Diffusione: 5.000

NETFORUM

Mensile

MERIDIAN COMMUNICATIONS

Data 03-2018
Pagina 38/52
Foglio 1 / 15

General Data Protection Regulation

Siete pronti?

Servizi a cura di Giacomo Broggi e Daniele Bologna

Il cosiddetto GDPR entrerà ufficialmente in vigore il prossimo 25 maggio, ma la strada verso l'adeguamento di Paesi e aziende è ancora lunga. Questa, è la fotografia fornita da Bruxelles e, in particolare, dalla commissaria Ue alla Giustizia, Vera Jourova, che "bacchetta" i Paesi ritardatari: in molti, a meno di settanta giorni dall'introduzione del nuovo regolamento, non hanno ancora provveduto ad adeguarsi alle nuove normative, che cambieranno molte cose

La bacchettata arriva dalla UE: l'Italia, e molti altri Paesi dell'Unione, non sono ancora pronti per il GDPR. Il General Data Protection Regulation entrerà ufficialmente in vigore il prossimo 25 maggio, ma la strada verso l'adeguamento di nazioni e aziende è ancora lunga. Questa, è la fotografia che fornisce Bruxelles e, in particolare, la commissaria Ue alla Giustizia, Vera Jourova, che "bacchetta" i Paesi ritardatari: ad oggi, ovvero a meno di settanta giorni dall'entrata in vigore del nuovo regolamento, in molti non hanno provveduto ad adeguarsi alle nuove normative. Non si tratta solo di un problema italiano: in Europa, sembrano fare eccezione solo Germania e Austria, i Paesi più diligenti da questo punto di vista, che hanno già provveduto ad approvare tutte le leggi necessarie per l'allineamento normativo con l'Unione Europea.

Corrado Dati, ITSM Business Unit Manager di SB Italia, società specializzata in soluzioni IT per la gestione, l'integrazione e l'ottimizzazione dei processi aziendali, commenta così: "Il 25 maggio è una data importante: il nuovo regolamento porterà più diritti per i cittadini europei e maggiore protezione per i consumatori. I dati che abbiamo raccolto con un'indagine sul grado di consapevolezza del GDPR da parte delle aziende italiane è in linea con l'allarme lanciato dall'Europa: le aziende interessate sono davvero in grave ritardo. Soprattutto in questo momento, affidarsi a professionisti preparati significa evitare di tralasciare aspetti importanti della normativa e farsi trovare pronti alla scadenza di maggio. Ricordiamoci che le sanzioni per chi non si adeguerà in tempo sono piuttosto salate: possono arrivare fino a 20 milioni di euro e fino a una quota pari al 4% del fatturato globale annuo".

DATA IMPORTANTE

IL GDPR SARÀ REALTÀ DAL 25 MAGGIO. PER MOLTI ESPERTI I VANTAGGI PER LE PERSONE SARANNO SUPERIORI AGLI OSTACOLI

PAURA DI FRONTE AL CAMBIAMENTO

Il 60% dei leader d'impresa in Europa ammette di non essere pronto per il GDPR. Il regolamento entrerà in vigore a maggio e i cambiamenti che porterà spaventano oltre mille dirigenti di aziende del Regno Unito,

La scadenza è importante, ma ci sono dei rischi: il 60% dei leader d'impresa in Europa ammette di non essere pronto per il GDPR. Il regolamento entrerà in vigore a maggio e i cambiamenti che porterà spaventano oltre mille dirigenti di aziende del Regno Unito, Francia, Germania, Spagna e Italia, intervistati sul tema

Francia, Germania, Spagna e Italia, intervistate sul tema da Senzing. Il 60% delle imprese europee leader hanno ammesso di non essere preparate per le prossime norme del regolamento generale sulla protezione dei dati. Secondo l'indagine, un quarto degli intervistati (24%) si considera "a rischio" quando si tratta di definirsi conforme al GDPR. Un ulteriore 36% si è classificato come "sfidato" dal regolamento, con solo il 40% che si definisce "pronto". Il GDPR, però, apporterà cambiamenti radicali all'industria del marketing. La direttiva dell'Information Commissioners Office (ICO) mira a garantire che qualsiasi società che tratti informazioni personali identificabili rispetti la legislazione in materia di consenso, portabilità dei dati e sicurezza informatica o subisca sanzioni pecuniarie fino al 4% del pro-

Chi è Senzing: dati semplici e affidabili

Senzing è un'azienda statunitense di software con sede in California, fondata da Jeff Jonas, ed è la prima società ad aver applicato il machine learning in tempo reale all'entity resolution. Il software di entity resolution G2 spicca, inn effetti, tra i più affidabili e semplici da usare per scoprire "chi è chi" all'interno dei propri dati. Il team di Senzing ha dedicato anni di lavoro a risolvere le complesse sfide portate dall'entity resolution e ha fornito il codice che si trova dietro ad alcuni fra i maggiori sistemi di entity resolution in tempo reale al mondo. In questo modo ha contribuito all'operatività di sistemi di importanza cruciale al servizio di governi, istituti finanziari, forze dell'ordine e multinazionali, fra i quali numerosi sistemi con un numero di record che va da 500 milioni a oltre 10 miliardi. Il software G2 di Senzing, creato in base al principio del Privacy by Design, aiuta imprese e organismi a orientarsi nelle proprie banche dati relative a persone e organizzazioni - contenenti dati personali strutturati quali nomi, indirizzi e altri elementi identificativi -, in modo da determinare con precisione "chi è chi". G2 rileva, inoltre, le connessioni fra diverse entità in modo da evidenziare anche "chi è collegato a chi". Le entità risolte e collegate vengono scomposte a scalare in merito ad adempienza, rilevamento di frodi, punteggio, referenza o sistemi di informazione, in modo da ridurre i rischi e generare decisioni imprenditoriali dotate di maggiore affidabilità.

prio fatturato o fino a 20 milioni di euro, a seconda di quale dei due importi sia più elevato. Le cifre più recenti, considerate in percentuale di tutte le imprese che operano all'interno dell'UE, potrebbero tradursi in decine di miliardi di multe, anche se l'ICO ha sottolineato che non intraprenderà una caccia alle streghe. Ciononostante, il 44% di tutte le imprese ha dichiarato di essere "preoccupato" per la propria capacità di conformarsi al GDPR.

IL CONTRIBUTO DI IAB

L'Interactive Advertising Bureau (IAB) Europe ha recentemente presentato uno standard tecnico volto proprio ad aiutare i marketer a soddisfare le esigenze relative ai contenuti degli utenti, riconoscendo le sfide che le aziende devono affrontare per seguire alcuni dei principi contenuti nel GDPR. Perché dal prossimo 25 maggio sarà una rivoluzione copernicana. Siamo in procinto di affrontare il cambiamento più grande e impattante degli ultimi anni in materia di privacy e protezione dati. Il centro studi della Scuola Internazionale Etica & Sicurezza (in collaborazione con Galdus, ente di formazione accreditato da Regione Lombardia) ha lanciato un'apposita survey e ha messo a disposizione delle aziende un indirizzo e-mail per rispondere al disorientamento e ai dubbi più comuni sulla nuova normativa in materia di protezione dei dati. L'analisi di Paola Guerra Anfossi, Fondatrice e Direttrice della Scuola Internazionale Etica &

Al servizio delle imprese In questa immagine, Paola Guerra Anfossi, direttrice della Scuola Internazionale Etica & Sicurezza, che si è posta al fianco delle aziende per supportarle nel delicato passaggio alle nuove normative sulla privacy

CRITEO
UN'EVOLUZIONE E NON UNA RIVOLUZIONE

L' executive vice president Emea della struttura, Cédric Vandervynckt, dialoga con Netforum con l'obiettivo di fare chiarezza sul regolamento e su quanto la stessa società abbia fatto per attrezzarsi, anche grazie a un approccio da sempre molto attento alla tematica

Il 25 maggio entrerà in vigore il General Data Protection Regulation. Diverse industry, compresa quella pubblicitaria, guardano con molta attenzione a quel giorno e molti operatori si stanno attrezzando, anche in un'ottica di educazione e formazione al mercato. È il caso di Criteo, che Netforum ha intervistato nella persona di Cédric Vandervynckt, executive vice president Emea della società francese. Un lungo scambio di battute, con l'obiettivo di fare chiarezza, in vista dell'ultima settimana di maggio, quando il nuovo GDPR cambierà molte cose.

Privacy e protezione del consumatore sono argomenti emersi con forza negli ultimi anni. Quali sono le principali evoluzioni?

Probabilmente l'armonizzazione delle diverse leggi sulla privacy dei dati locali. In particolare, con il GDPR le regole saranno le stesse in tutti i 28 stati membri dell'UE, incluso il Regno Unito. Ciò garantirà maggiore coerenza e certezza del diritto in tutta Europa, un aspetto molto importante per aziende come Criteo, che opera in più di 80 paesi. Inoltre, poiché il GDPR non si applicherà solo alle società europee, il suo impatto sulle pratiche di riservatezza delle aziende internazionali non dovrebbe essere sottovalutato. Con questo testo i legislatori europei stanno stabilendo uno standard mondiale. Allo stesso tempo, i diritti degli individui sono chiariti e rafforzati in modo significativo da questa nuova regolamentazione. Di conseguenza, possiamo sperare che il GDPR contribuirà a ristabilire fiducia tra i consumatori, il che, a sua volta, andrà a vantaggio delle imprese che offrono ai consumatori trasparenza e possibilità di scelta.

