ENTRA IN VIGORE IL GDPR

SALE LA SPESA PER LE IMPRESE IN SICUREZZA IT E ASSESSMENT

Il 25 maggio scatta il nuovo regolamento europeo sulla privacy. Uno studio di Idc prevede un esborso di 26 milioni di euro per le società in campo sanitario perché contestualmente è cresciuta la consapevolezza dell'importanza della tutela dei dati. Altro elemento a pesare sui bilanci sarà la consulenza di esperti per l'adeguamento: un grande ospedale può spendere fino a 150 mila euro

Alessio Chiodi
AboutPharma and Medical Devices
achiodi@aboutpharma.com

L'arrivo del nuovo Gdpr non sarà indolore da un punto di vista economico. Il cambiamento implica uno stravolgimento delle regole del gioco e le aziende healthcare lo sanno bene. Dovranno investire in un nuovo apparato che permetta una maggiore sicurezza dei dati e della privacy. Per quanto non sia facile valutare questo impatto, è possibile ricavare alcuni parametri di spesa. La società di ricerca di mercato Idc propone alcuni spunti sugli investimenti in sicurezza It della sanità italiana (aziende e operatori sanitari). Secondo le più recenti stime, nel 2018, Idc prevede una spesa da parte degli operatori e delle aziende sanitarie di circa 26 milioni di euro con un Cagr dell'8,3% tra il 2016 e il 2021. Più nel dettaglio, in Europa occidentale Idc prevede che la spesa in sicurezza It (in tutti i settori) direttamente correlata al Gdpr crescerà con un Cagr 2017-2021 del 19,5%. Il picco della spesa in sicurezza influenzata dal Gdpr si avrà, sempre secondo Idc, l'anno prossimo, nel 2019, con investimenti aziendali che supereranno i 3,7 miliardi di dollari. In Italia, la spesa in sicurezza It trainata dal Gdpr crescerà nel medesimo arco di tempo con un Cagr del 15,3% e culminerà anch'essa nel 2019 sfiorando i 230 milioni di dollari. Quest'anno, Idc prevede per le imprese italiane, un valore di spesa di quasi 200 milioni di dollari.

LA SITUAZIONE ITALIANA

"Le aziende e gli operatori sanitari sono in linea con il sistema Italia in generale. La spesa It è la più alta in ottica di compliance verso il nuovo regolamento privacy". A dirlo è Silvia Piai, Emea senior research manager di Idc Health Insights. "Quest'estate abbiamo fatto una survey in Italia. Il 15% delle aziende si dichiaravano 'Gdpr' compliant. Gli altri avevano piani abbastanza solidi per l'adeguamento. L'Italia è in una situazione medio-avanzata anche se non a livello di altri Paesi come la Germania, dove però il settore sanità poteva già fare riferimento ai regolamenti attuativi già adottati. Questo è un aspetto importante per il settore", continua Piai. Il primo tassello per gli investimenti riguarda l'analisi del rischio e la governance dei dati. "La nuova generazione di tecnologie di cybersecurity e per garantire la privacy – continua Piai – sfrutterà l'intelligenza articifiale per comprendere gli attacchi e i comportamenti anomali. Ma, il livello di attenzione verso questi aspetti non è ancora ai livelli europei, soprattutto se si considerano iniziative che stanno partendo ad esempio in Francia". C'è però un dettaglio che Piai evidenzia e che influenza gli investimenti: "C'è un atteggiamento difensivo da parte delle aziende italiane. Ci si allinea con le nuove normative per evitare le multe e il fall out mediatico in caso di problemi. E non per approfittare di una revisione delle strutture e i processi per la gestione del dato delle aziende. Uno storico tallone d'Achille delle aziende italiane. Spesso questi rinnovamenti sono opportunità che non vengono colte per questioni di budget".

