TDL | Trust in Digital Life

RGPD per le PMIs

Guida per le piccole e medie imprese su come affrontare la conformità della protezione dei dati

Una pubblicazione del gruppo di lavoro TDL
Dicembre 2018
Versione 1.0

Contenido

Introduzione

Ill 25 maggio 2018 è entrato in vigore il regolamento generale sulla protezione dei dati (RGPD), che rappresenta una significativa revisione della legislazione vigente in materia di protezione dei dati avviata in un periodo in cui pochissime persone utilizzavano Internet. Il RGPD sancisce infine in diritto i diritti inalienabili delle persone di disporre di dati relativi a loro adeguatamente protetti e gestiti, con pene severe e multe per le aziende che non rispettano.

Se la tua azienda è tra le molte migliaia in tutta l'UE e oltre che non sono a conoscenza del RGPD o delle conseguenze di non essere conformi, allora dovresti continuare a leggere. La nostra intenzione non è quella di approfondire i 99 articoli del regolamento, ma di fornire una panoramica dei principi guida che stanno dietro di loro e di come un potenziale incubo della compliance possa trasformarsi in vantaggio e vantaggio aziendale.

Ci sono nuove misure legislative, come il RGPD, che stanno per avere un impatto importante sulle imprese che detengono dati sui cittadini dell'UE. Il massiccio multe per inadempienza o violazione fino a 20 milioni di euro o il 4% del fatturato globale non sono, come forse si pensava prima, una burocrazia per scopi burocratici, né costi aziendali senza obiettivi commerciali. Al contrario, l'obiettivo della nuova legislazione è in realtà quello di aumentare la fiducia dei clienti nei servizi digitali e quindi accelerare l'adozione della tecnologia con tutti i relativi risparmi di efficienza e vantaggi economici. Inoltre, armonizza le leggi sulla gestione dei dati per le imprese di tutta Europa, riducendo contemporaneamente i costi legali a medio termine e facilitando maggiori opportunità di coinvolgimento dei clienti paneuropei.

In vista dell'introduzione del RGPD a fine maggio 2018, i cittadini di tutta l'Unione Europea sono stati barrati con e-mail e altre comunicazioni da rivenditori, istituzioni finanziarie, agenzie di viaggio online, fornitori di servizi, agenzie governative locali e molti altri ancora. Tutti cercavano di garantire che i clienti passati e presenti accettassero la conservazione continua delle proprie informazioni personali nei database aziendali e nei sistemi CRM (gestione delle relazioni con i clienti) e il loro uso futuro per scopi chiaramente identificati. Dietro questa attività si trova un enorme volume di lavoro di back office per rivedere, analizzare, convalidare e sistematicamente ripulire tutti i dati personali accumulati per garantire che ciò che è stato tenuto in archivio fosse lì legalmente.

Di conseguenza, la maggior parte dei cittadini divenne almeno consapevole dell'esistenza del nuovo regolamento, anche se non erano pienamente consapevoli dei dettagli. Il lo stesso può dirsi della maggior parte delle aziende e organizzazioni, grandi e piccole, con la differenza che, sebbene le società più grandi dispongano di sistemi molto più dati, generalmente dispongono di risorse molto più grandi per comprendere, interpretare e indirizzare ciò che deve essere fatto imprese di medie dimensioni.

Nonostante l'apparente stanchezza generale del RGPD che si è instaurata dallo scorso maggio, il regolamento non è scomparso e viene monitorato sotto gli occhi vigili delle autorità nazionali di protezione dei dati in ciascuno degli Stati membri dell'UE, così come l'organismo di supervisione generale basato Bruxelles. Mentre ci può essere un grado di clemenza per le PMI, in riconoscimento delle sfide che devono affrontare per raggiungere la conformità, ogni periodo di luna di miele dovrà inevitabilmente finire.

Cosa hai bisogno di sapere

Of the 99 articles and 173 recitals (or legal definitions) in the GDPR, most are open to potential interpretation. Unless you have the time and are prepared to study these in depth, it is unreasonable to expect SMEs to have the resources to grasp all that is required of them. So what gets to the heart of the regulation, the concepts that are key for any business to know and abide by?

Data breach notification

If you are unfortunate enough to have suffered a data breach, you are now obliged to notify the authorities as well as everyone you believe has been affected.

Good news!

There are not many exemptions for SMEs so it is important to highlight one that reduces the burden: SMEs are exempt from doing a record of processing (inventory).

