Che cos' è il GDPR?

Il 25 maggio 2018 è entrato in vigore il regolamento EU 2016/679 **GDPR** ("General Data Protection Regulation") ovvero il Regolamento Generale per la Protezione dei dati Personali.
Si tratta del più importante cambiamento privacy dopo 20 anni, ed ha come scopo la regolamentazione del trattamento dei dati personali nelle organizzazioni europee.
Il regolamento richiede che le aziende dimostrino di avere svolto una verifica interna al fine di accertare se i dati aziendali siano esposti al rischio e reitera la necessità' di implementare soluzioni di sicurezza sia tecnologiche che organizzative per un corretto adeguamento al rischio.

Perché adeguarsi?

La risposta è molto semplice: perché è **obbligatorio**. (Vedi Appendice I in merito a "controlli e ispezioni della GDF dal 25 maggio 2018"
Il GDPR è un atto legislativo vincolante e dovrà essere applicato in tutti i suoi elementi nell' intera Unione Europea. **Non richiede alcuna forma di legislazione applicativa da parte degli stati membri** e quindi non ci saranno proroghe per la sua attuazione.

L'adeguamento può costituire per le aziende una opportunità di adeguamento a strumenti che possano aiutarle a entrare nell'era digitale migliorando ed efficientando i loro processi interni e relazioni con l'esterno (clienti o fornitori).

Quali sono le sanzioni amministrative in caso di violazioni dei seguenti obblighi [articolo 83 comma 4 gdpr]?

Fino a 10.000 (per le imprese, fino al 2% del fatturato annuo, se superiore)

misure di protezione by-design, by-defualt;
nomina del rappresentante del titolare o dei responsabili non stabiliti nell'UE;
accordo tra contitolari per le responsabilità;
consenso dei minori in merito a servizi della società dell'informazione;
tenuta del Registro dei trattamenti;
adozione di misure di sicurezza adeguate;
comunicazione di data breach;
DPIA;
designazione del DPO.

Fino a 20.000 (per le imprese, fino al 4% del fatturato annuo, se superiore)

principi generali del trattamento dei dati;
condizioni di liceità, per il consenso o per la revoca;
norme trattamento di dati particolari, sensibili o giudiziari;
mancato rispetto diritti dell'interessato;
mancato rispetto principi per il trasferimento di dati extra-UE;
norme nazionali in materia di rapporti di lavoro, archivi storici, ricerca scientifica.

La responsabilità penale deriva da condotte volte a trarre profitto, per sé o per altri, oppure a cagionare grave nocumento al soggetto danneggiato, sempre salvo il caso in cui il fatto costituisca un più grave reato.

Descrizione	*Pena Prevista*	
	Reclusione	***Ammenda (euro)***
Mancata adozione delle misure di sicurezza	fino a 2 anni	da 10.000 a 50.000
Trattamento illecito dei dati personali al fine di trarre per sé o per altri profitto o di recare ad altri un danno	da 6 mesi a 3 anni	
False notizie o circostanze; produzione di atti o documenti falsi in dichiarazioni rese o esibite in un procedimento dinanzi al Garante o nel corso di accertamenti	da 6 mesi a 3 anni	
Inosservanza dei provvedimenti del Garante per la privacy	da 3 mesi a 2 anni	
Violazione della privacy su Internet ==> Illecita diffusione di dati personali:	fino a 3 anni	
Violazione della privacy su Internet ==> Frode informatica	da 6 mesi a 3 anni	da 516,00 a 1.032,00
Se il reato sul web viene commesso con abuso della qualità di operatore del sistema	da 1 a 5 anni	da 309,00 a 1.549,00

Sfatiamo alcuni falsi miti sul GDPR :

- **"GDPR è solo per grandi aziende": FALSO**.
  Il GDPR si applica a tutte le aziende che gestiscono dati personali
- **GDPR significa essere protetti da attacchi esterni: FALSO.**
  Gli attacchi esterni (virus, malware) costituiscono solo il 47% dei problemi di sicurezza sui dati. La maggioranza dei problemi è dovuta a errori non intenzionali che vengono fatti maneggiando dati in maniera non adeguata o a seguito di perdita di terminali contenenti dati importanti.

Cosa sono i "dati personali"?

