Dimentichiamo le frasi leggibili solo aumentando del 50% lo zoom sulla pagina, chiudiamo in un cassetto virtuale i tortuosi e spesso estenuanti percorsi per disiscriversi dai servizi di newsletter commerciali: la rivoluzione per la protezione dei dati digitali è alle porte, ed è qui per restare.

Non c'è da disperare: una volta presa confidenza con la materia ed aggiornate le procedure interne, in azienda ci si renderà conto che il Nuovo Regolamento Europeo per la Protezione dei Dati è molto più di un insieme di restrizioni, e che in effetti nasconde delle ottime possibilità di business.

Ma andiamo con ordine, rispondendo alla domanda che in tanti si sono posti negli ultimi mesi:

Cos'è il GDPR?

Si tratta di un pacchetto di norme che avranno effetto sull'intero territorio dell'Unione Europea e che coinvolgeranno le aziende, anche non europee, che acquisiscono e gestiscono i dati dei cittadini dell'UE.

Il regolamento UE 2016/679 (General Data Protection Regulation) stabilisce norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché norme relative alla libera circolazione di tali dati […] protegge i diritti e le libertà fondamentali

delle persone fisiche, in particolare il diritto alla protezione dei dati personali.

Pubblicato sulla Gazzetta Ufficiale dell'Unione Europea il 4 Maggio 2016 ed ufficialmente in vigore il 24 dello stesso mese, il GDPR diverrà definitivamente applicabile a partire dal 25 Maggio 2018
.

Ciò significa che entro quella data, tutte le aziende dovranno obbligatoriamente essersi adeguate alla nuova normativa.

Il Regolamento introduce regole più chiare in materia di informativa e consenso, definisce i limiti al trattamento automatizzato dei dati personali, pone le basi per l'esercizio di nuovi diritti, stabilisce criteri rigorosi per il trasferimento dei dati al di fuori dell'UE e per i casi di violazione dei dati personali (data breaches). (rif. sito Garante della Privacy)

Va bene, ma quale impatto avrà sulla mia azienda?

È la domanda che si sono posti quasi tutti, temendo scenari apocalittici in cui avrebbero dovuto distruggere tonnellate di dati (per fortuna, a differenza di alcuni anni fa, senza trovarsi con gli uffici sommersi di striscioline di carta scappate ai distruggidocumenti).

La realtà è che, date la specificità delle nuove regole e la consistenza delle sanzioni previste nei casi di mancato adeguamento, affidarsi a soluzioni arrangiate non è una buona idea.

Il GDPR prevede modifiche sostanziali al modo in cui vengono conservati ed utilizzati i dati raccolti (non solo online), ma anche alle modalità con cui le persone danno o meno il consenso al trattamento di quei dati.

Il primo passo dev'essere un'analisi delle pratiche in uso in azienda, così da sapere esattamente dove e come intervenire per garantire la conformità delle stesse.

La possibilità che si verifichino data breaches nei database aziendali è un rischio da evitare, così come i reclami ufficiali di clienti raggiunti da comunicazioni di marketing per le quali non hanno dato il consenso. Ma il “ segreto” del GDPR è che gli sforzi dedicati a questi aspetti possono essere trasformati in opportunità di business: evitare di frustrare clienti e potentials con comunicazioni indesiderate può andare a migliorare l’immagine del brand, mentre evitare ai team Marketing e Vendite di sprecare tempo targettizzando le persone sbagliate determina un miglioramento delle performance ed un’ottimizzazione delle risorse.

Insomma, le pratiche di adeguamento al nuovo regolamento europeo per la protezione dei dati possono essere ottime opportunità di crescita.

Ma prima di pensare ai benefici futuri, andiamo a vedere cosa serve per un adeguamento a regola d’arte.

Perché devo valutare i rischi privacy?

