Cos'è il DGPR?

Il 4 maggio 2016 è stato pubblicato sulla Gazzetta Ufficiale dell'Unione Europea il testo definitivo del Regolamento (UE) 2016 n. 679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, altrimenti detto GDPR (*General Data Protection Regulation*).

Il nuovo Regolamento contiene, insieme ad alcune conferme di elementi già noti nel campo della protezione dei dati personali (dettati in passato dalla 196/2003), numerose novità tipo l'introduzione di principi quali *Accountability* (responsabilità o meglio il rendere conto del proprio operato) o ai nuovi parametri connessi alla privacy by design (prevenire e non curare) e privacy by default (trattare solo i dati personali nella misura necessaria) e, ancora, l'introduzione dei registri dei trattamenti a carico dei titolari, la necessità del DPIA (*Data Protection Impact Assessment*), le nuove regole sui *Data Breach* ossia come agire in caso di violazione di dati personali, la figura del DPO (*Data Protection Officer),* sconosciuta al nostro ordinamento. Senza tacere la necessità di un diverso approccio alla protezione dei dati, non più basato sui requisiti minimi ma teso a misure idonee ed adeguate, caso per caso.

Il tutto con un forte aumento dei rischi e delle responsabilità, sia di carattere civile (cambia, e non poco, il regime di responsabilità in caso di danni arrecati per effetto del trattamento di dati personali) sia di carattere amministrativo-pecuniario (si rischiano sanzioni fino a 20.000.000 di euro o addirittura fino al 4% del fatturato mondiale annuo, se superiore e interdizione al trattamento dei dati personali).

La data alla quale bisogna essere pronti per il GDPR è il prossimo 25 maggio 2018.

Cosa guida tutto è il principio di **Accountability** e ognuno sarà libero di assumersi o meno le sue responsabilità.

Non si potrà fare tutto in una volta, e forse neanche tutto in tempo. Bisognerà quindi definire delle priorità. Inoltre sarà opportuno informare non solo il titolare, ma anche tutti i singoli responsabili del trattamento, ovvero quelli nominati tali in passato, ciò perché, a differenza di quanto previsto dal vecchio codice, l'interessato danneggiato potrà ricorrere indifferentemente nei confronti del titolare o dei singoli responsabili, a seconda di quello che gli pare più semplice e conveniente. Infine ciò che spinge di solito ad adeguarsi alle norme su questa materia è la paura delle sanzioni, ma la sicurezza dei dati sia come la sicurezza del patrimonio personale va attuata, e va attuata al meglio in quanto si protegge il proprio patrimonio e non si tratta di sola burocrazia.

Una definizione che va fornita prima di proseguire il discorso è quella di Data Breach o di Data Protection Violation, si può tradurre genericamente in violazione dei dati. Molto più praticamente si può identificare una qualunque violazione, sia essa un furto o un cryptolocker (malware informatico molto di moda) e questo oggi è molto più vicino alla realtà quotidiana.

Accountability, cosa significa in pratica? Significa che il legislatore europeo non ci dice più "cosa fare", ma ci fornisce dei principi da applicare. Se andremo in sede di giudizio, sarà il giudice a valutare se avremo applicato al meglio i principi della legge, senza scorciatoie o dimenticanze, sulla base degli usi e del progresso tecnologico. In sostanza scarica sul titolare e sui responsabili tutta la "responsabilità".

Cosa fare di sicuro

Le organizzazioni pubbliche e private di qualunque dimensione sono interessate al 100%, senza distinguo tra le aziende, chi tratta dati personali deve stare alle regole dettate dal DGPR. Sicuramente la modalità del trattamento di chi svolge attività produttive è diversa da chi eroga servizi assistenziali, ma il trattamento dei dati per l'elenco dei clienti e dei fornitori, le paghe esternalizzate è uguale per tutti e la posta elettronica è una cosa ormai imprescindibile e…..muove dati personali dei quali bisogna aver cura.

Per cui, cosa fare? Adeguarsi al DGPR

Cosa fare obbligatoriamente

Che differenza c'è fra il "cosa fare di sicuro" ed il "cosa fare obbligatoriamente". Si può dire che dopo aver definito chi rientra e come rientra nell'applicazione del dettato normativo ci saranno alcuni adempimenti ai quali ottemperare con certezza.