L'ASSESSMENT

Ciò che impatta di più in un'azienda è l'assessment. Soprattutto quan-

do una società gestisce dati sensibili. Pensiamo agli ospedali, enti terzi che gestiscono i database regionali o Big Pharma. Una quantità di informazioni su pazienti e trial clinici che necessitano altissimi livelli di sicurezza e di capacità gestionale. Un dettaglio non da poco. Per una gap analysis di un'azienda che non gestisce questi dati servono poche ore di lavoro al giorno. Se da una parte ci sono aziende che sanno autovalutarsi e capiscono gli step da percorrere, dall'altra ci sono realtà imprenditoriali che non sanno comprendere fino in fondo le proprie aree di rischio e hanno bisogno di una task force che valuti il peso specifico delle attività. L'It o l'Ict (tecnologie dell'informazione e comunicazione) vanno ridisegnate intorno all'azienda. Per far questo, per esempio in un grande ospedale che ha bisogno di un assessment e una messa in compliance, ci può volere una spesa di 100-150 mila euro. Qualora invece ci si trovi di fronte a un'azienda che non raggiunge i 30-40 dipendenti che non tratta dati sensibili, l'assessment non è impegnativo. Ci sono offerte che arrivano a 20 mila euro. Sono cifre indicative, ovviamente, ma danno l'idea della misura dei costi sostenuti e da sostenere. E si parla di prezzi su una consulenza annuale. In linea di massima, se consideriamo il monte ore di lavoro a persona, si va tra i 150 euro per un professionista junior e i 500 euro per un senior.

L'ADEGUAMENTO CONTINUO

Una necessità da non sottovalutare ma che è invece cruciale è l'adeguamento costante. Molti consulenti interpellati da AboutPharma ritengono che, anche se compliant, l'azienda va continuamente ritoccata e rivista. Anche se l'impresa è in regola con una serie di linee guida, l'evoluzione delle normative impone infatti un costante aggiornamento. Perché in caso di un mancato allineamento si rischiano sanzioni e la rincorsa per trovare una soluzione impone costi aggiuntivi ulteriori. Altro punto chiave: le spese che ciascuna struttura e società sosterranno rappresentano esse stesse la prova dell'adeguamento al Gdpr. Sarà la prova provata.

LE PRIORITÀ

In un'intervista rilasciata nel numero 154 di AboutPharma, Francesco Modafferi, dirigente del Dipartimento libertà pubbliche e sanità del Garante della protezione dei dati personali enuclea tre priorità. La prima è la designazione di un responsabile della protezione dei dati, il data protection officer. Una figura obbligatoria nel settore pubblico, mentre è richiesta ai privati solo per soggetti che effettuano trattamenti di dati su larga scala. In questo modo le aziende eviteranno il passaggio della consulenza del Garante in caso di dubbi sul trattamento dei dati, potendo, quindi, contare su una figura esperta all'interno del proprio organico. La seconda priorità riguarda l'istituzione di registri delle attività di trattamento, mentre la terza indica la creazione di una procedura per la gestione del data breach.

QUESTIONE DI REPUTAZIONE

Il peggiore scenario possibile? Un hacker che entra nel sistema, nessuna denuncia entro le 24 ore previste dal decreto,

Consapevoli o non consapevoli? Questo è il problema... da tempo

Facciamo qualche passo indietro. Il Gdpr, oltre a tutelare la privacy, è una cartina di tornasole della consapevolezza di una società del potenziale delle informazioni possedute. Nel corso degli anni, da quando si è iniziato a parlare del nuovo regolamento europeo sulla privacy, sono stati tanti i sondaggi che hanno testato nel corso del tempo la preparazione delle aziende life science. Nel 2016, per esempio, un'indagine condotta da Lloyd's, "Facing the cyber risk challenge", condotta su circa 350 leader di business europei, di cui 90 provenienti dai settori sanitario e medicale, ha rivelato che all'epoca l'impatto di una fuga di dati fosse estremamente sottovalutato. Addirittura solo il 12% degli intervistati riteneva che un furto di questo tipo potesse incrinare la propria reputazione e, di conseguenza, minare la fiducia dei clienti. Sempre in quel caso, il 97% degli intervistati aveva sentito parlare del Gdpr e solo il 3% aveva dichiarato di avere un'approfondita conoscenza del tema. Il 53% affermava di non aver pienamente compreso le implicazioni potenziali del Gdpr sul business. Un anno dopo, a novembre 2017, un altro sondaggio, stavolta condotto dalla società Sas, delineava uno scenario poco confortante basato su un campione di 340 dirigenti aziendali di vari settori e aree geografiche. In sostanza solo metà delle aziende intervistate aveva dichiarato che si sarebbe adeguato alla normativa europea che sarebbe entrata in vigore di lì a pochi mesi.

