilità ambientale. Fino a quando si è trattato semplicemente di rispettare le leggi e sottrarsi al rischio di sanzioni le aziende hanno cambiato poco o nulla nei loro cicli produttivi e nel loro business ma quando il rischio ha cominciato a diventare reputazionale e commerciale perché il rispetto dell'ambiente è diventato uno dei driver capaci di orientare le scelte di consumo, la musica, sebbene timidamente, ha iniziato a cambiare.

Certo c'è ancora tanta strada da fare. Il 43% dei consumatori dichiara di non essere capace di proteggere effettivamente la propria privacy per ragioni diverse tra le quali, senza alcuna sorpresa, spicca l'assoluta mancanza di consapevolezza circa i trattamenti dei propri dati personali svolti da una pletora di soggetti diversi. È così per il 79%. Ma è ancora più difficile da accettare che la metà degli utenti e consumatori che si dichiarano incapaci di proteggere i propri dati personali, imputano tale circostanza al fatto di essere "sotto ricatto": se vogliamo usare un servizio siamo costretti a cedere i nostri dati personali, rivelano.

Eppure la voglia di capire e proteggersi non manca. Il 26% degli utenti e consumatori italiani esercitano il diritto di accesso loro

riconosciuto dalla disciplina europea della materia per sapere chi tratta i loro dati, come e perché. Un dato che pone il nostro Paese sopra la media globale che è del 24%. In testa i Paesi nei quali, evidentemente, cittadini e consumatori sentono la loro privacy più minacciata: India (59%), Brasile (34%), Cina e Messico (30%).

E per la più parte dei consumatori è assolutamente chiaro che per sperare di veder tutelata più efficacemente la loro privacy bisogna leggere per davvero le informative sulla privacy (58%) e non rinunciare a gestire i cookie online attraverso i quali inizia la più parte delle attività di tracciamento (53%). Il 51% di utenti e consumatori si aspetterebbe che a difendere la loro privacy siano le Istituzioni nazionali e locali. Il 21% che lo facessero le singole società mentre il 19% ritiene che la difesa debba essere dei singoli e il 9% delle associazioni.

È uno spaccato interessante sul quale bisogna lavorare per fare in modo che, davvero, nell'universo dei dati si attivi una dinamica analoga a quella attivatasi nell'universo dell'ambiente, dell'ecologia e della sostenibilità ambientale, un universo nel quale la battaglia è lontana dal poter essere considerata vinta ma la strada che si sta percorrendo è quella giusta.

Fonte: HuffPostitalia (Guido Scorza, componente Garante Privacy)

L'origine dei dati personali ed il principio di finalità del trattamento: i limiti all'utilizzo dei dati pubblici

L'importanza di trattare i dati secondo le specifiche finalità

Le informazioni contenute in registri pubblici, liberamente consultabili dai professionisti nell'ambito della propria attività, non possono essere così utilizzate per attività promozionali. Il principio di finalità (o di limitazione della finalità) significa per i professionisti e per le aziende che il trattamento dei dati personali deve essere effettuato per una finalità specifica e ben definita e solo per scopi ulteriori, specifici e compatibili con la finalità iniziale.

È questa, in sintesi, la massima che possiamo ricavare da due provvedimenti sanzionatori pubblicati a distanza di 1 anno dal Garante della Privacy italiano e da quello tedesco del Land Baden-Württemberg. Ma vediamo nello specifico le condotte sanzionate dalle due Autorità privacy.

In Germania, il Commissario statale per la protezione dei dati e la libertà di informazione del Land Baden-Württemberg ha inflitto sanzioni da 50.000 euro e 5.000 euro ad un agente immobiliare e un geometra per la raccolta ed il trasferimento illecito di dati e per la violazione degli obblighi di informazione. In particolare, un proprietario di una nuova area di sviluppo aveva ricevuto una lettera da un agente immobiliare in cui gli era stato offerto un prezzo di acquisto per la sua proprietà.