Il nuovo regolamento privacy introduce molti cambiamenti ed uno dei suoi pilastri è il principio di accountability
(tradotto in “responsabilizzazione e obbligo di rendicontazione“) che riguarda tutti i soggetti. Infatti, il titolare del trattamento dei dati deve essere in grado di dimostrare di avere adottato un processo complessivo di misure giuridiche, organizzative e tecniche per la protezione e il trattamento dei dati personali, anche attraverso l’elaborazione di specifici modelli organizzativi: deve dimostrare in modo positivo e proattivo che i trattamenti di dati effettuati sono adeguati e conformi al regolamento europeo in materia di privacy.

In particolare, il titolare del trattamento dovrebbe essere tenuto a mettere in atto misure adeguate ed efficaci ed essere in grado di dimostrare il proprio grado di conformità delle attività di trattamento con il regolamento, compresa l’efficacia delle misure. Si passa da una concezione prettamente formale di mero adempimento ad un approccio sostanziale di trattamento dei dati sensibili, tutela dei dati e delle persone stesse ed è pertanto strettamente connesso con le misure di sicurezza e con l’analisi del rischio, con la valutazione di impatto privacy e con i principi privacy by design e privacy by default che devono essere presenti nella progettazione di servizi e programmi.

A questo punto una valutazione dei rischi compresa l’approvazione di un budget da dedicare al

progetto, la redazione del progetto, l'identificazione dei soggetti che parteciperanno, l'analisi del flusso di informazioni che l'azienda tratta, l'identificazione dei rischi e delle possibili soluzioni e la verifica della compatibilità con il regolamento sono essenziali anche per evitare le sanzioni che arrivano al 4% del fatturato globale annuo.

Chi è il Data Protection Officer e cosa fa?

Il DPO è una figura professionale richiesta dal GDPR che in realtà è già presente in molte aziende: Chief Privacy Officer (CPO), Privacy Officer e Data Security Officer sono figure che si occupano in parte di quanto previsto dal nuovo regolamento per il Data Protection Officer.

Si tratta quindi di professionisti con competenze in campo informatico, giuridico, di valutazione dei rischi e di analisi dei processi.

Diversi specialisti del settore suggeriscono la scelta di una risorsa già presente in azienda per questo ruolo, il regolamento individua alcune figure interne che non possono essere nominate DPO, ossia quelle in "conflitto d'interessi" (come ad esempio l'AD, il responsabile del marketing e quello delle risorse umane).

La soluzione più veloce ed efficace può essere quella di ovviare alla formazione di una risorsa, nuova o già interna che sia, affidando questo ruolo ad un professionista del settore già in possesso di tutte le competenze necessarie a svolgere il ruolo di DPO nel migliore dei modi.

Cosa devo fare per mettermi in regola con il GDPR?

La procedura è meno complicata di quanto appare. Ma metterla in azione senza i giusti strumenti sarebbe come cercare di mangiare una zuppa con la forchetta: estenuante e potenzialmente inutile.

Prima di apportare modifiche alle procedure interne, è bene averle chiare nel loro complesso. Un'analisi accurata delle practices aziendali tramite servizi di consulenza sul nuovo regolamento privacy è il primo passo per evitare di perdersi dettagli per strada e mettere a rischio la conformità dell'azienda: le sanzioni possono arrivare al 4% del fatturato annuale globale (e siamo certi che preferireste utilizzare quei fondi

in ben altro modo!).

In generale, avvalersi di un consulente privacy esterno specializzato in conformità GDPR è una garanzia in termini di risultati, ma anche una scelta mirata in termini di ottimizzazione delle risorse interne: il tempo ormai scarseggia e non tutte le aziende possono permettersi di dirottare una risorsa su un ambito nuovo e complesso come il nuovo regolamento per la privacy.

E se non mi adeguo cosa succede?

Non vogliamo metterla giù più tragica del necessario, ma potrebbe essere un disastro in termini di sanzioni e di percezione del brand da parte dei consumatori.

Chi si sentirebbe al sicuro nell'affidarsi ad un'azienda che non garantisce che i dati sensibili dei clienti sono al sicuro e non vengono raccolti o utilizzati senza il loro consenso?

Non importa che la sede dell'azienda sia dentro o fuori dall'UE: se i dati raccolti sono quelli di cittadini europei, è necessario che le procedure siano conformi a quanto previsto dal GDPR.