I principi al centro del RGPD sono:

- Potenzia i tuoi clienti informandoli - con chiarezza - su quali informazioni hai ottenuto e a quale scopo lo utilizzerai;
- Mostra il tuo impegno fornendo un modo semplice per i clienti di acconsentire e un meccanismo altrettanto semplice per rifiutare l'utilizzo dei propri dati, a meno che la tua azienda non abbia un chiaro scopo legittimo.
- Offrire gli strumenti per controllare e gestire i dati personali come e quando la loro situazione cambia;
- Rendi consapevoli i tuoi clienti che possono contestare legalmente la tua azienda se la tua azienda cambia il suo scopo o il suo uso per i dati personali (senza il consenso modificato), o la perde a causa di cure inadeguate.

I clienti hanno il diritto di:

- Oggetto per i loro dati utilizzati per qualsiasi marketing
- Completa divulgazione di come verranno elaborati i loro dati
- Oggetto per i loro dati che vengono elaborati automaticamente per scopi di profilazione
- Accesso completo ai dati
- Richiedere che i loro dati siano rettificati se inesatti
- Chiedete di cancellare i loro dati
- Ottenere una copia dei propri dati in una forma che possono portare al concorrente (nota come "portabilità dei dati")

Cosa dovresti fare

Effettuare un controllo dei dati

Identifica tutti i dati personali di cui sei responsabile e scopri dove risiede. Potresti essere sorpreso di quanto tenga.

Identificare l'elaborazione dei dati

Chiarire come si elaborano i dati personali e se tale elaborazione è in linea con i propri legittimi interessi commerciali.s.

- ***Richiedi il consenso:*** *se hai bisogno di tali dati a fini commerciali, dovrai verificare di avere il consenso esplicito per l'accesso e l'elaborazione dei dati.*
- ***Elimina e rimuovi:*** *in caso contrario, prendi in considerazione l'eliminazione dei dati e la rimozione di tali processi.*

Controlla la conformità del fornitore

Se utilizzi terze parti per aiutare a elaborare i dati, e quasi certamente fai, verifica i fornitori e chiedi loro di confermare la loro conformità a RGPD. Potrebbe anche essere necessario rivedere i contratti di servizio con loro al fine di indennizzarti in modo appropriato. A loro volta richiederanno indubbiamente la conferma da parte dell'utente del consenso verificabile per l'accesso ai dati e per l'elaborazione.

In breve, la soluzione semplice è quella di rendere la privacy dei tuoi clienti e la sicurezza dei dati personali la tua attività. Porta la mentalità del "cliente è il re" nella tua elaborazione digitale e online e non andrai molto lontano. Molte persone stanno diventando sempre più diffidenti nei confronti di qualsiasi informazione personale su Internet. Alcune piccole iniziative possono essere prese dalle aziende per minimizzare tali rischi adattando le tue pratiche di lavoro per presentare un vantaggio alla privacy ai clienti.

Mantienilo semplice, snello e cattivo

Un principio chiave all'interno del GDPR è la minimizzazione dei dati, il che significa non solo garantire di non possedere dati personali di cui non hai strettamente bisogno, ma anche di non tenerli per un periodo più lungo del necessario. Una violazione ha conseguenze per il cliente e, se non è necessario conservare i dati violati, si attende un'escalation delle multe. Le aziende innovative troveranno il modo di fornire un servizio con meno dati e potenzialmente differenziano la loro offerta ai potenziali clienti su questa base, in particolare per dati sensibili alla legalità o dati considerati sensibili dai potenziali clienti nel vostro settore.

Nessun pranzo gratis

È incredibile quante aziende siano incuranti dei software di terze parti (specialmente gratuiti) che utilizzano per creare siti Web e in generale cercano i provider di servizi Internet più convenienti o i sistemi di gestione delle relazioni con i clienti (CRM). Sebbene i più diffusi sistemi di gestione dei contenuti (CMS) siano protetti in modo affidabile, molti dei plug-in associati potrebbero non esserlo. Il software "gratuito" raramente arriva senza problemi: puoi essere abbastanza sicuro che il prezzo viene estratto nei dati dei tuoi clienti, quindi controlla, perché ora sei responsabile! I servizi economici possono anche utilizzare le stesse tecniche, il prezzo di negoziazione per la tua azienda oi dati dei tuoi clienti.

