KASPERSKY lab

Pronti, partenza, via: stringiamo il cerchio sulla conformità al GDPR

"L'adesione alla regolamentazione della privacy dei dati non è nulla di nuovo per le aziende con sede nell'UE."

Per poter vincere questa sfida, è importante capire i cambiamenti principali[1] che vi riguarderanno:

- Tutti i dati personali che controllate e gestite, a prescindere che vengano elaborati nell'UE o meno, dovranno essere trattati in modo equo e trasparente, con un utilizzo chiaro nei confronti dei soggetti a cui i dati appartengono (ovvero i cittadini).
- Nel caso di violazione delle normative, saranno applicate sanzioni pecuniarie severe con un valore fino al 4% del fatturato globale annuale o € 20 milioni (quello che risulterà essere il valore maggiore).
- Sarà necessario un consenso più rigoroso per l'utilizzo dei dati, agevolando ai cittadini la possibilità di revoca di tale consenso qualora lo desiderino.
- Le violazioni dei dati devono essere notificate entro 72 ore dal momento in cui il gestore dei dati ne viene a conoscenza.
- I soggetti interessati godranno di diritti più ampi per ottenere informazioni su modalità, posizione e scopi dell'elaborazione dei propri dati.
- La cancellazione dei dati (o "il diritto all'oblio") sarà semplificata, con i soggetti proprietari dei dati che potranno richiedere la cancellazione o l'interruzione del trattamento dei propri dati (dimostrando che la richiesta soddisfa determinate condizioni).
- Sarà abilitata la portabilità dei dati, che conferisce ai soggetti proprietari dei dati il diritto di ricevere i dati personali che li riguardano.
- I processi di elaborazione dei dati (o "Privacy by design") devono essere inclusi fin dalle fasi iniziali della progettazione dei nuovi sistemi, piuttosto che aggiunti in un secondo momento.
- Sarà obbligatoria la presenza di responsabili della protezione dei dati per le aziende la cui attività consiste in operazioni di elaborazione che richiedono un monitoraggio regolare e sistematico dei contenuti dei dati dei soggetti interessati su larga scala o in alcuni casi in cui vengono elaborati volumi significativi di dati di "categoria speciale".

Non c'è scampo: il Regolamento generale sulla protezione dei dati (GDPR) sta per arrivare e non importa il ramo aziendale in cui lavorate, reparto delle Risorse umane, dipartimento di marketing, legale o IT, il cambiamento vi riguarderà e avrà un impatto sulla vostra giornata lavorativa. Se gestite, possedete o utilizzate dati personali, che si tratti dei dati dei dipendenti, di informazioni sui clienti o sui potenziali clienti, il GDPR porterà dei cambiamenti alle vostre pratiche lavorative e sta a voi metterli in atto.

Sorreggere il fardello del GDPR

Proprio come un personal trainer trasmette la motivazione e lo schema per il successo, questa guida definirà un piano d'attacco per dare un taglio alla confusione e accompagnarvi al traguardo: la conformità al GPDR.

La conformità alla normativa in materia di privacy dei dati non è una novità per le aziende con sede nell'UE. Tuttavia, quando il GDPR entrerà in vigore il 25 maggio 2018, sostituendo la Direttiva sulla protezione dei dati 95/46/CE, queste aziende dovranno essere pronte ad affrontare un nuovo approccio verso la privacy dei dati, che consentirà ai cittadini dell'UE di avere un maggiore controllo sui propri dati personali e sul loro trattamento.

Grazie a campagne dedicate volte a formare le aziende di tutta Europa affinchè riescano a soddisfare i nuovi criteri - e considerando anche le relative multe in caso di mancanza di conformità - che cosa rappresenta tutto questo per gli individui all'interno di un'azienda? Il fardello che sono chiamati a sostenere è sopportabile?

