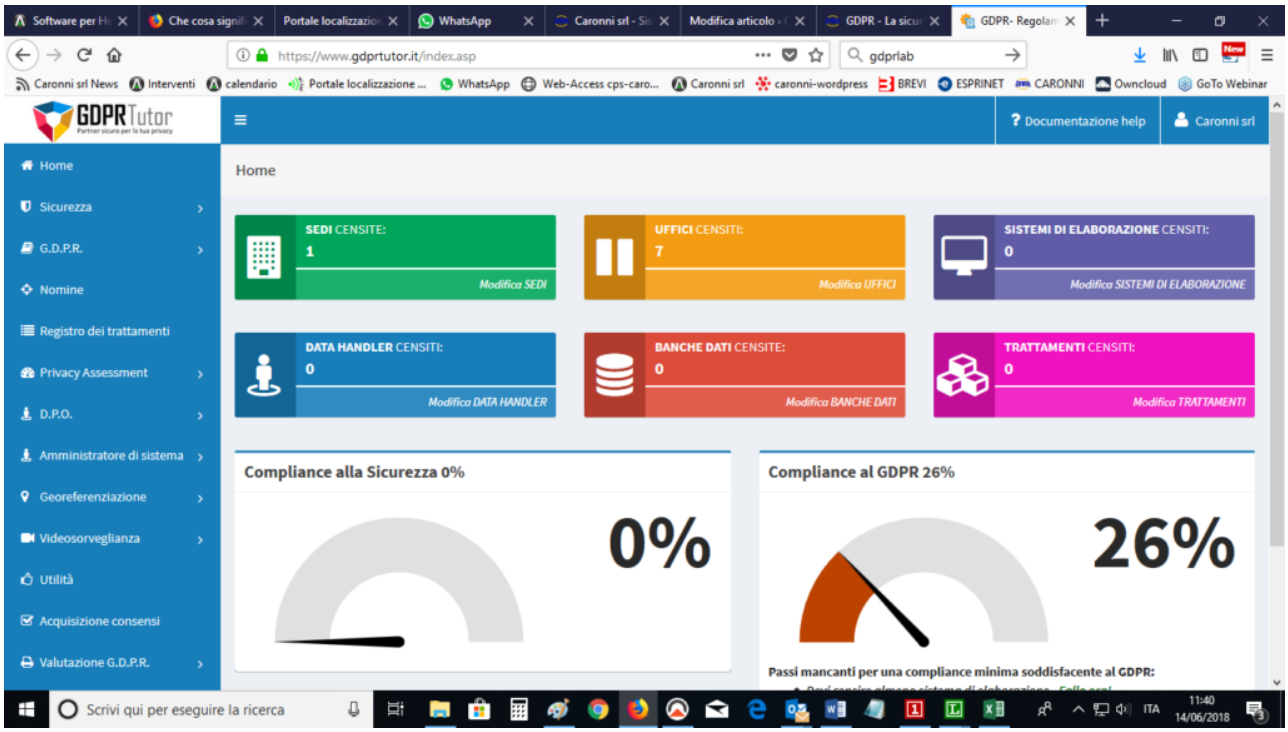
[GDPR – La sicurezza e la tutela dei dati sensibili]

GDPRTUTOR

E’ il Software cloud facile ed intuitivo che vi consente attraverso gli help online di compilare autonomamente tutte le sezioni fino alla creazione del registro dei trattamenti, del PIA di tutte le lettere di incarico e i mansionari di tutte le figure, nonché delle policy informatiche e delle policy privacy. Avrete un accesso annuale che vi permetterà di apportare le modifiche in tempo reale e essere compliance 100% al GDPR.

Richiedi l’account per la tua azienda e inizia subito! CREDENZIALI DEMO: **user:** democlienti **pwd:** gdprdemo

GDPRTutor
Partner sicuro per la tua privacy



chiamaci e richiedi la tua licenza aziendale ed inizia subito ad avviare le procedure per la conformità GDPR – tel. 0362 559383 – 1 commerciale

---

Valuta anche i servizi che Caronni srl rende disponibile:

1>analisi IT preventiva

Sopralluogo di analisi presso la vs. sede al fine di individuare eventuali punti necessari alla conformità. Da questo incontro viene rilasciato un documento con le azioni correttive che l'azienda decide in autonomia di intraprendere per assolvere alla compliance a livello IT. Le azioni correttive verranno su richiesta quantificate a parte.

