BUSINESS VALUE

General Data Protection Regulation
GDPR
Scadenza 25 maggio 2018

Premessa

Il **25 maggio 2018** entrerà in vigore il nuovo Regolamento (UE) 2016/679 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 e che abroga la direttiva 95/46/CE (**regolamento generale sulla protezione dei dati**) (c.d. **Regolamento** o **GDPR).**

Gli **obiettivi** del nuovo Regolamento sono soprattutto quelli di:

- armonizzare la normativa vigente in tema di protezione dei dati personali, creando un'unica legge condivisa, direttamente applicabile in tutti gli Stati membri dell'Unione Europea;
- aumentare il livello di protezione dei cittadini dell'Unione;
- adeguare il dettato normativo rispetto alle tecnologie esistenti ed emergenti.

Il GDPR impone una seria revisione sulle modalità attraverso le quali le società gestiscono la propria organizzazione, processi e tecnologie.

Principali principi del nuovo regolamento generale sulla protezione dei dati

Proporzionalità

I dati devono essere adeguati, pertinenti e **limitati a quanto necessario rispetto alle finalità** per le quali sono trattati.

Diritto all'oblio

Il Titolare del trattamento deve **garantire all'interessato la cancellazione dei dati personali** che lo riguardano senza ingiustificato ritardo (***Right to be forgotten***)

Portabilità dei dati

Obbligo di garantire all'interessato la **trasmissione diretta dei dati personali da un Titolare all'altro**, se tecnicamente fattibile senza impedimenti

Risk-based approach

Necessità per le imprese di effettuare un *Privacy Impact Assessment* (= valutazione dei rischi per i trattamenti previsti)

Implementazione di misure di sicurezza basate sull'analisi dei rischi e dei costi di attuazione.

Previsione espressa delle misure di sicurezza sono appropriate per ridurrei rischi (pseudonimizzazione, crittografia, l resilienza dei sistemi.

Privacy by design e Privacy by default

Obbligo di assicurare che le misure adottate attuino efficacemente i principi di *privacy by design e by default*

Consenso

Il consenso, oltre ad essere preventive ed inequivacabile, **deve essere esplicito** ed essere prestato liberamente: il GDPR richiede che l'interessato acconsenta al trattamento dei dati personali con atto positivo inequivocabile con il quale dimostra l'intenzione libera, specifica e informata di accettare il trattamento di dati personali che lo riguardano (e.g.: non ci sono caselle preimpostate).

Principi significativi (segue)

REGIME DI ACCOUNTABILITY

I Titolari devono effettuare i trattamenti dati personali conformemente ai principi privacy stabiliti dal GDPR ed essere in grado di comprovarlo (art. 5 del GDPR)

- *Policies* e processi interni di Titolari e Responsabili devono adeguarsi agli adempimenti richiesti dal GDPR.
- Titolari e Responsabili devono mantenere una registro - 'inventario'- in forma scritta da mettere a disposizione del Garante Privacy, ove richiesto, riguardo ai trattamenti dati effettuati sotto la propria responsabilità.
- *Privacy by design / by default*: i principi del GDPR devono essere implementati non sono al livello di processi organizzativi, ma devono essere riflessi anche nei servizi e nei prodotti (es. Certificazioni).
- *Privacy Impact Assessment* (PIA =Valutazione d'impatto sulla protezione dei dati): le attività di trattamento considerate ad alto rischio richiedono una valutazione preventive da parte del Titolare (es. Profilazione o Trattamento di dati sensibili).
- Se non sono adottate misure idonee per mitigare il rischio è necessario avviare una "*Prior Cosultation*" con l'Autorità Garante che fornirà le indicazioni necessarie .
- Misure tecniche e organizzative: obbligo di implementare misure adeguate al fine di proteggere i dati personali (es. pseudo minimizzazione e crittografia).
- *Data Breach Notification*: violazioni alla sicurezza dei dati devono essere notificate dai titolari a (i) Autorità Garante entro 72 ore (salvo che il rischio sia escluso) e (ii) soggetti interessati senza indebito ritardo in caso di rischio elevato.