Sono semplicemente "*informazioni relative a persone fisiche*".
Sono ritenuti dati, infatti, "qualsiasi informazione riguardante una persona fisica identificata o identificabile" , ovvero:

- i dati **identificativi**: quelli che permettono l'identificazione diretta, come i dati anagrafici, mail, numero di telefono, immagini, etc.;
- i dati **sensibili**: quelli che possono rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, lo stato di salute e la vita sessuale;
- i dati **giudiziari**: quelli che possono rivelare l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale (ad esempio, i provvedimenti penali di condanna definitivi, la liberazione condizionale, il divieto od obbligo di soggiorno, le misure alternative alla detenzione) o la qualità di imputato o di indagato.

Con l'evoluzione delle nuove tecnologie, altri dati personali hanno assunto un ruolo significativo, come quelli relativi alle comunicazioni elettroniche (ad es. indirizzo IP del proprio computer, MAC address di uno smartphone, etc.) e quelli che consentono la geo localizzazione, fornendo informazioni sui luoghi frequentati e sugli spostamenti.
ATTENZIONE: la normativa riguarda i dati personali di clienti, dipendenti e fornitori di una azienda

Cosa si intende per violazione dei dati?

Per violazione di dati si intende un qualsiasi incidente che metta a rischio i diritti e libertà degli individui. Alcuni esempi?

- Un dottore condivide per errore i dati medici con il paziente sbagliato
- La perdita o furto di foto da una pennina USB
- La perdita o il furto di un computer portatile, un tablet o un telefono con all'interno dei file che contengono un elenco di dati relativi a clienti

In questi casi, l'art. 33 impone al titolare di notificare la violazione all'autorità di controllo entro 72 ore dal momento in cui ne viene a conoscenza. Il tempo di riferimento da cui iniziano a decorrere i termini della notifica viene individuato quindi nel momento in cui il titolare acquisisce consapevolezza dell'avvenuta violazione .
Auguratevi che non debba mai succedere di impostare un timer di 72 ore per un motivo come questo per la vostra azienda!

Cosa dovranno fare le aziende per mettersi in regola?

Secondo il nuovo regolamento le aziende dovranno dimostrare:

- Di avere ricevuto un consenso esplicito per tutti i dati personali raccolti e di utilizzare i dati personali dei clienti in modo trasparente e appropriato (Art. 7) offrendo la possibilità di poterli modificare o cancellare in qualsiasi momento (Art. 16, 17, 18, 19, 20)
- Di preservare i dati personali dalla distruzione accidentale o illegale, dalla perdita, dalla modifica, dall'accesso e dalla divulgazione non autorizzati (Art. 7)
- Di essersi adeguate alla normativa tramite misure di data governance che includano documentazione dettagliata, registrazione e valutazione continua del rischio (Art. 7)

Qui di seguito gli step tecnologici necessari per poter garantire Riservatezza, Disponibilità e Integrità dei dati personali:

- Mappatura delle informazioni gestite dall'azienda per individuarne tipologia, posizione, utilizzo, provenienza, protezione per determinare il proprio livello di rischio;
- Formazione e sensibilizzazione degli utenti e dei gestori dei sistemi, inclusi i collaboratori esterni;
- Razionalizzazione dei permessi di accesso degli utenti e opportuna gestione password;
- Dismissione o aggiornamento di sistemi basati su piattaforme obsolete e applicazione regolare di patching;
- Verifica ed eventuale integrazione delle procedure di backup e restore dei dati;
- Revisione dei sistemi di sicurezza perimetrale e di protezione dei dispositivi utente - Firewall, Antispam, URL Filtering, Antivirus di Rete e per PC Client, Email gateway;
- Cifratura dei dati e delle comunicazioni con l'esterno, con particolare attenzione ai dispositivi mobili - smartphone, tablet, notebook, USB stick, etc. - e ai repository di dati su Cloud (Art. 32);
- Raccolta, conservazione e analisi dei log;

QUESTE LE NOSTRE SOLUZIONI:

Valutazione Certificata Settore IT :

Labonet si occuperà di redigere un documento contenete l'inventario e discovery della Vostra rete Aziedale. Tale documento evidenzierà eventuali vulnerabilità e anomalie, la presenza della registrazione dei Log di sistema e il monitoraggio intelligente degli accessi.

