REGOLAMENTO EUROPEO PRIVACY 679:2016
[GDPR] General Data PRIVACY Regulation

GUIDA SEMPLICE IN 13 PASSI

Liberamente tratta da ICO – Information Commitioner's Office

Privacy & Regolamento 679

Consulenza & Formazione per Aziende e Professionisti

1

CONSAPEVOLEZZA

I Titolari di Azienda devono assicurarsi che i responsabili delle decisioni chiave e tutte le persone dell'organizzazione siano consapevoli degli impatti del nuovo Regolamento , attraverso una adeguata **FORMAZIONE**

2

DATI & INFORMAZIONI

L'azienda deve documentare quali dati personali utilizza, da dove provengono e con chi li condivide. Occorre inoltre stabilirne le **FINALITA'.** Ovvero gli **SCOPI**.
A cosa mi servono questi dati ? Come li utilizzo ?

3

COMUNICAZIONE DELLE INFORMAZIONI

L'azienda deve implementare un **adeguato livello di comunicazione Interna ed Esterna** al fine di trasmettere i requisiti del Nuovo regolamento 679 , nonché gestire correttamente le successive modifiche ed integrazioni.

4

DIRITTI DEGLI INDIVIDUI

Occorre stabilire procedure per assicurare di rispettare tutti i diritti che gli individui hanno, compreso il modo per eliminare i dati personali e le relative modalità di gestione e trattamento dei dati informatici una volta che il rapporto sia cessato (email, ecc.)

5

SISTEMI DI ACCESSO AI DATI

Occorre stabilire procedure che indichino le modalità di accesso ai dati sia cartacei che informatici. Per questi ultimi definire criteri di PW e loro modifica periodica.
Stabilire una Policy Aziendale per la gestione dei dati informatici

6

REQUISITI LEGALI TRATTAMENTO DATI

L'azienda deve identificare le diverse tipologie di dati trattati e stabilirne le relative implicazioni Legali , ovvero i rischi che corre se non gestisce correttamente quei dati.
Implementare un Risk Assesment

7

CONSENSO

E' necessario ottenere il consenso firmato del trattamento dei dati da TUTTI i soggetti interni ed esterni all'azienda [Dipendenti, Consulenti, Fornitori, Clienti]
E' necessario stabilire il consenso per le specifiche FINALITA' e SCOPI

8

TUTELA DEI MINORI > 16 anni

Se tratti dati di MINORI [Scuole o Associazioni Sportive , Social] devi predisporre adeguati sistemi per verificare l'età degli individui e per raccogliere il consenso dei genitori o dei tutori per il trattamento dei dati specifici per lo svolgimento delle attività

9

VIOLAZIONI DEI DATI [DATA BREACHES]

Occorre predisporre specifiche procedure in grado di rilevare, segnalare e indagare i casi in cui può avvenire la violazione della protezione dei dati. Occorre impostare una corretta **VALUTAZIONE DEI RISCHI e MODALITA' di COMUNICAZIONE**

10

SICUREZZA INFORMATICA

L'azienda deve attuare principi di protezione dei dati informatici attraverso una adeguata struttura di protezione dei rischi ed attuare sistemi **ANTI VIOLAZIONE**

11

PRIVACY BY DESIGN & BY DEFAULT

L'azienda deve attuare principi di protezione dei dati sin dalla fase di progettazione [design] ,ed avere procedure chiare che prevedano il trattamento dei soli dati personali necessari al perseguimento delle finalità aziendali.

12

Responsabile della protezione dei dati [DPO]

L'azienda dovrebbe designare un responsabile della protezione dei dati, se richiesto, o qualcuno che si assuma la responsabilità dei dati a tutela della conformità Legale. Tale Ruolo dovrà fare parte della struttura organizzativa dell'azienda con precisi accordi con il Titolare.