Punti chiave del GDPR

Armonizzazione Leggi, Ambito ampliato

- **Riduzione degli oneri amministrativi:** non più necessarie Notifiche di trattamento ai Garanti privacy
- **One-Stop-Shop:** per le multinazionali, vi è un unico Garante privacy nella UE
- **Interesse legittimo:** base legale per effettuare trattamenti in specifiche circostanza
- **Ambito territoriale:** organizzazioni stabilite nella UE ed organizzazioni extra UE con business e/o attività di monitoring inidrizzati verso individui nella UE; Titolari e Responsabili extra UE devono nominare un loro Rappresentante UE per la privacy

Aumento degli Obblighi

- Accountability - Obbligo per i Titolari di adempiere e dimostrare di adempiere ai principi ed alle misure richieste dal GDPR
- Consenso
- Privacy by design e by default
- Misure da implementare preventivamente e durante l'esecuzione dei trattamenti
- Privacy Impact Assessment
- Analisi impatti privacy prima di effettuare un trattamento, in caso di Rischi Elevanti occorre richiedere la Prior Consultation del Garante
- Data Breach
- Notifica al Garante Privacy entro 72 ore, in alcuni casi necessario darne comunicazione anche agli Interessati
- DPO (Data Protection Officer)
- Aumento degli impegni e responsabilità dirette dei Responsabili
- Maggior oneri per i Responsabili (verso i Titolari, verso i propri Provider, nuovi adempimenti, responsabilità di fronte la legge)

Punti chiave del GDPR

Codici di condotta e Certificazioni

- Le organizzazioni che adotteranno i Codici di Condotta, una volta approvati dalla autorità comeptenti, potranno beneficiare dei vantaggi connessi alla valenza dei Codici, quali evidenza della compliance rispetto ad alcuni adempimenti privacy (misure di sicurezza, trasferimento dati extra UE,…).
- Anche nel caso delle Certificazioni le organizzazioni che si certificano dimostrano di essere compliant rispetto ad alcuni adempimenti privacy (caratteristiche di affidabilità dei Responsabili, misure di sicurezza, trasferimento dati extra UE,…).
- I sistemi di certificazioni Privacy devono preventivamente essere approvati dalle autorità Garanti Privacy. È prevista la costituzione di enti di controllo ad hoc.

Diritti degli Interessati

•Informativa

- Espressa diversificazione delle informative in caso di raccolta dei dati direttamente presso l'Interessati o meno, richiesto un maggior contenuto informativo ma allo stesso semplicità e chiarezza, promosso il ricorso a particolare ICONE semplificative stabilite/autorizzate delle autorità Garanti privacy

•Diritti di Opposizione

- Diritti di opporsi in ogni caso per motivi legittimi al trattamento e diritto di opporsi alla profilazione o al trattamento per legittimo interesse.

•Data Portability

- Diritto di ricevere indietro i dati in un formato standard e *machine-readible* senza oneri aggiuntivi, previsto anche la possibilità di richiedere il trasferimento diretto dei dati da un Titolare ad un altro

•Diritto all'oblio

- Diritto di ottenere la cancellazione dei dati, anche se resi pubblicamente disponibile, salvo che non prevalgano diritti di altri (es diritto di cronaca, etc)

•Profilazione

- Maggior controllo degli Interessati su profilazioni in base alla raccolta dei loro dati personali

Punti chiave del GDPR

Regime di responsabilità, sistemi di controllo e sanzioni

•Risarcimenti da parte di Titolari e Responsabili

- In caso di danni agli Interessati in relazione al trattamento dei loro dati personali

•Ricorsi verso Titolari e Responsabili

- Promossi dagli Interessati in caso di trattamenti dati non conformi al GDPR, presso le autorità Garanti Privacy o via giudiziarie ordinarie
- **Aumentati poteri di controllo delle autorità Garanti Privacy**
- Poteri investigativi, correttivi, autorizzativi e consultivi
- Poteri di imporre sanzioni pecuniarie di elevato valore (milioni di euro)

•EDPB European Data Protection Board

- Nuovo organismo privacy a livello europeo dotato di personalità giuridica, nasce dal già presente Working Party 29, dotato di maggiori ambiti e poteri di intervento (es Consistency Mechanism)
- **Severe Sanzioni amministrative** fino a 20 milioni di euro [in caso di imprese fino al 4% del fatturato se superiore a 20 milioni di euro] e ulteriori penali delegate agli Stati Membti

Trasferimento dati extra UE

•Decisioni UE di adeguatezza privacy di paese terzo o organizzazione internazionale

- Stabilite con decisione UE , non necessitano di autorizzazione del Garante privacy nazionale

- **Clausole Contrattuali Standard a livello UE**

- Stabilite con Decisione UE, non necessitano di autorizzazione del Garante privacy nazionale