Quali sono, secondo lei, i temi più cari agli inserzionisti e agli operatori della pubblicità digitale in relazione al GDPR?

Quando si parla di ecommerce e advertising online, proteggere la privacy dei consumatori ed essere onesti con loro sulle pratiche commerciali è una questione di rispetto. Quando i clienti capiscono esattamente come vengono utilizzate le loro informazioni e hanno il controllo sui loro dati di navigazione personali, si rafforza la loro fiducia in un'azienda. E quanto più un cliente si fida di un marchio, tanto più forte sarà la sua fedeltà a quel marchio nel lungo termine. Questo è il motivo per cui, senza attendere l'entrata in vigore del GDPR, Criteo sta già riconoscendo che i dati raccolti per i suoi servizi sono dati personali, ad esempio, dati di navigazione, ID utente, ID cookie o altri identificatori tecnici utilizzati per offrire il giusto annuncio all'utente giusto. E devono essere pro-

Aggiornamento in corso, si delinea grande interesse In questa foto, l'executive vice president Emea di Criteo, Cédric Vandervynckt, che commenta con Netforum l'impatto del GDPR in procinto di entrare in vigore

tetti ed elaborati in conformità con le leggi applicabili sulla privacy e sulla protezione. La nostra speranza è che facendo della trasparenza e dei meccanismi di scelta le regole più importanti, il GDPR contribuirà a ripristinare la fiducia nel nostro settore. Uno dei punti di maggiore discussione per il marketing digitale è che gli identificatori tecnici come i cookie e gli ID della pubblicità mobile vengono ora considerati dati personali. Per molte aziende con sede negli Usa questo cambiamento può rappresentare uno sviluppo inatteso, mentre in molti Paesi dell'UE era già la norma. Tutti gli stati membri dell'UE devono trattare i cookie e gli altri identificatori tecnici come dati personali e quando si raccolgono dati personali di qualsiasi genere, la raccolta deve avere basi legali. Per questo il GDPR identifica sei basi legali per la raccolta e il trattamento dei dati in Europa:

1. L'interesse vitale dell'individuo.
2. L'interesse pubblico.
3. L'esigenza contrattuale.
4. La conformità a obblighi legali.
5. Il consenso non ambiguo dell'individuo.
6. L'interesse legittimo del controllore dei dati.

È importante notare come tutte queste basi giuridiche abbiano lo stesso valore legale. Significa che sono autonome ed esclusive, l'una rispetto all'altra. Per le attività di marketing, le basi legali che potrebbero applicarsi sono il consenso non ambiguo dell'individuo e l'interesse legittimo del controllore dei dati.

In un recente post avete dichiarato che il prossimo GDPR rappresenta un'evoluzione e non una rivoluzione: perché?

Esatto. Nel complesso, queston aggiornamento normativo è un'evoluzione che allinea le politiche di tutela dei dati di tutti gli stati membri dell'UE, offrendo coerenza di applicazione da parte delle autorità preposte alla tutela dei dati in ogni stato membro dell'UE. Gli obiettivi del GDPR, del resto, sono chiari. Si vuole modernizzare il sistema giuridico per proteggere i dati personali in un'era di globalizzazione e di innovazione tecnologica, rafforzando i diritti dell'individuo e riducendo i carichi amministrativi per garantire un flusso libero di dati personali all'interno dell'UE. Poi, intende fare chiarezza e dare coerenza per quanto riguarda le regole di tutela dei dati personali e garantire un'applicazione coerente e un'efficace implementazione in tutta l'UE. Il GDPR protegge la privacy dei cittadini UE ed è valido per tutte le aziende che raccolgono o elaborano dati personali relativi a individui dell'Unione Europea, anche se la loro sede non è nell'Unione. Una conferma significativa per il settore del marketing digitale è che il GDPR si applica a qualsiasi informazione relativa a una persona fisica identificata o identificabile, e questo include identificatori tecnici, quali gli ID dei cookie e ID della pubblicità mobile. Entrambi sono ora esplicitamente compresi nella definizione di "dati personali". È importante notare che questi identificatori tecnici erano già considerati dati personali da molte DPA, incluse quelle francesi. Questo, quindi, per Criteo, non è un nuovo requisito. Noi seguiamo metodi collaudati per la conformità, pur continuando a garantire le performance ai nostri clienti. Credo che il GDPR rappresenti uno sviluppo positivo che promuoverà la fiducia nella nostra economia digitale, creando un ambiente di trasparenza, controllo e certezza per aziende e consumatori. Siamo abituati a rispettare i più severi standard UE e siamo preparati a supportare i nostri clienti e partner lungo tutto il percorso verso la conformità al GDPR.

Quali sono i temi più importanti per i consumatori, anche a partire dalle evidenze della vostra ricerca realizzata con Ipsos?

Mentre le aziende del marketing digitale stanno aggiornando le proprie pratiche per adeguarsi al GDPR, è importante ricordare che i cittadini UE sono consapevoli della pubblicità mirata, conoscono gli identificatori che la guidano e si aspettano di vedere annunci pertinenti. Criteo ha collaborato con Ipsos proprio per comprendere quali sono le aspettative degli utenti dell'UE e quale rapporto hanno con la pubblicità mirata online. Abbiamo intervistato 3.000 utenti internet, di età compresa tra i 16 e i 65 anni in Francia, Regno Unito e Spagna, ritagliando un campione demografico rappresentativo per quanto riguarda genere, età, regione e livello di reddito. E abbiamo scoperto che il 90% degli utenti internet è consapevole del retargeting comportamentale, mentre il 68% lo è del fatto che i cookie consentono la pubblicità mirata. Poi, il 75% si aspetta di ricevere annunci adatti ai propri interessi e il 73% preferisce vedere annunci pertinenti piuttosto che spendere di più per evitare di vedere gli annunci.

Cosa sta facendo Criteo per adeguarsi al regolamento?

Siamo onesti, il GDPR è stato discusso davanti alle istituzioni dell'UE per quasi cinque anni e ha previsto un periodo di transizione di due anni, quindi abbiamo avuto il tempo di lavorare. Tutte le misure e le pratiche che il nostro team di privacy ha implementato negli ultimi anni sono state fatte pensando al GDPR. Criteo, dunque, è sempre stata un passo avanti nel processo di preparazione al GDPR. Dalla fondazione, nel 2005, abbiamo sempre garantito che la nostra tecnologia avesse i più alti livelli di privacy e protezione dei dati, aiutando, allo stesso tempo, i clienti a soddisfare le aspettative degli acquirenti con pubblicità personalizzate e pertinenti. In quanto azienda globale con sedi in diversi paesi europei, siamo già abituati a rispettare requisiti a livello di paese in tutto il mondo. Infatti, non solo rispettiamo già gli elementi chiave del GDPR, ma siamo in grado di poter implementare rapidamente eventuali requisiti aggiuntivi. Siamo pronti ad accogliere la sfida del GDPR e prevediamo un impatto ridotto della nuova normativa sulla capacità dei nostri clienti e partner di lavorare con ▸

noi. Prima che tutti cominciassero a parlare di GDPR, Criteo si è affermata come uno dei primi leader di pensiero, affermando chiaramente il diritto dei consumatori di accedere ai propri dati, di sapere quali dati vengono raccolti, come vengono utilizzati, e come negare il consenso. A partire dal 2008, Criteo si è impegnata nel programma Ad Choices, che consente ai consumatori di vedere esattamente dove Criteo utilizza i dati e come protegge la loro privacy con un singolo click. Quando un consumatore sceglie esplicitamente di negare il suo consenso, noi interrompiamo immediatamente il tracciamento e il retargeting. Quindi, rimuoviamo tutti gli identificatori dai suoi browser, rendendone impossibile il retargeting in futuro. Per molti aspetti, il GDPR è la conferma che abbiamo fatto le cose giuste per molti anni, in particolare grazie all'approccio Privacy by Design che abbiamo implementato anni fa e che ora è richiesto dal regolamento. Gli esperti di privacy che lavorano in Criteo non fanno parte dei team Legal e Compliance. Lavorano direttamente nell'organizzazione di prodotto e Ricerca & Sviluppo e collaborano con i nostri ingegneri sin dalla fase iniziale della progettazione di tutti i nostri servizi e tecnologie, garantendo il rispetto dei potenziali vincoli normativi e soprattutto della privacy degli utenti. Rappresenta la pratica e l'impegno di lunga data di Criteo per garantire ai consumatori e ai marketer livelli di privacy e sicurezza leader di settore.
Tra gli elementi chiave del programma spiccano la supervisione di un Data Privacy Officer dal 2013, come ora richiesto dal GDPR; la costante valutazione dell'impatto sulla privacy per monitorare potenziali rischi durante il ciclo di vita del prodotto e mitigarli in modo proattivo; programmi di formazione aziendale sulla privacy per garantire che i nuovi prodotti e servizi siano sviluppati seguendo i più rigorosi codici di condotta. E inoltre, azioni di revisione e documentazione periodiche delle nostre politiche interne, al fine di modificare le policy sulla privacy esistenti, se necessario, e di applicarle ai nostri partner e fornitori.
Infine, disponiamo già di un ampio numero di certificazioni che vengono riviste annualmente dagli organismi che le disciplinano. Alcuni esempi: Network Advertising Initiative Standards, IAB Europe e la Digital Advertising Alliance Self-Regulatory Principles for Online Behavioral Advertising.