In particolare:

- Redazione del DPIA, *Data Protection Impact Assessment* si tratta della redazione di un documento volto a predisporre la valutazione dell'impatto sulla protezione dei dati personali (DPIA) dei trattamenti di dati che lo richiedano, in base all'art. 35 del GDPR.
- Istituzione della figura del DPO, si tratta di una figura singola o di un team multidisciplinare, che può anche essere individuata all'esterno dell'organizzazione del titolare e disciplinata da un contratto di servizio, che lavora in staff con il top management

Il DPO è il garante, nominato dal responsabile del trattamento, ovvero il titolare, lavora in autonomia e non può prendere istruzioni dal titolare, deve avere competenze specifiche ed effettuare segnalazioni e report del suo operato di controllo, ma non ne è responsabile. **Il responsabile è sempre il titolare.**

Anti Ransomware, i ransomware non sono virus e stanno diventando pervasivi, per questi si rendono necessari moduli specifici o attività volte alla neutralizzazione o minimizzazzione degli effetti sui dati. Questo per ridurre il rischio di criptazioni dei dati non volute e pagamenti di riscatti per riavere la disponibilità degli stessi.

Cancellazione/distruzione sicura dei dati, la cancellazione dei dati in modo sicuro è prevista dall'art. 17 del GDPR. Non basta più una distruzione sommaria bensì approfondita dei supporti magnetici o cartacei.

Disaster Recovery, Il DR non è solo un obbligo ma è necessario per il buon svolgimento dell'attività imprenditoriale. Non ci sono solo i terremoti e le inondazioni, ma anche altre sventure posso colpire i nostri dati. Il DR non è il back-up!

Business Continuity, la continuità operativa è una necessità, le macchine si fermano, si rompono, ma le organizzazioni devono poter lavorare con continuità La non continuità operativa comporta un rischio di perdita economica.

Valutazioni sul ***Cloud*** da farsi obbligatoriamente perché, i dati di cui si è responsabili, stanno a casa di qualcun'altro.

Cosa fare di consigliato

Security management, è un servizio in outsourcing che gestisce la sicurezza a livello perimetrale, attraverso la completa gestione dei firewall e delle sue attività ove si renda necessario l'aggiunta di hardware specifico.

Backup manuali e programmati, Il backup aziendale va implementato e semplificato, magari gestito in outsourcing, troppo spesso non lo si controlla e si spera che vada tutto bene o peggio….nemmeno ci si pensa.

Cosa fare opzionalmente

Security monitoring, monitoraggio periodico della sicurezza dei dati e delle vulnerabilità informatiche.

Encryption dei dati, Non c'è obbligatorietà ma va considerata come misura da implementare per rafforzare l'accountability, nel caso di violazioni di dati personali che sono stati preventivamente criptati non c'è obbligo di notifica dell'eventuale data breach al Garante; in caso contrario la notifica deve essere fatta entro 72 ore dall'avvenimento del fatto, con una sorta di autodenuncia, in seguito alla quale è quasi certo un controllo da parte delle autorità.

Controllo adempimenti GDPR, manutenzione e tenuta sotto controllo del DGPR

Le sanzioni

Le sanzioni che rischiano gli inadempienti :

Fino a 10 milioni di euro, o per le imprese, fino al 2 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore, in caso di violazione (fra l'altro) degli obblighi del titolare del trattamento e del responsabile del trattamento

Fino a 20 milioni di euro, o per le imprese, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore, in caso di violazione (fra l'altro) dei principi di base del trattamento, comprese le condizioni relative al consenso, dei diritti degli interessati, delle regole sui trasferimenti di dati personali a un destinatario in un paese terzo.

Non ultima la possibilità che venga inibita al trasgressore la possibilità, nel futuro, di trattare ancora dati personali, con la impossibilità di svolgere qualsiasi altra attività richiedente il trattamento dati di terzi.

Si occupa di controllare/sanzionare (in Italia) il **Garante per la protezione dei dati personali** conosciuto anche come **Garante della Privacy.**

Sono sanzioni importanti che nessuno si può permettere!