Nonostante i principali cambiamenti descritti, gran parte del lavoro di base è già stato realizzato ai sensi delle normative vigenti sulla protezione dei dati. Lungi dall'essere un fardello, la natura rigorosa del GDPR costituisce un aspetto vantaggioso per le aziende e può avere benefici incommensurabili per la salute e per il benessere futuri delle organizzazioni, se affrontato nel modo giusto.

I responsabili potrebbero essere impegnati nel compito di districare il quadro generale della normativa, mentre ogni dipendente deve dimostrare di essere all'altezza della sfida posta dall'integrità dei dati trattati. La sicurezza e la conservazione sicura dei dati in vostro possesso rivestiranno un'importanza ancora superiore. Con il fine e gli obiettivi del GDPR ben stabiliti, sta a tutti i membri dell'azienda impegnarsi per raggiungere questo traguardo fondamentale verso la conformità e diffondere le pratiche di gestione dei dati a tutto campo.

Proprio come quando si affronta un cambiamento nello stile di vita o ci si pone l'obiettivo di mettersi in forma per i mesi estivi, l'approccio verso il GDPR a livello dipartimentale può essere realizzato solo apportando lievi ma significativi cambiamenti che insieme garantiscono prontezza per l'entrata in vigore del GDPR nel 2018.

1 http://www.eugdpr.org/key-changes.html

Il grattacapo per vendite e marketing

"Il GDPR non ci rallenterà, aggiungendo adempimenti burocratici al team di vendita ed alle campagne e-mail rivolte a specifici contatti?"

Dati nei dipartimenti: approccio detox

- Quindi, da dove iniziare? Invece di avere una reazione istintiva o di adottare un approccio da "dieta aggressiva" verso questa problematica, affrontando la questione nel modo giusto, è possibile ottenere integrità dei dati sul lungo termine e la conformità al GDPR risulterà più semplice di quanto appaia.

Reclami comuni

Il team di vendita e di marketing è generalmente focalizzato sull'utilizzo dei dati dei clienti e dei potenziali clienti per veicolare le vendite e migliorare la brand awarness. Con vaste banche dati e campagne mirate, il dipartimento competente è chiamato ad aderire a rigorose linee guida di protezione dei dati e adottare una politica opt-out per garantire la conformità.

L'effetto del GDPR

Se utilizzate i dati personali per il marketing mirato e le campagne di vendita, siete chiamati a rispettare le normative aggiornate. Fare affidamento su caselle già selezionate nei moduli di consenso o utilizzare il marketing con contatti che non hanno specificamente annullato l'iscrizione non costituirà più consenso. Per l'elaborazione dei dati sensibili è necessario un consenso esplicito e volontario. Tuttavia, per i dati non sensibili è valido un consenso "ambiguo". Anche la misura della cancellazione dei dati deve essere realizzata ai sensi del "diritto all'oblio", che semplificherà agli individui la richiesta di rimozione dei propri dati dal vostro database.

Piano di fitness dei dati: cinque passaggi

- Coloro che formalizzano l'opt-out o che rimangono in silenzio, devono ora fornire esplicito consenso o procedere con l'opt-in per venire inclusi nel vostro database marketing. Ma prima di passare al setaccio tutto il database, pensate al modo migliore per recuperare un elenco di contatti utile e pulito come risultato finale.
- I contatti nel database devono scegliere di rispondere e selezionare l'opt-in, perciò cercate di motivare l'adesione servendovi di un importante call to action e di contenuti interessanti.
- Ai sensi del GDPR, il testo del consenso fornito insieme al materiale di marketing deve essere chiaro e conciso, nonché semplificare agli utenti la decisione sulla possibilità e le modalità di utilizzare i loro dati.
- Tenete traccia trasparente di coloro che decidono di aderire.
- È necessario il consenso esplicito per poter mettere in atto l'azione di marketing con un utente: la partecipazione ad un evento o un biglietto da visita lasciato a una fiera non bastano per poter aggiungere gli utenti al database di e-mail marketing. Gli utenti devono selezionare esplicitamente una casella come azione chiara e affermativa, fornire in alternativa una dichiarazione in forma differente o eseguire un'azione che indichi chiaramente il consenso da parte del soggetto all'elaborazione dei propri dati personali. Tali azioni potrebbero comprendere l'inserimento del proprio indirizzo e-mail in una sezione opzionale di un modulo online, che contenga una dichiarazione di non responsabilità circa l'uso dello stesso.

