

GDPR

- Il regolamento per la protezione dei dati personali -

Che cosa è il GDPR

Chi si deve adeguare

Cosa si rischia

Cosa è necessario fare

La nostra offerta



WINNER 2019

Alessandro Massolo

GDPR Projects

alessandro.massolo@piramisgroup.com

+39 3285974566

Cosa è il GDPR

Il **GDPR – General Data Protection Regulation** – è il regolamento 679/2016 dell'Unione Europea, applicabile dal 25 Maggio 2018, che **disciplina la protezione dei dati personali** delle persone fisiche. Dalla sua entrata in vigore **ha sostituito i contenuti della Direttiva 95/46/CE.**

In Italia è in vigore dal 19 Settembre 2018 il decreto di armonizzazione **D. Lgs 101/2018** tra il GDPR e la normativa italiana sulla privacy D.Lgs 196/2003.

Riguarda le organizzazioni pubbliche, le imprese private a prescindere da dimensione e settore, gli studi professionali, le cooperative sociali, le associazioni, i club; **tutti coloro che trattano dati personali digitali e cartacei devono:**

- adeguarsi alla normativa: **CONFORMITA'**
- dimostrare l'adeguamento: **RESPONSABILIZZAZIONE**
- proteggere i dati e monitorare la protezione: **GESTIONE**

In caso di violazioni al regolamento sono previste **sanzioni fino a 20 Milioni di euro o fino al 4% del fatturato.**



Dunque cosa riguarda

Art. 4

Dati personali

Informazioni che identificano una persona fisica, ad esempio: anagrafica, codice fiscale, partita IVA, dati bancari, recapiti telefonici, e-mail, immagini, indirizzi IP, dati relativi alla salute, comunicazioni elettroniche, geo-localizzazione, reati e condanne penali.

Trattamenti

Operazioni compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali, ad esempio: raccolta, registrazione, conservazione, estrazione, consultazione, modifica, cancellazione, copia, comunicazione, trasferimento

Basato sui principi.....

Art. 5

Principi

1. **Accountability**
2. **Liceità, correttezza e trasparenza**
3. **Limitazione della finalità**
4. **Minimizzazione dei dati**
5. **Esattezza**
6. **Limitazione della conservazione**
7. **Integrità e riservatezza**

Cosa è necessario fare

L'Art. 5 stabilisce che **mediante misure tecniche e organizzative adeguate va garantita una adeguata sicurezza dei dati personali**, compresa la protezione da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali.



Adottare misure organizzative



Adottare misure tecniche

Ambiti di intervento

Organizzazione

Identificazione ruoli privacy, nomine



Processi

Analisi trattamenti, valutazione rischi



Tecnologie

Adozione sistemi protezione dati



Documenti

Informative e Consensi, policy



Formazione

Responsabilizzazione dipendenti



Riepilogo misure per la sicurezza informatica



Applicare procedure di **autenticazione**, attraverso credenziali univoche, evitando account condivisi, con procedure di creazione e cancellazione delle password ben definite e con un livello di complessità adeguato.



Gestire account utenti adeguatamente, cioè considerare il **ciclo di vita dell'account**, dalla creazione alla dismissione dello stesso, prevedendo anche una procedura di revisione annuale.



Gestire i **log di accesso** e gli **eventuali accessi non autorizzati**, impostando delle procedure specifiche per entrambe le situazioni, fornendo una debita informativa a tutti gli interessati, e nel caso all'Autorità,



Mettere **in sicurezza le postazioni di lavoro**, attraverso logout automatici, update degli OS e degli antivirus, incoraggiando gli utenti a limitare a priori gli utilizzi degli strumenti aziendali per fini personali.



Rendere **sicuri gli handset aziendali mobili**, impostare adeguate sincronizzazioni, applicare tecniche di codifica per file e cartelle accessibili tramite autenticazione definite e attivabili in caso di furto e/o perdita.



Proteggere la rete aziendale con **firewall**, abilitare le funzionalità utili alla funzione organizzativa, inibendo servizi per finalità ricreative, proteggere la rete Wi-Fi aziendale, prevedere una **VPN** in caso di accesso da remoto.



Impostare la **sicurezza per i server aziendali**, permettendo l'accesso ad un numero ristretto di persone autorizzate ad accedervi, adottando una policy delle password specifica, backup ed aggiornamenti periodici.