Alcune ricerche vedono le aziende in ritardo nel processo di adattamento al nuovo quadro normativo: a questo proposito, quali sono i suoi consigli e quali i principali pericoli?
Sicuramente molte aziende sono in forte ritardo nel viaggio verso la conformità ed è per questo che stiamo lavorando con clienti e partner soggetti alle nuove normative, offrendo loro supporto e condividendo le migliori pratiche per gestire al meglio la transizione. Criteo fornisce le linee guida e le best practice per aiutare i clienti a soddisfare i propri obblighi legali, condividendo in modo proattivo le best practice, suggerendo proattivamente la formulazione per la raccolta di consenso sul proprio sito web e rassicurando i clienti sulla conformità della tecnologia e dei servizi Criteo. A lungo termine, siamo sicuri che una maggiore fiducia e trasparenza andranno a vantaggio di aziende e individui.

Cosa potrebbe accadere, qualora una società non armonizzasse le sue operazioni ai dettami del GDPR?
Le norme del GDPR si applicano alle imprese dell'Unione Europea e alle aziende situate fuori dall'Unione che, però, offrono servizi oppure prodotti all'interno del mercato UE. Tutte queste aziende, ovunque siano stabilite, dovranno rispettare le nuove regole che netranno in vigore. Imprese ed enti avranno, dunque, maggiori responsabilità e in caso di inosservanza delle regole rischiano delle pesanti sanzioni. Nella fattispecie, si va da un mera diffida di carattere amministrativo a sanzioni pecuniarie ingenti, fino a 20 milioni di euro oppure intorno al 4% del fatturato globale, qualunque sia il dato più alto.

Sicurezza, stilata in occasione della presentazione del corso "Data Protection: il professionista del trattamento e della protezione dei dati personali" - che si terrà dal 19 marzo al 10 settembre - è categorica: "Il GDPR avrà conseguenze importanti su tutte le organizzazione che acquisiscono, trattano ed elaborano i dati personali. Non solo si devono soddisfare tutti i requisiti, ma occorre anche essere in grado di produrre documenti che dimostrino la compliance in modo da giustificare le scelte intraprese. E' il principio dell'accountability". Un tema molto caldo, soprattutto, se si considera che la cybersecurity italiana vale un miliardo di euro e che la gestione dei dati determina il futuro economico delle organizzazioni.

I LIVELLI DI CONOSCENZA

Ma quanto conosciamo, davvero, il tema del Data Protection? Questo argomento, in Italia, è ancora materia da addetti ai lavori; si pensa che la data protection sia una norma da aggiungere alle altre, un costo da sostenere e non una straordinaria opportunità di crescita e di rilancio per un'azienda e il suo patrimonio di informazioni. Il GDPR introduce un approccio di data protection viva, in continuo movimento, condivisa tra le unità organizzative e spostata verso i diritti fondamentali degli individui: dal diritto di accesso a quello di rettifica, dal diritto alla cancellazione/oblio a quello di limitare il trattamento, dal diritto alla portabilità dei dati a quello di opposizione. Stavolta il legislatore vuole una vera svolta, viste anche le sanzioni previste che possono arrivare anche al 4% del fatturato annuo mondiale. Secondo l'ultima ricerca veicolata dall'Osservatorio Information Security & Privacy del Politecnico di Milano, in oltre un'impresa italiana su due (il 51%) è in corso un progetto strutturato di adeguamento alla nuova regolamentazione Ue in materia di trattamento dei dati personali che diventerà pienamente applicabile a partire dal 25 maggio (erano appena il 9% un anno fa). Mentre 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. Uno dei principali elementi

di novità è dato dalla figura del Data Protection Officer: il cosiddetto DPO (figura interna o esterna all'azienda) avrà un compito determinante, perché sarà un supervisore indipendente e avrà una posizione molto simile a quella dell'Organismo di Vigilanza (ex Decreto Legislativo 231/01) con la precisa finalità di garantire che l'organizzazione sia conforme a quanto indica il GDPR.

COME SCEGLIERE?

Come scegliere, dunque, il DPO, considerando le competenze giuridiche, normative, organizzative, gestionali e tecnologiche che deve avere? Viene in aiuto la norma UNI 11697:2017 che delinea le qualifiche e i requisiti di studio e professionali che i profili devono possedere. Alla norma UNI si collega il tema della certificazione volontaria, che è indubbiamente un elemento aggiuntivo in termini di garanzia, tanto per il singolo professionista quanto per l'organizzazione. Cosa faranno le aziende? "Possiamo testimoniare che le organizzazioni sensibili al tema e più mature, in termini di conoscenza della materia, ci chiedono un percorso formativo finalizzato alla certificazione e, allo stesso modo, i professionisti che desiderano intraprendere la professione di DPO" - commenta Paola Guerra, Direttrice della Scuola Internazionale Etica & Sicurezza -. Dalle aziende che abbiamo interpellato direttamente attraverso la nostra survey qualitativa *(un accurato lavoro di analisi sulle risposte raccolte, pari a circa il 20% del campione interpellato fatto di referenti di aziende di grandi dimensioni, nazionali e multinazionali, ndr)* ci risulta che i settori su cui si ritiene che il GDPR impatterà di più sono Telecomunicazioni)e Sanità; la metà delle aziende ha iniziato il processo di adeguamento, un quarto non era a conoscenza della norma UNI 11697:2017; infine, un quinto ritiene che la nuova norma non sia utile".

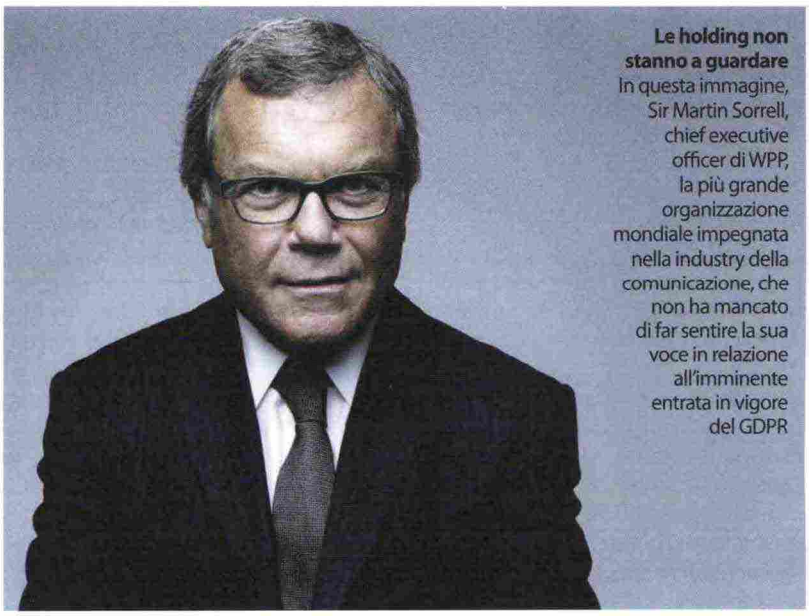
DOMANDE FREQUENTI

Il Centro Studi della Scuola Internazionale Etica & Sicurezza, per contribuire alla campagna di sensibilizzazione e informazione su uno dei temi più importanti legati al processo tecnologico degli ultimi anni, ha, dunque, messo a disposizione un indirizzo di posta elettronica per rispondere alle principali domande delle aziende, con l'obiettivo di chiarire il più possibile gli elementi più confusi della normativa.
Le domande che si immaginava potessero giungere sono soprattutto queste:

- La mia azienda deve adeguarsi alle normative contenute nel GDPR?
- Quali sono i principali passi da fare?
- Quali sono i diversi ruoli e le responsabilità previsti?
- Chi è il DPO? Devo nominarlo? Come è

Digital Academy, una proposta formativa

Sold out il primo corso in aula della IAB Digital Academy, intitolato "GDPR ed e-Privacy - dalla teoria alla pratica", che si è svolto presso lo Spazio Copernico di via Copernico 38, a Milano. IAB Digital Academy, iniziativa annunciata nel corso dell'ultimo IAB Forum 2017, amplia, dunque, la gamma di proposte formative di IAB Italia e offre un format modulare, poiché conta sull'esperienza di docenti indipendenti e super partes individuati dall'associazione; il tutto certificato attraverso un attestato assegnato dopo un test finale messo a punto sempre da IAB Italia insieme ai docenti coinvolti. Oggetto di studio all'interno dell'Academy sono gli aspetti pratici e l'impatto sul business delle tecnologie più all'avanguardia e delle nuove normative del settore, analizzando i rischi e le opportunità connessi alla nuova economia digitale. L'appuntamento della IAB Digital Academy, di cui è possibile consultare online il programma, è strutturato per venire incontro alle necessità degli operatori del settore digitale, dei professionisti e delle aziende che devono adeguare le proprie operazioni, o quelle dei clienti, ai nuovi Regolamenti europei in tema di Privacy. In aula sono presenti gli esperti provenienti dal dipartimento ICT&IP dello Studio Legale DGRS: Lapo Curini Galletti, Giulia Sala, Anna Maria Lorito e Alessandra Titone, che collaborano con IAB Italia anche alla realizzazione di approfondimenti dedicati a tematiche legislative legate al settore del digitale consultabili gratuitamente sul sito web dell'associazione. "Siamo fortemente convinti che la formazione e la divulgazione di una cultura digitale all'interno delle imprese italiane, di ogni dimensione, rappresentino due fattori strategici, in grado di far evolvere l'economia del nostro Paese, in particolar modo per quanto riguarda il settore del digitale" ha dichiarato Daniele Sesini, Direttore Generale di IAB Italia. "IAB Digital Academy è un nuovo tassello di un'offerta sempre più completa, personalizzata secondo le esigenze delle aziende. L'iniziativa risponde, inoltre, ad una necessità messa in luce dal Governo italiano che, attraverso gli incentivi alla formazione digitale previsti all'interno della Legge di Stabilità, mira a supportare il superamento del gap di competenze tecnologiche e digitali che ancora stanno frenando il paese", conclude Sesini.



