Nuovo regolamento UE 2016/679, cosa cambia rispetto alle attuali disposizioni sulla Privacy all'interno della Vostra Azienda?

Queste disposizioni devono venire applicate a tutte quelle aziende che trattano "dati personali" delle persone fisiche, limitazioni sull'obbligo di avere registri elettronici delle attività di monitoraggio e DPO figura di responsabilità del trattamento del dato sensibile, per le aziende sotto i 250 dipendenti.

Per quanto riguarda le disposizioni di protezione previste dalle passate normative, rimangono invariate le misure previste dalle certificazione UNI EN ISO 9001 per l'organizzazione aziendale, ISO 31000 che tratta il concetto di "rischio" e la ISO /IEC 27001:2005 (aggiornata 2013) per quanto riguarda la tecnologia delle informazioni, tecniche di sicurezza, sistemi di gestione della sicurezza delle informazioni e requisiti.

In aggiunta ulteriori obblighi quali:

L'informativa per la raccolta dei dati personali, deve essere accessibile, concisa e scritta con linguaggio chiaro e semplice, il consenso oltre che libero, specifico e informato deve essere inequivocabile. E' valido solo se la volontà espressa in modo NON equivoco per ogni singolo trattamento.

Introdotto il principio di "Accountability" ovvero della responsabilità "verificabile". E' obbligatorio documentare tutti i trattamenti effettuati poiché è sufficiente non avere i documenti per essere passibili delle sanzioni stabilite dal regolamento. (Precedentemente nella normativa italiana 196/2003 non vi erano obblighi in tal senso)

E' stato sancito l'obbligo per il titolare di comunicare le violazioni (data breach) subite all'autorità Garante senza ingiustificato ritardo entro 72 ore dal momento in cui né è avvenuto a conoscenza, nonché al soggetto interessato (se il dato non è criptato)

Diritto alla portabilità del dato

Diritto alla cancellazione " diritto all'oblio"

Un censimento di tutta la "tecnologia presente nell'azienda" creazione del documento PIA (Privacy Impact Assessment) censimento degli impatti privacy, in cui ogni fenomeno si valuta rischiosità complessiva,azioni intraprese e rischiosità residua in modo da realizzare la fotografica della situazione iniziale dell'azienda).

Dalla Valutazione PIA nasce poi un piano interno in cui viene stabilito in quale modo verrà mitigato il singolo rischio, coloro che sono incaricati di operare in tal senso e il costo previsto per l'attività.
Questo planning operativo deve essere costantemente monitorato e avrà impatto sul documento PIA successivo.

Facendo riferimento alla ISO/IEC 27001:2005 (aggiornata 2013) per la protezione informatica evidenziamo le funzioni che devono essere ben espresse nel documento:
INDIVIDUAZIONE mappare le possibili situazioni di rischio di violazione delle risorse, delle probabilità dell'evento e della gravità delle conseguenze
PROTEZIONE adottare in modo preventivo misure atte a evitare trattamenti non necessari e ridurre conseguenze negative
RILEVAZIONE istituire, secondo processi di qualità, un sistema di monitoraggio continuo in grado di segnare tempestivamente eventi legati al rischio privacy.
RISPOSTA predisporre misure correttive in caso di incidente, informando gli interessati e le autorità competenti.
RIPRISTINO predisporre pini di ripristino della normale operatività.

Differenza IMPORTANTE dalla precedente normativa Italiana sulla Privacy D.L. 196/2006 qui si dava disposizione ad attuare "MISURE MINIME DI SICUREZZA" che venivano descritte nella normativa, oggi si parla di "ATTURARE TUTTE LE MISURE NECESSARIE PER LA SICUREZZA DEL DATO" senza fare riferimento o riportare descrizione specifiche.

