PRIVACY News®

ANNO 9 - gennaio/marzo duemila19

CYBERCRIME

ATTACCHI IN CRESCITA: COSA STA SUCCEDENDO?

CODICE PRIVACY IN ITALIA, con il D.Lgs 101 non ci sono più scuse.
Ma le aziende non sono ancora pronte

BIG DATA: la nuova, vera ricchezza dell'economia globale. Ma la PRIVACY?

OMAGGIO PER I SOCI FEDERPRIVACY - Editore: Il Corriere della Privacy Srl - P.I. IT06199650489 - Testata registrata Tribunale di Firenze Reg. N.5871 del 08.05.2012- Direttore Responsabile Nicola Bernardi

8° Privacy Day Forum

l'evento annuale dei professionisti della protezione dei dati personali

Pisa, 19 giugno 2019

CNR Area della Ricerca

FEDERPRIVACY

www.federprivacy.org | urp@federprivacy.it

- Oltre 7.000 partecipanti in sette edizioni
- 40 speech tra plenaria e workshop tematici in altre 4 sale meeting
- Formazione & aggiornamento sul Codice privacy dopo il Dlgs 101/2018
- Tutte le ultime novità per gli addetti ai lavori, e molto altro...

EDITORIALE

Quante volte al giorno controllate la vostra casella di posta elettronica? Un sondaggio di qualche tempo fa evidenziava che il 34% degli utenti controllava la propria email sicuramente più di dieci volte al giorno, ma un altro 54% dichiarava invece che lo faceva immediatamente al ricevimento di ogni singolo messaggio.

Più che un'abitudine, sembra che ormai quella di controllare la posta in arrivo sia diventata per molti quasi un'azione compulsiva, forse per alcuni addirittura la prima cosa che fanno appena aprono gli occhi quando si svegliano la mattina. Ma quale sarebbe la vostra reazione se un giorno nel controllare la mail osservaste che lo schermo del vostro smartphone fosse completamente bianco? E se questo fosse dovuto al fatto che tutti i dati dei server del vostro provider, backup compresi, fossero andati completamente distrutti? Per quanto pensare ad uno scenario del genere possa sembrare per molti surreale ed angosciante, è proprio quello che è realmente accaduto l'11 febbraio scorso agli utenti di un provider di posta elettronica con sede negli Stati Uniti. E deve essere stata una scoperta agghiacciante anche per il fondatore del provider che ha sempre puntato molto sulla sicurezza e sulla privacy nei servizi di posta elettronica che per 18 lunghi anni ha messo a disposizione di migliaia di utenti americani. Almeno fino a quando non è stato bersagliato da un cyber attacco devastante che ha spazzato via un enorme patrimonio di dati accumulato in quasi due decenni di attività.

Secondo quanto infatti riportato dal provider stesso, si è trattato di un attacco hacker distruttivo che nel giro di poche ore ha cancellato non solo tutti i dati dei server, ma anche i file di backup, confermando che "tutti i dischi su tutti i server" erano stati praticamente formattati insieme all'intera infrastruttura dell'azienda.

Un evento tecnologico di una portata catastrofica tale da rendere finora vano ogni tentativo di ripristinare il servizio, tanto che il team dell'azienda ha pubblicato sul proprio sito un messaggio che ha più il tenore di una bandiera bianca che di una rassicurazione per gli utenti: "Considera che i dati della tua casella di posta elettronica siano persi, ma non ci siamo ancora arresi."

Se siete un utente privato che utilizza gratuitamente la mail a scopo personale, sicuramente questo episodio vi dovrebbe convincere una volta per tutte a dotarvi di un efficace sistema di backup che vi permetta di non perdere tutti i vostri file nel caso in cui il vostro provider dovesse rimanere in panne ed abbandonarvi a voi stessi con un semplice annuncio di commiato.

Se siete invece un'azienda, forse sarebbe inoltre opportuno non badare solo alla convenienza del prezzo che vi è offerto per un servizio di internet e posta elettronica professionale, ma guardare anche e soprattutto all'affidabilità del provider, scegliendo un operatore che possieda credenziali degne di fiducia, a partire da una certificazione dei sistemi di gestione della sicurezza delle informazioni , e quando saranno disponibili, anche una delle certificazioni di conformità al GDPR.

In mancanza di adeguate credenziali, se decidete poi di affidare i vostri dati ad un provider che se la suona e se la canta da solo in modo del tutto autoreferenziale, lo farete ovviamente a vostro rischio e pericolo.

Nicola Bernardi | Presidente di Federprivacy | @Nicola_Bernardi

PRIVACY News

EDITORE
Il Corriere della Privacy Srl

CODICE FISCALE E PARTITA IVA
IT06199650489

REDAZIONE
Via Brunetto Degli Innocenti n. 2
50063 Figline Valdarno (FI) - Italy

INDIRIZZI
Via Brunetto Degli Innocenti n. 2
50063 Figline Valdarno (FI) - Italy
Tel: +39 055/5276058
Fax: +39 055/5609184
Email: info@corriereprivacy.it
PEC: corrieredellaprivacy@pec.it
Web: www.corriereprivacy.it

DIRETTORE RESPONSABILE
Nicola Bernardi
nicola.bernardi@corriereprivacy.it

RESPONSABILE COMMERCIALE
Davide Sottili
davide.sottili@corriereprivacy.it

SEGRETERIA DI REDAZIONE
Magda Todor
magda.todor@corriereprivacy.it

COMITATO REDAZIONALE
Nicola Bernardi, Marco Soffientini,
Vittorio Lombardi, Davide Sottili,
Magda Todor, Michele Giannone

GRAFICA E IMPAGINAZIONE
EFFIGE 2.0 - Milano
info@effige.com - www.effige.com

STAMPATO DA
Ingraph - Seregno (MI)
info@ingraph.it - www.ingraph.it

Testata registrata presso il Tribunale di Firenze Reg. N.5871 del 08.05.2012

Questa copia di Privacy News - Il Corriere della Privacy, non è in vendita, ma è distribuita in Italia in direct mailing e spedita gratuitamente in esclusiva agli associati Federprivacy, nonché pubblicata online in versione sfogliabile sul sito www.federprivacy.org. Per scoprire come poterla ricevere e beneficiare di tutti gli altri vantaggi riservati ai soci Federprivacy, vedere pagina 21 di questa rivista, visitare il sito www.federprivacy.org, oppure scansionare il codice QR in questo riquadro:

IL PUNTO DI VISTA

PRIVACY & SOCIETÀ

IN PRIMO PIANO

FOCUS

PRIVACY IN AZIENDA

PRIVACY & SOCIAL

VIOLAZIONI E MULTE

PRIVACY DAL WEB

PRIVACY E CITTADINO

APPUNTAMENTI CON FEDERPRIVACY

Aumentano **ATTACCHI INFORMATICI** e **FURTI DI IDENTITÀ.** Che sta succedendo?

> ***Grazie al GDPR è l'azienda a dover garantire che i dati saranno trattati correttamente*** *mentre sono le autorità di garanzia che dovranno vigilare perché i cittadini da soli non saranno mai in grado di verificare che uso viene fatto dei loro dati*

Prima il furto dei token di Facebook, poi il baco di Google plus e l'annuncio della sua chiusura, infine le denunce di Clusit sull'aumento del furto di credenziali usate per attacchi informatici. Non dovrebbe sorprendere che Censis abbia certificato un calo di fiducia dei cittadini italiani nei confronti delle piattaforme social, dei motori di ricerca e dei servizi online. Che sta succedendo? Ne abbiamo parlato con il Garante della privacy, l'onorevole Antonello Soro. Di seguito una sintesi dell'intervista.

Oggi i dati di milioni di utenti vengono sfruttati come una miniera da sviluppatori, società di ricerche, aziende di marketing, società di servizi di ogni genere. Che cosa stanno facendo le Autorità europee per mettere un freno a questi comportamenti?

"Contro questi abusi, il GDPR rappresenta oggi un formidabile strumento per costringere gli Over The Top a gestire con maggiore trasparenza i dati personali dei loro utenti, a proteggerli con misure adeguate e a limitare in un perimetro chiaro gli usi che di questi dati essi possono fare."

Facebook ha scollegato 90 milioni di utenti della sua piattaforma dopo il furto dei loro token, le "tessere informatiche" che ci identificano e fanno accedere ai servizi online senza dover sempre immettere la password. Ci ha detto tutta la verità?

"Merito del GDPR. Prima del Regolamento europeo la protezione dei dati era considerata, negli Usa, recessiva rispetto alle esigenze del mercato. Il GDPR ci consente di intervenire anche rispetto a imprese situate fuori dall'UE ma che offrano beni o servizi a cittadini dell'Unione. Tutti sanno che dovranno fare attenzione a una platea di 500 milioni di persone, gli europei, e che noi potremo essere incisivi facendo valere le nostre tutele".

"La regola europea vale anche per le imprese non europee che operano stabilmente in Europa. La regola europea si sta facendo strada. Si pensi alla California che ha adottato il Privacy Act sul modello europeo. Lo stesso vale per Canada e Giappone che si sono ispirati all'Europa."

Pare che i dati sottratti a Facebook siano già in vendita nel mercato nero del web. Un altro grosso danno all'immagine di Facebook.

"Se confermato sarebbe molto grave. C'è anche da dire che oggi il danno reputazionale è più importante delle sanzioni. Oggi le aziende sanno che devono competere anche su questo aspetto con i concorrenti che vengono da altri paesi: la protezione dati diviene infatti una risorsa reputazionale importante."

Anche Google non ha ancora ammesso la rilevanza del possibile data breach collegato alla vulnerabilità di Google+ per questioni reputazionali. Sarebbero coinvolti 500 mila profili. Ci sono state denunce presso i suoi uffici?