Le holding non stanno a guardare In questa immagine, Sir Martin Sorrell, chief executive officer di WPP, la più grande organizzazione mondiale impegnata nella industry della comunicazione, che non ha mancato di far sentire la sua voce in relazione all'imminente entrata in vigore del GDPR

possibile sceglierlo adeguatamente?
- Quali sono gli obblighi di sicurezza?
- Quali sanzioni si possono ricevere?
- Che cosa significa, nel dettaglio, "principio dell'accountability"?
- Che cosa significa, invece, "privacy by design" e "impact assessment"?

Per ora, fino al prossimo 16 marzo, scrivendo a gdpr@scuolaeticaesicurezza.eu, il Centro Studi della Scuola Internazionale Etica & Sicurezza risponderà entro 24 ore dal ricevimento delle e-mail ai dubbi delle aziende, per consentire il percorso di adeguamento e, soprattutto, per evitare le sanzioni che - come già sottolineato - possono arrivare fino a 20 milioni di euro oppure, nel caso di un'impresa, fino al 4% del fatturato annuo a livello mondiale.

PAROLA DI SORRELL

Anche le grandi organizzazioni della comunicazione si stanno preoccupando. E fanno bene. Persino Sir Martin Sorrell si è scomodato, intervenendo direttamente nel dibattito pubblico sul tema: "È importante che la legge stia al passo con il progresso tecnologico", ha rimarcato. In un'intervista concessa a Beet.TV, il ceo di WPP, la più grande holding mondiale della comunicazione, ha sostenuto che, sebbene il provvedimento complicherà molto le cose, sarà utile per responsabilizzare le aziende, soprattutto, le più grandi del tech.

Il 25 maggio - ha spiegato Sorrell - gli operatori digitali dovranno essere pronti ad affrontare il regolamento generale sulla protezione dei dati della Commissione Europea e prestare molta attenzione al modo in cui utilizzano i dati dei cittadini UE oppure rischieranno una nuova sanzione pecuniaria fino al 4% del fatturato globale. "Il GDPR - ha detto, in particolare, Sorrell - renderà le cose molto più complicate, ma comprensibilmente, basti pensare a quanto sta succedendo in relazione alla consumer brand safety o a quella che io chiamo "political brand safety", ossia le presunte interferenze esterne alle elezioni negli Stati Uniti e non solo". Questo era ben lungi dall'essere il motivo per cui la Commissione Europea ha proposto il GDPR diversi anni fa, ma il punto, sostiene il ceo di WPP, è che il mondo si sta svegliando di fronte a un uso sofisticato dei

MICROSOFT A SUPPORTO DELLE IMPRESE

La multinazionale conferma la propria disponibilità e rivela anche i risultati di una ricerca realizzata in collaborazione con IDC: poche realtà sono già compliant, il lavoro che resta da fare è ancora tanto

Microsoft conferma il proprio impegno a supporto delle aziende italiane che nei prossimi mesi dovranno allinearsi al GDPR e ha sviluppato strumenti di autovalutazione, formazione e adeguamento. Se l'entrata in vigore della nuova normativa europea per la protezione dei dati si fa sempre più vicina, lo scenario italiano è ancora eterogeneo: secondo le nuove elaborazioni IDC per Microsoft, solo il 3% delle realtà con più di dieci addetti è compliant, il 43% ha appena iniziato l'analisi e il 54% ha già un piano per la conformità. Alcuni settori strategici come il Finance e la Pubblica Amministrazione sono quelli dove si registra un maggior tasso di compliance, rispettivamente il 10% e l'8%, e una maggiore presenza di roadmap già definite per l'adeguamento, rispettivamente, nel 76% e 85% dei casi. Mentre in altri settori altrettanto strategici, come il Manufacturing e i Servizi, è più alta la percentuale delle aziende che hanno da poco iniziato ad affrontare il problema, rispettivamente il 53% e il 60%.

PREOCCUPANO I REQUISITI TECNICI

Un quadro che si conferma anche tra le realtà più grandi, sopra i 250 addetti, non solo italiane, ma anche europee: secondo IDC, il ritardo è spesso dovuto alla percezione di alcuni requisiti della nuova normativa quali vere e proprie sfide tecnologiche e organizzative. Nello specifico, se si guarda al mercato italiano, oltre la metà delle imprese evidenzia come particolarmente impegnativi i requisiti tecnici, quali l'obbligo di notifica dei data breach entro 72 ore (70%), la necessità di implementare in modo sempre più strategico soluzioni di crittografia e/o anonimizzazione dei dati (60%) e la definizione di casi d'uso specifici nella gestione del consenso (48%). Al contempo, i processi organizzativi ritenuti più sfidanti dalle aziende italiane sono la classificazione di tutti i dati (67%), la sensibilizzazione dei dipendenti ai cambiamenti che intervengono nelle policy di sicurezza (62%) e l'eliminazione dei dati irrilevanti (62%). Cambiamenti importanti che naturalmente comportano anche dei costi e oltre due imprese italiane su tre concordano sui driver degli investimenti relativi ai progetti di compliance: la creazione di nuovi processi di documentazione (70%) e le attività di comunicazione interna e formazione (69%) vengono considerati i principali oneri. in questo quadro Altrettanto importante è il peso degli investimenti per soluzioni di Identity & Access Management (66%), per la mappatura dei dati (65%) e per l'aggiornamento dei processi di back-up (64%).

UN IMPEGNO PER FAVORIRE LA CONFORMITÀ

Uno scenario di luci e ombre, dunque, in cui la mancanza di risorse e competenze può rappresentare un ostacolo alla compliance. Consapevole che i prossimi due mesi saranno fondamentali, ma che l'esigenza di adeguamento alla normativa perdurerà oltre la data del 25 maggio 2018, Microsoft ha sviluppato alcuni strumenti per supportare le aziende italiane nel proprio percorso verso la conformità. Innanzitutto, ha reso disponibile un test di autovalutazione online gratuito, per consentire alle aziende di verificare il proprio grado di preparazione rispetto ai requisiti del GDPR e iniziare a definire un piano verso la compliance. Grazie al proprio ecosistema di 10 mila partner sul territorio, Microsoft offre, inoltre, consulenza a realtà di qualsiasi settore e dimensione attraverso un modello di adeguamento strutturato composto da quattro semplici passi e illustrato nel White Paper disponibile online, dal titolo "Percorso di Adeguamento al GDPR: Identificazione - Gestione - Protezione - Documentazione". La ricetta di Microsoft prevede di:

1. Identificare quali dati personali si possiedono e dove risiedono;
2. Gestire gli accessi e il modo in cui i dati vengono usati;
3. Stabilire controlli di sicurezza per prevenire, rilevare e risolvere vulnerabilità e violazioni;
4. Conservare la documentazione necessaria e gestire le richieste di dati e notifiche delle violazioni.

LUCI E OMBRE

LO SCENARIO NON È FACILE DA INTERPRETARE, PERCHÉ LA MANCANZA DI RISORSE E COMPETENZE PUÒ ESSERE OSTACOLO ALLA COMPLIANCE

MICROSOFT 365 E GLI STRUMENTI IN MANO ALL'AZIENDA PER SENTIRSI PIÙ CONSAPEVOLE

Con l'obiettivo di offrire risorse utili per la consapevolezza e la formazione delle aziende, Microsoft ha anche organizzato il Microsoft 365 Circle. Si tratta, in pratica, di un ciclo di webinar online, accessibili anche on demand, per restare sempre aggiornati sulle nuove tecnologie, tra cui sono già disponibili video e contenuti multimediali sul tema Cybersecurity e proprio GDPR. Microsoft offre, quindi, alle aziende soluzioni in linea con i requisiti del GDPR e i propri device e software sono dotati di funzionalità di gestione delle identità e degli accessi, di protezione delle informazioni, di tutela dalle minacce cyber e disaster recovery, e di gestione degli strumenti di sicurezza. In particolare, il Cloud di Microsoft integra alcune nuove funzionalità per aiutare le aziende ad essere in linea con i requisiti indicati dal GDPR, come Azure Information Protection per la tracciatura dei documenti oppure Office 365 Advanced Data Governance per gestire in modo intelligente i dati aziendali, classificandoli. Anche Microsoft 365, la nuova suite che include strumenti per la creatività e la collaborazione quali Office 365, Windows 10 ed Enterprise Mobility + Security, aiuta le aziende a proteggere i dati personali dalla perdita, dall'accesso e dalla divulgazione non autorizzati, rispettando i nuovi standard per la trasparenza e la privacy.

dati del pubblico. "Il fatto che le comunicazioni politiche possano essere più invasive, così come quelle commerciali, è inevitabile. Nella battaglia per i dati, di cui vediamo protagoniste Google e Facebook e, sempre di più, anche Amazon, questi ultimi hanno una rilevanza sempre maggiore ed è necessario che la legge stia al passo con il progresso tecnologico, cosa che molto spesso non accade. Ed è questo il vero problema", ha aggiunto Sorrell. "Regolamentare il settore è importante e penso che le sette sorelle *(le prime cinque aziende tecnologiche occidentali, più Tencent e Alibaba, ndr)* capiscano che, le loro dimensioni, il loro potere e il loro successo, determinino anche una grande responsabilità".