13

ATTIVITA' INTERNAZIONALI

Se l'azienda opera in un contesto Internazionale sono necessarie procedure specifiche che stabiliscano una supervisione e controllo nella gestione e trattamento dei dati nei vari contesti internazionali.

Questa piccola ma utile check list ti aiuterà a prepararti per il prossimo 25 Maggio 2018 a implementare in modo corretto quanto previsto dal Nuovo Regolamento Europeo 679:2016 – GDPR

SCOPRI I DETTAGLI DEI 13 PASSI FONDAMENTALI

Molti dei concetti e principi del **Nuovo Regolamento Europeo 679:2016** - GDPR sono più o meno gli stessi di quelli dell'attuale Legge sulla Privacy , ovvero il Decreto legislativo 196 del 2003.
Pertanto le Aziende che hanno mantenuto attivo e correttamente applicato il vecchio modello possono ritenersi fortunate in quanto si trovano ad avere un Sistema di analisi, gestione e trattamento dei dati sufficientemente conforme.
Inoltre chi ha mantenuto in piedi il vecchio DPS , si trova già con una pur minima Valutazione dei Rischi che può essere considerata la base del **Nuovo Data Impact System** .

Tuttavia, nel nuovo Regolamento 679 ci sono nuovi elementi e miglioramenti piuttosto significativi . Sarà necessario quindi per le Imprese fare alcune cose per la prima volta ed altre cose in modo diverso.

Questi **13 punti della Check List** ti possono aiutare a capire quali sono le principali innovazioni introdotte dal Nuovo regolamento e potrai così facilmente fare in modo autonomo una tua **GAP ANALYSYS** , ovvero verificare quanto ancora sei distante dalle nuove regole che dovrai implementare.

Ti consiglio di iniziare quanto prima a pianificare il tuo approccio di conformità al nuovo GDPR e soprattutto iniziare a coinvolgere le persone chiave della tua organizzazione, in particolare chi si occupa dei SISTEMI INFORMATICI.
Sarà infatti necessario mettere in atto nuove procedure, stabilire nuove POLICY AZIENDALI in materia per esempio di gestione e trattamento dei dati informatici . L'azienda dovrà soprattutto stabilire un **BUDGET ADEGUATO** per conformarsi al NUOVO GDPR.

Privacy & Regolamento 679
Consulenza & Formazione per Aziende e Professionisti

1

CONSAPEVOLEZZA

Ogni Azienda, attraverso una **ADEGUATA FORMAZIONE,** deve assicurare che i responsabili di funzione e tutti gli incaricati delle decisioni, nonché le persone chiave presenti nella propria organizzazione, siano consapevoli del fatto che la legge sulla Privacy sta cambiando e deve essere adattata entro il **25 Maggio 2018** alle regole del Nuovo regolamento 679:2016, cosiddetto DGPR GDPR.

Al fine di valutare l'**IMPATTO** che il **NUOVO REGOLAMENTO** avrà sull'azienda, sarà necessario identificare le aree che potrebbero avere maggiori problemi di conformità ai sensi del nuovo GDPR.

E' necessario partire quindi da una **VALUTAZIONE DEI RISCHI** dell'Azienda in grado di analizzare quali implicazioni significative, in termini di risorse e strumenti, sono necessari per l'attuazione di **TUTTI I REQUISITI** del nuovo GDPR.

Per affrontare il nuovo GDPR ed avere la **GIUSTA CONSAPEVOLEZZA** è necessario prepararsi per tempo e non lasciate i preparativi all'ultimo minuto. E' necessario quindi stabilire un corretto **ACTION PLAN**

2

DATI & INFORMAZIONI – MAPPATURA , FINALITA' ed ESATTEZZA dei DATI

Ogni Azienda deve documentare, attraverso una specifica mappatura quali sono i dati personali che vengono trattati, da dove provengono, con chi lo condividi e soprattutto per quali **FINALITA' o SCOPI.** E' necessario a tal scopo predisporre una **specifica procedura** .