Processi di business

La maggior parte di questi si riferisce ai processi aziendali, e non, come la maggior parte delle aziende tende a pensare, a una responsabilità dell'IT che ha un ruolo nella convalida dei fornitori, ma nel contesto del RGPD il suo ruolo principale è l'eliminazione delle violazioni. L'IT sarà inoltre responsabile per il rilevamento e la segnalazione di violazioni (Avete strumenti per questo? Molti non lo fanno). Tale segnalazione va al controllore nominato della società che deve decidere se deve essere segnalato all'autorità di vigilanza nazionale per la protezione dei dati. Una serie di violazioni minori nel tempo può indicare un fallimento sistemico che deve essere affrontato. L'autorità di vigilanza si aspetta un registro di tutte le violazioni minori interne e, se indicano una tale questione sistemica, si aspetteranno che venga affrontato, soprattutto se porta a una violazione più grave in seguito.

Tutela della vita privata sin dalla progettazione

Siti Web pubblici

Molti siti web hanno installato Google Analytics senza pensare molto ai dati che raccolgono sui visitatori.
Se non hai mai preso una decisione unica basata sull'analisi dei dati web, dovresti considerare di eliminarla. E mentre ci sei, controlla la privacy e le politiche sui cookie del tuo sito web; considerare se il software di analisi e tracciamento (compresi i pulsanti dei social media) che impieghi valgono il problema di renderli conformi a RGPD.

Per quanto riguarda la privacy degli utenti, il RGPD ha tentato di mettere in legge i sette principi della "privacy by design" che non si applicano solo allo sviluppo del software, ma anche ai processi e alle procedure aziendali. In altre parole, ogni PMI deve avere un processo per trattare i dati personali.

Riesaminare i processi della vostra azienda in base a questi principi può aiutare a capire quanto siete vicini o lontani dall'avere la giusta cultura di leadership per mitigare i rischi e massimizzare le opportunità di business. Se segui questi principi alla lettera, potresti trovare scarsa necessità di consenso e i tuoi servizi avranno poche o eventuali impostazioni sulla privacy. Tutta la privacy è contestuale: comprendi quali dati devi elaborare, ma il tuo cliente? Trovando i modi per rendere chiaro ai vostri clienti quali dati raccogliate e cosa fate con esso, attenuerete le vostre sfide di gestione della privacy.

I sette principi della "privacy by design" sono:

- Proattivo non reattivo: preventivo non correttivo
  Adottare un approccio proattivo alla protezione dei dati e anticipare i problemi e i rischi relativi alla privacy prima che accadano, invece di aspettare fino a quando non è troppo tardi.

- Privacy come impostazione predefinita
  Progettare sistemi, servizi e processi per proteggere automaticamente i dati personali. Sviluppa la privacy in tutte le pratiche commerciali della tua azienda e i clienti impareranno a fidarsi del fatto che i loro dati siano adeguatamente protetti.

- Privacy incorporata nel design
  Incorpora la protezione dei dati nella progettazione dei tuoi sistemi, servizi e processi, rendendo la privacy parte delle funzionalità principali.

- Funzionalità completa - somma positiva, non somma zero
  Garantire un vantaggio reciproco assicurando che ogni sistema supporti la privacy e la sicurezza e che non vi siano inutili compromissioni.

- Sicurezza end-to-end: protezione completa del ciclo di vita
  Immediate misure di sicurezza che garantiscono la gestione sicura del ciclo di vita dei dati dalla raccolta iniziale fino alla rimozione sicura.

- Visibilità e trasparenza: tienilo aperto
  Qualunque pratica commerciale o tecnologia che utilizzi dovrebbe operare secondo le premesse e gli obiettivi verificabili in modo indipendente.

- Rispetto per la privacy degli utenti: mantenerli incentrati sull'utente
  Mantieni l'interesse degli individui al primo posto nei progetti di sistema offrendo forti impostazioni predefinite sulla privacy, controlli user-friendly e avviso appropriato.

Lista di controllo

La logica aziendale si riduce a considerare i dati come una risorsa aziendale quantificabile. L'investimento richiesto per proteggere queste attività può essere paragonato all'approccio di una compagnia assicurativa a fornire indennità per coprire casa e contenuti.

Le PMI possono adattarsi agilmente al nuovo RGPD el modo in cui le aziende troveranno difficile.

Questa breve lista di controllo ti aiuterà a rispettare il GDPR. Essere in grado di rispondere "sì" ad ogni domanda non garantisce la conformità, ma dovrebbe significare che stai andando nella giusta direzione.