SANZIONI DIETRO L'ANGOLO

Il nuovo Regolamento europeo sulla Data Protection (GDPR), che sostituirà la Legge sulla Privacy attualmente in corso in Italia, è, dunque, sotto i riflettori. La scadenza del 25 maggio, quando entrerà in vigore, è vicina, e conviene ripetere la domanda: le aziende interessate sono pronte? Quali gap devono ancora colmare? Sottovalutare l'importanza del GDPR e la necessità di adottare misure organizzative o tecniche per proteggere i dati personali significa esporsi - l'abbiamo detto - a sanzioni che possono arrivare a cifre importanti. Nonostante manchino poco più di due mesi all'ora X, ricerche recenti hanno infatti messo in luce il ritardo o la mancanza di informazioni aggiornate sugli adempimenti e sulle misure da adottare. Tornando al lavoro svolto in questa direzione da SB Italia, società specializzata in soluzioni IT per la gestione, l'integrazione e l'ottimizzazione dei processi aziendali, vale la pena entrare un po' più a fondo sulle risultanti dell'apposito sondaggio dedicato alle imprese che desiderano conoscere il proprio livello di preparazione in tema di GDPR. La ricerca effttuata mirava, in particolare, a ritrarre il profilo del comportamento delle aziende nei confronti dell'adeguamento al GDPR, proprio al fine di individuare tutte quelle aree dove c'è ancora bisogno di supporto. E sono molte.

CONSAPEVOLEZZA

Per prima cosa, è importante essere consa-

OGURY
PER GLI UTENTI IL TRADE-OFF ORA È SEMPLICE

Il ceo e founder della struttura, Jean Canzoneri, ha analizzato con Netforum le richieste e le ricadute della normativa europea che entrerà in vigore il prossimo 25 maggio. Con l'opt-in ci sarà meno advertising. Ma sarà più interessante

Il conto alla rovescia è partito ormai da tempo, ma prima di maggio ci sono ancora due mesi abbondanti a disposizione. L'attesa per l'entrata in vigore del GDPR si fa snervante per le aziende che non hanno ancora predisposto i propri asset alle nuove regole, mentre c'è chi vive la situazione tranquillamente, forte di un'attenzione al consumatore inserita nel business plan dal giorno zero. Ci sono realtà che hanno tenuto un atteggiamento trasparente verso gli utenti, raccontando in modo chiaro e conciso - ovvero in un solo scroll - il come e il perché raccolgono i loro dati, accettando da subito il trade-off tra spiazzare alcuni utenti e la volontà di garantirgli informazioni che sarebbe meglio non ignorare.

Data base e trasparenza

"Abbiamo un database di 400 milioni di persone - spiega a Netforum Jean Canzoneri, ceo e founder di Ogury -, costruito proponendo a ogni utente uno specchietto informativo nel momento in cui entra in contatto con la nostra SDK. Avremmo potuto disporre di un database più ampio, ma abbiamo preferito perdere qualche dato per adesioni mancate alle nostre policy piuttosto che ottenerlo in modo poco trasparente. Noi chiediamo un consenso informato alla raccolta dati già dall'inizio, fa parte del nostro business plan. E adesso, con l'arrivo del GDPR, per noi cambierà poco, mentre altri dovranno adeguarsi e modificare i loro piani".

Ormai ci siamo, il prossimo 25 maggio entrerà in vigore il GDPR: cosa chiede alla industry?

"Il GDPR intende dare più potere all'utente attraverso diversi step. Innanzitutto, richiede un opt-in vero, informato. Il consenso deve essere espresso attraverso un'azione, cliccando "accetto", e dev'essere preceduto da una spiegazione chiara, corta e comprensibile dei modi e degli scopi per cui si richiede il permesso di raccogliere i dati. L'opt-out dev'essere altrettanto semplice, rimuovere il consenso dev'essere facile così come esprimerlo. Questi sono gli aspetti più difficili da affrontare, ma non sono gli unici. La norma-

tiva richiede anche un giro di vite sulla sicurezza dei dati e anche sul periodo di conservazione degli stessi, che non potrà superare i tre anni. Inoltre, i chief data officier diventeranno delle figure necessarie e dovranno svolgere compiti molto importanti".

Quali effetti vuole creare nel comparto?
"Le finalità e le pratiche di raccolta dati non sono sempre chiare agli utenti, e questo aspetto ha creato molta incertezza tra gli utenti. Il GDPR vuole riportare su internet una situazione di fiducia".

In un simile scenario, quali vie si possono, allora, percorrere per spingere gli utenti a fare opt-in?
"Penso sia fondamentale essere chiari e molto trasparenti. Il trade-off, per un consumatore, è facile: l'advertising sui siti ci sarà comunque, ma se si accettano i termini le inserzioni saranno di meno e più rilevanti. Non sarà proibito, poi, incentivare l'opt-in attraverso compensi di vario tipo, anche di carattere economico".

Su quali comparti si noteranno gli effetti maggiori?
"Non sono molti gli editori che riescono a sfruttare adeguatamente i dati che raccolgono. Sebbene siano uno dei principali canali di contatto con gli utenti, l'editoria subirà solo dei rallentamenti. I player del segmento dei big data che non saranno allineati con le nuove regole imposte dal GDPR, al momento dell'entrata in vigore, invece, potrebbero soffrire una recessione".

Un database da 400 milioni di persone
In questa foto, Jean Canzoneri, ceo e founder di Ogury, che racconta a Netforum tutte le pratiche e le procedure messe in atto dall'azienda per fronteggiare le nuove norme in tema di privacy e sicurezza dei dati

pevoli dei cambiamenti che ci attendono e dei costi per eventuali negligenze. Secondo i dati raccolti da SB Italia, soltanto il 15,6% degli intervistati ritiene che i vertici aziendali e i principali responsabili del business siano pienamente consapevoli del cambiamento indotto dal GDPR; il 50% pensa che lo siano solo in parte, mentre il 10% afferma che non lo siano per niente. Dal lato della consapevolezza dei rischi, sembra che ci sia maggiore attenzione: alla domanda "In azienda c'è consapevolezza che il "costo" di una mancata compliance al GDPR porta a sanzioni molto più elevate, nei casi più gravi fino a 20 milioni di euro, o se superiore, fino al 4% del fatturato annuo?" ha risposto positivamente il 71,8%. Le aziende dovranno poter dimostrare di aver applicato misure e processi per essere compliant. Alla domanda se, in azienda, sia stata definita una struttura completa di procedure per fornire supporto e direzione alle attività di compliance alla nuova norma, ha risposto negativamente quasi la metà degli intervistati, il 40%, a testimonianza di come, ancora, non ci sia nelle aziende una visione globale della normativa e di tutto quello che sarà necessario fare per poterla rispettare. Sul lato della conoscenza dei dati interessati dalla nuova normativa, il 62% degli intervistati ha affermato che la propria azienda ha documentato quali siano i dati personali in uso, da dove provengono questi dati e con chi sono condivisi. Afferma, inoltre, che è stato pianificato un audit informativo attraverso l'organizzazione per creare una mappa completa dei flussi dei dati.

I DIRITTI DEGLI UTENTI

Il GDPR sottolinea come gli utenti abbiano diritto di sapere come sono raccolti i loro dati personali, come vengano utilizzati e per quali scopi. E ancora, quali possono essere gli usi secondari e a quali terze parti possono essere comunicati. Alla domanda se l'azienda abbia aggiornato le proprie procedure per ottenere il consenso degli individui e se abbia reso trasparenti le proprie attività di raccolta dei dati, poco più della metà ha affermato che, in parte, l'azienda è pronta, mentre il 24% ha dichiarato di non esserlo. Solo il 16% si dichiara completamente pronto. L'azienda, inoltre,

deve essere in grado di gestire, con apposite procedure, eventuali richieste degli individui di poter accedere ai propri dati personali, come richiesto dal GDPR. Per il 32% degli intervistati, il sistema attuale non è ancora pronto a gestire le richieste, di nuovo un 32% afferma di esserlo in parte, mentre il 24% del tutto. Sempre per quanto riguarda la gestione interna dei dati sensibili, sembra che le aziende siano pronte: si dichiarano, appunto, "pronte in tutto" il 38,8 %, e "in parte" il 44,4% per quanto riguarda l'adozione di misure per permettere l'accesso solo alle persone autorizzate per prevenire danni o utilizzi non conformi dei dati. Solo il 4,4% dichiara che la propria azienda non è ancora pronta. Invece, di fronte al rischio di un attacco, le aziende quanto sono preparate? Alla domanda se l'azienda si sia dotata di una procedura per la gestione di un incidente informatico con furto o modifica di database di dati personali e se abbia predisposto opportune procedure per notificare le autorità competenti e gli individui, un preoccupante 48% dichiara di non essere pronto a questa evenienza. Per prevenire eventuali attacchi, è importante mantenere sempre aggiornato il proprio software aziendale. Sul fronte delle procedure per la gestione degli aggiornamenti software, alla domanda "L'azienda dispone di una procedura per gli aggiornamenti software, per evitare l'utilizzo malevolo di eventuali vulnerabilità nel software?", il 94% degli intervistati si dichiara pronto, in tutto o in parte. Buona appare anche la situazione della sicurezza dello storage: la totalità degli intervistati afferma che l'"azienda dispone di misure e tecnologie per prevenire la perdita, il furto, la compromissione dei dati personali, mentre l'88,88% afferma che sì, l'azienda è pronta (del tutto o in parte).

