2021 DIGITAL 360 AWARDS

Azienda: ACTIVE121 SRL

Soluzione: PrivacyOS

PRIVACY·OS

Il più innovativo e completo

Consent Manager

del mercato

active121

CIO & GDPR: come abbattere il rischio di danni per l'azienda (e per se stessi)

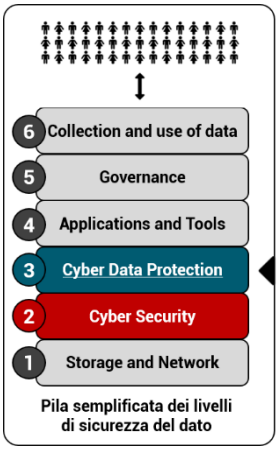
Analizzando tutte le sanzioni GDPR dal 2018 ad oggi scopriamo che più **dell'80% del totale** riguarda "**violazioni di sostanza**", ovvero **illeciti su dati personali e consensi** (principalmente nelle attività di Marketing e Sales attraverso strumenti di e-commerce, CRM, email marketing) e meno del 20% interessa le "violazioni di forma" con irregolarità sulla governance o sulla documentazione. Ma in questo scenario che indica chiaramente la direzione che il Garante persegue, le aziende paradossalmente sperano di tutelarsi continuando a rafforzare il versante meno critico, quello della "paper governance", lasciando scoperto il fronte più esposto alle minacce.

Più del 95% delle volte la **causa di innesco** della sanzione (che poi, come una valanga, travolge trascinando a valle di tutto, spesso scoperchiando in azienda vasi di Pandora di illeciti) è legata ad un **evento esterno**: un prospect, un cliente, un dipendente, un ex cliente o un concorrente che contesta una newsletter di troppo, una telefonata inopportuna o la genuinità del consenso raccolto e comunque il mancato rispetto dei propri diritti.

Fai click qui e scarica il white paper sulle Sanzioni GDPR 2018-2021 in Italia ed Europa

Prevenendo le cause di innesco si riducono drasticamente i danni legati al GDPR

Per raggiungere questo traguardo la cyber security è indispensabile ma non sufficiente. La cyber security ha un approccio ON/OFF sulla protezione delle informazioni ed è progettata considerando l'azienda come proprietaria del dato.



Il GDPR capovolge questa prospettiva: il proprietario del dato è il cittadino ed è (anche) lui a decidere cosa farne. Le regole della Data Protection sono sfumate e condizionate: dipendono da consensi, scadenze, opposizioni e prevedono la limitazione e la cancellazione, logiche estranee alla protezione che la cyber security può offrire.

Per questo è indispensabile estendere la pila dei livelli di sicurezza del dato anche con strumenti di **Cyber Data Protection** a partire dalla gestione dei consensi, con un **Consent Manager di 2ª generazione**.

Marketing, E-commerce, Sales, HR a rischio senza Cyber Data Protection

Nella gestione quotidiana dei dati personali, le principali aree di criticità sono due.

- **Introdurre in azienda misure e strumenti idonei ad evitare illeciti**

  Garantire la conformità al GDPR degli applicativi aziendali può essere complicato, soprattutto con il **CRM** o quando i processi vengono affidati all'esterno come spesso avviene nel **Marketing**, nell'**E-commerce** o nell'**HR** per la selezione del personale.

  Anche in un contesto aziendale prudente ed attento le principali cause di illecito (involontario) sono dovute a tre fattori:

  - **disallineamento dei Consensi** dovuto a Rettifiche, Opposizioni e Scadenze;
  - non rispetto della **Data Retention** e delle conseguenti **cancellazioni**;
  - mal gestione dei **Diritti degli interessati** (causa principale di contestazione).

- **Documentare per dimostrare la propria liceità (tutelando l'azienda e se stessi)**

  Il GDPR è basato sull'Accountability, ovvero sulla responsabilizzazione del Titolare che ha **l'onere della prova** nel dimostrare la propria buona fede ed a cui spetta il compito di **recuperare informazioni e Prove di Genuinità in caso di contestazioni o ispezioni.**

  La realtà è che spesso in caso di problemi, in azienda inizia la "caccia al tesoro".

  Le informazioni per tutelare l'azienda diventano "**critiche**", la loro presenza è data per scontata e vengono richieste d'urgenza al team **ICT che ne diventa responsabile**, spesso senza aver mai ricevuto indicazioni su che dati raccogliere e come organizzarli.

Per questo è fondamentale presidiare le aree critiche e maggiormente esposte con adeguati strumenti di Cyber Data Protection, a partire dal **Consent Manager di 2ª generazione**.

PrivacyOS, il primo e più innovativo Consent Manager di 2ª generazione

PrivacyOS è una piattaforma di Cyber Data Protection in cloud per la gestione dei Consensi, classificata per funzionalità ed affidabilità come **Consent Manager di 2ª generazione.**

Il progetto PrivacyOS è iniziato nel 2016 come framework API per la gestione dei consensi di marketing fino a diventare nel 2018 un prodotto completo. Oggi PrivacyOS è in assoluto la prima, più innovativa e completa **Piattaforma Enterprise di Consent Management SaaS** presente sul mercato, utilizzata da numerose organizzazioni e gruppi internazionali.