Il team legale

"Assicurarci che il nostro staff comprenda e aderisca alle normative e che i nostri contratti e SLA con i fornitori siano conformi al GDPR metterà a dura prova le nostre risorse."

Solo il 38%
dei responsabili IT ha una buona conoscenza del GDPR.

Reclami comuni

Il team legale deve già affrontare una serie di norme per garantire che l'azienda aderisca alle leggi sulla privacy e sulla protezione dei dati e sarebbe perdonato se mostrasse timore nei confronti dell'impatto del GDPR sulle attività quotidiane.

L'effetto del GDPR

Non tutto il carico deve ricadere sulle spalle del dipartimento legale. Tuttavia, sono presenti aree principali su cui il dipartimento legale deve concentrarsi. La gestione dei contratti e le trattative con clienti e fornitori rappresenta una di tali aree. Ai sensi del GDPR, la vostra attività sarà responsabile per qualsiasi violazione delle norme associate ai dati elaborati internamente, tramite terzi o per mezzo di partner con cui collaborate. Pertanto, è cruciale garantire conformità a tutto campo. Team e database di marketing interni, agenzie di comunicazione e centri di dati in outsourcing: se non si rispettano le regole o se si verifica una violazione, la vostra attività ne pagherà le conseguenze. Assicurarsi di applicare rigidi criteri di tutela dei dati è di primaria importanza.

Piano di fitness dei dati: cinque passaggi

- Eventuali contratti che si estendano oltre il termine del GDPR, dovranno essere rivisti e aggiornati secondo necessità, per garantire che soddisfino le nuove norme sul trattamento dei dati.
- Assicurarsi che eventuali nuovi contratti o trattative tengano conto del GDPR, onde evitare il panico dell'ultimo minuto quando tra un anno tutto dovrà essere aggiornato.
- A tale scopo, è opportuno aggiungere clausole specifiche facilmente modificabili per garantire la conformità al GDPR quando entrerà in vigore.
- Per semplificare tale operazione, segnatevi in agenda il momento in cui apportare tali modifiche nei piani.
- Collaborate con i vostri fornitori per garantire la conformità. La normativa interessa anche i fornitori per cui collaborando potrete ottimizzare le risorse e garantire una risposta solida da entrambe le parti.

Il tallone di Achille di finanza e contabilità

Il **32%**
dei responsabili IT ha una consapevolezza bassa o nulla del fatto che, secondo il GDPR, le aziende europee debbano riferire una violazione dei dati entro 72 ore.

"Il GDPR avrà un enorme impatto sul nostro modo di lavorare, con ancora più occhi puntati sul nostro dipartimento per garantire che elaborazione e protezione dei dati seguano alla lettera la normativa."

Reclami comuni

Il settore finanziario rappresenta una realtà altamente regolamentata, già in prima linea per la contabilità, trattando grandi quantità di informazioni personali e sensibili ogni giorno.

L'effetto del GDPR

A causa del volume dei dati personali con cui lavorano, finanza e contabilità costituiranno importanti punti di riferimento per il responsabile della protezione dei dati e per le autorità di controllo incaricate di garantire la conformità al GDPR. La sicurezza dei dati personali che si muovono attraverso i sistemi è il fattore che potrebbe essere soggetto a importanti multe in caso di violazione. Tuttavia, grazie a responsabili già abituati a operare sotto stretti controlli regolamentari, il GDPR contribuirà solo a rafforzare la natura solida e trasparente della funzione finanziaria.