IN DIFESA

Anche per quanto riguarda le difese antimalware, sembra che la situazione nelle aziende sia positiva: alla domanda se l'azienda si sia dotata di efficaci difese antivirus/antimalware per proteggere i dati nei sistemi informatici, il 55% dichiara che la propria azienda è pronta del tutto, mentre il 33% in parte. Infine, per quanto riguarda il mobile working, alla domanda se l'azienda

Una questione di diritti umani In questa foto compare il chief privacy officer di Sizmek, Ari Levenfeld, che racconta a Netforum gli sforzi compiuti dalla piattaforma ad-tech sul fronte dell'adeguamento alle nuove norme

SIZMEK LA PRIORITÀ È ESSERE CONFORMI

Il chief privacy officer, Ari Levenfeld, illustra a Netforum il modo con cui la società, che offre la più grande piattaforma pubblicitaria buy-side indipendente, si stia avvicinando all'entrata in vigore del regolamento, il 25 maggio. E prevede un rinnovato focus dedicato al targeting contestuale

"Abbiamo profuso un grande impegno nel documentare la nostra base giuridica per l'elaborazione dei dati nell'ambito del GDPR e sul piano legale per sottolineare le nostre posizioni nei contratti con i nostri clienti e fornitori, nominando un DPO. Abbiamo integrato la privacy nella nostra piattaforma, costruito e documentato le pratiche di sicurezza. E abbiamo un piano in atto per affrontare il tema ePrivacy"

Il 25 maggio 2018. Una data molto importante per l'Unione Europea, i suoi cittadini e le aziende che vi operano. Come tutti più o meno sanno, quel giorno entrerà in vigore il General Data Protection Regulation, una legge che è volta ad armonizzare le norme sulla protezione dei dati in tutto il continente. Ma che porta con sé anche dubbi e domande, legate specialmente al processo di conformità alle nuove regole. Per approfondire il tema, Netforum ha intervistato il chief privacy officer di Sizmek, Ari Levenfeld, il quale racconta gli sforzi compiuti dalla piattaforma ad-tech.

All' inizio dello scorso febbraio, il vostro attuale chief executive officer, Mark Grether, ha dichiarato a Beet.tv di essere "piuttosto preoccupato", soprattutto come consumatore, per il GDPR. Quali sono, secondo lei, le ragioni che l'hanno spinto a tale affermazione?

Il GDPR è una legge volta ad armonizzare le norme sulla protezione dei dati in tutti i mercati dell'UE e a promuovere l'accountability e la trasparenza delle imprese che trattano i dati personali dei cittadini dell'UE. Sizmek condivide e sostiene tutti questi obiettivi, che sono importanti per i diritti umani fondamentali dei cittadini UE. Tuttavia, il rispetto del GDPR è oneroso e in alcuni casi non è del tutto nero o del tutto bianco capire cosa significa essere compliance. Le autorità di regolamentazione hanno dato diversi pareri su vari aspetti della nuova legge, ma non vi è ancora accordo. Di conseguenza, potrebbe verificarsi un'interruzione o addirittura una riduzione dei contenuti e dei servizi digitali gratuiti che sono diventati fondamentali, se non addirittura essenziali per la nostra vita.

E in questa sitiazione incerta, come sta modificando la sua proposizione Sizmek, considerando che l'attività della società è fortemente legata ai dati?

Non c'è dubbio che i dati siano il carburante che guida la maggior parte delle aziende digitali, che siano piattaforme leader nel buy-side, come Sizmek, o siti web cui facciamo affidamento per news, informazioni o servizi. Fortunatamente, Sizmek ha trascorso gli ultimi anni a prepararsi per il nuovo regolamento, costruendo una policy dedicata, compilando la relativa documentazione e mettendo in atto sistemi per allineare le pratiche con il GDPR. Sebbene il tempo e lo sforzo siano stati significativi, prendiamo molto seriamente la nostra responsabilità nei confronti dei nostri clienti e, di conseguenza, diamo la priorità a risultare conformi al GDPR.

Recentemente lei ha dichiarato a Digiday che, come conseguenza diretta del GDPR, le DSP faranno un maggiore uso del targeting contestuale. Perché?

E come vi siete equipaggiati in questa direzione?

È possibile che non tutti saranno pronti per il GDPR quando entrerà in vigore, il prossimo 25 maggio. La legge riguarda i dati personali, che includono identificatori pseudonimi come cookie ID e indirizzi IP. E se un'azienda non si è preparata e non dispone di una base giuridica per trattare i dati personali, dovrà affidarsi ad altre fonti per condurre le proprie campagne di marketing digitale. Il targeting contestuale si basa sulle categorie di contenuti di una determinata pagina web e non sui dati personali. Di conseguenza, è un'opzione molto più favorevole al GDPR cui i marketer possono fare affidamento. Anche in questo caso, abbiamo speso gli ultimi dieci anni a sviluppare la soluzione di targeting contestuale leader del mercato: Peer39.

Come cambieranno, invece, le differenti attività inerenti la misurazione delle campagne con il GDPR?

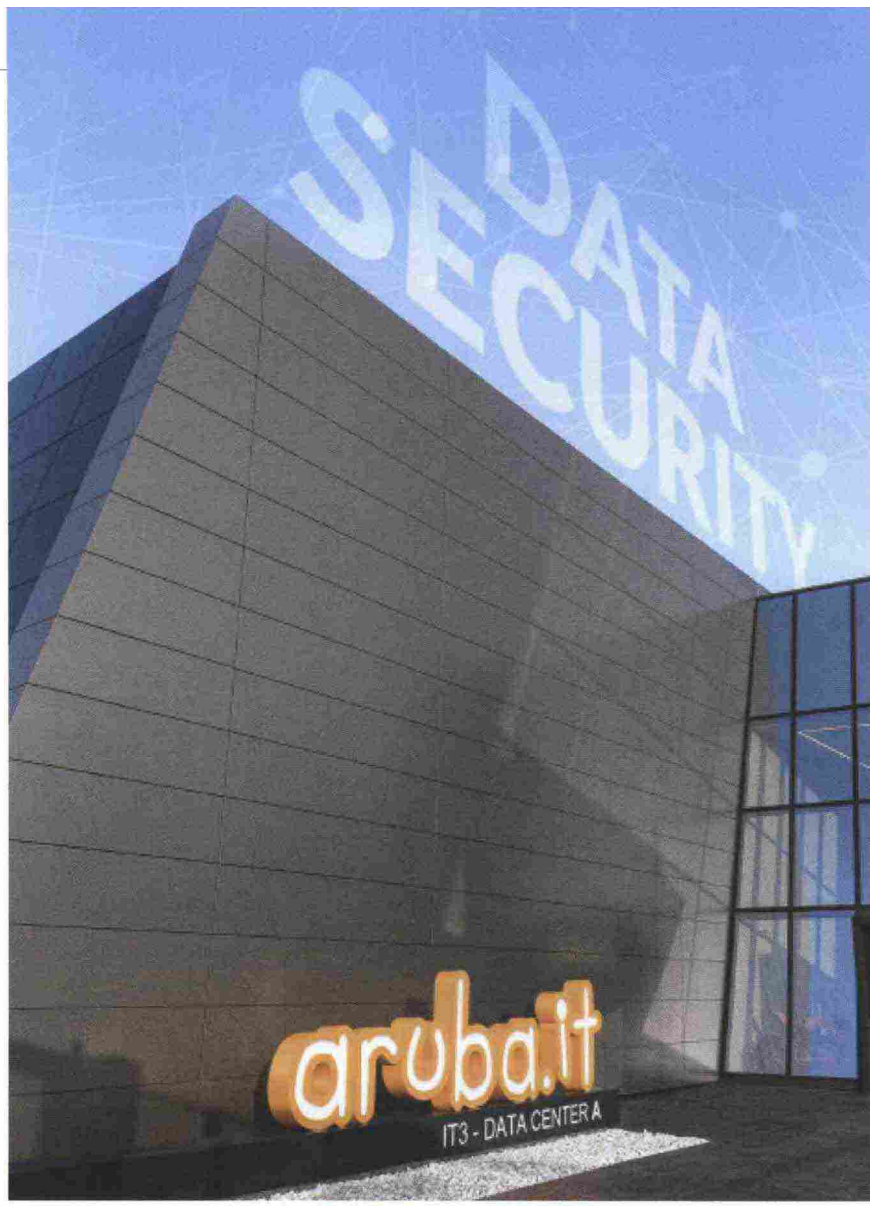
Le misurazioni basate su dati personali, quali cookie ID oppure indirizzi IP, devono, comunque, tenere conto delle indicazioni contenute nel GDPR. In Sizmek, questo è un aspetto centrale del business. Per questo, stiamo considerando la conformità al GDPR per tutti i nostri prodotti di misurazione, al pari di come stiamo lavorando con precisione su tutti gli altri aspetti della nostra attività.