Il 45% delle organizzazioni intervistate aveva un piano strutturato per adeguarsi in vista della scadenza del 25 maggio e più della metà (58%) sosteneva che la propria azienda non era del tutto consapevole delle conseguenze derivanti dalla mancata conformità al regolamento. La maggior parte degli intervistati sosteneva che il regolamento Gdpr avrebbe avuto un impatto enorme sulla propria organizzazione. Tuttavia, solo il 42% ha affermato che le propria organizzazione era consapevole di tale impatto. Inoltre solo il 45% delle organizzazioni aveva messo in atto un processo strutturato per adeguarsi alla nuova normativa, ma di queste solo il 66% riteneva che tale processo sarebbe stato in grado di soddisfare appieno i requisiti di conformità. Altro dato emerso da quel sondaggio riguardava le grandi organizzazioni (con più di cinquemila dipendenti). Meglio attrezzate per gestire il regolamento Gdpr secondo lo studio. Il 54% degli intervistati era pienamente consapevole dell'impatto, rispetto ad appena il 37% delle aziende di piccole dimensioni. Da aggiungere che solo il 24% delle organizzazioni diceva di avvalersi della consulenza esterna per adeguarsi al regolamento privacy, ma solo il 34% di quelle che già disponevano di un processo strutturato in atto si sono affidate a società di consulenza. Sul piano reputazionale, infine, molti enti ritenevano che l'impegno investito nel processo di conformità sarebbe risultato vantaggioso anche per i clienti. Dal sondaggio emergeva che il 29% delle organizzazioni era convinto che la soddisfazione degli utenti finali sarebbe aumentata proporzionalmente al loro impegno per adeguarsi al regolamento europeo. E oggi?

Secondo uno studio pubblicato a febbraio di quest'anno dall'Osservatorio del Politecnico di Milano, un'impresa italiana su due (il 51%), ha avviato un progetto strutturato di adeguamento alla nuova regolamentazione Ue in materia di trattamento

diffusione di dati sensibili, ricatti multimilionari, sfiducia dei clienti. Il peggior incubo per un ceo che deve gestire centinaia di migliaia di informazioni supersensibili e che oltre a dover affrontare l'imbarazzo e il pubblico ludibrio, dovrà pagare anche una multa milionaria. Fino al 4% dell'intero fatturato per carenze nella compliance. A cascata ne va dell'immagine della compagnia stessa. Perdita dei clienti e isolamento nel mercato. Un disastro, insomma.

L'utilizzo oculato dei dati (nonché la loro difesa e tutela), offre invece grandi vantaggi di business. Poco importa, inoltre, la grandezza dell'azienda. Quello che è importante è la reputazione del marchio. L'impatto reputazione del data breach, comunque, è difficilmente quantificabile essendo una conseguenza indiretta di una violazione. Secondo molti esperti, la maturità necessaria per accogliere il Gdpr è di prevalenza delle multinazionali. Le realtà più piccole preferiscono, invece, investire nel proprio core business anziché in compliance. Per fare questo ed evitare che l'emorragia di informazioni non si trasformi in un bagno di sangue reputazionale, l'aziende si deve tutelare di sua iniziativa. Innanzitutto attraverso figure professionali nuove (il data protection officer) e attraverso, soprattutto, una presa di coscienza forte del panorama in cui si muoverà presto. "Si passa dall'età dell'adolescenza in cui c'era il legislatore che diceva cosa fare, all'età della maturità in cui bisogna sapere cosa fare", ha detto Tommaso Stranieri, partner di Deloitte risk advisory.