Contratto di Assistenza Periodica:

Con una cadenza trimestrale, Labonet effettuerà una visita on site comprendente le seguenti attività:

- Verifica ed eventuale implementazione aggiornamenti del Firewall,
- Verifica ed eventuale implementazione aggiornamenti del Sistema Operativo ("S.O."),
- Verifica ed eventuale implementazione aggiornamenti Antivirus e Antimalware (vedi Appendice II per soluzioni proposte)
- Recovery da backup dei dati con invio dei log di funzionamento dei backup in copia a Labonet. Questo permetterà un monitoring continuo in tempo reale in caso di anomalie. (vedi Appendice III per soluzioni proposte)

Inoltre, verranno tenuti presso le Vostra sede Nr. 2 corsi/ anno per Aggiornamento sulla Sicurezza. Tali corsi avranno come target tutti i dipendenti della vostra azienda e durata di 1,5 h ciascuno. Questo perché il 58% delle minacce informatiche è causato da negligenza o azioni dolose dei dipendenti. Svolgere iniziative di formazione attiva per prevenire gli errori più comuni, come l'apertura di allegati sconosciuti. Oltre a consolidare la sicurezza, queste azioni consentono di ottenere la conformità alle seguenti disposizioni fondamentali del GDPR)

Infine Labonet offre anche la possibilità di fungere da Responsabile della Protezione Dati (Data Protection Officer – "DPO").

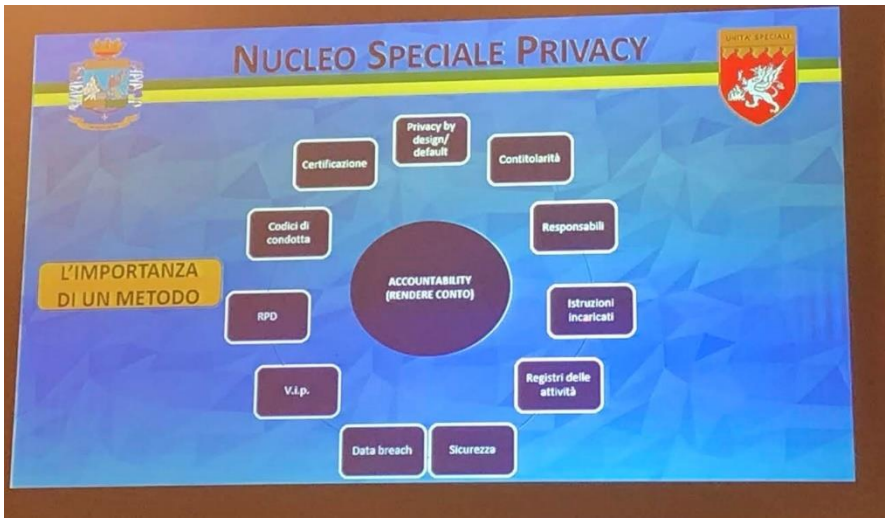
Il DPO è la figura di riferimento introdotta dal GDPR. Il DPO, figura storicamente già presente in alcune legislazioni europee, è un professionista che deve avere un ruolo aziendale (sia esso soggetto interno o esterno) con competenze giuridiche, informatiche, di risk management e di analisi dei processi. La sua responsabilità principale è quella di osservare, valutare e organizzare la gestione del trattamento di dati (e dunque la loro protezione) all'interno di un'azienda (sia essa pubblica che privata), affinché questi siano trattati nel rispetto delle normative privacy europee e nazionali. È chiaro come l'introduzione di tale figura serva non solo a spostare da un soggetto (titolare/responsabile del trattamento) ad un altro (il DPO appunto) tutta una serie di responsabilità in ambito di protezione dei dati, ma anche e soprattutto per permettere ad un soggetto specifico, specializzato, esperto in materia di occuparsi esclusivamente della protezione dei dati, rimanendo sempre aggiornato sui rischi, i problemi e le misure di sicurezza necessarie a garantire un livello di tutela adeguato.