In particolare il nuovo GDPR si sofferma sul concetto dei diritti fondamentali nel **trattamento dei dati che avvengono in rete**. In un mondo sempre più interconnesso, la possibilità che i dati personali finiscano in mani poco raccomandabili è molto alto. Pensiamo ad esempio a tutte le commessioni in CLOUD.
Oltre a ciò il DGPR impone una corretta gestione dei dati personali inesatti o da modificare qualora questi siano stati condivisi con altre organizzazioni. In questo caso l'azienda dovrà comunicare all'altra organizzazione l'inesattezza del dato, richiedere immediatamente la sua modifica / cancellazione. L'azienda sarà in grado di fare ciò solo nel caso che essa sappia quali sono i dati personali, da dove provengono e con chi sono stati condivisi, attraverso appunto una specifica MAPPATURA che definisca : **TIPO DI DATO – FINALITA' E SCOPI – MODALITA' DI TRATTAMENTO - MISURE DI TUTELA PER LA PROTEZIONE E L'ARCHIVIAZIONE.**

AUDIT PERIODICI di personale terzo potrebbero essere utili a MONITORARE l'effettiva applicabilità di questo importante PUNTO.

3

COMUNICAZIONE DELLE INFORMAZIONI

L'AZIENDA deve implementare una specifica **procedura per la gestione delle informazioni** sulla privacy, interne ed esterne, e stabilire le regole previste specificatamente dal nuovo GDPR.

Per esempio quando l'azienda **raccoglie i dati personali** dei dipendenti, dei clienti, dei fornitori, dei consulenti, ecc. , informazioni riguardanti **l'identità, l'indirizzo civico , il codice fiscale, i dati bancari, ed eventualmente anche quelli relativi la salute, le scelte politiche, la religione**, ecc. è necessario che l'azienda stabilisca come intende utilizzare tali informazioni e come vengono protette e tutelate da attacchi esterni.

Tutto ciò di solito viene realizzato attraverso un **Policy sulla Privacy** o specifiche lettere Informative sulle quali viene anche richiesto il consenso.
Oltre a ciò nel GDPR ci sono alcune richieste aggiuntive che l'azienda dovrà comunicare come ad esempio:

- La base legale per l'elaborazione dei dati , ovvero quali sono le **modalità di TUTELA**
- I periodi di conservazione dei dati
- Il diritto delle persone di lamentarsi verso il GARANTE per la PRIVACY se pensano che ci sia un problema nel modo in cui si sta gestendo i loro dati.

Il GDPR richiede che TUTTE le informazioni siano fornite in linguaggio sintetico, facile da capire e chiaro.

4

DIRITTI DEGLI INDIVIDUI – DIRITTO ALL'OBLIO

Ogni Azienda deve attuare procedure in grado di assicurare che coprano tutti i diritti fondamentali degli individui, compreso il modo in cui si eliminano i dati personali sia forniti elettronicamente che in forma cartacea. **Il DIRITTO ALL'OBLIO** è una delle novità del nuovo GDPR. I principali diritti degli individui riscontrabili nel GDPR sono :

- ☐ accesso ai dati da parte del soggetto
- ☐ correzione delle imprecisioni
- ☐ cancellazione delle informazioni [DIRITTO ALL'OBLIO]
- ☐ prevenzione del marketing diretto
- ☐ impedimento della profilazione automatizzata
- ☐ portabilità dei dati ad altre persone

Nel complesso, i diritti che le persone godranno sotto il GDPR sono i come quelli già in atto con l'attuale D.Lgs. 196/2003 ma con alcuni miglioramenti significativi. **Se l'azienda è quindi già conforme ai vecchi requisiti la transizione al nuovo GDPR dovrebbe essere relativamente facile**. Il periodo transitorio attuale, **fino al Maggio 2018** è un buon momento per controllare le procedure e capire quanto ogni azienda è distante rispetto alle nuove regole.