Dati dei clienti

- ✓ Hai davvero bisogno di queste informazioni su un individuo? Sai per cosa lo userai?
- ✓ Le persone le cui informazioni sono in possesso sanno che ce l'hai, e sono in grado di capire a cosa servirà?
- ✓ Sei soddisfatto che le informazioni siano conservate in modo sicuro, sia su carta sia su computer? E il tuo sito web: è sicuro?
- ✓ Sei sicuro che le informazioni personali in tuo possesso siano accurate e aggiornate?
- ✓ Eliminate o distruggete regolarmente informazioni personali non appena non ne avete più bisogno?
- ✓ L'accesso alle informazioni personali è limitato solo a coloro che necessitano di una conoscenza rigorosa

Dati del personale

- ✓ Se vuoi inserire i dettagli del personale sul tuo sito web, ti sei consultato a riguardo?
- ✓ Se vuoi monitorare il personale, ad esempio controllando il loro uso della posta elettronica, gli hai detto di questo e spiegato perché?
- ✓ Hai istruito il mio staff nei loro compiti e responsabilità ai sensi del RGPD e regolarmente ti assicuri che li mettano in pratica?
- ✓ Se ti viene chiesto di trasmettere informazioni personali, sei tu e il tuo staff chiari quando il RGPD ti consente di farlo?

La politica è importante

- ✓ Se usi CCTV, è coperto dal GDPR? In tal caso, stai visualizzando degli avvisi che dicono alla gente perché hai una CCTV? Le telecamere sono nel posto giusto o si intromettono nella privacy di qualcuno?
- ✓ Sapresti cosa fare se uno dei tuoi dipendenti o singoli clienti ti chiede una copia delle informazioni in tuo possesso?
- ✓ Hai una politica per affrontare i problemi di protezione dei dati?
- ✓ È necessario informare l'ufficio del Commissario nazionale per le informazioni? Se l'hai già fatto, la tua notifica è aggiornata o è necessario rimuovere o modificare?

Conclusione

Molte persone stanno diventando sempre più diffidenti nei confronti di qualsiasi informazione personale su Internet, anche se troppi sono ignari dei rischi. Alcuni semplici passaggi che possono essere intrapresi dalle aziende per ridurre al minimo tali rischi; educati velocemente e adatta le tue pratiche lavorative per presentare ai clienti un vantaggio in termini di privacy.

Scopri di più!

Per ulteriori consigli pratici per le aziende su come implementare i requisiti RGPD.

- *Il garante europeo della protezione dei dati (GEPD), l'autorità indipendente per la protezione dei dati dell'UE: https://edps.europa.eu/data-protection/data-protection/reference-library_en*
- *Il comitato europeo per la protezione dei dati (EDPB): https://edpb.europa.eu/our-work-tools/our-documents_en*
- *L'ufficio del Commissario per l'informazione del Regno Unito: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/*

Il RGPD sta già avendo un forte impatto sulle imprese, grandi e piccole, che detengono dati sui cittadini dell'UE. Le massicce multe per mancata conformità o violazione fino a 20 milioni di euro o il 4% del fatturato globale non sono, come forse si pensava prima, una burocrazia per scopi burocratici, né costi aziendali senza obiettivi commerciali.

Assumersi la responsabilità

Non ci si può aspettare che piccole imprese tengano il passo con il volume dei regolamenti emergenti, ma devono farlo o rischiare il loro sostentamento. Ogni uomo d'affari può comprendere l'importanza di avere una serie di principi guida e questo è solo un nuovo set per comprendere e inculcare nella cultura aziendale. Quindi, per renderlo più chiaro: la gestione della nuova sfida è un problema di leadership esecutiva, non uno da consegnare al marketing, alle vendite o all'IT.

Il paradosso della privacy

Man mano che i clienti realizzano i loro nuovi diritti, anche se è solo un piccolo numero che inizia a interrogare i tuoi sistemi e processi e a sollevare preoccupazioni con le autorità di vigilanza, il costo per la tua azienda potrebbe aumentare rapidamente. Abbracciare le nuove leggi e cercare modi per rendere più semplice per i clienti dimostra che si desidera che abbiano questi nuovi diritti, facilmente accessibili e facilmente comprensibili. Se le autorizzi con controllo e trasparenza sui dati personali in tuo possesso e su ciò che fai, i premi arrivano in termini di lealtà e fiducia dei clienti, offrendo più dati per più servizi.

Un'opportunità di business

Per le aziende dinamiche e lungimiranti che abbracciano la nuova legislazione è un'opportunità di business. Se questo non è abbastanza allettante, allora vale la pena notare che le persone saranno massicciamente più autorizzate dal RGPD con diritti sui "loro" dati personali. Se la tua azienda abusa o abusa della loro fiducia nel modo in cui elabori i loro dati, allora hanno nuovi diritti di agire in giudizio o anche di cercare azioni legali collettive!