2>Rilascio licenza privata cloud software GDPRTUTOR per aziende : semplice ed intuitivo – in offerta *Software in cloud facile ed intuitivo. Attraverso gli help online compilerete autonomamente tutte le sezioni fino alla creazione del registro dei trattamenti, del PIA di tutte le lettere di incarico e i mansionari di tutte le figure, nonché delle policy informatiche e delle policy privacy. Avrete un accesso annuale che vi permetterà di apportare le modifiche in tempo reale e essere compliance 100% al GDPR.*

3>Su richiesta possiamo fornire consulenza e formazione da parte di un nostro incaricato sull'uso del software e alla compilazione dei dati richiesti dal software:

-formazione GDPR presso di voi . A fine corso compreso anche test singolo incaricato.

-Su richiesta anche supporto alla compilazione dei quesiti proposti dal software. **costo orario o forfettario in base al numero di incaricati .**

GDPR – La sicurezza e la tutela dei dati sensibili una normativa a lungo desiderata.

GDPR – La sicurezza e la tutela dei dati sensibili. Questa normativa segna la storia del web, come l'evento più importante degli ultimi 20 anni. Si tratta, infatti, di una revisione di un intervento già esistente del lontanissimo 1995. La protezione dei dati diverrà una parte fondamentale di ogni azienda e le costringerà ad adeguarsi, rispettando i requisiti minimi e stringenti che la normativa richiede.

Per adeguarsi ci sarà tempo fino al 25 maggio 2018, ma si calcola che almeno il 50% di tutte le società aziende interessate a questo fenomeno non saranno in grado di rispettare i requisiti richiesti.

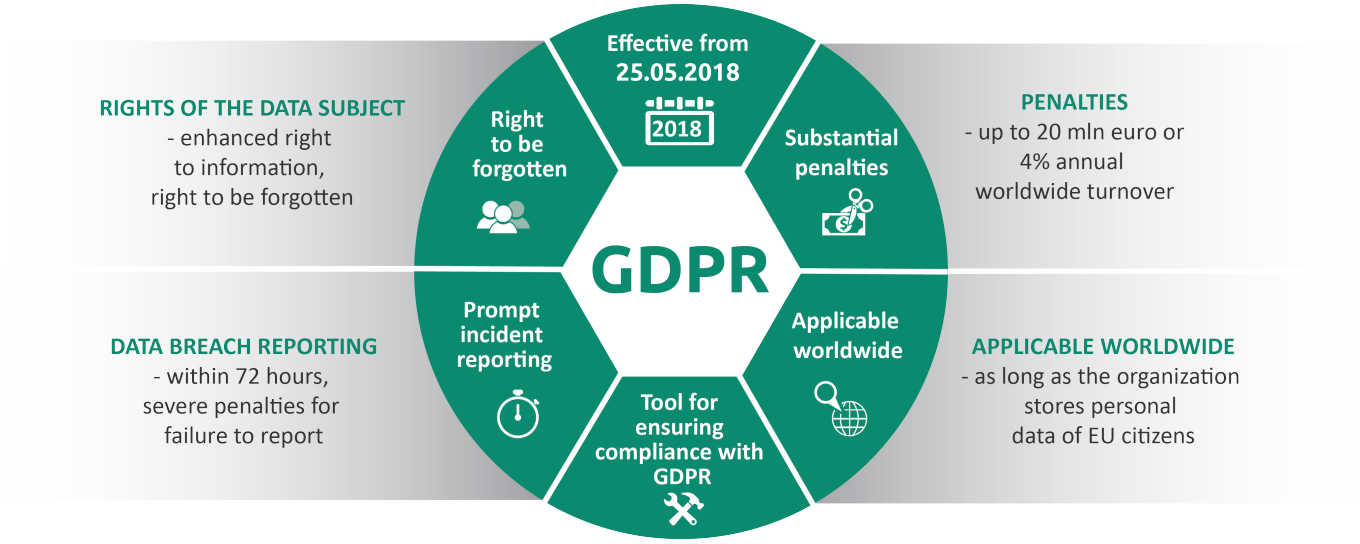
La normativa costringe ogni singolo Paese Europeo a standardizzarsi a una regola comune, in questo caso il GPDR (UE n. 679/2016, Regolamento Generale sulla protezione dei Dati). Questo costituisce un passo fondamentale che porta a un livello molto più alto la politica della protezione dei dati a livello continentale.

Ciò che cambia rispetto al vecchio intervento è l'ampliamento della giurisdizione di tutte le società che trattano i dati personali dei cittadini Europei. Indipendentemente dal fatto se la società/azienda in questione abbia la sede legale o tratti tali dati in Europa; queste aziende dovranno comunque nominare un responsabile all'interno dell'Europa.

GDPR – La sicurezza e la tutela dei dati sensibili avrà pesanti ripercussioni.

se non verrà rispettato, con multe fino al 4% del fatturato globale o fino a 20 milioni di euro, a seconda di quale sia la cifra maggiore tra le due. Il danno maggiore sarà il danno d'immagine che subirà, come quello di un'azienda poco attenta alla privacy dei propri clienti. Nel 2018 la reputazione è tutto.

