Agenda Digitale.eu
IL PRIMO GIORNALE SULL'AGENDA DIGITALE ITALIANA

GDPR, quanto costerà a una pmi adeguarsi (e come ottimizzare la spesa)

LINK: https://www.agendadigitale.eu/infrastrutture/gdpr-quanto-costera-a-una-pmi-adeguarsi-e-come-ottimizzare-la-spesa/

GDPR, quanto costerà a una pmi adeguarsi (e come ottimizzare la spesa)di Giuseppe Vaciago, Partner R&P Legal e fondatore di Tech&Law Center 3 ore fa 27 dicembre 2017 Il GDPR comporterà una spesa significativa per le aziende e le pmi devono investire con oculatezza il budget limitato disponibile. Ecco come Personaggi G Giuseppe Vaciago Argomenti G GDPR L Legge europea 2017 P privacy S servizi it V vaciago Quanto costa il GDPR alle aziende? La risposta ad una simile domanda di questo tipo non esiste ovviamente in termini assoluti, ma alcune riflessioni sul tema sono possibili e doverose. IAPP (International Association of Privacy Professionals) ed Ernst & Young hanno recentemente pubblicato una ricerca su un campione di 600 esperti di privacy provenienti da tutto il mondo dalla quale emergono i seguenti dati: Il 75% delle multinazionali Europee (ossia società con più di 75.000 dipendenti nel mondo) hanno previsto un investimento di almeno 5 milioni di euro per l'adeguamento al GDPR con l'assunzione di almeno 2 o 3 dipendenti dedicati a tempo pieno al tema privacy. Interessante notare che gli stessi tipi di investimenti vengono effettuati dal 50% delle grandi multinazionali statunitensi. Delle circa 30.000 aziende seguite dai 600 esperti coinvolti in tale tipo di ricerca, solo il 60% sarà 'fully compliant' ossia pienamente conforme al GPDR entro maggio 2018. A distanza quindi di 7 mesi dall'entrata in vigore della normativa, molte società (soprattutto le PMI) si stanno rendendo conto di non riuscire ad arrivare in tempo alla scadenza prevista dal Regolamento Europeo. Il valore medio di investimento per l'adeguamento al GDPR per le aziende nel 2016 era di 349.000 euro, mentre nel 2017 è salito a 480.000 euro. Tale importo è rappresentato sia dai costi HR derivanti dal ruolo del DPO, dai costi dei consulenti e dagli investimenti in IT derivanti dalla necessità di essere compliant alla normativa. L'investimento complessivo nel 2017 è stato di 6,5 Miliardi di Euro su 30.000 aziende. Questi numeri ci fanno capire che il GDPR rappresenta un costo di non poco conto per le aziende e un'opportunità unica per i consulenti in materia. La scelta di aver dato due anni per l'adeguamento ha fatto proliferare il numero degli esperti in materia che hanno deciso di investire sulla privacy nella convinzione - non sempre corretta - che la consulenza in tema di GDPR sia simile ad altre attività di compliance già precedentemente svolte. Fatte queste premesse, il contesto italiano può difficilmente essere paragonato a quello Europeo. Il numero delle PMI ha raggiunto nel 2016 quota 145.000. Sono numeri assolutamente unici che devono far pensare a modalità alternative di gestione del processo di adeguamento al GDPR. Non esistono statistiche in merito all'investimento medio delle realtà nazionali in materia di privacy, ma è difficile ipotizzare che una PMI con un fatturato non superiore ai 5 milioni di Euro, possa e voglia investire, nel suo complesso, più di 50.000 euro per l'adeguamento e più di 25.000 euro per la gestione ordinaria degli adempimenti previsti dal GDPR. Una capacità di investimento così ridotto obbliga sempre di più a scelte strategiche in merito al processo di adeguamento al GDPR. Alcune realtà prediligono la scelta 'legal' e preferiscono puntare sull'adeguamento più formale che sostanziale della normativa (revisione delle informative, policies dei dipendenti, registro del trattamento, regolamentazione del trasferimento dei dati all'estero). Altre invece puntano sulla scelta 'tech' e sfruttano l'occasione di riorganizzare infrastrutture IT spesso assolutamente inadeguate anche al rispetto delle misure minime previste dall'attuale Codice della Privacy (si pensi ad esempio all'assenza di sistemi di

Agenda Digitale.eu
IL PRIMO GIORNALE SULL'AGENDA DIGITALE ITALIANA

autorizzazione efficaci, alla necessità di creare piani di business continuity e disaster recovery, all'utilizzo di piattaforme cloud che non gestiscono il dato in modo compliant con la normativa europea o alla totale assenza di audit di seconda parte sui fornitori di servizi IT). Il risultato di questa scelta 'a metà' è che, secondo IDC, il 78% delle aziende italiane non è pronto per il GDPR e difficilmente - mi permetto di sostenere - lo sarà entro maggio del 2018. Dando per scontato che il risicato budget messo a disposizione per l'adeguamento al GDPR rimanga pressoché identico o aumenti in maniera non significativa nei prossimi mesi, quali sono le soluzioni che un'azienda italiana deve adottare per essere compliant? Senza alcuna pretesa di esaustività, provo a dare tre suggerimenti: Scelta del consulente: il GDPR porta ad un cambio di paradigma nella gestione del dato e il principio di accountability (ossia essere in grado di dimostrare l'adeguatezza dei propri processi di compliance) impone la necessità di valutare attentamente i professionisti che accompagneranno l'azienda al processo di adeguamento. Tale incarico non può essere assegnato solo ad un professionista del settore legale, ma neanche esclusivamente ad una società informatica. La scelta deve ricadere su una proposta che contenga le due professionalità in modo congiunto e coordinato. Nominare il DPO: per le società che devono avere tale figura professionale, il suggerimento è nominarlo il prima possibile evitando di 'pescare' all'interno dell'azienda, salvo che non vi sia un soggetto con una competenza specifica in materia. L'investimento nel DPO prima di maggio 2018 può consentire di facilitare il raccordo con i consulenti che stanno già lavorando in materia e a tendere risparmiare nella gestione futura degli adempimenti. Investimento in infrastrutture IT: esistono raramente soluzioni 'low cost' nel caso in cui si voglia adeguatamente intervenire in ambito IT adeguandosi agli standard riconosciuti a livello internazionale. Il GDPR, infatti, costituisce un'opportunità unica non solo per trattare adeguatamente i dati personali dei propri dipendenti o di terzi (clienti, fornitori etc), ma anche di costituire un sistema di protezione del proprio know-how aziendale oggi sempre più spesso messo in pericolo da attività illecite commesse da dipendenti infedeli o da cyber-criminali. Fino ad ora abbiamo parlato di costi per l'adeguamento al GDPR, ma quanto costerà a un'azienda non adeguarsi? Anche se oramai lo sanno tutti, mi permetto di ribadirlo. Nel caso di violazione più grave la sanzione oscillerà tra 20 Milioni di euro e il 4% del fatturato. Per una società di 5 milioni di euro di fatturato, il 4% è 200.000 euro. Non potrebbe essere quello un parametro di riferimento per tarare un budget idoneo per l'adeguamento a tale normativa? Consapevole che la mia sia una provocazione, ritengo che sia arrivato il momento di reagire al GDPR in modo serio e strutturato decidendo di investire sul futuro: nessuna società, anche la più 'offline', potrà permettersi, nei prossimi anni, di prescindere da un trattamento idoneo, adeguato e sicuro del dato personale.