La lettera non conteneva alcuna informazione sull'origine dei suoi dati e, anche quando è stato chiesto, il destinatario non ha ricevuto alcuna risposta. L'autorità ha accertato che un geometra si era avvalso della sua autorizzazione per ispezionare il catasto elettronico e in due casi aveva identificato diverse centinaia di proprietari di immobili a loro insaputa e ha trasmesso tali informazioni ad un agente immobiliare. Quest'ultimo, a sua volta, ha scritto ai proprietari con un'offerta di prezzo di acquisto per i loro immobili senza fornire le informazioni necessarie, in particolare senza informare sull'origine dei dati. Come precisato, non esisteva un rapporto commerciale ed i proprietari non potevano presumere che i loro dati sarebbero stati disponibili nel registro fondiario per scopi pubblicitari. Il fatto che i proprietari di immobili non possano opporsi né all'iscrizione nel registro catastale né alla trasmissione di dati è qui di particolare importanza, in quanto i loro dati sono raccolti sulla base di un obbligo legale.

Tuttavia, questo obbligo legale non serve ad effettuare attività promozionali, ma piuttosto a garantire la certezza del diritto nelle transazioni immobiliari. Inoltre, agli interessati non è stata fornita alcuna informazione sul trattamento dei dati, anche quando sono stati contattati. Tuttavia, questa informazione è un prerequisito essenziale per l'interessato per poter far valere i propri diritti.

Anche il Garante privacy italiano si è pronunciato a seguito di un reclamo per la ricezione di un contatto su Linkedin finalizzato a proporre servizi immobiliari in riferimento ad uno specifico immobile di proprietà. Anche in questo caso, si è contestato l'utilizzo

successivo dei dati acquisiti in un registro pubblico per finalità diverse ed ulteriori rispetto a quelle per cui il registro è stato costituito, e cioè per la verifica della titolarità di un immobile e per esigenze di certezza dei rapporti giuridici.

Fonte: Federprivacy

Data breach: pianificare per prevenire il "panico d'organizzazione"

La simulazione: un buon modo per tenersi pronti a un eventuale data breach

Si dice che il presupposto per gestire correttamente un data breach consista nell'avere un'organizzazione preparata. Ma come? In alcuni approcci viene ad esempio proposta una simulazione di incidente per testare la procedura e individuare eventuali punti critici. Eppure, per quanto tale intervento possa avere un indubbio fascino si pone al di fuori dei margini della pianificazione bensì attiene maggiormente ad una fase di verifica e correzione. Insomma: può essere utile, ma deve quanto meno coordinarsi ad una corretta pianificazione preventiva e soprattutto all'assetto organizzativo predisposto dall'organizzazione.

A differenza di un penetration test che individua vulnerabilità di sicurezza da risolvere, una simulazione di data breach deve essere infatti in grado di individuare criticità anche di natura non strettamente tecnica ma collegate ad aspetti organizzativi e dunque – volendo approssimare – al fattore umano.

Non è infrequente, infatti, che emerga un "panico d'organizzazione" nel momento in cui si entra a conoscenza della compromissione di dati e sistemi, producendo così comportamenti non programmati e soprattutto incoerenti con gli obiettivi di sicurezza e tutela degli interessati. Uno dei fattori più rilevanti che può generare tale esito consiste in una attribuzione di ruoli e responsabilità non definita o incoerente, che ha l'effetto di impattare fortemente sulla capacità di rilevazione o reazione.

Ad esempio, se vengono compromesse tempestività o completezza d'informazione, la ricaduta riguarda tutti i processi decisionali a seguire: analisi, mitigazione, damage control, gestione delle comunicazioni (interne ed esterne) e degli adempimenti normativi. Diventa dunque necessario agire in modo preventivo andando a definire ruoli e responsabilità (anche con una matrice RACI), flussi informativi e andando ad intervenire su possibili "colli di bottiglia" decisionali. In tal senso la comunicazione interna è un elemento critico, cui devono seguire interventi di sensibilizzazione e addestramento relativi alla procedura e alle istruzioni operative fornite.