Il GPDR in breve



L'intero impianto normativo è basato sulle singole specificità di ogni azienda e dei rischi contestualizzati di ogni realtà. Si chiede, perciò di prendere coscienza di ogni rischio reale che l'azienda potrebbe procurare direttamente al cliente con una potenziale fuga di dati.

Si chiede perciò, di acquisire una maggiore responsabilizzazione e una maggiore garanzia sulla sicurezza dei dati raccolti.

Ecco elencati brevemente i principali requisiti che il GDPR richiede:

- Porre la Privacy degli utenti come elemento principale dell'azienda. Pertanto si dovrà individuare ogni possibile vulnerabilità della propria rete, creando di conseguenza un piano di messa in sicurezza dei dati. Dovrà quindi approcciarsi con una tecnica "risk based", dove le misure tecniche ed organizzative possano tutelare l'azienda stessa e i clienti.

- Formazione del personale. Chiunque si trovi nella posizione di dover gestire i dati sensibili deve essere conscio dei rischi e attraverso una formazione adeguata deve conoscere i limiti entro i quali poter svolgere correttamente la propria mansione.

- **Privacy by Design**. Le misure di protezione dei dati devono essere pianificate con le relative applicazioni informatiche di supporto a partire dalla progettazione dei processi aziendali. Verranno processati, di conseguenza, solo i dati veramente necessari allo svolgimento del proprio compito.

- **Breach Notification**. Ogni qualvolta potrebbe paventarsi la possibilità di una perdita di dati sensibili, l'azienda è obbligata a notificare a tutti i propri clienti quest'avvenimento, entro e non oltre le 72 ore.

- Instituire la figura del **DPO (Data Protection Officer)**. Avrà il compito di vigilare su tutti i processi interni dell'azienda e dovrà fungere da consulente, per risolvere qualsiasi problema legato alla sicurezza dei dati.

- **Richiesta di consenso** e "Right be Forgotten". Le richieste di consenso dovranno essere rese chiare e accessibili, senza campi pre-compilati. Inoltre bisognerà garantire a ogni utente il diritto alla cancellazione dalla lista dei dati personali in mano all'azienda. L'utente, infine, dovrà avere la possibilità di richiedere informazioni per maggiori chiarimenti sul trattamento dei dati personali e sensibili e ottenere, anche una copia gratuita di questi documenti.

Conclusione

Questa nuova normativa ha riportato i riflettori della ribalta sullo spinoso problema della Data Protection. Un tema che ha toccato da vicino molte aziende, soprattutto negli ultimi anni, come hanno dimostrato i recenti attacchi della famiglia WannaCry.

Attacchi informatici su vasta scala, che hanno colpito più di 150 Paesi tra Europa e Asia. Attacchi che hanno colpito milioni di aziende che nella maggior parte dei casi hanno colpito aziende con reti aziendali non aggiornate (Windows XP o sistemi non aggiornati) o poco attente sul lato della sicurezza IT.

Dotarsi di soluzioni complete, facili da implementare nella propria azienda e soprattutto soluzioni sicure, diventa da questo momento in poi di importanza assoluta per la vita di qualsiasi azienda.

Team Consulenza

GDPR – La sicurezza e la tutela dei dati sensibili Consulenza. Caronni srl ha organizzato un team di consulenti in grado di dare supporto preciso alle piccole e medie imprese al fine di definire le arree di intervento per il settore IT per il conseguimento della messa in sicurezza e il rispetto delle idoneità alle direttive del GDPR 2018. Conttate lo 0362 559383 per le informazioni commerciali e prenotare l'intervento presso la vs. azienda. Oppure manifestate il vs. interesse per essere richiamati scrivendo a commerciale@caronni.it

---

Tags: GPDR sicurezza dati sicurezza informatica sicurezza reti aziendali

---

Attacco KRACK: tutte le Wi-FI sono vulnerabili

Attacco KRACK: tutte le Wi-FI sono vulnerabili

Mathy Vanhoef, un ricercatore dell'università di Leuven ha individuato una serie di gravissime vulnerabilità nel protocollo WPA2 (Wi-Fi Protected Access II): WPA2 è il protocollo di protezione più usato per rendere sicure le reti Wi-Fi moderne.
Le vulnerabilità individuate affliggono il protocollo WPA2 stesso e non uno specifico hardware o software: insomma, queste falle sono un pericolo per chiunque abbia una rete Wi-Fi.
Vanhoef ha chiamato questo attacco **KRACK, che sta per Key Reinstallation Attack.**

Come funziona l'attacco Krack?