Rendere **sicuro il sito web**: con protocollo TLS, con unica porta per applicazione, con ridotti account "administrator" e in caso di gestione di cookie non tecnici (anonimizzati) o funzionalità che prevedono l'utilizzo di dati personali, fornire informativa all'interessato e richiedere il consenso.



Garantire la **business continuity** e predisporre un'adeguata politica di **backup/restore** dei dati trattati, sia da un punto di vista di sicurezza elettronica sia da un punto di vista di **sicurezza fisica** dei locali.



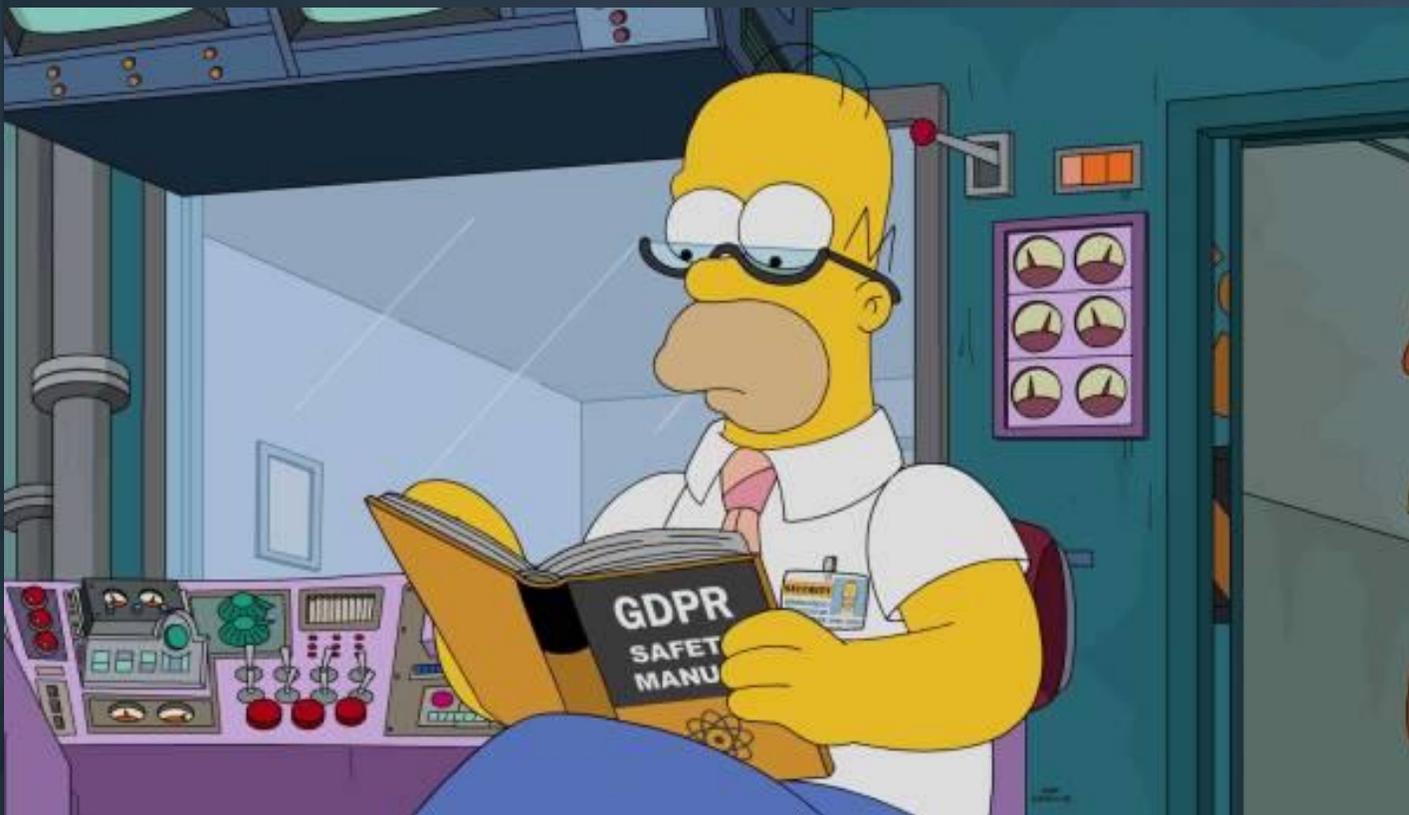
Applicare **misure di sicurezza tra sedi**: specifiche misure di codifica per lo scambio di informazioni, **protocolli di protezione, confidenzialità ed autenticità delle informazioni scambiate** anche con terze parti