"Diverse associazioni hanno fatto denunce e molte segnalazioni a difesa dei consumatori. Ci siamo attivati e non da soli. Considerato il carattere transnazionale di queste aziende non ci muoveremo più come singola autorità ma concordemente con le altre autorità europee. Per questo abbiamo creato una piattaforma apposita per lo scambio di informazioni e la cooperazione avanzata".

Fonte: **Agi - Intervista di Arturo di Corinto ad Antonello Soro, Presidente del Garante per la protezione dei dati personali**

CYBERCRIME, attacchi gravi in crescita del 31%

*"**122** è il valore medio di attacchi gravi di cybercrime fatti registrare nel primo semestre 2018"*

La curva dei crimini informatici non ha ancora iniziato il suo tratto discendente. Anzi: dopo il 2016 e 2017, già etichettati come gli anni peggiori, l'anno in corso, con 730 attacchi gravi registrati e analizzati, pari a una crescita del 31% rispetto al semestre precedente, si appresta a battere il primato. Ci sono anche crimini informatici che hanno messo a segno percentuali di crescita a tre cifre, per esempio nel settore auto motive (+200%), e le tecniche, nella maggior parte dei casi, sono alla portata di tutte le tasche dei cyber criminali. È, infatti, il malware semplice, cioè un prodotto a costi decrescenti, il vettore di attacco più utilizzato (40% del totale). Lo scenario è quello delineato dalla nuova edizione del Rapporto Clusit, redatto dall'Associazione italiana per la sicurezza informatica. A conferma del quadro negativo del rapporto Clusit, ci sono anche le percentuali dello studio «The State of Cyber Resilience 2018» di Accenture, diffuso lo scorso 11 ottobre, nell'ambito della World Energy Week andata in scena a Milano, secondo cui gli attacchi causati da personale interno alle organizzazioni sono più frequenti (33%) rispetto agli attacchi esterni (28%) che sono, però, in crescita.

Il cybercrime è fuori controllo. In termini numerici, si legge nel Rapporto Clusit, nel 2017 si è assistito a una crescita del 240% degli attacchi informatici rispetto al 2011, anno a cui risale la prima edizione del rapporto Clusit, e del 7% rispetto al 2016. Ma più che il dato numerico, spaventa l'elemento qualitativo: oggi il fenomeno intralcia non solo la vita privata dei cittadini, ma anche il piano finanziario e geopolitico. Leggendo tra le cifre, emerge che il cybercrime (il cui scopo è sottrarre informazioni, denaro, o entrambi), è sempre la prima causa di attacchi gravi a livello mondiale (76% degli attacchi complessivi, in crescita del 14% rispetto al 2016).

Ma sono già in corsia di sorpasso gli attacchi compiuti con finalità di Information Warfare (la cosiddetta guerra delle informazioni) con il +24% rispetto al 2016 e il cyber espionage (lo spionaggio con finalità geopolitiche o di tipo industriale, tra cui va ricompreso il furto di proprietà intellettuale), che cresce del 46%. Ad accrescere lo stato di allerta ci sono i dati sui costi, quintuplicati, per un importo complessivo di 500 miliardi di dollari nel 2017 (circa 435 miliardi di euro).

Non fa ben sperare l'anno in corso: nel primo semestre si è registrata una media di 122 attacchi gravi al mese (rispetto ai 94 al mese nel 2017). In linea con i dati precedenti, nei primi sei mesi del 2018 il cybercrime è stato la causa dell'80% degli attacchi informatici a livello globale, risultando in crescita del 35% rispetto all'ultimo semestre 2017; ad aumentare maggiormente quest'anno (69% rispetto ai sei mesi precedenti) sono però le attività riferibili al cyber espionage.

Secondo Clusit, «sempre più gli attacchi prescindono sia da vincoli territoriali che dalla tipologia dei bersagli. L'aumento di attacchi gravi perpetrati ai danni di un target disomogeneo e diffuso geograficamente su scala globale dimostra la capacità, la determinazione e l'organizzazione degli attaccanti, che puntano a massimizzare il risultato economico con un approccio tipico della criminalità organizzata».

LEGGI L'ARTICOLO ON-LINE

Fonte: **Italia Oggi**

CYBERCRIME costa ad aziende 5.200 miliardi di dollari

*Il **settore higt-tech** è quello che nei **prossimi 5 anni** correrà i rischi maggiori con un aumento dei costi in cyber security*

LEGGI L'ARTICOLO ON-LINE

"A livello mondiale possono essere 5.200 miliardi di dollari i costi addizionali e i mancati ricavi delle aziende nel corso dei prossimi cinque anni dovuti ai cyber-attacchi, poiché la dipendenza da modelli di business abilitati da Internet è attualmente di gran lunga superiore all'abilità di introdurre misure di sicurezza adeguate in grado di proteggere asset strategici". E' il nocciolo di un analisi condotta da Accenture su oltre 1.700 Ceo e top manager di aziende in diversi Paesi.

Per quattro intervistati su cinque (79%) il progresso dell'economia digitale sarà seriamente compromesso se non ci sarà un netto miglioramento della sicurezza su Internet, mentre oltre la metà (59%) ritiene che il Web sia sempre più instabile sotto il profilo della cyber-sicurezza e non sa come reagire.

Al contempo, tre quarti degli intervistati (75%) ritengono che sia necessario uno sforzo congiunto per far fronte alle sfide in materia di cyber security, in quanto nessuna organizzazione è in grado di risolvere il problema da sola.

Più della metà dei dirigenti (56%) si definisce sempre più preoccupata della sicurezza su Internet e vedrebbe con favore l'entrata in vigore di norme di business più rigorose introdotte da istituzioni o autorità governative.

Secondo lo studio, il cybercrime "pone sfide significative in quanto può compromettere le attività aziendali, la crescita e l'innovazione del business, nonché l'introduzione di nuovi prodotti e servizi, con un costo per le aziende di migliaia di miliardi di dollari". Ovviamente, scrive Accenture, "il settore high-tech, con oltre 753 miliardi di dollari di costi emergenti, corre i rischi maggiori, seguito da life science e automotive, la cui esposizione ammonta rispettivamente a 642 e 505 miliardi di dollari".

Fonte: **Ansa**

GARANTE PRIVACY UE: le persone devono sapere se sono profilate, da chi e come

> ***Il nuovo sistema**, prevede Buttarelli, **reggerà 7-10 anni**, poi si inizierà a discutere di come aggiornarlo, il futuro va discusso adesso*

La materia è delicata, ma inevitabile "non possiamo tornare ai pizzini e ai volantini, non possiamo tornare alla carta perché non investiamo abbastanza in sicurezza". Le domande al Garante europeo per la Protezione dei Dati, in occasione della presentazione del rapporto annuale del suo ufficio, scivolano rapidamente verso i problemi di trasparenza legati alla prossima campagna elettorale europea, e Giovanni Buttarelli al suo ultimo anno di mandato quinquennale (ma non è ancora detto che non si ricandidi) non si tira indietro.

Anche la Piattaforma Rousseau è un esempio della necessaria evoluzione della politica. "I pro e i contro di questa piattaforma, per chi la ama e chi no, devono servire a fare un passo avanti nella democrazia elettronica… tornare ai pizzini o ai volantino non va bene". Ma la democrazia elettronica deve crescere, "non è solo quella all'interno di un partito politico, ma riguarda anche consultazioni di Comuni, Reagioni…". Ma ci sono problemi, in Olanda ad esempio ricorda "si sono dovuti fare dei passi indietro circa alcuni test di voto elettronico (che pure comincia ad essere un passo inevitabile) perché ci sono stati rumors di interferenze di potenze straniere, ma non possiamo tornare alla carta perché non investiamo tanto in chiave di sicurezza". Nonostante l'esperienza olandese però, secondo Buttarelli le interferenze straniere nella campagna elettorale per le europee "per ora sono state meno del previsto, grazie ai tanti interventi di regolazione che si stanno attuando".

Secondo il Garante la raccolta di dati personali "per finalità di propaganda elettorale è legittima, ma è molto diversa da quella commerciale", e spiega che "non si può raccogliere un dato per aziende di nostra fiducia e poi vederlo passarlo a organizzazioni politiche che mi mandano un messaggio per votare un rappresentante politico, e poi dicono 'avevamo il suo consenso'".

E qui si apre anche un altro problema da gestire: "Un sistema di profilazione può definirci bene, ma può anche sbagliare – avverte Buttarelli – ed in quel caso allora c'è discriminazione di fatto, perché verrò classificato in una maniera non corretta, non sarò 'io'". per il Garante europeo inoltre "le persone devono poter sapere se sono profilate, e con quale profilo".

Il grande regolamento del settore è quello chiamato "GDPR", entrato in servizio oramai quasi un anno fa, con il quale siamo stati inondati di mail di aziende e organizzazioni varie che ci chiedevano di confermare il nostro consenso all'utilizzo dei nostri dati. Questo sistema, prevede Buttarelli, "reggerà 7-10 anni, poi si inizierà a discutere di come aggiornarlo, ma – ammonisce – il futuro va discusso adesso, questo diremo alla politica dopo le prossime elezioni".

LEGGI L'ARTICOLO ON-LINE

Fonte: EU News

DATA BREACH, più di un milione i dati violati nei primi quattro mesi di GDPR

A quattro mesi dalla piena operatività del GDPR, in Europa è già iniziata la corsa alle segnalazioni che riguardano casi di violazioni dei dati personali. Così anche in Italia, dove dal 25 maggio a oggi, sono almeno un milione i cittadini i cui dati sono stati persi, modificati o divulgati senza autorizzazione. Ma la cifra è ampiamente sottostimata in quanto non c'è obbligo da parte dei titolari di un trattamento di dati di informare l'Autorità sulla quantità di profili coinvolti. Le notifiche, che devono essere inviate dal titolare di un trattamento di dati entro 72 ore dalla scoperta di un data breach, hanno riguardato principalmente il furto o lo smarrimento di dispositivi che contengono informazioni.