Il diritto alla portabilità dei dati è nuovo. Si tratta di tutte quelle condizioni nelle quali si devono fornire i dati sia elettronicamente che in a formato cartaceo . Il nuovo GDPR richiede che vengano stabiliti criteri di informazione e consenso nel caso tali dati siano comunicati ad altri soggetti.

5

SISTEMI DI ACCESSO AI DATI – CREDENZIALI DI AUTENTICAZIONE

Entro il **25 maggio 2018** ogni azienda dovrà aggiornare le procedure e definire le modalità con cui gestire la nuova documentazione prevista dal Regolamento 679/2016, in particolare stabilire le modalità di autenticazione e di accesso ai vari dati aziendali.
Con il GDPR cambieranno le regole per trattare la documentazione relativa all'accesso ai dati.
Ogni azienda dovrà stabilire specifiche **Policy e Procedure** per dimostrare le modalità di accesso ai dati attraverso specifiche **credenziali di autenticazione** e loro corretta gestione e modifica.

In alcuni casi, al fine di tutelare il diritto alla privacy delle persone, possono essere utilizzati dei codici identificativi, o cosiddette **PSEUNONIMIZZAZIONI**, così da eliminare tentativi di accesso indiscriminato [si pensi ad esempio alle commesse dei supermercati o qualunque persona che lavora in front-end con gli utenti]

La **POLICY AZIENDALE** dovrà inoltre stabilire regole precise da condividere con i collaboratori al fine di stabilire i canali di **accesso alle informazioni online**.
Le aziende dovrebbero inoltre considerare la stesura di un'analisi **costi/benefici** per strutturare una piattaforma informatica adeguata.

6

REQUISITI LEGALI DEL TRATTAMENTO DEI DATI – FINALITA'

Ogni azienda dovrà esaminare i vari tipi di trattamento dei dati che utilizza e gestisce, conoscere **la base legale** per utilizzarli in conformità ai principi del **NUOVO REGOLAMENTO.**

Avere una visione legale relativamente ai dati trattati, significa definire le **FINALITA' del TRATTAMENTO dei DATI** ma stabilire anche una **Valutazione dei Rischio** specifica relativamente alla mancata gestione dei dati stessi alla luce dei **DIRITTI specifici degli INTERESSATI**.

Tutto questo meccanismo sarà piuttosto complesso e diverso sotto il nuovo GDPR, perché i diritti di alcuni individui saranno modificati in base alla questione legale necessaria per le **FINALITA'** dei loro dati personali. **Per FINALITA' intendiamo lo SCOPO** per cui tu Azienda hai bisogno di quel mio dato.

L'esempio più ovvio è che le persone avranno un **forte diritto di ottenere la cancellazione dei loro dati** personali nel caso in cui l'azienda tratti i dati in **DIFFORMITA'** a quanto stabilito.

SCOPI & FINALITA' dovranno essere definite e gestite attraverso specifiche **INFORMATIVE e LETTERE DI CONSENSO.**

7

RICHIESTE DI CONSENSO

Ogni azienda dovrà STABILIRE in modo documentato come sta richiedendo, ottenendo e registrando il consenso al trattamento del dati personali sia del **personale dipendente interno**, sia dei **clienti** che dei **fornitori**.
E' necessario stabilire ed ottenere il consenso anche per tutte le attività che vengono svolte ON-LINE come per esempio le Campagne Marketing e/o iscrizioni a INFO NEWS.

Come il precedente D.Lgs. 196/2003 , il nuovo GDPR identifica i riferimenti e le modalità sia per il **«consenso formale»** che per il **«consenso esplicito».**

La differenza tra le due tipologie di consenso non è ancora così chiara dato che entrambe le forme di consenso devono essere fornite liberamente, ma soprattutto devono essere specifiche, spiegate in modo chiaro e inequivocabili.
Il consenso deve essere sempre verificabile e le aziende devono mettere in atto procedure chiare per gestire correttamente e rendere disponibili in ogni momento **TUTTI i consensi** dei soggetti verso i quali l'azienda tratta i dati, sia in forma cartacea che informatica.

