Vediamo di capirci qualcosa…

Pubblicazione nella Gazzetta Ufficiale dell'Unione Europea n.19/2016: 4 Maggio 2016.
Entrata in vigore: 25 maggio 2016. Tutti i soggetti interessati hanno due anni di tempo per adeguare le operazioni di trattamento alle nuove Norme prima dell'applicabilità in tutti i Paesi della UE: 25 maggio 2018.

Il Regolamento sarà immediatamente applicabile senza necessità di recepimento.
Per quanto riguarda l'Italia, il Regolamento sostituisce non integralmente il Codice Privacy in vigore dal 1°Gennaio 2004.
Il Garante privacy ha in corso una ricognizione normativa per verificare quali parti del Codice privacy e quali provvedimenti generali del Garante sopravvivranno alla riforma.

La prima cosa da fissare bene è quindi che il regolamento non andrà a sostituire in toto il codice della privacy perché ci sono delle parti che NON possono essere abrogate.
Trattamento illecito dei dati regolato dall'art.167 Sanzioni penali.
Ricordiamoci che l'Unione Europea non ha competenza sulla legislazione in materia penale di uno stato membro.

Quindi chi è tenuto a osservare il GDPR?

Il Regolamento si applica:

1) al trattamento di dati personali effettuato da un titolare stabilito nella UE

2) al trattamento di dati personali effettuato da titolari non stabiliti nell'Unione Europea se il trattamento ha ad oggetto dati personali di interessati che si trovano nella UE e riguarda l'offerta di beni o servizi (anche non a pagamento) ai suddetti interessati

3) il monitoraggio del loro comportamento nel territorio dell'Unione Europea. Notate che a differenza del d.lgs. 196/03 adesso si parla di dati personali senza distinzioni. I dati personali sono tutti: compresi quelli sanitari o giudiziari ai quali servono delle accortezze aggiuntive.

E' più semplice domandarsi chi non lo deve osservare!

Sono esclusi i casi di **trattamento di dati puramente personale da parte di persone fisiche**, come la gestione della corrispondenza privata, o l'uso personale dei servizi di social networking.
Le attività miste (ad esempio, l'invio di corrispondenza che comprende sia contenuti personali, sia contenuti connessi alle imprese) non sono invece esenti, e devono pertanto seguire le indicazioni del Regolamento 679/2016. Inoltre per l'applicazione della normativa non incide né il settore né la grandezza nell'organizzazione: gli stessi adempimenti si applicano alle piccole imprese e grandi multinazionali, con pochissime eccezioni.

Ricorrendo tali presupposti qualsiasi ente/azienda mondiale, anche non avente sede nella UE sarà soggetta al Regolamento.

Gestionale Toscana Srl
Per informazione chiama il 0574870700 oppure scrivi a info@gestionale.toscana.it

esempi: un sito web australiano raggiungibile anche dal territorio UE che cede prodotti o servizi (anche non pagamento) e presenta offerte in una lingua del territorio UE o fa riferimento all'Euro **è tenuto ad osservare le norme del codice europeo**.
i grandi colossi tipo **Google,** che hanno i loro server in territori più confacenti alle loro politiche aziendali, non possono più scrivere che adempiono alla normativa nel paese in cui tali server sono collocati. ***Basta che anche solo un cittadino della UE utilizzi i suoi servizi…***

Appurato che tutti dobbiamo osservare il codice europeo sulla privacy…

Che dobbiamo fare nella pratica?

La filosofia del GDPR ruota attorno ai processi di DOCUMENTABILITA'
Si introduce un concetto nuovo e rivoluzionario rispetto al vecchio codice: tutto quello che sarà la presa di coscienza dell'azienda nei confronti del GDPR dovrà essere documentata analiticamente.