Chi non segnala i data breach - «È importante che il GDPR funzioni da stimolo per gli investimenti sul rafforzamento della sicurezza informatica - spiega il Garante europeo della protezione dei dati, Giovanni Buttarelli -, anche perché un sistema sicuro oltre ogni dubbio non può esistere e l'aggiornamento deve essere costante».

Guardando i dati italiani confrontati con gli altri Paesi europei (Italia: più di due notifiche al giorno, di cui 34 a luglio e 58 ad agosto. Francia: dal 25 maggio a oggi, sono state 3.767. Regno Unito: 1.750 solamente a luglio) è possibile ipotizzare che «in molti casi i data breach non vengano segnalati, soprattutto da parte di aziende o professionisti che hanno subito una qualche violazione di dati personali. Il costo nel caso di una violazione sarebbe altissimo soprattutto dal punto di vista reputazionale, anche perché nei casi più gravi sarebbe necessario inviare una notifica a tutti i soggetti coinvolti (ossia agli interessati al trattamento) e sarebbe alta la possibilità di perdere affidabilità agli occhi della clientela..

Nel caso in cui un'organizzazione trascuri di notificare una violazione all'Autorità infatti, questa può incorrere in sanzioni fino a dieci milioni di euro (o fino al 2% del fatturato annuo totale se superiore a dieci milioni di euro). Ben più impegnative sarebbero le sanzioni amministrative pecuniarie nel caso in cui l'organizzazione non rispetti altre norme del regolamento alla cui violazione potrebbero conseguire sanzioni amministrative pecuniarie fino a venti milioni di euro (o fino al 4% del fatturato annuo mondiale se superiore a 20 milioni di euro). Oltre alle responsabilità penali introdotte o modificate dal D.Lgs 101/2018 che armonizza il Codice Privacy al GDPR.

Tra l'altro, la violazione recidiva delle disposizioni del GDPR, rappresenta uno degli elementi che il Garante utilizza nella valutazione della gravità della violazione e, di conseguenza, nell'irrogazione della sanzione. Ma c'è anche da considerare che il GDPR è un'evoluzione, non una rivoluzione. E chi rispettava le normative previgenti non ha avuto grossi problemi nell'adeguarsi.

Per prime le società delle telecomunicazioni e le Pubbliche Amministrazioni, per le quali l'obbligo di notificare al Garante una fuga di dati era già previsto e le cui segnalazioni sono state venti dal 1 gennaio al 25 maggio. Ma l'obbligo è previsto anche per le violazioni informatiche che non coinvolgono dati personali, che in questo caso non devono essere inviate al Garante ma solo all'Agenzia per l'Italia Digitale (Agid) e che solo nel mese di luglio sono state 724.

> ***72 ore** dalla scoperta di un **data breach** è il tempo entro il quale deve essere inviata dal titolare di un trattamento di dati la notifica all'ufficio del Garante per la protezione dei dati*

LEGGI L'ARTICOLO ON-LINE

Fonte: **La Stampa**

DATA BREACH: online archivio di email e password

> ***773 milioni*** *di indirizzi email univoci e poco meno di* ***22*** *milioni di password uniche*

Un mastodontico "bottino" di data breach è stato trovato online, sul servizio di hosting Mega, e sarebbe l'ennesima notizia del suo genere se non fosse per le dimensioni: in un archivio nominato Collection #1 erano contenuti quasi 2,7 miliardi di righe, corrispondenti a 87 GB di dati, raccolti da migliaia di fonti differenti. Il risultato di diversi hackeraggi compiuti in passato e poi raccolti in un'unica gigantesca lista. Eliminando i doppioni, il database conteneva quasi 773 milioni di indirizzi email univoci e poco meno di 22 milioni di password uniche.

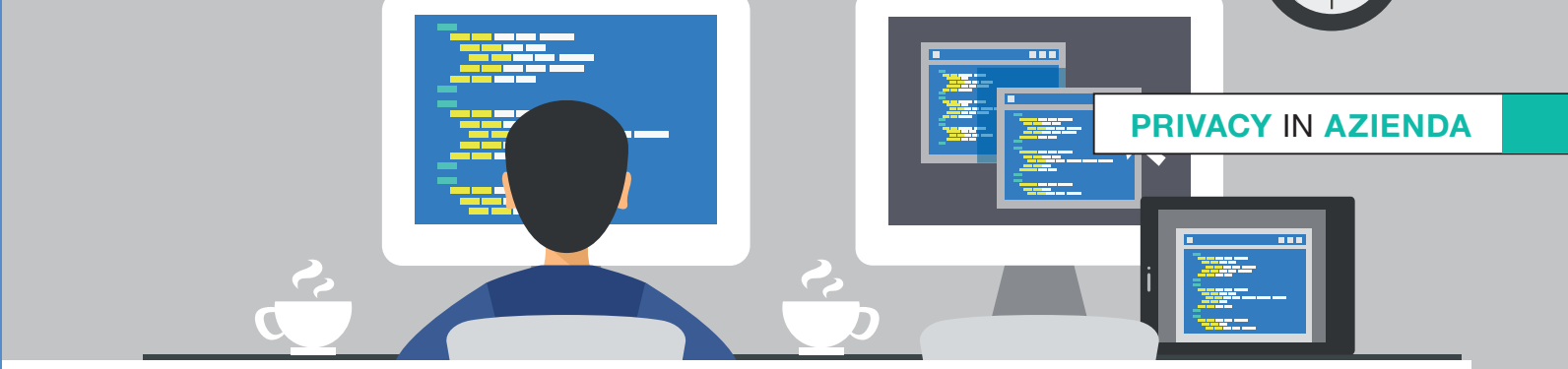
La scoperta è stata segnalata dal noto ricercatore di sicurezza Troy Hunt, l'autore di Have I been pwned. Per chi non lo conoscesse, si tratta di un servizio che permette di verificare in poche mosse se la propria casella di posta sia finita nel "bottino" di qualche operazione di furto dati, anche risalente ad anni addietro: digitando un indirizzo all'interno della maschera di ricerca si visualizzano i riferimenti della violazione o delle violazioni informatiche che hanno permesso a soggetti ignoti di ottenere quella email. Gli utenti registrati possono anche verificare se la propria email sia stata oggetto di data breach che hanno ottenuto dati "sensibili", quali password o numeri di carta di credito. In alternativa, anche chi non è registrato può fare una simile verifica con il motore di ricerca Password pwned.

E il problema di Collection #1 sono proprio le password. Alcune, tra cui quella dello stesso Hunt, erano chiaramente leggibili cioè non più crittografate tramite hashing. "Posso dire che i miei dati personali sono presenti e accurati e che indirizzi email e password da me usate molti anni fa sono corretti", ha scritto il ricercatore, a conferma della validità dei contenuti del database.

La parzialissima buona notizia è che l'archivio è stato ora rimosso da Mega, a seguito di alcune segnalazioni di utenti sul forum del servizio di hosting. La cattiva è che "se siete all'interno di questo breach", ammonisce Hunt, "una o più password che abbiate usato in passato stanno circolando, esposte agli occhi altrui". Insomma, a distanza di anni persistono ancora le conseguenze di passate violazioni informatiche di massa, come quelle ai danni di Dropbox nel 2014, di Yahoo (attaccata a più riprese) e di Tumblr nel 2016.

LEGGI L'ARTICOLO ON-LINE

Fonte: **ICT Business**



VIOLAZIONI INFORMATICHE, una su 5 arriva dai dipendenti

> *Nelle aziende **in aumento le violazioni** imputabili a dipendenti o soggetti interni e la loro scoperta è tardiva*

Secondo un recente report rilasciato da Verizon, le violazioni imputabili a dipendenti o soggetti interni alle aziende sono in aumento e la loro scoperta è di solito molto tardiva, impiegando diversi mesi almeno nel 65% dei casi. La prima motivazione che muove chi agisce dall'interno è, prevedibilmente, il profitto personale, con il 47,8% dei casi analizzati in cui un dipendente è stato corrotto o ha venduto di sua volontà dei dai rubati in azienda.
Il secondo motivo, però, è più preoccupante, in quanto nel 23,4% dei casi l'interno ha rubato dati o causato violazioni informatiche per il semplice gusto di farlo. Questo significa che è complesso capire fino in fondo le motivazioni che spingono queste persone e per rendere le cose più semplici Verizon ha raccolto in 5 categorie differenti il personale di fornitori che tipicamente rappresenta un pericolo per i dati aziendali.
La prima è quella in cui trova posto il lavoratore distratto: una persona che ha scarsa considerazione per le politiche di sicurezza dell'azienda e installa programmi non autorizzati, sposta dati su dispositivi non autorizzati o, più in generale, compie azioni non approvate dal dipartimento It e delle quali i responsabili restano all'oscuro, rendendo difficile chiudere le falle che questi lavoratori aprono verso l'esterno.
La seconda è quella del classico dipendente insoddisfatto, una persona che danneggia l'azienda per la quale lavora o nella quale si trova temporaneamente per un sentimento di rivalsa. Di solito questa categoria tende a distruggere i dati piuttosto che inviarli all'esterno.
Come terza classificazione troviamo il tipico fornitore incompetente, un partner commerciale che non ha implementato politiche di sicurezza adeguate e accede in modo improprio, o tramite equipaggiamenti compromessi, alle risorse aziendali.
Si passa poi alla categoria dei criminali per scelta che si divide in due. La prima è quella degli agenti infiltrati, ovvero dipendenti che sono stati contattati da concorrenti o organizzazioni criminali per compiere del lavoro sporco dall'interno in cambio di denaro.
L'altra categoria dei criminali per scelta è quella dei dipendenti che agiscono di propria iniziativa e rubano dati da vendere poi ad acquirenti senza scrupoli. Costoro non sono stati avvicinati dall'esterno, ma hanno intuito una possibilità di profitto e si muovono in prima persona per cercare chi potrebbe pagarli.
Molto spesso, le minacce dall'interno sono sottovalutate nel processo che porta a costruire le difese informatiche di un'azienda e questo giustifica i lunghi tempi che trascorrono prima della scoperta dei problemi. Per fortuna, al giorno d'oggi non mancano le contromisure in grado di rilevare anche i più subdoli movimenti interni e sono conosciute come tecnologie e pratiche di "Threat Hunting".
Sotto questo cappello viene raggruppato tutto ciò che può portare a scoprire una violazione che abbia già oltrepassato il perimetro esterno e stia operando all'interno dell'azienda. L'uso del Threat Hunting è importantissimo anche per limitare i danni delle intrusioni informaticheperpetrate da soggetti esterni e quindi la sua corretta implementazione aumenta sensibilmente la robustezza delle difese aziendali.

