# GDPR IN PILLOLE

**LE TAPPE**

**ENTRATA IN VIGORE**

**24 MAGGIO 2016**

**DIRETTA APPLICAZIONE**

**25 MAGGIO 2018**

**LE SANZIONI**

**VIOLAZIONI MENO GRAVI FINO A 10.000.000 € O IL 2% DEL FATTURATO**

**VIOLAZIONI GRAVI FINO A 20.000.000 € O IL 4% DEL FATTURATO**

**LICEITA':** ogni trattamento deve trovare fondamento in un'idonea base giuridica; **i fondamenti sono indicati all'art. 6 del GDPR** e sono sinteticamente: consenso, adempimento obblighi contrattuali, interessi vitali della persona interessata o di terzi, obblighi di legge cui è soggetto il titolare, interesse pubblico o esercizio di pubblici poteri, interesse legittimo prevalente del titolare o di terzi cui i dati vengono comunicati.

**RESPONSABILIZZAZIONE: Il nuovo regolamento introduce in modo forte ed inequivocabile il concetto di "responsabilizzazione" (accountability) di titolari e responsabili. Cosa vuol dire? Significa che titolari e responsabili DEVONO adottare politiche, attività e comportamenti in grado di dimostrare inequivocabilmente la concreta adozione di misure finalizzate ad assicurare l'applicazione del regolamento.**

**DATA PROTECTION BY DESIGN AND BY DEFAULT:** rappresentano la necessità di configurare il trattamento prevedendo fin dall'inizio di ogni processo le garanzie indispensabili legate al trattamento dati. In sostanza è un concetto che prevede la protezione dei dati sin dalla progettazione ed ideazione di un'attività. Ne consegue che è NECESSARIA un'analisi preventiva dimostrabile, che si traduce poi in azioni predefinite e ben organizzate (il default).

**Il DPIA:** (Data Protection Impact Assessment) è la valutazione del rischio inerente particolari trattamenti che possono impattare sulle libertà e i diritti degli interessati. Gli impatti dovranno essere analizzati attraverso un apposito processo di valutazione TARATO sulla propria realtà specifica (analisi "preconfezionate" possono non garantire un risultato reale inficiando, tra le altre cose, il concetto di "responsabilizzazione" di cui sopra).

**ABRUZZO CONSULTING SRL**
Via D. Spezioli (Theate Center)
66100 CHIETI (CH) - ITALY
Tel. +39 0871 411530
Fax +39 0871 411530
www.abruzzoconsulting.it

In collaborazione con:

Renato Gambella
Data Protection Officer
Certificato nr. DPO-0075

Renato Gambella
Delegato Provinciale

Attestato di competenza
TÜV SÜD Italia:
Integrazione con i
Sistemi Qualità

**AZIONI CHIAVE**

**RESPONSABILIZZAZIONE DELLA PROPRIETA' E/O DEL MANAGEMENT AZIENDALE**

**ANALIZZARE LE OPERAZIONI DI TRATTAMENTO IN OGNI ASPETTO**

**INDIVIDUARE E NOMINARE LA FIGURA DEL DPO SE NECESSARIO**

**EFFETTUARE UNA VALUTAZIONE DEI RISCHI**

**DEFINIRE LE MISURE DI SICUREZZA IN RELAZIONE AI RISCHI**

**RIDEFINIRE LE POLICY INERENTI IL TRATTAMENTO DATI**

**REGISTRO DEI TRATTAMENTI:** **i titolari e i responsabili** del trattamento, ad eccezione di quelli che impiegano meno di 250 dipendenti **e che non effettuano trattamenti particolari** (altrimenti vige l'obbligo anche per questi soggetti) devono tenere un registro delle operazioni di trattamento. È uno strumento **fondamentale** ed **indispensabile** per poter davvero definire delle politiche di gestione concrete e tarate sulle proprie attività, oltre che per effettuare una sana valutazione del rischio**.** Il consiglio è quello di redigerlo anche per i soggetti non formalmente obbligati, quale valido strumento per dimostrare l'adozione del principio di "responsabilizzazione" (come sarebbe altrimenti possibile avere contezza di cosa si tratta, come si tratta, e giustificare l'adozione o meno di determinati presidi di sicurezza senza un'analisi delle operazioni che si effettuano?).