- **Clausole Contrattuali Standard a livello nazionale**

- Stabilite dal Garante privacy nazionale, sottoposte a check EDPB

- **Clausole Contrattuali ad hoc a livello nazionale**

- Stabilite dal Garante privacy nazionale ad hoc

•BCR Binding Corporate Rules

- Stabilite con procedura EDPB, riguardano il caso di multinazionali, sia per il caso Titolare che Responsabile

•Esenzioni

- Trasferimenti ammessi in caso di rapporti contrattuali e pre, consenso Interessati, …., per alcuni casi di legittimo interesse-trasferimenti saltuari ma a determinate, esistenza e dimostrata aderenza ad appositi Privacy CoC o Certificazioni Privacy

BUSINESS VALUE

Ruoli e responsabilità

Il Titolare del Trattamento:

- adotta soluzioni e strumenti già in ottica P*rivacy by design e by default*;
- implementa misure di sicurezza opportune rispetto all natura, all'oggetto, al contesto e alle finalità del trattamento, nonché al rischio per i diritti e le libertà delle persone fisiche;
- dimostra la conformità delle operazioni di trattamento rispetto ai principi sanciti dal Regolamento (es. misure tecniche e organizzative; adeguate *policy* e procedure in materia di protezione dei dati; registro delle categorie di attività di trattamento, etc.)
- effettua *la Privacy Impact Assessment* (PIA) in tutte le circostanze nelle quali la tipologia dei dati ed i relativi trattamenti lo rendano necessario;
- implementa strumenti e procedure atte a rilevare tempestivamente violazioni nel trattamento dei dati personali (*Data breach*) notificando entro 72 ore l'accaduto all'Autorità garante;
- notifica la violazione agli Interessati nel caso vi siano rischi rilevanti per la tutela dei loro dati personali nonché rischi per i loro diritti e libertà

Ruoli e responsabilità

Il Responsabile del Trattamento:

- tratta i dati personali eseguendo le istruzioni ricevute dal Titolare che sono sempre espressamente previste in un contratto o da altro atto giuridico che indichi con chiarezza gli obblighi in capo al soggetto designato (Oggetto; Durata; Natura e finalità del trattamento; Tipologia dei dati; Categorie di interessati; Obblighi e diritti del titolare);
- assicura che tutti coloro che trattano i dati personali su sue indicazioni si siano impegnate a rispettare i vincoli di riservatezza;
- ha numerosi e nuovi obblighi di assistenza nei confronti del Titolare al fine di consentire a quest'ultimo il rispetto dei propri obblighi;
- implementa e mantiene tutte le misure tecniche e organizzative adeguate;
- prevede la presenza del Data Protection Officer ove prescritto o in vista delle caratteristiche dei trattamenti effettuati;
- assume maggiori rischi connessi ad una sua immediata e diretta responsabilità relativamente ai trattamenti a lui affidati;
- costituisce un diretto interlocutore sia per l'Interessato che per le Autorità di controllo;
- risponde dell'eventuale attività di terzi suoi fornitori dovendo garantire il rispetto dell'applicazione della normativa da parte di tali soggetti.

Il DPO – Data Protection Officer

Chi è?

- *Esperto della legge sulla protezione dei dati*
- *Competente in materia di sicurezza delle informazioni e di Information Technology*
- *Risponde direttamente e unicamente all'executive management*
- *Opera in piena indipendenza e in assenza di conflitti di interesse*
- *Dotato di risorse umane e finanziarie necessarie per adempiere agli obblighi normativi*

Cosa fa?

- *Consiglia, sensibilizza, e informa il titolare e il responsabile sugli obblighi del Regolamento*
- *Conserva la documentazione richiesta dal*
- *Controlla che le violazioni siano comunicate e documentate*
- *Assicura e controlla che venga effettuata la Data Protection Impact Analysis e venga richiesta l'autorizzazione preventiva*
- *Coopera con il Garante e supporta le sue richieste*
- *Cura la formazione dei responsabili dei trattamenti*

Come viene nominato?

- *Un gruppo di imprese può nominare un DPO principale per l'intero gruppo*
- *Gli organismi pubblici devono designare un DPO ma questi può coprire più enti*
- *Nei casi diversi da quelli elencati prima i titolari, o associazioni di titolari, possono designare un DPO*
- *Deve essere designato per un periodo di almeno 4 anni se dipendenti e di 2 se consulente esterno*
- *Il Garante è informato della sua nomina*

Quando è necessario?