LEGGI L'ARTICOLO ON-LINE

Fonte: **Il Sole 24 Ore**

CODICE PRIVACY IN ITALIA: il quadro normativo è completo senza più alibi per le imprese

*Con **il D.Lgs 101/2018 il quadro normativo è completo** e non ci sono più alibi per le aziende. il Garante in questi primi otto mesi, nell'erogare le sanzioni, terrà conto del fatto che siamo in una fase iniziale di attuazione*

LEGGI L'ARTICOLO ON-LINE

Pubblicato in Gazzetta Ufficiale lo scorso 4 settembre, il Decreto 10 agosto 2018 n.101 di adeguamento al GDPR è entrato in vigore il 19 settembre 2018 e crolla l'ultimo alibi per le aziende: temporeggiare non è più possibile per adeguarsi alle nuove, stringenti regole a tutela della privacy dei cittadini europei. Il decreto è il modo in cui l'Italia adegua la propria normativa alla rivoluzione privacy voluta dall'Europa, nota appunto con il nome di GDPR (General data protection regulation).

È vero che le regole sono già scattate il 24 maggio (quando il regolamento GDPR è entrato automaticamente in vigore), ma si aspettava il decreto italiano per adeguare la normativa nazionale alle forti novità.

Ossia per ora si eviterà di essere troppo punitivi verso le aziende ritardatarie. Si eserciterà una certa gradualità. Il legislatore va incontro così a quanto richiesto dal Parlamento (nel parere dato dalla Commissione speciale Camera e Senato a questo decreto), che però addirittura avrebbe voluto una temporanea sospensione delle ispezioni del Garante.

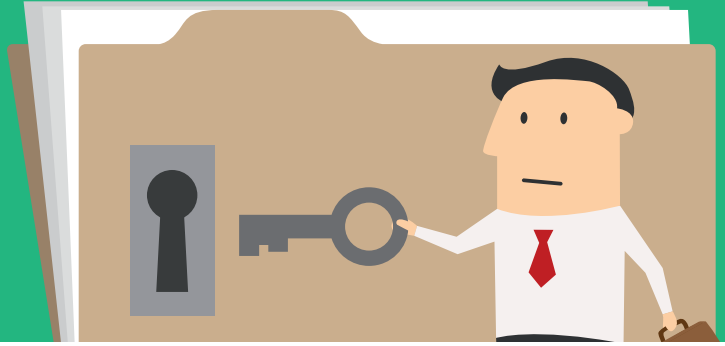
Il tutto è un forte indizio, comunque, su quanto siano in ritardo le aziende italiane nell'adeguarsi, rischiando così sanzioni fino a 20 milioni di euro o il 4% del fatturato globale. Per aiutare la vita delle PMI, un'altra delle novità del decreto è che si chiede al Garante Privacy di promuovere linee guida per fissare modalità di adeguamento semplificate ad hoc per loro.

"Adesso le regole sono complete e l'arbitro può fischiare il calcio d'inizio", dice Modafferi.

L'arbitro sarà appunto il Garante Privacy, che in questi giorni farà ispezioni, sanzioni. Ma non solo. "Restano da fare ancora alcune regole di secondo livello, da parte del Garante Privacy, come previsto dal decreto", aggiunge.

Tra le regole in arrivo, ce ne sono alcune che faranno la differenza per la ricerca e il mercato nell'ambito sanitario. Introdurranno infatti modalità innovative per l'uso di big data sanitari, genetici, biometrici dei cittadini, nel rispetto della loro privacy. La promessa di fondo è la possibilità di usare grandi masse di dati per migliorare l'attività di prevenzione e cura grazie alle tecnologie di intelligenza artificiale.

Fonte: Repubblica



DPO: obbligo, requisiti, compiti, e certificazioni

> *Nonostante le molteplici informazioni fornite dall'Autorità Garante,* ***sono ancora molte le aziende e le pubbliche amministrazioni*** *che* ***conoscono*** *poco la figura del* ***Data Protection Officer***

Tra le novità introdotte dal GDPR, c'è la figura del Responsabile della Protezione dei Dati o "Data Protection Officer" (DPO). Benché l'Autorità italiana per la privacy vi abbia dedicato abbondante documentazione sul proprio sito istituzionale, pubblicando anche un'apposita scheda informativa, molte aziende e pubbliche amministrazioni conoscono ancora poco questa figura. Utile è sicuramente un riepilogo delle principali informazioni che occorre conoscere per adeguarsi alle nuove regole:

DESIGNAZIONE - Devono nominare obbligatoriamente un DPO tutte le pubbliche amministrazioni ed enti pubblici, eccetto le autorità giudiziarie. L'obbligo riguarda anche tutti i soggetti (enti e imprese) che nelle loro attività principali trattano su larga scala dati sensibili, relativi alla salute o alla vita sessuale, genetici, giudiziari e biometrici, oppure che svolgono attività in cui i trattamenti richiedono il controllo regolare e sistematico degli interessati. Un gruppo di imprese o soggetti pubblici possono nominare un unico DPO. Le imprese, che non ricadono invece nell'obbligo di legge, possono comunque decidere di dotarsi ugualmente di un DPO. Il titolare del trattamento deve comunicare i dati di contatto del DPO all'Autorità di Controllo attraverso l'apposita procedura online.

COMPITI - Il DPO, ha il compito di informare e consigliare il titolare o il responsabile del trattamento da lui preposto, nonché i dipendenti, in merito agli obblighi derivanti dal Regolamento Europeo e dalle altre disposizioni dell'UE o delle normative locali degli Stati membri relative alla protezione dei dati. Deve poi verificare che la normativa vigente e le policy interne del titolare siano correttamente attuate ed applicate, incluse le attribuzioni delle responsabilità, la sensibilizzazione e la formazione del personale, ed i relativi audit. Su richiesta, deve fornire pareri in merito alla valutazione d'impatto sulla protezione dei dati, sorvegliandone poi i relativi adempimenti. Il DPO funge inoltre da punto di contatto sia con il Garante della Privacy che con gli interessati, che possono rivolgersi a lui anche per l'esercizio dei loro diritti. E' consentito assegnare al DPO ulteriori compiti e funzioni, a condizione che non diano adito a un conflitto di interessi e che questi gli consentano di avere a disposizione il tempo sufficiente per l'espletamento dei compiti attribuiti dall'art.39 del Regolamento Europeo.

REQUISITI - I titolari del trattamento devono designare come DPO un professionista che possiede una conoscenza specialistica della normativa e delle prassi di gestione dei dati personali, che sia in grado di adempiere alle proprie funzioni in piena indipendenza e in assenza di conflitti di interesse, operando come dipendente, oppure anche sulla base di un contratto di servizi. E' richiesto inoltre che il titolare metta a disposizione del DPO personali le risorse umane e finanziarie necessarie all'adempimento dei suoi compiti.

CERTIFICAZIONI - Allo stato attuale, non esistono titoli abilitanti o attestati formali che determinano l'idoneità di un DPO. Tuttavia, eventuali certificazioni delle competenze professionali, specialmente quando sono rilasciate da enti indipendenti di terza parte, costituiscono un valido strumento ai fini della verifica del possesso di un livello di conoscenza della disciplina.

LEGGI L'ARTICOLO ON-LINE

Fonte: **Federprivacy**

FACEBOOK tutti possono trovarvi dal vostro numero di cellulare

> *Nonostante sia possibile nasconderli, numero di telefono, l'indirizzo email e il **numero di cellulare** possono ancora essere usati per **cercare l'utente** in determinati casi*

Qualche tempo fa, con l'intento dichiarato di migliorare la sicurezza, Facebook introdusse l'autenticazione a due fattori. Chi la adotta, per fare login su Facebook non deve soltanto inserire la password ma anche un codice univoco che gli viene inviato tramite SMS sul cellulare.
Ovviamente - diceva Facebook presentando il sistema - questo numero telefonico viene adoperato unicamente per le operazioni di autenticazione e non è condiviso con gli altri utenti della piattaforma. Chi lo desidera può pubblicare il proprio numero di cellulare tra i dettagli del proprio profilo tramite le solite opzioni.
Tutti hanno accettato questa spiegazione sino a che Jeremy Burge, di Emojipedia, ha pubblicato un tweet in cui accusava Facebook di usare il numero di telefono indicato per l'autenticazione a due fattori anche per altri fini.
In particolare, quel numero può anche essere usato per cercare l'utente che ne è proprietario, e non c'è modo di disattivare questa possibilità, che viene attivata come impostazione predefinita: al limite si può restringerne l'uso ai soli Amici (o agli Amici degli amici).
Burge non ha tutti i torti. Sebbene infatti sia possibile nascondere il proprio numero di telefono, l'indirizzo email e il numero di cellulare possono ancora essere usati per cercare l'utente in determinati casi, per esempio «qualcuno carica le informazioni di contatto su Facebook dal cellulare», come spiega un articolo dell'Aiuto di Facebook.
Questa decisione di Facebook non è soltanto una seccatura e una potenziale minaccia per la privacy: può avere ripercussioni anche su quella sicurezza che l'autenticazione a due fattori dovrebbe contribuire a rafforzare (e in effetti rafforza, se fatta come si deve).
L'esperto di sicurezza Zeynep Tufekci, intervenuto sulla questione, commenta infatti: «Usare la sicurezza per indebolire ulteriormente la privacy è una mossa vile, soprattutto perché i numeri di telefono possono essere "dirottati" per indebolire la sicurezza» con pratiche come il SIM swapping.
Tufekci sottolinea come a questo punto gli utenti debbano aver ben chiaro che qualsiasi dato fornito a Facebook non può più essere considerato privato, nemmeno un numero di telefono ufficialmente adoperato soltanto «per ragioni di sicurezza».
Facebook, dal canto proprio, non sembra particolarmente preoccupata della figuraccia che questa scoperta le sta facendo fare. Anzi, per bocca di un portavoce ha precisato che questo comportamento - la possibilità per tutti di cercare gli utenti attraverso i numeri di telefono - «non è una novità» ed è «applicata a qualsiasi numero di telefono che venga aggiunto al profilo».