In termini generali, pensa che questo regolamento possa favorire alcuni tipi di player a spese di altri?

Le imprese che hanno dedicato tempo e risorse alla preparazione alla nuova legge saranno avvantaggiate rispetto a quelle che non si sono preparate. Il tempo e l'impegno dedicati al GDPR, e il lavoro svolto, costituiranno il principale elemento di differenziazione.

In sintesi, quali sono le principali azioni intraprese da Sizmek per essere conforme? E quali sono, infine, le prossime sfide che si presenteranno per quanto riguarda la privacy e la tutela dei consumatori?

Sizmek ha un Chief Privacy Officer dedicato alla preparazione al GDPR. Abbiamo profuso davvero un grande impegno nel documentare la nostra base giuridica per l'elaborazione dei dati nell'ambito del GDPR e anche sul piano legale per definire al meglio le nostre posizioni nei contratti con i nostri clienti e fornitori. Abbiamo nominato un DPO, integrato la privacy nella nostra piattaforma, costruito e documentato le nostre pratiche di sicurezza, e stilato un piano in atto per affrontare il tema dell'ePrivacy. La prossima sfida, in questo senso, sarà l'armonizzazione delle norme nei diversi mercati, in modo che gli aspetti migliori del coraggioso passo intrapreso dall'UE possano essere integrati in altri mercati.

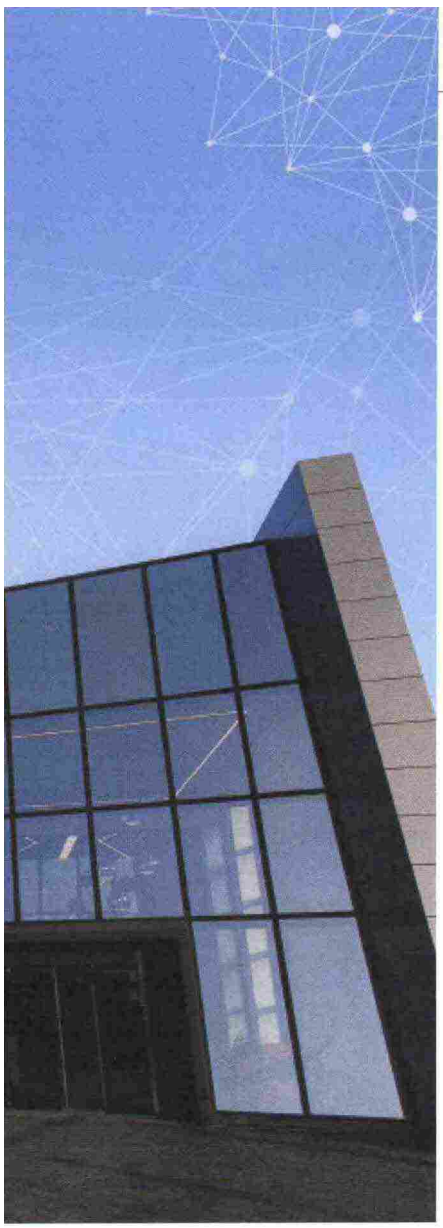


disponga di misure e policy per la sicurezza di notebook, smartphone, collegamenti in rete, dati personali trattati e conservati, il 55,5% afferma che sì, in parte l'azienda è pronta, mentre l'11,1% degli intervistati afferma che l'azienda non è ancora pronta per quanto concerne questo aspetto. Corrado Dati, Business Unit Manager IT Service Management di SB Italia, conferma: "Dai nostri dati emerge una forte criticità nella corretta gestione dei dati personali: le aziende devono lavorare ancora molto per assicurare la piena trasparenza e definire i flussi interni. Per noi di SB Italia l'approccio di fronte al GDPR deve essere globale: occorre che le aziende abbiano una chiara visione di insieme della normativa, in modo da assicurare il pieno rispetto delle regole e poter gestire in modo organico ed efficiente l'intero flusso dei dati, dalla raccolta alla cancellazione. Ciò che risulta, invece, ben chiaro a tutti è l'entità gravosa di eventuali sanzioni. L'implementazione di un sistema di gestione e compliance come il GDPR - continua Dati - può, inoltre, essere preso come spunto di miglioramento dalle aziende che hanno in programma una revisione dei requisiti, delle procedure e della messa in atto di contromisure per la salvaguardia della custodia delle informazioni. L'introduzione e l'adeguamento al GDPR permettono, inoltre, di regolamentare e rafforzare le misure minime di sicurezza, potenziando i controlli per la prevenzione di perdite o furto di informazioni (data breach, data loss prevention, ecc), non solo riguardanti i dati personali delle persone fisiche, ma anche in una visuale più allargata inerente ai copyright, alle proprietà intellettuali, ai progetti. Per tutti questi motivi crediamo sia necessario fare informazione e affidarsi a professionisti competenti".

L'esperto
In questa foto, Corrado Dati, ITSM Business Unit manager di SB Italia, società specializzata in soluzioni IT per la gestione, l'integrazione e l'ottimizzazione dei processi aziendali

PIENA APPLICAZIONE

Il 25 maggio 2018 è, quindi, la data di scadenza ufficiale - uguale per tutti i paesi dell'Unione Europea - per la piena applicazione del General Data Protection Regulation, il regolamento che mette al centro le persone, ne riconosce il diritto all'oblio e le informa in modo trasparente, leale e dinamico sul trattamento delle proprie informazioni. Non si tratta soltanto della principale evoluzione della normativa comunitaria fin dall'introduzione della Direttiva dell'Unione Europea sulla protezione dei dati, ma anche di un cambiamento di consapevolezza grazie al quale "difendere i dati" diventa difendere le persone, la loro identità. Il GDPR nasce, quindi, con l'intento di armonizzare le direttive a livello europeo, fissando delle regole chiare e precise su come mantenere e conservare i dati e, addirittura, prevede di creare una nuova figura aziendale con il ruolo di Data Protection Officer, specificatamente adibito a queste dinamiche. Parallelamente, sono diverse le associazioni e organizzazioni di service provider che hanno cercato di anticipare la regolamentazione in termini di sicurezza e protezione dei dati. Tra le prime, trova posto il CISPE, di cui Aruba è socio fondatore, una coalizione nata nel 2016,



che oggi raccoglie oltre venti tra i maggiori provider di infrastrutture cloud attive in quindici Paesi europei. Il CISPE ha dato vita a un Codice di Condotta (CoC) che precede l'entrata in vigore del GDPR, poiché, allineandosi ai suoi requisiti, ne condivide l'obiettivo principale: ridare ai cittadini il controllo dei propri dati personali, sapere dove questi dati si trovano e semplificare il contesto normativo per il commercio internazionale, unificando la regolamentazione all'interno dell'UE. Ai sensi del Codice di Condotta stilato dal CISPE, infatti, i provider di infrastrutture cloud non possono effettuare alcuna attività di data mining oppure tracciare i profili relativi ai clienti per effettuare eventuali attività di marketing, pubblicità o simili, per scopi personali o per la rivendita a terzi.

SERVIZI CLOUD

Nel caso del CISPE, i servizi cloud dichiarati a norma del Codice di Condotta sono identificati da un particolare marchio di garanzia - "CISPE service-declared"- che offre ai clienti dei servizi che lo espongono, la tranquillità di sapere che i dati ospitati presso le loro infrastrutture si trovano all'interno di data center localizzati entro i confini dell'Unione Europea e che sono conformi, già oggi, a determinati requisiti in termini di protezione e sicurezza delle informazioni. Non c'è bisogno di attendere il 25 maggio - dunque - per iniziare a corazzarsi, è essenziale arrivarci preparati e non aspettare la fatidica data a braccia conserte: questo termine è da considerarsi come un'opportunità per favorire la sicurezza e la crescita aziendale - magari velocizzandola -, creare posti di lavoro e, finalmente, beneficiare di un mercato digitale che potrebbe essere paragonato a quello statunitense o a quello cinese. Un altro tema di respiro internazionale, che rappresenta un aspetto importante di valutazione quando si inizia a usare un servizio cloud è il "data lock-in", ossia la difficoltà che si può incontrare qualora si decida di spostare i propri dati da un cloud provider a un altro. OCF, Open Cloud Foundation, è un'associazione di aziende tecnologiche che nasce con l'obiettivo di elaborare un framework che assicuri l'apertura del cloud, facendo convergere su questo obiettivo fornitori di tecnologie e servizi, cloud provider, aziende clienti, società di ricerca ed entità "regolatorie". Lo scopo è quello di preservare e garantire la libertà di scelta delle aziende clienti nel disegno dei loro business e di evitare il pericolo del lock-in che può essere esercitato da fornitori poco trasparenti.