Tanto la sensibilizzazione che le istruzioni operative devono chiarire a tutti gli operatori autorizzati all'acceso ai dati cosa sia un evento di violazione dei dati personali e cosa fare, fornendo strumenti adeguati alla rilevazione e al reporting, nell'ottica di produrre in ogni caso una registrazione conforme all'obbligo di cui all'art. 33.5 GDPR. Non solo: è necessario che qualora siano o possano essere coinvolti soggetti esterni all'organizzazione si dovranno individuare e contrattualizzare le modalità operative di assistenza, fra cui la definizione di un eventuale Service Level Agreement (SLA).

Il livello logicamente successivo, riguardante invece gli snodi decisionali, richiederà una particolare attenzione nell'individuare

quali soggetti – management, consulenti o funzioni interne – vadano coinvolti perché la progressiva formazione della volontà dell'organizzazione in risposta al data breach sia rendicontabile e conforme tanto ai requisiti normativi che alle best practices di sicurezza.

Fonte: Federprivacy

Responsabile della security di Uber condannato e poi licenziato per aver tenuto nascosto un attacco hacker

Nascondere un data breach è un reato punibile penalmente

L'ex responsabile della sicurezza di Uber, Joe Sullivan, è stato dichiarato colpevole di aver tenuto nascosto un attacco informatico del 2016, che ha portato al furto dei dati personali di oltre 57 milioni di persone tra utenti e dipendenti della compagnia. Le informazioni rubate a Uber comprendevano nomi, indirizzi e-mail e numeri di telefono, oltre ai numeri di patente di 600mila autisti.

Come riportato dal New York Times, la giuria del tribunale di San Francisco ha condannato Sullivan per due capi d'accusa. Il primo per aver ostacolato la giustizia, non avendo rivelato la violazione all'agenzia statunitense per la tutela dei consumatori, la Federal trade commission (Ftc), e il secondo per depistaggio, ovvero l'occultamento di un reato alle autorità.

L'attacco del 2016 è avvenuto a seguito del ritrovamento su Github, sito usato dai programmatori informatici per condividere i codici sorgente dei programmi che stanno sviluppando, delle credenziali di accesso per lo storage di Amazon web services di Uber. Recuperate le credenziali, i cybercriminali hanno scaricato i backup dei database di Uber, per poi contattare l'azienda e ottenere un riscatto di 100mila dollari in bitcoin. I responsabili dell'attacco sono poi stati individuati e nel 2019 hanno ammesso di aver violato i database della compagnia.

Come osserva il New York Times, è la prima volta che un dirigente d'azienda affronta un'azione penale per un attacco informatico e la condanna di Sullivan potrebbe cambiare il modo in cui le aziende affrontano tali incidenti. I pubblici ministeri statunitensi hanno anche dimostrato come Sullivan abbia condiviso i dettagli dell'attacco e del pagamento del riscatto con amministratore delegato di Uber dell'epoca, Travis Kalanick, e con il responsabile per la tutela della privacy dell'azienda. Mentre non avrebbe rivelato alcun dettaglio al consulente legale di Uber, che poi non avrebbe comunicato la reale portata dell'incidente al nuovo amministratore delgato, Dara Khosrowshahi.

Proprio sotto la nuova gestione di Khosrowshahi, Uber ha infine licenziato Sullivan, ha ammesso pubblicamente la violazione, ha pagato 148 milioni di dollari in danni agli utenti coinvolti dall'attacco e risolto il suo caso con i pubblici ministeri lo scorso luglio, promettendo piena collaborazione nel processo contro Sullivan. Il 16 settembre Khosrowshahi ha anche testimoniato contro di lui. Inoltre, nel 2018, dopo aver rivelato l'attacco, Uber ha stretto un accordo con la Ftc promettendo di implementare un programma di tutela della privacy per 20 anni e di "riferire alla Ftc di qualsiasi incidente informatico relativo alle informazioni personali di utenti e dipendenti".