LEGGI L'ARTICOLO ON-LINE

Fonte: La Repubblica

La **PRIVACY 4.0** ridisegna il **SISTEMA SANZIONATORIO** per punire gli illeciti

> *Il **decreto legislativo n. 101/2018** va a disciplinare le sanzioni penali che caratterizzeranno la nuova era **"digitale"** della protezione dei dati*

Le modifiche al codice della privacy per adeguare la normativa italiana al GDPR introducono nuove ipotesi di reato per chi non è in regola. L'obiettivo è aggiornare la disciplina in materia di trattamento dei dati alle esigenze della digital transformation, all'impiego delle nuove tecnologie, al fenomeno dei big data e dei grandi archivi. Il decreto legislativo n. 101/2018, pensato per adeguare la normativa nazionale italiana alle disposizioni del GDPR (già in vigore dal 2016, e attuato dal 25 maggio 2018), contiene una parte che va a disciplinare le sanzioni penali che caratterizzeranno la nuova era "digitale" della protezione dei dati.

Nuove sanzioni - il testo finale del decreto, che va a modificare il Codice privacy del 2003 rimasto, così, in vita in quelle parti non disciplinate (o non in conflitto) con il Regolamento, prevede delle fattispecie di reato e ha allargato il quadro precedente con nuove ipotesi più adatte ai tempi tecnologici.

Trattamento illecito di dati - In primis, la vecchia ipotesi del trattamento illecito di dati è rimasta ben salda nell'articolo 167 del Codice Privacy, e apre il Capo II dedicato, appunto, agli "Illeciti penali".

L'articolo in questione diventa, però, più complesso e si articola in tanti punti ben distinti. Il primo stabilisce che chiunque, al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato, effettua operazioni di trattamento dei dati in violazione di specifiche disposizioni di legge e arreca nocumento all'interessato, è punito con la reclusione da sei mesi a un anno e sei mesi. Più grave è l'ipotesi prevista dal secondo punto, dove entra l'ipotesi "classica" (e più generica) di trattamento illecito e secondo la quale chiunque, al fine di trarre per sé o per altri profitto ovvero per arrecare danno all'interessato, procedendo al trattamento di dati personali (anche in violazione di misure di garanzia) arreca nocumento all'interessato, è punito con la reclusione da uno a tre anni. La stessa pena si applica, nota il terzo punto, a chi proceda al trasferimento dei dati personali verso un Paese terzo o un'organizzazione internazionale al di fuori dei casi consentiti. Quest'ultima diminuita, secondo il quarto punto, se è stata applicata e riscossa una sanzione amministrativa.

Comunicazione e diffusione illecita di dati personali - Un nuovo articolo, il 167-bis, introduce un'ipotesi innovativa volta a punire chiunque comunichi o diffonda, al fine di trarre profitto per sé o altri ovvero al fine di arrecare danno, un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala. La pena prevista è la reclusione da uno a sei anni.

Acquisizione fraudolenta di dati su larga scala - La terza ipotesi, prevista dall'articolo 167-ter punisce chiunque, al fine di trarne profitto per sé o altri ovvero di arrecare danno, acquisisce con mezzi fraudolenti un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala. La pena prevista è la reclusione da uno a quattro anni.

Falsità nelle dichiarazioni al Garante - Infine, l'articolo 168 punisce chiunque, in un procedimento o nel corso di accertamenti dinanzi al Garante, dichiari o attesti falsamente notizie o circostanze o produca atti o documenti falsi. La pena prevista è la reclusione da sei mesi a tre anni.

LEGGI L'ARTICOLO ON-LINE

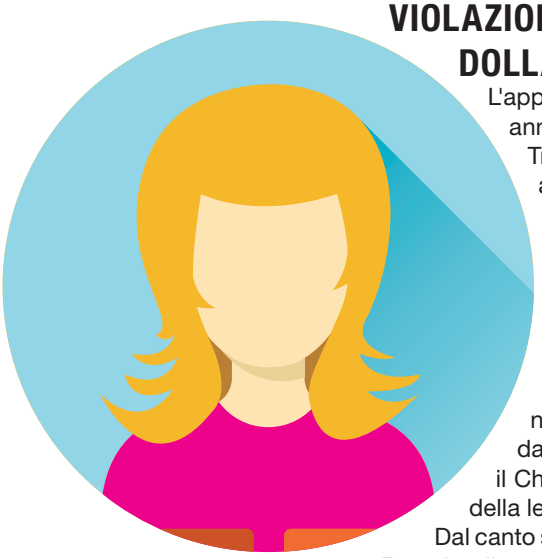
Fonte: **IPSOA Quotidiano - Articolo a cura di Giovanni Ziccardi**

USA: ATTACCO HACKER CATASTROFICO A PROVIDER DI POSTA ELETTRONICA, CANCELLATI TUTTI I DATI DEGLI UTENTI

VFEmail.net, un provider di posta elettronica sicuro con sede negli Stati Uniti ha perso tutti i dati e anche i file di backup dopo che degli hacker sconosciuti hanno distrutto l'intera infrastruttura statunitense, cancellando nel giro di poche ore e senza una ragione apparente un enorme patrimonio di dati accumulato in quasi due decenni di attività. Avviato nel 2001 da Rick Romero, VFEmail fornisce servizi di posta elettronica privati e sicuri a società e utenti finali, sia gratuiti che a pagamento. Descrivendo l'evento come "catastrofico", dopo aver notato che tutti i server del suo servizio erano offline senza alcun preavviso, il provider di servizi di posta elettronica americano, che ha sempre affermato di puntare molto sulla privacy degli utenti, ha reso noto che l'attacco ha avuto luogo l'11 febbraio 2019, e che "tutti i dati" sui propri server statunitensi, sia primari che di backup, sono stati comp Al momento non pare essere in vista alcuna soluzione, tanto che sul proprio sito il team di VFEmail.net scrive ai propri utenti: "Considera che i dati della tua casella di posta elettronica siano persi, ma non ci siamo ancora arresi." Tuttavia, poco dopo, VFEmail ha confermato che "tutti i dischi su tutti i server" erano stati cancellati, formattando praticamente l'intera infrastruttura dell'azienda, inclusi gli host di posta, gli host di macchine virtuali e un cluster di server SQL, in poche ore.

Fonte: The Register

VIOLAZIONE PRIVACY DI MINORI: MULTA DA 5,7 MILIONI DI DOLLARI PER L'APP TIKTOK



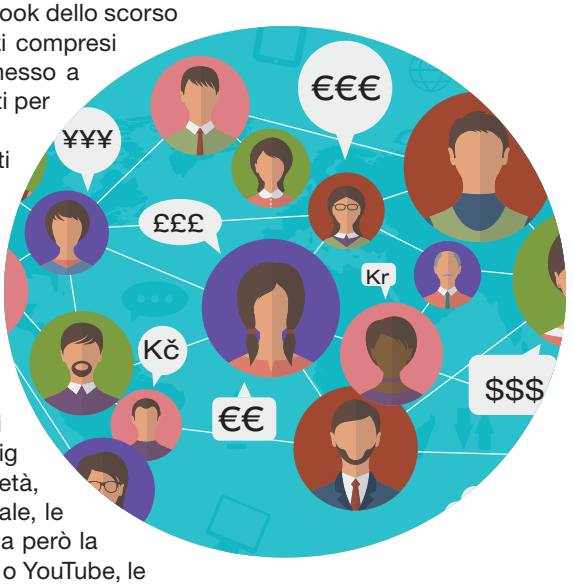
L'app musicale TikTok - creata in Cina ma oggi di proprietà di Bytedance, che lo scorso anno l'ha fusa con l'altra propria controllata Musical.ly - è stata multata dalla Federal Trade Commission, ente statunitense preposto alla tutela dei consumatori, per aver violato la privacy dei propri utenti minorenni: la sanzione record da 5,7 milioni di dollari è stata comminata per una palese violazione del Children's Online Privacy Protection Act, legge che negli USA regola la protezione della privacy dei minorenni in Rete, che vieta la raccolta di dati sensibili dai minori di 18 anni senza il consenso dei genitori o dei tutori legali. "L'operatore era a conoscenza del fatto che la app fosse utilizzata da minorenni, eppure ha deliberatamente mancato di ottenere il consenso dei genitori prima di raccogliere nomi, indirizzi email e altri dati sensibili di utenti di età inferiore ai tredici anni", si legge in una nota diramata dalla Federal Trade Commission: "Questa sanzione record serva da monito ai titolari di servizi online dedicati ai minoti: prendiamo molto sul serio il Children's Online Privacy Protection Act, e non tollereremo la flagrante violazione della legge da parte delle società".

Dal canto suo TikTok, oltre che a pubblicare video tutorial sulla salvaguardia della privacy in Rete, ha disposto per gli utenti minorenni un app "parallela" a quella ufficiale che non permetta in alcun modo la condivisione o la cessione di dati sensibili.