L'azienda quindi una volta "censita tutta la tecnologia" dovrà verificare:

- Di avere tutti Server e Computer con licenze valide e aggiornabili (windows XP, windows vista, windows 2000 NO IN REGOLA)

Sistemi operativi client	Service Pack o aggiornamento più recente	Fine del supporto Mainstream	Fine del supporto Extended
Windows Vista	Service Pack 2	10 aprile 2012	11 aprile 2017
Windows 7	Service Pack 1	13 gennaio 2015	14 gennaio 2020
Windows 8	Windows 8.1	9 gennaio 2018	10 gennaio 2023
Windows 10	con aggiornamenti disponibili	13 ottobre 2020	14 ottobre 2025

- Dove presente una rete di più computer, che questa sia protetta con un adeguato FIREWAL aggiornabile e monitorabile per la visualizzazione e il controllo dei log, sull'utilizzo e la possibile l'intrusione.

- Sulle macchine interessate nel trattamento dei dati personali, consigliamo di avere archivi “criptati” in modo da aumentare la loro sicurezza e limitare i rischi in caso di “data brech”.
- Avere un sistema di backup funzionante, documentato, controllato e periodicamente verificato.
- Avere un sistema pianificato e documentato per il ripristino del dato in caso di “problema “
- Monitorare “chi” utente, tratta il dato sensibile e “quando”, log delle operazioni effettuate.
- Avere un sistema di protezione Antivirus Antispyware valido e aggiornato per la protezione delle macchine.

Mantenere aggiornato il REGISTRO DELLE ATTIVITA’ DI TRATTAMENTO che sostituisce il DPS della normativa Italiana, dove riportarle finalità del trattamento e le attività del trattamento quali: processi di raccolta, registrazione, organizzazione,conservazione,consultazione,elaborazione,modificazione,selezione,estrazione,raffronto,utilizzo,interconnessione,blocco,comunicazione,diffusione,cancellazione, distruzione dei dati.
E’ importate ricordare che per “archivi” non si devono ricordare solo quelli presenti sulle macchini centrali quali server, ma anche i dati presenti sui singoli PC se fatte copie dei dati per la loro elaborazione.

Esempio registro trattamento:

Nome del Titolare del Trattamento:	Indirizzo: Numero di telefono: Indirizzo e-mail: Indirizzo PEC:
Nome del Responsabile per la protezione dei dati personali:	Indirizzo: Numero di telefono: Indirizzo e-mail: Indirizzo PEC:

TRATTAMENTO	UFFICIO	FINALITA'	TIPI DI DATI PERSONALI	CATEGORIE D'INTERESSATI	CONSENSO	INFORMATIVA	CONSERVAZIONE	MISURE DI SICUREZZA TECNICHE E ORGANIZZATIVE	CONTITOLARE DEL TRATTAMENTO	RAPPRESENTANTE DEL TITOLARE	RESPONSABILE DEL TRATTAMENTO	DESTINATARI DELLE COMUNICAZIONI DEI DATI PERSONALI	PAESE TERZO O ORGANIZZAZIONE INTERNAZIONALE	SE APPLICABILE, LE GARANZIE ADEGUATE PER IL TRASFERIMENTO

(possibile allegato tutto schermo)

I principali rischi che bisogna prevenire sono la “VIOLAZIONE DEI DATI PERSONALI”

> La violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l’accesso ai dati personali trasmessi, conservati o comunque trattati. Perdita dei dati per guasto tecnico, errore umano o minaccia informatica quali virus o simili.

Gli strumenti che possiamo offrire al cliente per prevenire gli aspetti sopra citati sono:

- Software Antivirus Antispyware ESET SECURITY, ESET ANTIVIRUS , BRM WEB PROTECT , BRM ANTIVIRUS.
- Software per il Backup dei dati, BRM Backup
- Software di controllo della login e di accesso ai dati tramite sistema operativi professional e server Microsoft e software di Audit Netrwix
- B.R.M per il controllo dello stato della macchina, la login degli utenti, l’utilizzo delle risorse del pc i log del sistema operativo
- Firewall per la sicurezza delle reti tra computer.