**MISURE DI SICUREZZA:** le misure adottate devono **"garantire un livello di sicurezza adeguato al rischio"** del trattamento, la valutazione dell'adeguatezza è quindi da valutare caso per caso. Ne consegue che NON è possibile avere la certezza di adottare misure e presidi adeguati senza una valutazione del rischio (ovviamente tarata in equilibrio con le dimensioni e l'attività del titolare o del responsabile del trattamento. Ad esempio un laboratorio analisi mediche ha rischi legati alla tipologia di dati trattati molto diverse da un piccolo artigiano del legno arredo che lavora conto terzi).

**NOTIFICA DELLE VIOLAZIONI DI DATI PERSONALI:** **tutti i titolari** dovranno notificare all'autorità Garante le violazioni di dati personali di cui vengano a conoscenza, **entro 72 ore** e comunque "senza ingiustificato ritardo", ma **soltanto se ritengono probabile che da tale violazione derivino rischi** per i diritti e le libertà degli interessati Ne consegue, ancora una volta, che senza un'adeguata valutazione del rischio diventa impossibile effettuare un'oggettiva analisi della violazione occorsa e quindi decidere in modo consapevole "se si deve segnalare o meno". Inoltre devono essere predisposti sistemi per poter prevenire e mappare gli eventi che intervengono sui dati (accessi abusivi, perdita, cancellazione, furto etc.etc.).

**ABRUZZO CONSULTING SRL**
Via D. Spezioli (Theate Center)
66100 CHIETI (CH) - ITALY
Tel. +39 0871 411530
Fax +39 0871 411530
www.abruzzoconsulting.it

In collaborazione con:

Renato Gambella
Data Protection Officer
Certificato nr. DPO-0075

Renato Gambella
Delegato Provinciale

Attestato di competenza
TÜV SÜD Italia:
Integrazione con i
Sistemi Qualità

## AZIONI CHIAVE

**REDIGERE IL REGISTRO DEI TRATTAMENTI**

**(A PRESCINDERE DALL'OBBLIGO GIURIDICO)**

**EFFETTUARE LA PIANIFICAZIONE DEL DPIA (DATA PROTECTION IMPACT ASSESSMENT)**

**VALUTARE TUTTI I CASI DI RISCHIO ELEVATO PER I DIRITTI E LE LIBERTA' DEI SOGGETTI INTERESSATI**

**RIELABORARE I CONTRATTI CON I RESPONSABILI ESTERNI**

**PIANIFICARE PROCEDURE DI CONTROLLO DEI RESPONSABILI**

**CODICI DI CONDOTTA E SCHEMI DI CERTIFICAZIONE**: è prevista la possibilità di aderire a specifici codici di condotta o a schemi di certificazione per attestare l'adeguatezza delle misure di sicurezza adottate e la corretta applicazione del GDPR. Questi strumenti sono utili sia per adottare un adeguato sistema di gestione, sia in caso di controllo da parte delle autorità potendo in determinati casi essere addirittura certificabili (processo in corso di definizione).

**IL DPO (DATA PROTECTION OFFICER) O RPD (RESPONSABILE DELLA PROTEZIONE DEI DATI)**: la sua designazione da parte del **Titolare del trattamento e dei Responsabili,** è obbligatoria in determinati casi, mentre è facoltativa per gli altri soggetti. La nomina sarà obbligatoria nei seguenti casi: **a)** il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali; (sintetizzando la PA) **b)** quando le attività principali del **Titolare del trattamento o del Responsabile** del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala (alcuni esempi: istituti di vigilanza privata, telecomunicazioni, chi effettua profilazione marketing….). **c)** quando le attività principali del **Titolare del trattamento o del Responsabile** del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9 (dati particolari | sensibili stato di salute geolocalizzazione etc, etc.) o di dati relativi a condanne penali e a reati di cui all'articolo 10. (alcuni esempi ospedali cliniche, laboratori analisi mediche, chi effettua geolocalizzazione…).

**FORMAZIONE E ISTRUZIONE:** è essenziale che le persone autorizzate a trattare i dati e tutti i soggetti coinvolti siano formati ed istruiti con costanza.