Fonte: Rockol

BIG DATA: PRIVACY VENDESI. ECCO QUANTO VALIAMO PER AMAZON E YOU TUBE

Opinioni, desideri, foto e commenti sono la nuova ricchezza delle multinazionali del web. Secondo quanto rilevato dal quotidiano britannico The Independent (che riprende i dati di una ricerca effettuata dalla società Money Guru), sul dark web, i dati personali degli utenti, ottenuti dopo l'attacco hacker a Facebook dello scorso mese di settembre, vengono infatti ora offerti al miglior acquirente a prezzi compresi tra un minimo di 3 a un massimo di 12 dollari. L'attacco informatico ha messo a rischio più di 50 milioni di profili e i dati "trafugati" potrebbero essere utilizzati per commettere furti di identità o per ricattare gli utenti.



Solo per il recente furto a Facebook, ai prezzi indicati, il valore dei dati rubati sarebbe quindi compreso tra 150 e 600 milioni di dollari. Il problema del valore dei big data non riguarda però solo le azioni criminali, ma anche l'economia legale. L'acquisizione dei big data può infatti avvenire con diverse modalità lecite: accedendo ad Api (Application Programming Interface) messe a disposizione dai servizi web; utilizzando software di web scraping; importando i dati da database con strumenti già usati per la movimentazione di dati in sistemi di Data Warehousing; leggendo flussi continui di dati tramite sistemi capaci di catturare eventi, elaborarli e salvarli in modo efficiente su un database. Questi dati vengono poi filtrati da informazioni ridondanti, inaccurate o incomplete. Quando parliamo di big data, del resto, ci si riferisce quasi sempre a dati sensibili: informazioni sull'età, sul sesso, le preferenze e i desideri di acquisto, ma anche la posizione attuale, le abitudini, i viaggi, etc. L'esempio più rilevante di utilizzo dei big data riguarda però la sfera del marketing. Quando andiamo su Amazon, ma anche su eBay, Netflix o YouTube, le proposte mostrate dai banner sembrano rivolte proprio a noi e ai nostri gusti; e non si tratta di una coincidenza.

Nel campo del marketing i big data servono a profilare, permettendo di proporre in modo mirato prodotti o servizi sulla base di necessità o preferenze personali. I big data possono, dunque, essere raccolti, aggregati, analizzati, profilati, trasmessi e rivenduti e sono la nuova, vera, ricchezza dell'economia globale. Conoscere le abitudini dei consumatori è oggi un "asset" fondamentale per tutte le aziende. Ma quanto valgono davvero questi dati? Un interessante studio del Wall Street Journal ha stabilito che ciascuno di noi vale per Facebook 80,95 dollari, i nostri amici 0,72$ ciascuno e la nostra pagina completa quasi 1.800$.

Fonte: Affaritaliani.it

WHATSAPP, BUG NELLE VIDEOCHIAMATE: DIETRO LO SQUILLO C'È L'HACKER

Ancora una grana per Facebook sul fronte della protezione dei dati personali degli utenti. Questa volta l'azienda di Menlo Park ha avuto a che fare con un bug che ha colpito WhatsApp e che poteva permettere agli hacker di acquisire il pieno controllo dell'applicazione di messaggistica. Per entrare nel servizio WhatsApp bastava che gli utenti presi di mira rispondessero a una videochiamata.

Il bug ha interessato il servizio WhatsApp sia su cellulari Android che iPhone e Facebook ha riparato la falla nei giorni scorsi, come svelato dai media Usa. Facebook non ha indicato se il bug sia stato effettivamente usato per portare a termine degli attacchi. La vulnerabilità è stata scoperta a fine agosto da un team di ricerca di Google Project Zero; il ricercatore Travis Ormandy ha commentato su Twitter: "Questo era veramente un problema gigantesco, bastava rispondere a una chiamata in arrivo da un potenziale hacker e l'applicazione WhatsApp sarebbe stata completamente compromessa". Per Facebook si tratta dell'ennesimo problema legato alla sicurezza degli utenti. Dopo lo scandalo Cambridge Analytica, con cui una app sviluppata da terzi ha avuto accesso illecito ai dati di 87 milioni di iscritti del social network, a fine settembre l'azienda di Menlo Park ha rivelato un'intrusione che ha messo a rischio almeno 50 milioni di profili di cui almeno 5 milioni in Unione europea. L'attacco hacker potrebbe costare al social network di Mark Zuckerberg anche una multa fino a 1,63 miliardi di dollari dalle autorità Ue, se verrà accertata una violazione delle norme della General data protection regulation (Gdpr).

L'intrusione del social network è stata resa possibile, ha spiegato la società, dallo sfruttamento da parte di "attori esterni" di tre vulnerabilità che riguardano la funzione 'Visualizza come' e la nuova versione del caricamento video introdotta a luglio 2017, che a sua volta ha generato in modo errato un token di accesso all'app mobile di Facebook. Facebook ha già provveduto a rimediare i bug.

Fonte: Il Corriere delle Comunicazioni

LAVORO: necessarie POLICY CHIARE all'utilizzo dei post sui social

> *Tutto quello che viene scritto sui social, anche fuori dall'orario di lavoro, può essere usato contro un lavoratore, se ha* ***contenuti offensivi verso il datore di lavoro*** *e i colleghi*

L'utilizzo dei social media diventa ogni giorno di più un argomento critico sul posto di lavoro: la crescente sensibilità delle aziende verso le comunicazioni dei propri dipendenti, unita all'uso sempre più massiccio che questi fanno delle comunicazioni "social", aumenta in maniera esponenziale il rischio di conflitti su questo tema. Conflitti che sono acuiti da un problema: il confine tra le condotte lecite e quelle illecite non è sempre facile da definire.

Il concetto generale che i lavoratori devono fissare – ma che troppo spesso, ingenuamente, dimenticano – è che tutto quello che viene scritto sui social, anche fuori dall'orario di lavoro, può essere usato contro di loro, se ha contenuti offensivi verso il datore di lavoro e i colleghi. Spesso i lavoratori dimenticano che i social media sono piattaforme aperte a una massa indistinta di persone (anche quando si usano filtri di accesso ai propri profili) e così, varcando il sottile confine fra libertà di espressione e dignità altrui, si espongono anche a responsabilità per possibili illeciti penali, come la diffamazione.

Un'invettiva che può generare un danno d'immagine all'azienda, un insulto di troppo al superiore, la rivelazione di fatti che dovrebbero restare riservati, sono tutti esempi di come il dipendente può essere sanzionato, sul piano disciplinare, per via di un post mal riuscito su Facebook, Twitter, LinkedIn o simili.

Il caso più frequente è quello delle offese verso l'azienda e i suoi dirigenti. La giurisprudenza sul tema ha un approccio rigoroso e poco tollerante, anche se prevale l'analisi del caso concreto; in generale, a fronte di decisioni che riconoscono la possibilità di licenziare per giusta causa chi pubblica frasi offensive verso l'azienda o i colleghi sui social, non mancano decisioni che escludono la rilevanza disciplinare delle comunicazioni che, pur avendo contenuti caratterizzati da un forte antagonismo, restano entro i limiti della satira o della critica.

Considerato che molto spesso i lavoratori hanno poca coscienza dei limiti (e dei rischi) connessi all'utilizzo dei social media, sarebbe opportuno e consigliabile elaborare delle specifiche policy aziendali, con le norme di comportamento da tenere in materia di utilizzo dei social network.

I casi visti sinora, seppure complessi, hanno sempre un'attinenza, diretta o indiretta, con il rapporto di lavoro. Ma che succede se il dipendente posta sui social media messaggi che, pur essendo particolarmente sconvenienti (testi razzisti, incitamento alla violenza o alla droga, e così via), non c'entrano nulla con il lavoro? Una risposta certa ancora non esiste, ma è probabile che la strada che seguiranno i giudici sarà simile a quanto già accade di fronte a condotte che non rilevano direttamente sul rapporto di lavoro (per esempio un dipendente viene arrestato per spaccio di droga): tali condotte possono essere contestate solo se l'impresa prova che hanno incidenza negativa sul rapporto di lavoro.

LEGGI L'ARTICOLO ON-LINE

Fonte: **Il Sole 24 Ore**

LAVORATORE CONTROLLATO
da remoto ma solo se informato

*“Nell’era della **tracciabilità totale** difendere il fronte del divieto di controllo a distanza sui lavoratori è tanto impossibile quanto inopportuno”*