In base a quanto riportato da Bloomberg, secondo i procuratori Sullivan non avrebbe comunicato l'attacco alle autorità

per proteggere la sua reputazione, in quanto avrebbe dovuto migliorare la sicurezza di Uber dopo essere entrato nella società nel 2015. Mentre gli avvocati di Sullivan, come riporta il New York Times, hanno sostenuto come "l'unico obiettivo del signor Sullivan - in questo incidente e in tutta la sua illustre carriera - è stato quello di garantire la sicurezza dei dati personali delle persone su Internet". Ora Sullivan rischia fino a otto anni di carcere per aver ostacolato la giustizia, ma secondo quanto si legge su Bloomberg la pena potrebbe essere molto più breve.

Fonte: Wired

Pentha Memo…

Memorandum sulle scadenze privacy, iniziative, eventi e servizi curati da Pentha e dalla rete di collaboratori (non è quindi esaustivo di tutti gli adempimenti contabili, fiscali, previdenziali e societari obbligatori).

Per ulteriori informazioni siamo a completa disposizione ai recapiti in calce.

Data scadenza	Descrizione
On demand	Corsi di formazione sul Regolamento Europeo Gdpr 2016/679

Le sanzioni del GDPR

Riepilogo di alcune fattispecie di violazione riscontrate dai garanti europei e relativi provvedimenti sanzionatori dopo l'introduzione del GDPR 2016/679

Riportiamo, nella tabella che segue, una selezione di violazioni e contestazioni effettuate dal garante italiano o da quelli di altri paesi europei, con l'indicazione della relativa sanzione applicata all'ambito di attività del destinatario al fine di fornire indicazioni utili, ancorché non precise e/o senza garanzia che sarebbero ugualmente replicabili in casi analoghi, ma significative per valutare l'impatto di una eventuale violazione simile.

Sono state volutamente tralasciate le sanzioni applicate a BIG DATA (Google, Amazon, Facebook ecc.) e alle aziende multiutility (telefoniche, gas ecc.) in quanto difficilmente ripetibili e applicabili alle piccole e medie realtà nazionali.

TIPOLOGIA VIOLAZIONE	***SANZIONE APPLICATA***	***DESTINATARIO***	***ANNO***
Controllo illecito sulla navigazione Internet dei dipendenti	€ 84.000,00	Comune di Bolzano	2021
Mancata o tardiva nomina del Data Protection Officer (DPO)	€ 75.000,00	Ministero delle finanze (MEF)	2021
Accesso indiscriminato ed ingiustificato a dati sanitari	€ 400.000,00	Ospedale portoghese	2020
Misure di sicurezza insufficienti	€ 460.000,00	Ospedale olandese	2020
Inidonea o omessa informativa per finalità commerciali	€ 200.000,00	Azienda polacca	2020
Errata base giuridica (consenso per raccolta dati nei rapporti di lavoro)	€ 150.000,00	Azienda greca	2020
Misure di sicurezza insufficienti	€ 50.000,00	Associazione Rousseau (M5S)	2020
Diffusione illecita di dati	€ 30.000,00	Università italiana	2020
Accesso illecito a dati sanitari	€ 30.000,00	Ospedale italiano	2020
Diffusione illecita dati personali	€ 10.000,00	Comune italiano	2020
Marketing aggressivo	€ 200.000,00	Call Center italiano	2020