Piano di fitness dei dati: cinque passaggi

- Accertatevi di definire un processo di escalation chiaro all'interno del dipartimento al fine di segnalare immediatamente eventuali violazioni dei dati alle autorità, qualora dovesse accadere il peggio.
- Una verifica dei dati valuterà quali modifiche è necessario apportare alle pratiche attuali per garantire la conformità. Questo non significa ripartire da zero con le politiche, ma aggiornarle per assicurarsi di spuntare le nuove caselle del GDPR.
- Automatizzare i processi contribuirà a ridurre l'errore umano e i rischi relazionati con le violazioni dei dati, che siano esse intenzionali o meno.
- Rivedete le procedure di memorizzazione dei dati per la conservazione e la distruzione dei record personali, poiché i parametri cambieranno in virtù del GDPR.
- Ponete la protezione dei dati al centro di tutti i processi in corso e non pensate alla procedura come un compito aggiuntivo, ma come parte fondamentale per l'azienda.

Il grattacapo per il reparto Risorse umane

Il **29%**
dei responsabili IT ha una consapevolezza bassa o nulla del fatto che le normative riguardino i dati personali europei archiviati all'interno e all'esterno dell'Europa.

"Con a carico il compito arduo dell'archiviazione, della salvaguardia e della cancellazione dei dati delle Risorse umane, che già costituiscono un grattacapo normativo, il GDPR porterà sicuramente solo maggiore pena per questo dipartimento?"

Reclami comuni

Il reparto Risorse umane gestisce una grande quantità di dati personali: dai CV dei dipendenti attuali, degli ex dipendenti come dei candidati che non sono stati assunti, passando per i dati dei dipendenti tra cui informazioni di contatto e dati bancari.

L'effetto del GDPR

Ai sensi del GDPR, i dipendenti godranno di diritti migliori circa l'uso e la conservazione dei dati, con relativo grattacapo per i datori di lavoro. Tuttavia, anche se l'impatto sul dipartimento Risorse Umane è significativo, la sfida non è insormontabile. Il dipartimento dovrà attuare una politica di maggior trasparenza sulle intenzioni d'uso dei dati personali e dovrà offrire ai dipendenti la possibilità di richiederne l'eliminazione. Ciò vale per i dipendenti attuali e per gli ex dipendenti.

Piano di fitness dei dati: cinque passaggi

- Per alleviare la pressione sulle Risorse Umane, il primo passo logico per capire dove è necessario apportare delle modifiche è una verifica dei processi e delle politiche attuali di gestione dei dati.
- Ciò consentirà di sapere il momento in cui è necessario aggiornare contratti dei dipendenti, manuali e politiche aziendali.
- Informate il vostro personale, fornendo ulteriori dettagli ai dipendenti e a coloro che richiedono lavoro allo scopo di raccogliere, ai sensi della legge, i loro dati e di assicurarsi che conoscano i loro diritti.
- Per una risposta rapida a una violazione dei dati, nominate un individuo o un team di risposta che reagisca a qualsiasi incidente.
- Una formazione costante su come identificare e rispondere ad una violazione, abbinata a politiche adeguate, assicurerà che tale aspetto del regolamento venga affrontato con calma e fiducia.

L’irritazione del reparto IT

“Il mio incarico non prevede il possesso o la gestione dei dati personali, quindi perché dovrei preoccuparmi del GDPR?”

Il **22%**

dei responsabili IT non è sicuro che la propria organizzazione sarà pienamente conforme al GDPR entro il 25 maggio 2018.

Reclami comuni

Per i professionisti del reparto IT, garantire la continuità dell’infrastruttura aziendale e mantenere solidi e affidabili i sistemi rappresenta la sfida principale. Il GDPR non è un aspetto che incrocia esplicitamente la loro traiettoria. Tuttavia, gli efficaci processi IT rappresentano la base per garantire e mantenere la conformità al GDPR, nonché per raggiungere un approccio semplificato, sicuro e trasparente.