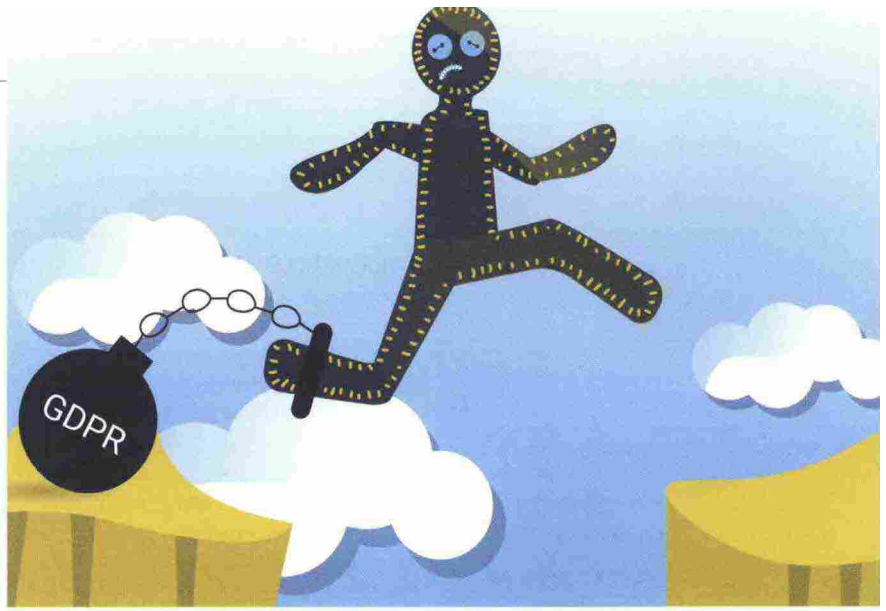
CRESCITA STABILE
PER ASSICURARE ALLE IMPRESE UN PROGRESSO COSTANTE DIVENTA OGGI NECESSARIO TUTELARE IL CONCETTO DI CLOUD APERTO

ACCELERAZIONE

In uno scenario cloud in forte accelerazione come quello attuale, molto presto ogni livello tecnologico dell'offerta ICT sarà a disposizione in modalità "as a service". Questo porterà le aziende clienti a poter fare affidamento su molti più servizi di outsourcing e a valore aggiunto offerti attraverso il cloud. Diventerà, quindi, essenziale evitare, da un lato, la nascita di nuovi sistemi a silos, dall'altro, che operatori cloud di prima grandezza possano imporre al mercato degli "standard" che si caratterizzerebbero inevitabilmente come chiusi e limiterebbero la dinamicità del mercato. Per assicurare una crescita stabile per qualsiasi business, oggi, e sempre più in futuro, sarà necessario tutelare il concetto di cloud aperto: permettere ai clienti di cambiare con facilità il proprio fornitore e consentire l'accesso a degli stack cloud eterogenei manterrà attiva la competizione e spingerà gli operatori a sviluppare e offrire importanti innovazioni. Grazie a questo tipo di iniziative - tra cui CISPE e OCF - è già possibile individuare i provider che si stanno attivando in tal senso, anche in anticipo rispetto all'evoluzione normativa, compiendo una serie di passaggi che garantiscono un sistema più attento alla sicurezza e alla trasparenza dei servizi in cloud. Tutto questo, però, non fa cambiare il rischio principale: un numero significativo di imprese italiane rischia di incorrere in pesanti multe a seguito del proprio ritardo di preparazione in vista dell'implementazione del Regolamento Generale Europeo sulla Protezione dei Dati nel prossimo maggio. E questo - come rilevato in precedenza - è il risultato di una ricerca condotta da Senzing, impresa di software con sede in California.

LA RICERCA: MILLE COINVOLTI

La ricerca - "Finding The Missing Link in GDPR Compliance" - si basa sulle opinioni espresse da oltre mille dirigenti di imprese con sede in Regno Unito, Francia, Germania, Spagna e Italia. Le aziende italiane sono estremamente preoccupate riguardo alla loro capacità di adempiere alle disposizioni del GDPR: quasi la metà (43%) si dichiara "allarmata", mentre molte altre dimostrano un'inquietante mancanza di consapevolezza riguardo alle conseguenze del GDPR e confidano pericolosamente nel fatto che non ne saranno toccate. Sempre secondo la ricerca di Senzing, le imprese riceveranno mediamente 89 richieste collegate al GDPR



al mese, per le quali dovranno effettuare ricerche in una media di 23 diverse banche dati e dedicare a ciascuna di esse circa cinque minuti. Su base mensile, il tempo dedicato alla semplice ricerca di dati sarà di oltre 10.300 minuti (172 ore), vale a dire oltre otto ore di ricerca per giorno lavorativo - l'equivalente di un impiegato dedicato a tempo pieno esclusivamente alle ricerche legate al GDPR. Il problema risulta particolarmente grave per le grandi aziende, per le quali c'è da attendersi una media di 246 richieste al mese, per le quali dovranno effettuare ricerche in una media di 43 diverse banche dati e dedicare a ciascuna di esse oltre sette minuti. Il tempo totale che dovranno dedicare mensilmente a tali ricerche è stimato in oltre 75.500 minuti (1.259 ore), vale a dire quasi 60 ore di ricerca per giorno lavorativo - l'equivalente di 7,5 impiegati dedicati a tempo pieno unicamente alle ricerche legate al GDPR. Secondo Jeff Jonas, fondatore e ceo di Senzing, "I risultati della ricerca evidenziano le reali dimensioni della sfida costituita dall'adempimento alle disposizioni del GDPR. A poco più di due mesi dalla sua entrata in vigore, il fatto che il 43% delle imprese italiane si dichiarino preoccupate in merito alla loro capacità di essere pronte ad adempiere al nuovo regolamento rappresenta un grave segnale d'allarme. Non soltanto il management, ma anche gli azionisti hanno tutte le ragioni per innervosirsi davanti a simili cifre: per molte società quotate in Borsa il rischio di vedersi affibiare multe salate è infatti elevato e la loro quotazione ne risentirebbe. Le grandi aziende italiane appaiono particolarmente vulnerabili".

IMPATTO NOTEVOLE

Soltanto il 29% delle imprese italiane appare consapevole del rischio di incorrere in multe molto severe, nel peggiore dei casi pari a 20 milioni di euro o al 4% del fatturato annuale. Un inquietante 24% ritiene che non subirà alcuna conseguenza da eventuali multe, mentre il 12% dichiara di "ignorarne" l'impatto. Un alto numero di imprese italiane si dichiara preoccupato in merito alla propria capacità di gestione in termini di GDPR di ciascuna delle proprie banche dati. Oltre una su dieci (13%) non si dichiara fiduciosa a riguardo, mentre soltanto un terzo (32%) si dichiara "molto fiducioso". A poche settimane dalla sua entrata in vigore, questi risultati evidenziano l'ampiezza della sfida davanti a cui si trovano le imprese italiane per essere "pronte al GDPR". Molte aziende italiane stanno tuttavia almeno cominciando a prendere consapevolezza della portata del compito di pianificazione che le attende in vista del GDPR. La metà (50%) sta programmando una revisione dei propri sistemi di trattamento dei dati dei clienti, mentre il 16% intende impiegare un maggior numero di analisti per la raccolta dati; e un ulteriore 10% progetta di affidare la gestione dei propri dati a terzi. Un preoccupante 13% dichiara tuttavia di "non sapere" quali azioni intraprendere e oltre un quarto (26%) ritiene di essere già a posto e di non dovere prendere alcuna misura. A riguardo, Jonas ha commentato: "Se, da un lato, sono preoccupato riguardo alla capacità delle imprese italiane di essere pronte per l'entrata in vigore del GDPR, dall'altro ritengo, comunque, incoraggiante il fatto che molte di loro stiano investendo in nuove infrastrutture informatiche in modo da ripulire i propri sistemi a fronte di questo enorme cambiamento normativo. Resta allarmante il fatto che la maggioranza delle imprese italiane non siano consapevoli delle multe in cui potrebbero incorrere in caso di inadempienza; per alcune di esse queste potrebbero risultare fatali, e anche quelle più grandi - e in ogni caso i loro azionisti - potrebbero subire un danno notevole. Un numero significativo di imprese italiane, molto semplicemente, non comprende i pericoli a cui sta andando incontro: non c'è da stare tranquilli".

ANELLO MANCANTE

L'ELEMENTO CHE OGGI APPARE PIÙ PREOCCUPANTE SEMBRA COSTITUITO DALLA INSUFFICIENTE RICERCA PER SINGOLO SOGGETTO

IMPRESE A RISCHIO

Sulla base delle risposte ricevute, Senzing calcola che un quarto (24%) delle imprese UE siano "a rischio" di non poter adempiere alle disposizioni, mentre un ulteriore 36% è "in difficoltà" e soltanto il 40% è classificabile come "pronto". Considerando queste percentuali in proporzione al volume d'affari complessivo delle imprese europee, le multe potrebbero potenzialmente ammontare a decine, se non a centinaia di miliardi di euro. Jonas ha aggiunto: "Essere in grado di scoprire chi è chi e dove si trovano i relativi dati è il primo principio per adempiere alle disposizioni del GDPR. I risultati della ricerca indicano che l'anello mancante è costituito dalla ricerca per soggetto singolo. Alle imprese italiane sfugge quanto sia urgente la necessità di poter effettuare una ricerca efficiente per soggetto singolo in modo da scoprire rapidamente le singole identità nei propri dati. In mancanza di ciò, vale a dire del fattore chiave per essere pronti in vista del RGPD, molte imprese sono destinate a essere inadempienti". Per colmare la lacuna della ricerca per soggetto singolo, Senzing ha lanciato anche "G2 for GDPR", un software sviluppato per consentire alle imprese di migliorare i propri dati in maniera rapida e conveniente, includendo banche dati multiple, input errati, errori di digitazione, duplicazioni e varianti dei nomi. E aggregando tutti i dati relativi allo stesso soggetto, allo scopo di facilitare l'adempimento al GDPR.