L'attacco sfrutta il momento nel quale l'access point e il dispositivo (smartphone, pc ecc…) instaurano la connessione. Questo processo si compone di ben 4 passaggi: tra questi quello più delicato è il terzo passaggio, durante il quale viene condivisa una chiave crittografica che, almeno teoricamente, dovrebbe essere usata per una sola connessione.
La chiave però viene inviata più volte per ovviare all'eventualità che il client non riesca a ricevere la chiave stessa. Ed è qui che sta il fulcro del problema: l'attacco può ingannare il dispositivo e indurlo a reinstallare una chiave crittografica già usata.

Questo tipo di attacco risulta essere molto efficace contro dispositivi **Linux** o **Android**. In questi due casi infatti, il client usato da Linux e quello di Google non installano una chiave già usata, ma addirittura **una che in pratica non cifra i dati.**
In questo caso l'attacco quindi si può portare a termine anche senza ricavare la chiave crittografica.
L'attacco ha due limiti positivi: prima di tutto infatti l'attacco non può essere portato via Internet, ma deve essere eseguito da un punto entro il raggio d'azione della rete Wi-Fi bersaglio. In secondo luogo l'attacco prende di mira i dispositivi stessi e non gli access point.
Una volta eseguito l'attacco, l'hacker è in grado di catturare tutte le informazioni che transitano tra il dispositivo e l'access point come ad esempio le credenziali di qualsiasi sito non protetto adeguatamente da protocolli di sicurezza.

Come proteggersi

Per proteggersi da questa vulnerabilità si consiglia di tenere aggiornato il firmware degli access point, router e dispositivi wifi.
Di seguito le dichiarazioni dei maggiori produttori:
Sonicwall ha dichiarato che i loro dispositivi Wifi sono già protetti da questa vulnerabilità
Netgear ha rilasciato una lista di prodotti che possono essere attaccati. Vedere il link:
https://kb.netgear.com/000049498/Security-Advisory-for-WPA-2-Vulnerabilities-PSV-2017-2826-PSV-2017-2836-PSV-2017-2837
Dlink ha emanato un avviso che sta aspettando degli aggiornamenti da parte del produttore dei sui Chip
Microsoft rilascerà aggiornamento automatico di sicurezza per Windows 10
Apple ha già rilasciato gli ultimi aggiornamenti di sicurezza

---

App False nel Google Play

App False nel Google Play

Negli ultimi giorni,una serie di applicazioni false sono state diffuse nel Play Store di Google. In particolare, digitando nello spazio di ricerca WhatsApp, tra i risultati, accanto alla app originale ne vengono visualizzate due false ma recanti come sviluppatore 'WhatsApp Inc." (lo sviluppatore legittimo) e grafica praticamente identica a quella dell'app originale. Inutile dire quanto questa somiglianza abbia influito sull'alto numero di download: a primo sguardo effettivamente le due applicazioni erano praticamente indistinguibili da quella originale.

Ci sono sempre più false app nel Google Play. Stranamente, queste false app hanno buone valutazioni e un alto numero di download. Questo fenomeno indica chiaramente la crescente tendenza delle false app nel mondo Android. Queste false app somigliano alle loro controparti originali ma hanno ovviamente finalità truffaldine e/o illegali: potrebbero infatti rubare i dati dell'utente, mostrare pubblicità non richieste, spingere in basso le valutazioni e i download della app più popolari. Sostanzialmente queste si appoggiano sulla popolarità delle app autentiche per ingannare gli utenti.

L'installazione di queste app provocano un forte rischio di sicurezza aziendale in quanto potrebbero accedere ai dati presenti all'interno della rete.

Misure di sicurezza

Non valutare mai un'app prima di usarla. Ricorda, una app autentica potrebbe richiederti una valutazione ma non ti obbligherà mai a farlo. Fai attenzione alle app che chiedono insistentemente la tua valutazione, anche prima che tu possa accedere all'app. App che mostrano tali comportamenti sono quasi sicuramente false e dannose.

Prima di scaricare qualsiasi app, verifica le sue recensioni degli altri utenti. Potrebbe infatti aver acquisito valutazioni false.

Installa sul tuo smartphone una soluzione di sicurezza affidabile che possa bloccare l'installazione di app false e dannose.

Quick Heal TOTAL SECURITY per Android è il prodotto ideale per proteggersi da queste minacce.

Il prodotto ha numerose funzioni:

- Analisi dispositivo con vari tipi di scansione
    - Rapida
    - Approfondita
    - Programmata
- Gestione Privacy
    - Blocco telefonate
    - Blocco numeri internazionali
    - Parental Control
- Anti-theft
    - Localizzazione
    - Telefonata da remoto
    - Acquisizione audio e video da remoto
    - Tentativi di sblocco non autorizzati
- Ottimizzazione prestazioni
    - Controllo utilizzo dati
- Protezione
    - Backup dati su cloud
- e molto altro…

---

per avere informazioni aggiuntive

chiama direttamente un nostro responsabile:

0362 559383 – 1 commerciali

commerciale@caronni.it