Diffusione di dati di c.v.	€ 80.000,00	Ospedale Cardarelli Napoli	2020
Gestione errata procedure di whistleblowing	€ 30.000,00	Università italiana	2020
Comunicazione illecita di dati personali particolari	€ 20.000,00	Università italiana	2020
Comunicazione illecita di dati personali per bugs software FSE	€ 150.000	ASL (con rischio di ribaltamento sanzione ai produttori del sw)	05/2021
Mancato oscuramento dati nel FSE	€ 190.000	ASL (con rischio di ribaltamento sanzione ai produttori del sw)	06/2021
Mancata esposizione cartelli videosorveglianza	€ 3.000	Piccolo Hotel (sanzione parametrata sul fatturato)	11/2020
Poca sicurezza nel software utilizzato e mancata nomina di sub responsabili del trattamento	€ 20.000	Fornitore software segnalazioni Whistleblowing	07/2021
Violazione norme sui cookies	€ 50.000	Giornale Le Figaro	08/2021
Mancata nomina di responsabili/sub responsabili	€ 800.000 al titolare € 400.000 al responsabile € 30.000 al sub responsabile	Roma capitale ATAC spa Flow Bird	07/2021
Chiamate promozionali illecite (anche per acquisizione liste dati da altre società)	€ 3.200.000	Sky Italia	10/2021
Diffusione illecita di dati personali (prescrizioni agli assistiti appese fuori dallo studio con mollette da bucato)	€ 10.000 e pubblicazione sul sito del Garante	Medico MMG italiano	11/2021
Nomina DPO inadeguato	€ 18.000	Azienda Lussemburghese	11/2021
Data breach a seguito di misure di sicurezza deboli	€ 400.000	Vettore aereo (Transavia - Olanda)	11/2021
Mancata denuncia di possibile data breach (anche se poi non si è verificato) a seguito di smarrimento di un plico contenente dati personali spedito a mezzo corriere	€ 87.000	Banca polacca	11/2021
Impedimento all'esercizio dei diritti dell'interessato, mancato riscontro alle richieste dell'interessato	€ 150.000	Tim	12/2021
Registrazione telefonate assistenza clienti in assenza di informativa e accordo sindacale	€ 30.000	Società di trasporto pubblico	12/2021
Utilizzo indebito dei dati dei dipendenti (finalità non dichiarate nell'informativa)	€ 400.000	Società trasporto metropolitano francese	11/2021
Dati dei dipendenti "dimenticati" su un vecchio server on line e non protetto	In via di definizione	Società trasporto metropolitano francese	12/2021
Telemarketing aggressivo	€ 26,5 milioni	Enel Energia	01/2022
Misure di sicurezza insufficienti che hanno comportato la sottrazione e la diffusione di dati particolari	€ 7.000	Fornitore IT (nominato REDT) di una casa di riposo italiana	12/2021
Telemarketing aggressivo: mancata nomina e vigilanza sulla catena degli appaltatori	€ 400.000 € 200.000	Titolare del trattamento	02/2022

	€ 90.000	Responsabile del trattamento (call center) Sub responsabile del trattamento (che non ha risposto al Garante)	
Informativa inidonea (basi giuridiche e data retention non corrette)	€ 7.500 e pubblicazione del provvedimento	ASL Frosinone	01/2022
Sistematica richiesta della fotocopia carte di identità ai propri clienti quale presupposto per esercitare i diritti dell'interessato	€ 525.000	Società editoriale olandese	03/2022
Consenso per finalità di marketing "estorto" all'interessato e caselle pre-flaggate	€ 2.100.000	Banca Spagnola	03/2022
Richiesta casellario giudiziale senza averne motivo	€ 2.000.000	Amazon	02/2022
Telemarketing a numeri reperiti in rete	€ 5.000	Agenzia immobiliare affiliata Tecnocasa	04/2022
Richiesta sproporzionata di dati per accedere al proprio account (richiesta copia bolletta luce per accedere al proprio profilo su società interinale)	€ 240.000	Michael Page società interinale	04/2022
Discriminazione su cittadini presunti evasori fiscali	€ 500.000 + € 2.750.000	Agenzia entrate olandese	04/2022
Riprese con telecamere di aree non di pertinenza del titolare ed assenza di cartelli informativi	€ 2.000	Circolo ricreativo privato	04/2022
Rilevazione temperatura e questionari COVID senza corretta base giuridica	€ 200.000 € 100.000 €20.000	Aeroporto Bruxelles Aeroporto Bruxelles sud Società che somministrava questionari	

Fonte: Pentha s.r.l.

Pentha s.r.l. Servizi Integrati per le Imprese
Via Gobetti, 37 – 12100 Cuneo
Telefono 0171 489095 – Fax 0171 631346
Web www.pentha.eu Mail pentha@pentha.eu
http://www.facebook.com/pages/Pentha-srl-Servizi-Integrati-per-le-imprese/89151469538