**TRASFERIMENTI INTERNAZIONALI DI DATI:** saranno da adottare maggiori garanzie per il trasferimento dati all'estero.

**ABRUZZO CONSULTING SRL**
Via D. Spezioli (Theate Center)
66100 CHIETI (CH) - ITALY
Tel. +39 0871 411530
Fax +39 0871 411530
www.abruzzoconsulting.it

In collaborazione con:

Renato Gambella
Data Protection Officer
Certificato nr. DPO-0075

Renato Gambella
Delegato Provinciale

Attestato di competenza
TÜV SÜD Italia:
Integrazione con i
Sistemi Qualità

**AZIONI CHIAVE**

**FORMARE COSTANTEMENTE IL PERSONALE**

**REDIGERE LE NUOVE INFORMATIVE**

**VERIFICARE CON COSTANZA CHE LE PROCEDURE IN ESSERE PERMETTANO SEMPRE L'ESERCIZIO DEI DIRITTI DEI SOGGETTI INTERESSATI**

**AUDIT CON CADENZA PERIODICA E STABILITA**

**E SOPRATTUTTO NON LASCIARE NULLA AL CASO**

**SOGGETTI:** i dati trattabili saranno trattabili solo tramite persone specificamente autorizzate (gli incaricati odierni) o responsabili espressamente nominati.

**INFORMATIVE:** dovranno contenere **nuovi e più dettagliati riferimenti** rispetto al Codice Privacy. Ad esempio saranno da specificare i dati di contatto del DPO, la base giuridica del trattamento, qual è il suo interesse legittimo, se si trasferiscono i dati personali in Paesi terzi, attraverso quali strumenti, il periodo di conservazione dei dati o i criteri seguiti per stabilire tale periodo di conservazione, il diritto di presentare un reclamo all'autorità di controllo, se il trattamento comporta processi decisionali automatizzati (anche la profilazione), la logica di tali processi decisionali e le conseguenze previste per l'interessato. Ancora una volta ci si chiede senza una vera analisi delle operazioni di trattamento, come è possibile predisporre le informative indicando tutti gli elementi necessari?

**DIRITTO "ALL'OBLIO":** è un diritto alla cancellazione dei propri dati personali in forma rafforzata. Si prevede, infatti, l'obbligo per i titolari (se hanno "reso pubblici" i dati personali dell'interessato di informare della richiesta di cancellazione gli altri titolari che trattano i dati personali oggetto della richiesta di "oblio". Ancora una volta si richiama un concetto di controllo del processo di trattamento in capo a titolare.

**DIRITTO ALLA PORTABILITA':** è il diritto di ricevere i dati personali forniti a un titolare, in un formato strutturato, di uso comune e leggibile da dispositivo automatico, e di trasmetterli ad un altro titolare del trattamento senza impedimenti. Non si applica ai trattamenti non automatizzati e sono portabili solo i dati trattati con il consenso dell'interessato o sulla base di un contratto stipulato con l'interessato.

*IL PRESENTE DOCUMENTO CONTIENE ALCUNI SPUNTI DI RIFLESSIONE LEGATI AI NUOVI ISTITUTI DEL GDPR NON È DA INTENDERSI COME ESAUSTIVO, COMPLETO O COME UN PARERE PROFESSIONALE, MA ESCLUSIVAMENTE UNO SPUNTO DI RAGIONAMENTO. I RIFERIMENTI UFFICIALI AD OBBLIGHI, ISTITUTI E INDICAZIONI UFFICIALI DA TENERE PRESENTI SONO QUELLI NORMATIVI, O EMANATI DALLE COMPETENTI AUTORITÀ.*

**ABRUZZO CONSULTING SRL**
Via D. Spezioli (Theate Center)
66100 CHIETI (CH) - ITALY
Tel. +39 0871 411530
Fax +39 0871 411530
www.abruzzoconsulting.it

In collaborazione con:

Renato Gambella
Data Protection Officer
Certificato nr. DPO-0075

Renato Gambella
Delegato Provinciale

Attestato di competenza
TÜV SÜD Italia:
Integrazione con i
Sistemi Qualità