ADDIO AL CONSENSO SUI DATI CLINICI E TERAPEUTICI

Un'altra novità del regolamento prevede che non sia più necessario il consenso del paziente per il trattamento dei dati personali con fini terapeutici e di cura (articolo 9). Ma, come spiegano gli avvocati dello studio legale Stefanelli&Stefanelli sul proprio sito, in Italia esiste una legge, il cosiddetto Codice privacy (decreto legislativo 196/2006), che, al contrario, prevede il consenso informato anche per questi scopi. L'articolo 8 della bozza del decreto legislativo di attuazione delle legge delega 163/2017 per l'adeguamento del nostro ordinamento del Gdpr intitolato "Misure di garanzia per il trattamento dei dati genetici, biometrici e relativi alla salute" prevede che il trattamento di queste particolari categorie di dati sia subordinato all'osservanza di misure di garanzia molto precise. A stabilirle sarà il Garante per la protezione dei dati personali attraverso un provvedimento adottato con cadenza biennale a seguito di una consultazione pubblica. Nell'adozione si devono tenere presenti

dei dati personali (erano appena il 9% un anno fa) e un altro 34% sta analizzando nel dettaglio requisiti e piani di attuazione. Contemporaneamente, cresce al 58% (rispetto al 15% di un anno fa) la percentuale di aziende che hanno già un budget dedicato all'adeguamento al Gdpr. Insieme al mercato, sottolinea l'Osservatorio in una nota, cresce la consapevolezza della necessità di un approccio di lungo periodo nella gestione della sicurezza: nel 50% delle imprese è in corso un piano di investimenti pluriennale, anche se il 21% dichiara di stanziare un budget in sicurezza solo in caso di necessità. E si definiscono i ruoli nelle organizzazioni: il 39% delle imprese sta inserendo in organico nuovi profili che si occupano di security e il 49% di privacy. Aumentano responsabilità e competenze richieste al chief information security officer ed emergono nuove professioni come il security administrator, il security architect, il security engineer e il security analyst. Il 28% delle imprese ha già in organico o collabora con un data protection officer con il compito di facilitare il rispetto della nuova normativa.

non solo le linee guida sulla protezione delle informazioni, ma anche raccomandazioni, prassi e l'evoluzione tecnologica e scientifica del settore.

LA CIRCOLAZIONE DEI DATI DENTRO E FUORI L'EUROPA

Ma che succede se un'azienda ha un fornitore con base in un Paese fuori dai confini dell'Ue e deve trasferirgli dei dati? Cosa prevede il Gdpr? Se lo chiede l'avvocato Alessandra Delli Ponti in un articolo pubblicato sempre sul sito dello studio legale Stefanelli&Stefanelli. Secondo la direttiva europea 95/46/Ce, il trasferimento è vietato. Tuttavia vi sono delle deroghe o, comunque, degli ammorbidimenti. Tre i casi in cui è possibile. Primo: che la Commissione abbia deciso che il Paese terzo o l'organizzazione internazionale in questione garantiscono un livello di protezione adeguato. Secondo: che il titolare o il responsabile del trattamento possa effettuare il trasferimento in presenza di garanzie adeguate. Terzo: che in mancanza di una decisione di adeguatezza della Commissione o della predisposizione di garanzie adeguate, l'articolo 49 del Gdpr prevede una serie di deroghe e condizioni che, a prescindere dal livello di protezione dei dati personali apprestato, consentono il trasferimento extra Ue di dati personali.

Partiamo dal principio. Nel primo caso, la Commissione dovrà prevedere un esame periodico del funzionamento delle decisioni di adeguatezza assunte. Se qualcosa dovesse andare storto e la Commissione dovesse rilevare degli errori, allora il trasferimento sarà vietato. Ma se il Paese non rientra negli standard della Commissione? Ecco che entra in gioco il secondo punto, ossia le garanzie adeguate, cioè dei meccanismi che garantiscono che il dato sarà trattato in conformità ai principi della normativa dell'Unione europea. L'ultima spiaggia, se i primi due casi non consentissero il trasferimento dei dati fuori dall'Ue, è rappresentata da una serie di deroghe. La prima riguarda, per esempio, il fatto che l'interessato abbia espressamente acconsentito al trasferimento dopo essere stato informato sui possibili rischi. Un'altra situazione riguarda la necessità del trasferimento per la conclusione di un contratto stipulato tra il titolare dei dati e un'altra persona: se ci sono motivi di interesse pubblico; se c'è necessità di utilizzare le informazioni in sede giudiziaria; se il trasferimento serve a tutelare gli interessi vitali di una persona che si trova in una condizione di incapacità fisica o giuridica per dare il proprio consenso; oppure, ultima cosa, se il dato trasferito viene da un registro di consultazione pubblica.