L’effetto del GDPR

Il GDPR influenzerà il dipartimento IT in molteplici modi e si incrocerà con altri dipartimenti nel momento in cui aggiorneranno e snelliranno i processi attivi. Ad esempio, il team di marketing richiederà supporto per le campagne opt-in e via e-mail, al fine di assicurarsi che la tecnologia tenga traccia dei moduli di consenso, ecc. Con un peso maggiore sui cittadini che hanno la possibilità di accedere alle proprie informazioni e richiederne la rimozione o che intendono comprenderne il trattamento in modo più approfondito, i sistemi e i programmi che contengono queste informazioni devono essere facili da navigare e devono garantire la piena trasparenza per chi ne fa uso. Inoltre, mettere al sicuro i dati in possesso della vostra organizzazione è di vitale importanza.

Piano di fitness dei dati: cinque passaggi

- Lavorare con altri dipartimenti nell’organizzazione per capire le loro esigenze e l’impatto sul software e sui sistemi in uso, nonché il tipo di supporto necessario per garantire conformità al GDPR.
- Catalogare ogni singolo dato personale al fine di assicurare la trasparenza e un facile accesso alle informazioni, elementi necessari ai fini della rendicontazione o della soddisfazione delle richieste dei soggetti interessati a cui appartengono i dati.
- Impostare percorsi di controllo chiari per ogni singolo dato personale che si muove nell’ambito della organizzazione.
- Applicare misure specifiche sulla privacy per proteggere le informazioni e ridurre al minimo la probabilità e l’impatto delle violazioni dei dati, comprese la crittografia e la trasformazione in forma anonima.
- Applicare i requisiti del GDPR nella fase di progettazione di eventuali nuovi software o aggiornamenti di infrastrutture, al fine di garantirne la conformità e assicurare che i dati siano al sicuro e conservati in modo integro.

Il 17%
dei responsabili IT ha ammesso che la propria organizzazione è poco o per nulla preparata per il GDPR.

Invito all'azione: esercizi di gruppo

Il lavoro illustrato potrebbe sembrare scoraggiante, ma le aziende e i singoli dipartimenti stanno già mostrando progressi soddisfacenti nel garantire l'integrità dei dati. Per contribuire al miglioramento e alla continuità aziendale in condizioni di picco, le abitudini verso la sicurezza dei dati personali devono essere rafforzate e mantenute su tutta la linea.

Piano di fitness dei dati: cinque passaggi

- **Guardare lontano.** Usare un approccio poco convinto per la preparazione dell'azienda al GDPR non vi premierà. La chiave è implementare le nuove procedure del futuro. Se non adottate le giuste misure ora, l'attività potrebbe paralizzarsi.
- **Nominare un coach.** Ogni dipartimento ha bisogno di un responsabile che riunisca le informazioni e garantisca che tutti siano in linea con la pianificazione.
- **Schiarirsi le idee.** Raggiungere un cambiamento nei dipartimenti e nell'organizzazione richiede una mente aperta e la volontà di cambiare i processi per la salute dell'attività sul lungo termine.
- **Garantire formazione continua.** Le politiche di protezione dei dati devono essere regolarmente aggiornate e comunicate in modo chiaro a tutti i dipartimenti, al personale e ai fornitori.
- **Lavorare con un personal trainer.** Il supporto di terze parti non solo vi aiuterà a rimanere in pista, ma anche a garantire l'integrità dei dati nel futuro.

Se non specificatamente menzionato, tutte le statistiche contenute in questo whitepaper provengono da una ricerca condotta in Aprile 2017 da Airlington Research per conto di Kaspersky Lab. Per questa ricerca, è stato chiesto ad oltre 2.300 IT decision maker di tutta Europa, provenienti da aziende con più di 50 dipendenti, quale fosse la loro visione e livello di conoscenza sul tema GDPR.

For more information about Kaspersky products and services contact your account rep or visit www.kaspersky.com

Kaspersky Lab
Kaspersky Lab, 1st Floor
2 Kingdom Street
London, W2 6BD, UK
www.kaspersky.com