PREZZI
Valutazione Certificata*..... € 75,00 (IVA esclusa)
Assistenza Periodica GDPR* (4 visite + 2 corsi/ anno)..... € 500,00 (IVA esclusa)
* Valido per Professionisti/Aziende fino a max 3 utenti/device)

APPENDICE I

Privacy: controlli e ispezioni della GDF dal 25 maggio 2018

https://www.informazionefiscale.it/privacy-gdpr-controlli-ispezioni-sanzioni-guardia-di-finanza



Il **25 maggio 2018** è ufficialmente non soltanto il giorno della nuova privacy ma anche quello in cui partirà l'**attività di controllo della Guardia di Finanza**. Nello specifico, le ispezioni partiranno da subito sugli adempimenti obbligatori e fondamentali per l'adeguamento al GDRP:

- nomina del DPO, il responsabile della protezione dati;
- controlli sulle misure previste in caso di data breach (da intendere non come situazioni estreme ma come tutti quei casi di perdita accidentale e occasionale di dati, come il furto di un pc, di un hardisk e via di seguito);
- registro dei trattamenti: sarà la base dell'attività ispettiva, il punto dal quale la Guardia di Finanza partirà per valutare le misure per la tutela della privacy messe in atto.

APPENDICE II

Quick Heal Internet Security

Anti Ransomware // Safe Banking // Protezione Malware // Anti-Keylogger // Sicurezza Web // Sicurezza Email // Protezione Drive USB // Firewall // Firewall // Parental Control // Core Protection

	VALIDA PER	DURATA	PREZZO AL PUBBLICO (iva compresa)
ANTIVIRUS PRO	1 PC	12 mesi	€ 29,90
		36 mesi	€ 59,80
	3 PC	12 mesi	€ 39,90
		36 mesi	€ 79,80
INTERNET SECURITY	1 PC	12 mesi	€ 39,90
		36 mesi	€ 79,80
	3 PC	12 mesi	€ 49,90
		36 mesi	€ 99,80
TOTAL SECURITY	1 PC	12 mesi	€ 49,90
		36 mesi	€ 99,80
	3 PC	12 mesi	€ 79,90
		36 mesi	€ 159,80
TOTAL SECURITY MULTI DEVICE	3 DEVICE	12 mesi	€ 79,90
		36 mesi	€ 159,80
	5 DEVICE	12 mesi	€ 99,90
		36 mesi	€ 199,80
TOTAL SECURITY per TABLET ANDROID	1 TABLET	12 mesi	€ 9,90
TOTAL SECURITY PER SMARTPHONE ANDROID	1 DEVICE	12 mesi	€ 9,90
TOTAL SECURITY per MAC	1 MAC	12 mesi	€ 49,90

* i rinnovi mantengono lo stesso prezzo
* prezzi di acquisto ancora più vantaggiosi pianificando acquisti di pacchetti di licenze

APPENDICE III

Backup su Qnap con dischi crittografati 256 bit + 2° copia su disco esterno crittografato

Consigliato da 1 a 2 pc:

TS-253BE-4G ..... € 500,00 (IVA esclusa)

Consigliato da 3 a 5 pc:

TS-451P-8G .....€ 720,00 (IVA esclusa)

TVS-682-I3-8G ..... € 1.525,00 (IVA esclusa)

2 configurazioni:

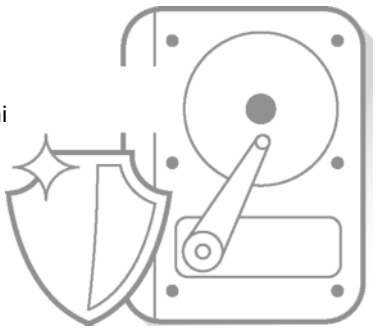
Nr. 02 Dischi in Raid + 1 Disco est. Usb 3.0 tutti da 3tb ..... + € 390,00 (IVA esclusa)

Nr. 04 Dischi in Raid + 1 Disco est. Usb 3.0 tutti da 3tb ..... + € 630,00 (IVA esclusa)

Installazione e configurazione presso vs sede ..... + € 150,00 (IVA esclusa)

Come QNAP può aiutare a proteggere

QNAP NAS consente di crittografare tutti i dati o singole cartelle, utilizzando la crittografia AES 256-bit. Altri meccanismi di protezione dei dati includono le configurazioni RAID, snapshot e S.M.A.R.T. (Self-Monitoring Analysis and Reporting Technology - Tecnologia di analisi e report in monitoraggio automatico).



3° livello consigliato: Cloud con Xopero