Utilizzare tecniche di **criptazione dei dati**, attraverso algoritmi riconosciuti, tra cui ad esempio gli SHA-256, SHA-512 o SHA-384



Adottare il principio di privacy-by-design ogni qual volta vi è lo sviluppo di un nuovo servizio, tenendo in considerazione il principio di **minimizzazione dei dati**, evitando l'utilizzo di dati personali in fase di test.



PIRAMIS GROUP
EVOLVING BUSINESS

L'Offerta

EASYGDPR – la soluzione per l'adeguamento al GDPR



Piattaforma software in cloud computing e consulenza dedicata

Questionario digitale

con cui vengono mappati in ambito privacy:

- organizzazione
- processi
- tecnologie
- documenti
- competenze

Elaborazione report

- Risultati Indicatori % del livello di conformità e gap analisi
- Soluzioni organizzative e tecnologiche per l'adeguamento

Redazione documenti

- Nomine
- Consensi
- Informativa
- Policy di sicurezza
- Data Breach
- Sito Web
- Videosorveglianza
- Adeguamenti COVID-19

Per dipendenti

Sessioni di formazione per i collaboratori, on line:

- Il decreto
- Il modello privacy
- La sicurezza dati
- Impatti operativi
- Test

EASYGDPR: offerta con noleggio



Portale in cloud: credenziali accesso

Inizio: informazioni base azienda

Identikit: mappatura organizzazione e tecnologie «as is»

Risultati: report indicatori conformità «as is»

Soluzioni: report dettaglio soluzioni adeguamento

Documenti: consensi, informative, nomine, procedure - (20)

Test privacy: verifica Soluzioni messe in atto

Formazione e test on line: per dipendenti/collaboratori

Chatbot: supporto AI on line al processo di adeguamento

Assistenza: supporto per tutta la durata del servizio

99,00 € mese per 36 mesi*

**IVA esclusa, costo deducibile al 100% e detrazione IVA 100%*



Benefici.... oltre a «mi sento più al riparo dalle sanzioni»

«Il progetto GDPR mi ha aiutato a comprendere come ridurre la superficie di attacco, a **mitigare il rischio di eventuali attacchi informatici**, a **ridurre costi di ripristino**, ad **evitare fermo sistemi e conseguenti mancati guadagni** ».

- Responsabile IT azienda minimarket alimentari -

«L'adeguamento al regolamento mi ha consentito di qualificare ulteriormente la mia Azienda nei bandi di gara e **acquisire punteggi maggiori nella parte tecnica dei capitolati**».

- Amministratore azienda costruzioni edili -

«Abbiamo subito affrontato l'adeguamento appena il regolamento europeo è diventato decreto legge; **abbiamo apprezzato particolarmente il supporto post conformità**. Siamo seguiti in questo periodo di emergenza per i **nuovi adempimenti**, e per **armonizzare gli aspetti di sicurezza sul lavoro con quelli privacy**.

- Direttore Generale azienda produzione laminati -

«Ho vissuto inizialmente l'adeguamento come un mero obbligo normativo, necessario per evitare sanzioni; in corso d'opera però mi sono resa conto che **stavo migliorando aspetti organizzativi ed operativi: ordine nei processi, incarichi più mirati, maggior cura di dati e pratiche**».

- Proprietaria azienda demolizioni e smaltimento -

«I soci del nostro club sono persone in vista e particolari; oggi grazie all'adeguamento posso dimostrare che i loro dati sono protetti con tecnologie adeguate e quindi garantirmi **un ulteriore elemento di fidelizzazione**»

- Presidente Yacht Club -

«Con questo progetto **ho capito il valore della protezione dei dati dei miei Clienti**, il bene principale dello Studio e **responsabilizzato i miei collaboratori** nel trattamento dei dati durante le attività lavorative. Inoltre mi sento più preparato ad affrontare una verifica ispettiva».

- Socio studio commercialisti -



La guida sicura per l'adeguamento al GDPR

Alessandro Massolo – Piramis Group

alessandro.massolo@piramisgroup.com

Tel. +39 3285974566