PrivacyOS permette di presidiare in maniera sicura e conforme al GDPR **tutto il ciclo di vita dei Consensi**, dalla raccolta alla cancellazione diventando **Master dei Consensi**. Gestisce tutte le basi giuridiche, la Data Retention, Rettifiche, Opposizioni, Diritto all'Oblio, Prove di Genuinità e tutti gli **Eventi della Privacy** che utilizza per mantenere aggiornati ed allineati gli applicativi dell'azienda in maniera semplice e veloce (attraverso un'interfaccia standard API/REST) evitando disallineamenti sui Consensi e conseguenti drammatici trattamenti illeciti.

In caso di contestazioni, denunce ed ispezioni **PrivacyOS ricostruisce automaticamente ed in tempo reale tutta la storia della Privacy dell'interessato con le informazioni e le Prove di Genuinità che permettono all'azienda di tutelarsi (senza coinvolgere nella crisi il team ICT)**.

PrivacyOS protegge l'azienda, rende autonomo il DPO, libera il CIO

PrivacyOS è stato progettato per risolvere le due maggiori criticità del GDPR in azienda:

- **evitare i trattamenti illeciti** (soprattutto nelle attività di **Sales**, **HR** e **Marketing**);
- **documentare ed esporre le prove** che tutelano l'azienda, il Titolare, il DPO ed il CIO.

In oltre, PrivacyOS offre 4 importanti benefici:

1. è sempre **aggiornato con il Regolamento italiano ed europeo**;
2. è elencabile tra gli "***Strumenti di prevenzione e mitigazione del danno***" (misure richieste ai Titolari dall'art. 32 del GDPR tra le attività per l'Accountability);
3. ha un ruolo di "**Autorevole Controllore Super Partes**" verso gli altri applicativi, a dimostrazione, in sede ispettiva, dell'Accountability di Titolare, DPO e CIO;
4. permette al CIO di **ricollocare all'esterno il Rischio della gestione dei Consensi** grazie all'architettura in cloud (probabilmente questa è l'opportunità più strategica).

PrivacyOS è una soluzione in **cloud**, **pronta all'uso**, sempre **aggiornata con il Regolamento** e con **tutta l'intelligenza necessaria già a bordo** per **gestire in maniera corretta ed ordinata i Consensi** ed orchestrarli con gli applicativi aziendali. La gestione centralizzata rende il DPO autonomo sulle verifiche e la reportistica, **senza dipendere dal Marketing e dal team ICT**.

Quali sono le alternative per l'azienda?

PrivacyOS è una soluzione unica, tuttavia si confronta spesso con due insidiosi "competitor":

- la scelta dell'azienda di non fare nulla per quanto riguarda la Cyber Data Protection;
- le soluzioni custom basate su CRM.

Tralasciando il primo scenario (che però in alcuni casi si rivela essere il male minore), **il CRM non può tutelare l'azienda** per il semplice fatto che non è concepito per questo scopo:

il CRM è progettato per sfruttare i dati personali, non per proteggerli.

Benché ad un'analisi superficiale questa scorciatoia possa sembrare innocua, con il CRM la tutela dell'azienda può venir compromessa senza che ci se ne renda conto, almeno fino al "**momento della verità**", in sede ispettiva, quando le prove e le informazioni necessarie alla **difesa propria e dell'azienda risultano inadeguate o assenti** ed il **CIO si trova a dover giustificare alle Autorità (ed all'azienda) le regole di Data Protection adottate dal CRM.**

Il GDPR prevede la retroattività: una contestazione emersa oggi può costringere l'azienda che deve difendersi a recuperare informazioni e prove anche di mesi o anni addietro.

Per questo è fondamentale adottare sin da subito una soluzione **professionale**, progettata per **prevenire gli scenari più critici**, attuali e futuri, **sempre efficiente ed aggiornata con il GDPR** (vincolo che con le soluzioni custom è particolarmente complicato e costoso garantire, considerando anche che ad ogni aggiornamento del CRM l'azienda rischia di dover revisionare o perdere del tutto ogni personalizzazione, rimanendo scoperta ed azzerando l'investimento).

2021 DIGITAL 360 AWARDS

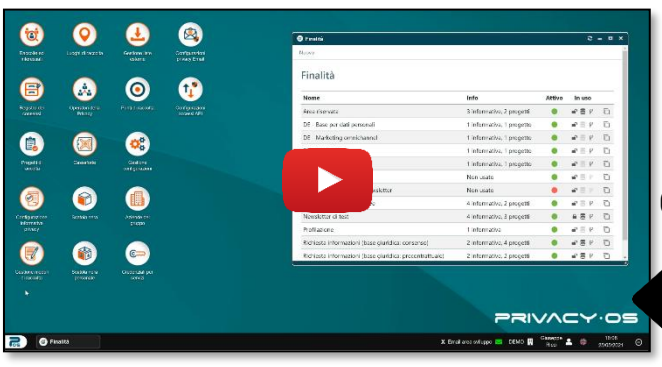
Prosegui con queste risorse

CLICK

Scopri l'unicità di PrivacyOS

CLICK

Scopri i vantaggi di PrivacyOS



CLICK

Guarda la DEMO e scopri come funziona PrivacyOS

active121