8

TUTELA DEI MINORI di età inferiore ai 16 Anni

Se l'azienda o l'organizzazione accoglie personale minore **con età inferiore ai 16 anni** , dovrà iniziare a pensare ora a mettere in atto i sistemi per verificare l'età delle persone e per raccogliere il consenso dei genitori o dei tutori per l'elaborazione dei dati personali.
Le attività più comuni dove questo si rende necessario sono : **SCUOLE, PALESTRE, ASSOCIAZIONI SPORTIVE, ATTIVITA' SOCIAL** ecc.

Infatti per la prima volta, il NUOVO GDPR introdurrà una protezione speciale per i dati personali dei minori in particolare nel contesto dei **servizi commerciali in rete come i social network**.
I minori infatti meritano una specifica protezione relativamente ai loro dati personali, in quanto **possono essere meno consapevoli dei rischi**, delle conseguenze e delle misure di salvaguardia interessate nonché dei loro diritti in relazione al trattamento dei dati personali.

In breve, se un'azienda raccoglie informazioni sui minori allora avrà bisogno del consenso di un genitore o di un tutore per elaborare i loro dati personali in modo lecito.
Questo potrebbe avere implicazioni significative se l'azienda fornisce servizi ai bambini e raccoglie i loro dati personali. Il consenso deve essere sempre verificabile e quando vengono raccolti i dati sui minori è necessario definire una specifica informativa per la privacy in un linguaggio che sia comprensibile ai minori.

9

VIOLAZIONI DEI DATI [DATA BREACHES]

Ogni Azienda deve assicurarsi di disporre di specifiche e dettagliate procedure per rilevare, segnalare e indagare su una violazione dei dati personali.
Alcune aziende sono già tenute a notificare all'ente competente il caso in cui subiscano una violazione dei dati personali. Però, il **GDPR introdurrà un obbligo di notifica di violazione su tutta la linea**.
Questo sarà una vera novità per molte imprese.
Non tutte le violazioni dovranno essere notificate al Garante Privacy: solo quelle in cui è probabile che l'individuo subisca qualche forma di danno, ad esempio un furto d'identità o una violazione della riservatezza.
L'azienda deve quindi assicurare di avere e mettere in atto le **giuste procedure** per **rilevare, segnalare e indagare su una violazione dei dati personali**. Questo potrebbe coinvolgere la valutazione dei tipi di dati e la documentazione sulla quale rientrerebbero l'obbligo di notifica in caso di violazione.

L'azienda dovrà notificare entro 72 ore (senza giustificato ritardo) i casi e le persone i cui dati sono stati oggetto di violazione.
Le imprese più grandi dovranno sviluppare politiche e procedure per la gestione delle violazioni dei dati.

SICUREZZA INFORMATICA

Con il termine sicurezza informatica si intende un assieme di mezzi e tecnologie tesi alla protezione dei **sistemi informatici** in termini di **disponibilità, confidenzialità e integrità** dei beni stessi e delle informazioni in essi contenute.
A questi tre parametri si tende attualmente ad aggiungere **l'autenticità** e la **tutela delle informazioni**, anche in virtù delle modifiche apportate dal **nuovo regolamento 679:2016**.

Nella sicurezza informatica sono coinvolti elementi tecnici, organizzativi, giuridici e umani.
Per valutare la sicurezza informatica è solitamente necessario individuare **le minacce, la vulnerabilità e i rischi associati** agli asset informatici, al fine di proteggerli da possibili attacchi sia interni che esterni, che potrebbero provocare danni diretti o indiretti in una organizzazione aziendale.