In breve, la nuova legislazione è un riequilibrio di diritti e poteri tra l'individuo e il fornitore nell'era digitale. Le aziende che non rispondono rapidamente si troveranno lasciate indietro dai concorrenti che fanno o colpiscono con multe o cause legali abbastanza grandi da distruggere le imprese.

Un'istantanea RGPD

Consapevolezza

Assicurati che il personale sia a conoscenza delle modifiche alla gestione dei dati influenzate dal RGPD

Informazioni in tuo possesso

Documenta quali dati personali tieni da dove proviene e con chi li condividi: un controllo dei dati.

Comunicare

Esamina le tue attuali informazioni sulla privacy e apporta le modifiche necessarie per allinearli al RGPD.

Diritti del cliente

Controlla i tuoi processi e procedure per assicurarti che coprano tutti i diritti dei clienti, compreso il modo in cui i tuoi dati personali verranno eliminati o forniti in un formato comunemente utilizzato.

Consenso

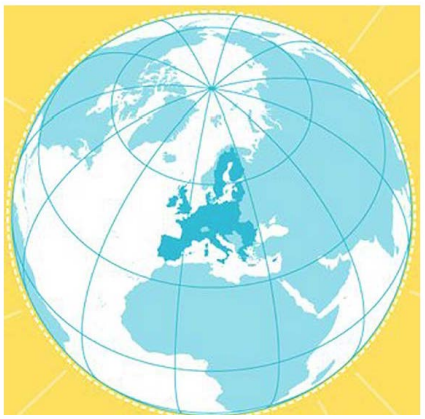
Esaminare la richiesta, registrare e gestire il consenso per soddisfare gli standard RGPD

Richieste di accesso del cliente

Aggiorna le tue procedure per gestire le richieste all'interno delle tempistiche RGPD.

Leggi nazionali di attuazione

Più della metà degli Stati membri dell'UE ha promulgato leggi che implementano il RGPD e talvolta queste leggi contengono requisiti aggiuntivi.



Base legale per l'elaborazione dati personali

Identificare e documentare le basi legali per l'elaborazione delle informazioni personali e aggiornare di conseguenza l'informativa sulla privacy

Bambini

Valutare se è necessario mettere in atto sistemi per verificare l'età delle persone e ottenere il consenso dei genitori o dei tutori per l'elaborazione dei dati.

Violazioni dei dati

Assicurati di disporre delle giuste procedure per rilevare, segnalare e indagare su una violazione dei dati personali.

Protezione dei dati in base alla progettazione

Controlla i tuoi processi e procedure per assicurarti che coprano i diritti dei tuoi clienti, compreso il modo in cui i tuoi dati personali verranno eliminati o forniti in un formato comunemente utilizzato.

Responsabile della protezione dei dati

Designare qualcuno che si assuma la responsabilità della conformità alla protezione dei dati e il loro ruolo nella struttura di governance della propria azienda.

Internazionale

Se operate in più di uno Stato membro dell'UE, **stabilite** la vostra autorità di vigilanza sulla protezione dei dati di piombo. Se la tua attività online utilizza fornitori di servizi non UE, devi assicurarti che siano anche conformi a RGPD

trustindigitallife.eu

Trust In Digital Life Association
avenue Maurice Dekeyser 11 1090 Jette, Bruxelles

office@trustindigitallife.eu
+44 141 588 0892

TDL | Trust in Digital Life

La visione di TDL è che la fiducia deve diventare una proprietà intrinseca di qualsiasi transazione online che coinvolge informazioni personali, incorporando progressi legali, aziendali e tecnici, supportando le politiche di cyber security e integrando considerazioni sociali in modo che i cittadini e gli utenti finali riconoscano servizi, transazioni e dati affidabili ed essere pronti a pagare per loro. Le TIC affidabili aumenteranno la fiducia e la fiducia nella società moderna, offriranno nuovi e attraenti modi di vivere e lavorare e rafforzeranno ulteriormente i valori democratici e sociali dell'Europa.

La missione dell'associazione è di fornire ai suoi membri una piattaforma europea di sviluppo del business al fine di stimolare lo sviluppo e l'accettazione da parte degli utenti di tecnologie ICT innovative ma pratiche. Guidato dal suo programma di ricerca strategico, TDL funge da incubatore per un portafoglio di progetti sprint volti a convalidare concetti di tecnologia nuovi e innovativi, promuove la collaborazione intersettoriale e aggrega i risultati in raccomandazioni del settore per i responsabili politici e la Commissione europea.

trustindigitallife.eu

Trust In Digital Life Association
avenue Maurice Dekeyser 11, 1090 Jette, Bruxelles

office@trustindigitallife.eu
T +44 141 588 0892

TDL | Trust in Digital Life