- *Se il trattamento è effettuato da un ufficio pubblico*
- *Se il trattamento è effettuato da un'organizzazione e riguarda più di 5.000 interessati in un periodo di 12 mesi*
- *Se riguarda il trattamento di dati particolari o dati di minori*
- *Se i trattamenti richiedono controllo regolare e sistematico degli interessati*

Sanzioni dal 25 maggio 2018

Violazione	Sanzione Amministrativa
Omessa o inidonea informativa	Sanzioni fino 20 milioni di euro oppure il 4% del fattura mondiale annuo se superiore
Cessione non autorizzata dati personali	Sanzioni fino 20 milioni di euro oppure il 4% del fattura mondiale annuo se superiore
Trattamento illecito dei dati	Sanzioni fino 20 milioni di euro oppure il 4% del fattura mondiale annuo se superiore
Mancata dimostrazione di avere adempiuto agli obblighi generali sulle misure di sicurezza adeguate al rischio	Sanzioni fino 10 milioni di euro oppure il 2% del fattura mondiale annuo se superiore

Punti di attenzione immediata

- Analizzare il quadro normativo e identificare le obbligazioni direttamente applicabile alla propria organizzazione.
- "Inventariare" la tipologia di dati personali trattati, la localizzazione degli stessi e i processi aziendali e la tecnologia impattata.
- Verificare la necessità di creare l'ufficio del DPO.
- Verificare se le informative e i consensi utilizzati all'interno e all'esterno dell'organizzazione sono in linea con i requisiti del GDPR.
- Rivedere i processi organizzativi impattatati dai diritti dell'interessato (es. diritto di accesso).
- Rivedere le *policies* di conservazione dei dati personali.
- Rivedere le modalità di trasferimento di dati personali fuori dall'Unione Europea, se presenti.
- Implementare l'approccio della *Privacy By Design* rispetto ai sistemi usati e ai servizi/prodotti offerti.
- Implementare un sistema di registrazione e documentazione delle operazioni di trattamento effettuate dall'organizzazione.
- Implementare un sistema di misure di sicurezza adeguato alle attività di trattamento svolte e ai rischi correlati.
- Implementare processi di monitoraggio del *data breach* e delle relative notifiche.
- Implementare un idoneo processo di formazione all'interno della propria organizzazione.

BUSINESS VALUE

L’Approccio proposto

Fase 1: Analisi impatto della normativa

L'obiettivo di questa fase è di fornire alle funzioni aziendali competenti un quadro chiaro che consenta di raffrontare e di sintetizzare le modifiche introdotte dalle nuova normativa. In questa fase sono previste le seguenti azioni:

a) Analisi dell'Organizzazione

- Obiettivo: Raccolta delle informazioni per la comprensione del contesto di riferimento;

b) Identificazione normative applicabili

- Obiettivo: Definizione del quadro normativo applicabile per singola linea di Business;

Fase 2: Assessment situazione attuale e definizione degli interventi di adeguamento

L'obiettivo è di valutare la compliance aziendale rispetto alle nuove disposizioni previste dal Regolamento EU e, sulla base di una gap analisys, definiremo le azioni di intervento per adeguare il complesso delle attività di alle modifiche normative. In particolare il percorso progettuale prevede un **audit iniziale** per una prima valutazione della conformità aziendale agli obblighi di legge (documentazione e processi) in termini di:

- attuale struttura di governance aziendale e rispetto degli obblighi di reporting interni in materia di privacy;
- analisi della struttura organizzativa (organigramma e Funzionigramma) con la individuazione degli interlocutori direttamente ed indirettamente coinvolti nella definizione, gestione e trattamento delle informazioni oggetto della normativa relativa alla privacy con specifico riferimento :
  - alle modalità di raccolta dei dati personali/sensibili,
  - alle modalità di acquisizione del consenso al trattamento da parte degli interessati,
  - alle finalità e scopi del trattamento,
  - alle misure di sicurezza adottate,
  - alla comunicazione e/o trasferimento dei dati in favore di soggetti terzi residenti nel territorio dell''Unione Europea e/o fuori dal territorio dell'Unione Europea.