E' necessario quindi disporre di una **specifica competenza interna** relativa la **gestione informatica**, ed una **infrastruttura tecnologica adeguata** in grado di **prevenire** ogni possibile violazione, perdita, distruzione o utilizzo improprio dei dati presenti all'interno dell'azienda.

11

PRIVACY BY DESIGN & PRIVACY BY DEFAULT

Ogni Azienda dovrà iniziare a valutare le situazioni in cui sarà necessario **condurre una valutazione dell'impatto** sulla protezione dei dati in forma preventiva con strumenti di **RISK ASSESSMENT**.

Chi lo farà? Chi altro deve essere coinvolto? Il processo verrà eseguito centralmente o localmente?
È sempre stata una buona pratica adottare un approccio alla **privacy «by design»** ed effettuare una valutazione dell'impatto sulla privacy come parte dei processi aziendali e tenerlo sotto controllo attraverso **specifici Audit.**

Un approccio «by design» è sempre stato un implicito requisito dei principi di protezione dei dati. Tuttavia, con il GDPR questo diventerà un requisito legale espresso.

Si noti che non è sempre necessario eseguire un **RISK ASSESSMENT**, anche se consigliabile , ma **è richiesto in situazioni ad alto rischio**, ad esempio dove si sta sviluppando una nuova tecnologia o in cui è probabile che un'operazione di profilazione possa influire in modo significativo sugli individui. Si noti che dove un RISK ASSESSMENT indica l'elaborazione di dati ad alto rischio, verrà richiesto di consultare preventivamente il Garante per chiedere la sua opinione riguardo alla conformità dell'operazione di elaborazione al GDPR.

RESPONSABILE PROTEZIONE DEI DATI o DPO – Data Protection Officer

L'azienda dovrà designare un responsabile della protezione dei dati **(DPO) o DATA PROTECTION OFFICER** , se richiesto, o qualcuno di esperto che si assuma la responsabilità della conformità alla protezione dei dati secondo il Nuovo Regolamento, e valutare come questo ruolo si definirà all'interno della struttura e della **GOVERNANCE dell'azienda**.

Il GDPR richiederà ad alcune imprese di designare un DPO, ad esempio alle **autorità pubbliche** o alle realtà le cui attività comportano il **monitoraggio regolare e sistematico dei dati di persone interessate su ampia scala.**
L'importante è assicurarsi che qualcuno in azienda, **eventualmente un consulente esterno**, si assuma la responsabilità della protezione dei dati, qualcuno che abbia le conoscenze, il sostegno e l'autorità per farlo in modo effettivo e concreto.

Ale aziende spetta quindi di capire già adesso se verrà richiesto di designare un DPO e, in tal caso, valutare se l'attuale approccio alla protezione dei dati è adeguato ai requisiti del GDPR.

13

ATTIVITA' INTERNAZIONALI – COMPLESSO

Se l'organizzazione opera a livello internazionale, sarà necessario determinare a quale autorità di controllo della protezione dei dati fare riferimento in ogni nazione.

Il GDPR contiene disposizioni abbastanza complesse per capire quale sia l'autorità di controllo per la protezione dei dati che assume la guida per la gestione delle denunce che hanno una portata internazionale, ad esempio laddove un'operazione di processamento dei dati incide sulle persone in un certo numero di Stati membri.

Per farla semplice, **l'autorità è determinata in base a dove l'azienda ha la sua amministrazione principale** o **dove vengono prese le decisioni sull'elaborazione dei dati**. In un'azienda tradizionale questo è facile da determinare. È più difficile per società complesse e dislocate in diverse zone, dove le decisioni sulle diverse attività di elaborazione sono prese in differenti posti.
In caso di incertezza su quale sia l'autorità di controllo di riferimento per l'impresa, sarebbe utile mappare dove l'azienda prende le decisioni più significative a proposito dell'elaborazione e del trattamento dei dati.

Questo potrà aiuterà a determinare lo **'stabilimento principale'** e quindi l'autorità di riferimento.