Non solo: anche i tempi massimi per la notifica di un data breach sono ora indicati con precisione, pertanto è bene dimenticarsi della possibilità di procedere con l'adeguamento al GDPR e con gli adempimenti privacy per poi lasciarli nel dimenticatoio: non si tratta di fare uno sforzo una tantum, qui si fa sul serio e tutti i dipartimenti coinvolti nella raccolta e nella gestione dei dati devono essere proattivi.

Cosa può fare per me Studio Synthesis?

In una parola: moltissimo. I nostri consulenti privacy hanno alle spalle una lunga esperienza in tutti i settori che gravitano intorno all'adeguamento al nuovo regolamento: da quello informatico a quello legale, ci occupiamo di fornirti tutti gli strumenti necessari ad essere in regola con quanto previsto dalla checklist di adempimenti per la privacy.

L'esperienza con aziende di molteplici settori e di diverse dimensioni in materia di compliance normativa, sicurezza dei dati, responsabilità penale, i servizi di consulenza in materia di

trattamento dati personali (e molto altro) ci permette di offrirti un pacchetto di servizi completo e mirato.

Partendo da un'accurata analisi delle pratiche aziendali in materia di protezione dei dati, siamo in grado di elaborare una strategia mirata ed efficace che comprenda tutti gli aspetti toccati dal GDPR: consenso all'utilizzo dei dati, diritto degli utenti ad avere le proprie informazioni cancellate, sicurezza informatica per evitare data breaches, formazione specifica del personale che lavora quotidianamente con i dati.

Non solo: i nostri consulenti privacy possono svolgere le mansioni di Data Protection Officers, garantendo un controllo continuo sulle procedure interne ed occupandosi delle successive modifiche ed integrazioni delle normative vigenti (o in procinto di diventarlo).

Avrai al tuo fianco un professionista attento e dedicato, una risorsa importante per non doverti preoccupare di adeguamento e adempimenti privacy aziende: penserà a tutto lui.

Se invece preferisci che sia una risorsa interna a svolgere queste mansioni, possiamo occuparci di darle la formazione GDPR necessaria a svolgere i suoi compiti nel modo migliore per l'azienda.

La nostra stretta collaborazione con un gruppo di aziende che si occupa di sviluppare software CRM e di analisi dei dati ci consente inoltre di proporre soluzioni informatiche in grado di garantire la sicurezza dei dati e un costante aggiornamento delle procedure (come il fantomatico "consenso" attorno al quale ruota una parte importante del GDPR) per permettere ad ogni risorsa di lavorare nel modo migliore, ottimizzando i tempi.

I consulenti privacy Studio Synthesis affiancano le aziende passo dopo passo:

- analisi dei gap da colmare
- controllo dei processi di gestione degli incidenti
- identificazione PII e mappatura dei dati
- controllo dello stato degli strumenti di cybersecurity
- valutazione di terze parti
- valutazione dell'impatto del GDPR
- creazione dell'architettura di sicurezza
- protezione dei dati personalizzata
- consulenza DPO
- revisione delle policy interne

Materiali aggiuntivi

Proponiamo alcuni articoli e del materiale utile che abbiamo preparato per spiegare il nuovo regolamento sul trattamento e sulla protezione dei dati personali.

Guida pratica al GDPR (regolamento generale sulla protezione dei dati)

GDPR e CRM: quali obblighi e scadenze?

Protezione dei dati e adeguamento delle aziende: “manca attenzione e il tempo stringe "

Corso e-learning sul GDPR

Stiamo per pubblicare, sul nostro Portale Formazione , un corso online dedicato alla protezione dei dati composto di moduli e completo di esempi pratici.

È uno strumento importante perché tutti i dipendenti siano a conoscenza delle nuove norme europee: potete accedere alla pagina dedicata attraverso questo link .

Vorrei saperne di più

Puoi contattarci per fissare un appuntamento con i nostri consulenti scrivendoci all’indirizzo email info@studiosynthesis.biz o compilando il seguente form .

end faq

{accordionfaq faqid=accordion1 faqclass="lightnessfaq defaulticon headerbackground headerborder contentbackground contentborder round5" active=item1}