Fase 2: Assessment situazione attuale e definizione degli interventi di adeguamento

- **Analisi dei sistemi informatici** e delle modalità di archiviazione dei dati personali di terzi e delle procedure di sicurezza per la gestione ed il trattamento dei dati;
- **Gap analisys per la definizione delle criticità rilevate** nell'attività precedente, propedeutiche alla individuazione delle azioni da intraprendere per garantire la compliance con gli aggiornamenti normativi con la determinazione delle relative priorità;
- **Definizione interventi di adeguamento** con la predisposizione di un documento informativo che inquadra le soluzioni per l'implementazione di misure atte a garantire la conformità delle attività con la normativa vigente e superare le criticità riscontrate.
- **Definizione delle linee per la Progettazione Privacy by Design;**
- **Definizione dei requisiti del data protection officer** (DPO);

Fase 3: Implementazione di processi e definizione di policy interne

L'obiettivo di questa si impronta ,in relazione alle criticità riscontrate ed alle azioni di miglioramento ipotizzate, potrà riguardare:

- **Definizione del "Modello Organizzativo Privacy"**:
  - distribuzione compiti e responsabilità nell'ambito delle strutture preposte al trattamento privacy;
  - elenco dei trattamenti dei dati personali con individuazione dei dati trattati;
  - aggiornamento informative;
  - verifica delle attività degli amministratori di sistema;
  - programmazione degli eventi formativi interni;
- **Redazione di una Compliance Level Map (**CLM mappa del livello di applicazione delle procedure in materia di compliance),
- **Redazione e revisione di clausole**:
  - il consenso al trattamento dei dati;
  - la nomina di responsabili esterni,
  - la nomina di amministratori di sistema;
- **Aggiornamento,** anche attraverso l'invio di newsletters giornaliere e circolari mensili, delle novità normative in materia di Privacy;
- **Gestione** dell'inventario dei sistemi e degli archivi contenenti dati personali di terzi**;**
- **Individuazione ,** con condivisione del management azienda del *profilo professionale del Data Protection Officer (DPO);*
- **Progettazione** di un sistema di "Privacy by Design "

Fase 4: Formazione

L’obiettivo di questa fase è di realizzare una programmazione di eventi informativi e moduli formativi per assicurare che tutti gli interlocutori coinvolti acquisiscano le nuove modalità di comportamento dettate dalla nuova normativa che entrerà in vigore nel corso del 2018.

Fase 5: Attività di supporto continuo e fine tuning sistema di gestione della privacy

L’obiettivo di questa fase è fornire un Servizio di “early warning” sulle nuove disposizioni in materia di trattamento di dati personali e assistenza sulle eventuali attività da intraprendere ed implementare per mantenere costantemente la conformità del sistema di gestione della privacy alla normativa vigente.

Supporto legale on-going

L'obiettivo è quello di fornire un supporto legal costante nella valutazione degli impatti tecnico-normativi con particolare interesse:

- **Analisi e interpretazione** della normativa presente nel Nuovo Regolamento Privacy (DPGR), e redazione di memorandum informativi
- **Verifiche** di allineamento delle documentazioni di change normativo, revisione di politiche aziendali dei Codici Etici e di buona condotta;
- **Assistenza** nella stesura degli atti e della «modulistica privacy»; redazione e/o revisione delle clausole contrattuali in materia di trattamento dei dati personali; predisposizione e/o revisione di accordi interni tra contitolari del trattamento, tra titolare e responsabile e tra responsabile e sub-responsabile.
- **Comunicazioni** verso il Garante della Privacy ed altri enti istituzionali;
- **assistenza** nello svolgimento di attività formative specifiche per le figure professionali coinvolte in ambito privacy.

I Deliverable

- Fotografia generale sullo stato dell'Impianto Privacy
- Raccolta delle specifiche necessità di adeguamento normativo rispetto al contesto del cliente
- Stesura di un report di Gap Analysis, con indicazione delle sanzioni a seconda del gap e Piano di Azione
- Revisione generale dell'impianto documentale obbligatoriamente previsto dalla normativa
- Servizio di Audit interno effettuato da Auditor certificati secondo lo schema ISDP©10003:2015 DATA PROTECTION (unico accreditato)
- Stesura della documentazione
- Affiancamento in certificazione

RIFERIMENTI E CONTATTI

BUSINESS VALUE S.r.l.
Via di Panico 54
00186 Roma RM - Italia
Telephone:+39 06 686 1458
Fax: +39 06 686 1592
Email: bpiperno@businessvalue.it
Website: www.businessvalue.it

Bruno Piperno - bpiperno@businessvalue.it - *mob. +39 337 794041*
Francesco Antonelli - antonelli@businessvalue.it - *mob. + 39 348 3835076*
Francesco De Paolis - depaolis@businessvalue.it - *mob. +39 335 6225252*

BUSINESS VALUE