La nuova disciplina dei controlli sul lavoro ha segnato una svolta nell’approccio a questa controversa problematica. Da un lato, ha ridimensionato il ruolo delle autorizzazioni sindacali o amministrative, esentando le imprese dal richiederle per installare gli strumenti strettamente finalizzati al lavoro. Dall’altro, ha osato prevedere che le informazioni acquisite tramite strumenti autorizzati o esentati sono utilizzabili anche a fini disciplinari, purché siano state acquisite nel rispetto della normativa privacy. L’intenzione era quella di sollevare le imprese da alcuni oneri autorizzatori e dare loro maggiori certezze sulla fattibilità dei controlli, in cambio dell’osservanza delle regole privacy. Che la scommessa riuscisse dipendeva, però, da diverse variabili: che il concetto di “strumento di lavoro” non fosse inteso troppo restrittivamente; che le imprese rinfrescassero ed eventualmente adeguassero i loro codici privacy, in specie migliorando le informative ai lavoratori; che il Garante si facesse carico delle nuove responsabilità, ma a partire dal concetto che quando insiste in un ambiente caratterizzato da un potere di controllo la privacy deve rassegnarsi a qualche passo indietro, a pena di provocare fenomeni di rigetto. Quest’ultimo punto merita qualche attenzione in più. A detta di alcuni, il ruolo della disciplina della privacy, di recente rinnovata dal GDPR e dal decreto attuativo, non sarebbe cambiato alla luce della riforma dei controlli: come valeva prima, la privacy vale adesso. Si tratta, a mio giudizio, di una conclusione frettolosa. Il fatto che il nuovo art. 4 abbia posto il rispetto di quella disciplina (l’unica, tra l’altro, a riguardare le modalità dei controlli, visto che le autorizzazioni concernono l’installazione degli strumenti) come condizione dell’utilizzazione probatoria delle informazioni acquisite per tale via rappresenta una novità di rilievo, sia perché rafforza l’effettività di quelle norme, sia perché conduce, o dovrebbe condurre, a interpretarle in un certo modo. Sarebbe paradossale, infatti, se da condizione per poter utilizzare i dati raccolti la privacy si trasformasse in un impedimento di fatto alla possibilità di raccoglierli. Da cui la ragionevolezza del principio secondo cui i controlli informatici debbono poter essere effettuati in alcune circostanze e a certe condizioni. Due esempi possono dare un’idea. In alcune decisioni il Garante ha affermato che la rilevazione di anomalie del servizio può giustificare un controllo, ma mostrandosi sempre restio ad acconsentire che, nel gestirlo, possa essere varcata la soglia del carattere anonimo del dato. È una posizione che potrebbe essere rimeditata. Dovrebbe poi essere ammesso un controllo mirato su un dipendente qualora sia emersa una plausibile ragione di sospetto nei suoi confronti. Ciò detto, sarebbe ardito ritenere verificate, ad oggi, queste varie condizioni, per quanto vi siano segnali di metabolizzazione del nuovo approccio. Fatto sta che anche dalle sentenze delle Corti europee si ricava una sostanziale conferma dell’indirizzo riformatore, che, saltando qualche passaggio, sintetizzerei così: il lavoratore può essere controllato anche da remoto purché ne sia preventivamente informato e i controlli non siano eccessivamente invasivi e in generale sproporzionati.

LEGGI L’ARTICOLO ON-LINE

Fonte: **Il Sole 24 Ore**

CONDOMINIO a norma con la privacy dopo il GDPR

Qual è il ruolo dell'amministratore? E quali sono i suoi doveri? Quali dati si possono trattare?
Con il GDPR anche il condominio deve trattare i dati in modo corretto

LEGGI L'ARTICOLO ON-LINE

Il GDPR ha ribadito la necessità di un corretto trattamento dei dati personali in ambito condominiale.

Il ruolo dell'amministratore - Poiché il condominio non ha una propria personalità giuridica, risulta impossibile qualificarlo quale titolare del trattamento dei dati personali della compagine condominiale. I singoli condomini, di conseguenza, non possono che essere riconosciuti, reciprocamente, quali contitolari dei predetti dati personali. Più controverso è invece determinare il titolo in base al quale l'amministratore è tenuto a trattare i dati dei condomini. Da un punto di vista di fatto è innegabile che sia proprio quest'ultimo a compiere la maggior parte delle operazioni di trattamento dei dati personali relativi alla gestione del condominio. Di conseguenza si potrebbe concludere che anche quest'ultimo debba essere a sua volta qualificato come titolare del trattamento. Tuttavia lo stesso non può che essere qualificato come titolare autonomo e non come contitolare (assieme ai condomini) del trattamento.

L'alternativa a tale soluzione sarebbe invece quella di considerare l'amministratore quale responsabile (esterno) del trattamento dei dati. In questo caso l'assemblea dovrebbe allora procedere a deliberare espressamente detto incarico, impartendogli le necessarie istruzioni scritte alle quali lo stesso dovrebbe poi scrupolosamente attenersi.

I dati personali che possono essere trattati - I dati personali che l'amministratore può trattare indipendentemente dal consenso dei condomini interessati sono rappresentati dai rispettivi dati anagrafici, necessari per la gestione e l'amministrazione delle parti comuni. Un discorso a parte va fatto per quanto riguarda l'utilizzo del numero di telefono e dell'indirizzo di posta elettronica dei condomini.

Per quanto riguarda il primo, l'Autorità Garante ha sempre negato che l'amministratore potesse disporne senza il consenso dell'interessato, qualora lo stesso non risultasse nemmeno dagli elenchi pubblici. In ogni caso, come evidenziato dall'Autorità Garante, occorre che l'amministratore, nel fare uso del recapito telefonico dei condomini, tenga sempre ben presente il principio di proporzionalità tra gli interessi della gestione delle parti comuni e della riservatezza dei privati. In tutti i casi l'utenza telefonica del condomino non può essere comunicata dall'amministratore a terzi estranei alla compagine condominiale Discorso analogo si può fare per quanto riguarda l'indirizzo di posta elettronica per così dire semplice. La posta elettronica certificata, al contrario, è stata espressamente individuata dal legislatore quale mezzo per l'invio degli avvisi di convocazione delle assemblee condominiali quindi utilizzabile anche senza il consenso del condomino interessato.

La morosità condominiale – Secondo l'Authority il trattamento da parte del condominio dei dati relativi alla morosità dei condomini è, sul piano generale, del tutto lecito e può comportare anche una giustificata comunicazione di dati tra i soggetti interessati nell'ambito del condominio; al contrario, il trattamento di dati realizzato per esempio mediante la predetta esposizione in bacheca, così come in altre analoghe forme, relativamente a una presunta situazione di morosità, si pone in contrasto con i principi di pertinenza e di non eccedenza.

Fonte: **Italia Oggi**

06 2019	10	Master Privacy Officer & Consulente della Privacy "Executive" - 56° edizione	Roma	Palazzo dell'Informazione
06 2019	19	Privacy Day Forum 2019	Pisa	CNR - Area della ricerca
09 2019	9	Master Privacy Officer & Consulente della Privacy "Executive" - 57° edizione	Milano	Istituto Pirelli
09 2019	17	Corso di formazione manageriale per Data Protection Officer	Pisa	CNR - Area della ricerca
11 2019	18	Master Privacy Officer & Consulente della Privacy "Executive" - 58° edizione	Figline Valdarno (Firenze)	Villa Casagrande

LEGGI GLI APPUNTAMENTI ON-LINE

FEDERPRIVACY **Federprivacy** è la principale associazione in Italia il cui più importante scopo è radunare tutti i professionisti della privacy e della protezione dei dati, nonché tutti gli altri addetti ai lavori che si occupano di tali tematiche, come i consulenti della privacy, data protection officer e privacy officer. Anche coloro che aspirano ad acquisire una qualificazione nell'ambito della privacy possono beneficiare di tutti i vantaggi e le soluzioni riservate agli associati, per il migliore svolgimento delle proprie attività in conformità della legislazione vigente.
Federprivacy è una associazione apolitica, aconfessionale, indipendente, senza scopo di lucro e le sue finalità sono le seguenti:
- **promuovere** con ogni mezzo la divulgazione, la conoscenza ed il rispetto delle normative vigenti in materia di privacy e protezione dei dati su tutto il territorio nazionale ed internazionale
- **assistere, rappresentare e tutelare** gli associati in tutte le sedi in cui siano coinvolti direttamente o indirettamente gli interessi collettivi degli associati
- **fornire** direttamente o indirettamente agli associati **servizi, prodotti, aggiornamenti, assistenza e informazioni su tematiche e problematiche** connesse alle loro attività inerenti la privacy e la protezione dei dati
- **fornire** agli associati linee guida ed orientamenti in materia di privacy e protezione dei dati da assumere ed adottare a livello collettivo
- **svolgere la funzione di osservatorio e di centro di ricerca** indirizzato a monitorare i fenomeni e le evoluzioni della privacy e della protezione dei dati
- **cooperare** con autorità, istituzioni, enti pubblici ed altre associazioni per conseguire la migliore interpretazione ed applicazione della normativa vigente in materia di privacy e protezione dei dati
- **perseguire e promuovere** l'attuazione di normative riguardanti il trattamento e la protezione di dati personali ed altre materie affini adeguate ai reali contesti socio-economici nazionali ed internazionali, salvaguardando sempre il diritto fondamentale alla riservatezza dell' individuo
- **contribuire alla crescita tecnica e professionale** di tutti gli associati, anche mediante corsi di qualificazione, di aggiornamento e di specializzazione, l'istituzione di borse di studio
- **perseguire e promuovere** la valorizzazione e lo sviluppo delle **professioni** afferenti la privacy e la protezione dei dati
- redigere, aggiornare e far rispettare il proprio codice etico e deontologico e le proprie norme di autoregolamentazione
- svolgere in generale ogni attività, anche arbitrale, che sia nell'interesse degli associati.

PERCHÉ DIVENTARE SOCIO

Iscrivendoti a Federprivacy, entri a far parte della principale associazione di professionisti della privacy, e potrai:
- Ricevere l'**attestato di qualità** rilasciato da Federprivacy per distinguerti nello svolgimento della tua professione
- Ricevere la **newsletter settimanale** e le **circolari** per essere costantemente aggiornato
- Aggiornare la tua preparazione professionale con **formazione ad hoc, meeting e convegni**
- Ricevere **gratuitamente e in esclusiva il magazine** trimestrale Privacy News (3 numeri cartacei e 1 numero digitale)
- Accedere a **moduli, schemi, formule e check list**
- Consultare gratuitamente la **banca dati giuridica** in materia di privacy
- Pubblicare on line nel **Registro Soci** la tua **scheda personale** per una maggiore visibilità

DIVENTA SOCIO

INFORMAZIONI

Privacy News - Il Corriere della Privacy

EDITORE & STAMPA- Il Corriere della Privacy Srl - Codice Fiscale e Partita iva IT06199650489 - Sede Legale: Via Brunetto Degli Innocenti n. 2 - 50063 Figline Valdarno (FI) - Italy -Indirizzo postale: Via Brunetto Degli Innocenti n. 2 - 50063 Figline Valdarno (FI) - Italy - Testata registrata presso il Tribunale di Firenze Reg. N.5871 del 08.05.2012 - La rivista è stampata da Ingraph, Seregno (MI)- finito di stampare a marzo 2019.

ABBONAMENTI - Privacy news è un magazine trimestrale edito da il Corriere della Privacy, che non è in vendita, ma viene distribuito, nonché reso disponibile nella versione sfogliabile sul sito www.federprivacy.org, in direct mailing, e spedito in omaggio a tutti i soci Federprivacy in regola con il pagamento delle quote associative annuali. Se si desidera leggere Privacy News del Corriere della Privacy, ma non si è soci Federprivacy, è comunque possibile farlo accedendo alla versione sfogliabile sul sito www.corriereprivacy.it.

AUTORI & PUBBLICAZIONI - Tutti i contributi pubblicati da Privacy News del Corriere della Privacy sono concessi dai rispettivi autori a titolo del tutto gratuito. Per proporre la pubblicazione di articoli, casi accaduti, fotografie, o qualsiasi altro genere di materiale nel Corriere della Privacy, dopo aver preso visione dell'informativa sul trattamento dei dati personali, scrivere a redazione@corriereprivacy.it

NOTE LEGALI - La redazione di Privacy News del Corriere della Privacy si applica per garantire la completezza e la correttezza dell' informazione; tuttavia non si assume responsabilità per il materiale contenuto nel giornale, né per quello elaborato a propria cura, né per quello fornito dagli autori che collaborano con la nostra testata. Qualora dovessero essere segnalati degli errori, si provvederà a correggerli. I contenuti del giornale possono non essere esaurienti, completi, precisi o aggiornati; possono essere ripresi da fonti esterne quali agenzie di stampa o altri fonti pubbliche per i quali non si assume alcuna responsabilità. Non è possibile garantire l'esatta rispondenza dei testi dei provvedimenti normativi resi disponibili in linea con quelli ufficialmente adottati. Pertanto, ai fini legali, l'unico testo giuridico valido resta quello pubblicato dal Garante per la protezione dei dati personali e sulla Gazzetta Ufficiale, che prevalgono sempre in caso di discordanza.

PUBBLICITÀ SUL MAGAZINE PRIVACY NEWS E ONLINE SUL SITO WEB WWW.CORRIEREPRIVACY.IT

Pagina pubblicitaria interna magazine Euro 700,00 + iva
Seconda e terza pagina di copertina magazine Euro 900,00 + iva
Quarta di copertina magazine Euro 1.200,00 + iva
Articolo publiredazionale magazine cartaceo e online Euro 300,00 + iva.
Banner online 150x150 pixel - CPI (Costo per impressione*) Prezzo €0.001
Banner online 990x40 pixel - Testata - CPI (Costo per impressione*) Prezzo: €0.0015
Banner Footer online 990x100 pixel - CPI (Costo per impressione*) Prezzo: €0.0007
Formati accettati: per pubblicità online JPEG,JPG,PNG,GIF, SWF (FLASH) **per pubblicità magazine cartaceo** PDF JPEG,JPG,PNG,GIF.
Per pubblicare inserzioni pubblicitarie sul magazine e sul sito www.corriereprivacy.it contattare Il Corriere della Privacy, scrivendo a info@corriereprivacy.it.

INFORMATIVA PRIVACY

Vi informiamo che, per l'esecuzione dei rapporti con i propri clienti ed iscritti, Il Corriere della Privacy Srl raccoglie i dati a questi riferiti, acquisiti anche verbalmente, direttamente o tramite terzi, qualificati come "dati personali" dal Regolamento UE 2016/679 e dal D.Lgs. n. 196/2003.
La normativa in oggetto prevede innanzitutto che chi effettua trattamenti di dati personali è tenuto ad informare il soggetto interessato su quali dati vengano trattati e su taluni elementi qualificanti il trattamento, che, in ogni caso deve avvenire con correttezza liceità e trasparenza, tutelando la Vostra riservatezza ed i Vostri diritti. Pertanto forniamo le seguenti informazioni:
Titolare del Trattamento Il Titolare del trattamento dei Vostri dati personali è Il Corriere della Privacy Srl con sede legale in Via Degli Innocenti n.2 – 50063 Figline Valdarno (FI). Il Titolare è contattabile all'indirizzo email info@corriereprivacy.it o all'indirizzo email privacy@corriereprivacy.it
Natura dei dati trattati Trattiamo i dati anagrafici e fiscali, nonché i dati di natura economica che sono necessari per lo svolgimento dei rapporti con gli iscritti. Generalmente, non trattiamo alcun dato qualificabile come "particolare" o di natura giudiziaria; qualora si rendesse necessario trattare dati di questo tipo, richiederemo preventivamente il consenso dell'interessato.
Finalità del trattamento I dati dei nostri iscritti vengono trattati per espletare loro i servizi richiesti, per il conseguimento delle finalità associative, e in relazione alle esigenze contrattuali ed ai conseguenti adempimenti degli obblighi legali e fiscali, nonché per consentire una efficace gestione dei rapporti finanziari, commerciali e amministrativi. I dati verranno trattati per tutta la durata del rapporto ed anche successivamente, per l'espletamento di obblighi di Legge e per finalità amministrative e commerciali.
Modalità del trattamento Il trattamento dei dati avviene mediante l'utilizzo di strumenti e procedure idonei a garantirne la sicurezza e la riservatezza e potrà essere effettuato sia mediante supporti cartacei, sia attraverso l'ausilio di strumenti elettronici per il tempo strettamente necessario a conseguire le finalità per cui sono stati forniti.
Base giuridica del trattamento, obbligo o facoltà di conferire i dati e conseguenze dell'eventuale rifiuto
I dati vengono trattati al fine di adempiere agli obblighi previsti da leggi, da regolamenti e dalla normativa comunitaria, ovvero da disposizioni impartite da Autorità a ciò legittimate dalla Legge e da organi di vigilanza e controllo. Per quanto concerne questo tipo di dati il loro mancato conferimento da parte dell'aderente comporterà l'impossibilità di instaurare o proseguire il rapporto, nei limiti in cui tali dati sono necessari all'esecuzione dello stesso.
Per quanto riguarda i dati che non siamo obbligati a conoscere, questi verranno trattati sulla base del consenso dell'interessato e il loro mancato ottenimento sarà da noi valutato di volta in volta, e determinerà le conseguenti decisioni rapportate all'importanza per noi dei dati richiesti e da Voi non conferitici.
Comunicazione e diffusione I dati che raccogliamo dai nostri iscritti, non vengono da noi "diffusi", con tale termine intendendosi il darne conoscenza a soggetti indeterminati in qualunque modo, anche mediante la loro messa a disposizione o consultazione, fatta eccezione di alcuni dati dei soci quali, nominativo e/o ragione sociale, recapiti telefonici, fax, indirizzo web e di posta elettronica aziendali. I dati personali dell'interessato potranno invece essere da noi "comunicati", con tale termine intendendosi il darne conoscenza ad uno o più soggetti determinati, nei seguenti termini:-a soggetti incaricati all'interno della nostra Struttura di trattare i dati, ed in particolare agli addetti all'Ufficio amministrazione,- a soggetti che possono accedere ai dati in forza di disposizione di Legge, o di normativa comunitaria, nei limiti previsti dalla Legge;-a soggetti che hanno necessità di accedere ai dati per finalità ausiliarie al rapporto intercorrente, nei limiti strettamente necessari per svolgere i compiti ausiliari loro affidati (es. gli istituti di credito e gli spedizionieri);-a soggetti nostri consulenti, nei limiti necessari per svolgere il loro incarico presso di noi, previa nostra lettera di incarico che imponga il dovere di riservatezza e sicurezza nel trattamento dei dati.
I diritti dell'interessato Il Regolamento UE 2016/679 conferisce agli interessati l'esercizio di specifici diritti. In particolare, in relazione al trattamento dei Vostri dati personali, avete diritto di chiedere:
l'accesso ai Vostri dati; la rettifica; la cancellazione; la portabilità dei Vostri dati; la limitazione del trattamento; l'opposizione al trattamento.
Inoltre, potete proporre reclamo nei confronti dell'Autorità, che in Italia è il Garante per la Protezione dei Dati Personali.
In qualsiasi momento, potete chiedere di esercitare i Vostri diritti all'indirizzo di posta elettronica privacy@corriereprivacy.it, fax +39 (0)55 56.09.184, indirizzo postale: Via Brunetto Degli Innocenti n. 2 - 50063 Figline Valdarno (FI) - Italy.

FEDERPRIVACY

Corso di formazione manageriale

DATA PROTECTION OFFICER

con il patrocinio del
CNR Area della Ricerca di Pisa

Area della Ricerca di Pisa
Consiglio Nazionale delle Ricerche

TÜV SÜD Italia

con il riconoscimento
di TÜV Italia

- **18 GIORNI FULL IMMERSION**
- **124 ORE TRA MATERIE DEL DIRITTO E DELL'INFORMATICA**
- **MATERIALE DIDATTICO PER APPROFONDIRE**
- **ESERCITAZIONI ED ESAME FINALE**
- **ATTESTATO DI COMPETENZA**

Specializzati come **DATA PROTECTION OFFICER**

Non perdere tempo, iscriviti!
Classe a numero chiuso

per maggiori informazioni: **formazione@federprivacy.it**

FEDERPRIVACY

- Più di 2.000 professionisti associati
- 10.000 lettori della nostra newsletter
- Attestato di Qualità ai sensi della Legge 4/2013
- Polizza RC Consulenza Privacy in convenzione
- Formazione & aggiornamento professionale
- Certificazione Privacy Officer con TÜV Italia

Associazione professionale iscritta presso il Ministero dello Sviluppo Economico

www.federprivacy.org | urp@federprivacy.it | @Federprivacy | Numero Verde 800 910 424

QR Code: Chi siamo