Esempi:
- Non nomino un DPO perché la mia azienda non ne ha bisogno: **si dovrà preparare una documentazione che spieghi analiticamente i perché e i motivi che hanno portato a questa decisione.**

- Ho predisposto queste misure minime a protezione dei dati: **si dovrà predisporre una documentazione del perché si ritiene che per tipologia di dato e fatturato aziendale queste misure minime sono considerate ottimali.**

- Ritengo che la mia azienda non debba tenere un PIA: si **dovrà predisporre un documento che spieghi le motivazioni che hanno portato a questa scelta.**

- Non ho un registro dei trattamenti: si **dovrà predisporre una documentazione che spieghi che la tipologia di dati trattati non necessita di tale adempimento.**

- Non ho nominato gli incaricati: **si dovrà garantire e dimostrare che tutti gli incaricati sono stati formati adeguatamente e sono stati edotti sui compiti e comportamenti.**

Tutto ciò che si decide di osservare o di non osservare a seconda della tipologia dei dati trattati e dell'azienda si deve comunque documentare.
L'onere della prova spetta sempre al Titolare (accountability).

Quali sono i passi necessari per adempiere al GDPR?

Nomina del titolare del trattamento dati.
Il Titolare del Trattamento, ora chiamato **Data Controller o Responsabile del trattamento**, è dotato di un potere decisionale in ordine alle tecniche da adottare e alle misure organizzative, al fine di garantire la conformità al Regolamento delle operazioni di trattamento dei dati. E' la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali.
OBBLIGATORIO? SI!

Gestionale Toscana Srl
Per informazione chiama il 0574870700 oppure scrivi a info@gestionale.toscana.it

Nomina del Responsabile del Trattamento o Data Processor
Figura facoltativa nel Codice della privacy, **la sua nomina diventa obbligatoria e va documentata con un *atto*** stipulato in forma scritta o anche in formato elettronico che regoli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento.
OBBLIGATORIO? SI!
Possono essere nominati anche più responsabili, responsabili esterni (commercialista, ecc) o sub responsabili.

Il Responsabile del Trattamento o Data Processor
Può nominare a sua volta, ma previa autorizzazione del Data Controller altri sub Data Processor.
I Data Processor possono essere anche più di uno. Questo per chiarire che i casi vanno visti volta per volta e individuata la linea della completezza ma anche della semplicità

Incaricati al Trattamento (Data Handler)
Anche se nella traduzione italiana del GDPR non compare mai il termine incaricato del trattamento e pur non essendo espressamente prevista dal GDPR questa figura come figura giuridicamente autonoma, il Garante italiano, nella guida all'applicazione del regolamento, giustifica e considera non incompatibile con il regolamento la figura dell'incaricato.

Infatti, nel documento del Garante "**Guida all'applicazione del Regolamento europeo in materia di protezione dei dati personali**", voce dell'indice **TITOLARE, RESPONSABILE, INCARICATO DEL TRATTAMENTO**, sezione **Cosa non cambia?** si trova scritto: *...Pur non prevedendo espressamente la **figura dell' "incaricato" del trattamento** (ex art. 30 Codice), il regolamento **non ne esclude** la presenza in quanto fa riferimento a "persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile".*
Il garante consiglia di mantenere le figure e le nomine

La nuova figura del D.P.O.
Del tutto nuova è la figura del **Responsabile della protezione dei dati** (Data Protection Officer o DPO) introdotta dall'art. 37 del Regolamento. L'obbligo di designazione del DPO (da parte del titolare o del responsabile del trattamento) non è generale ma si applica solo se:

1) il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali;
2) le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che richiedono **il monitoraggio regolare e sistematico degli interessati su larga scala;**
3) le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di dati personali sensibili, sanitari, sulla vita o sull'orientamento sessuale, genetici, biometrici, o di dati relativi a condanne penali e a reati.

Ma che significa trattamento sistematico su larga scala?

Pensate ad un azienda che deve raccogliere dati per gestire le buste paga:
Il trattamento non è su larga scala perché localizzato ai soli dipendenti e anche se sistematico non può ritenersi campo di applicazione per l'obbligatorietà del DPO.
Ma il commercialista, che riceve i flussi per l'elaborazione delle buste paga sistematicamente e da centinaia di clienti, non è da considerarsi su larga scala?
Per il concetto dell'**accountability** si deve produrre una documentazione che spieghi le ragioni della non nomina e come si intende procedere diversamente (art. 37).
Per questo molti Garanti europei caldeggiano la nomina del DPO anche nelle aziende medio piccole.

Ma chi è il DPO?
Il **Data Protection Officer** è una figura del tutto autonoma e **non** deve ricevere, dal titolare o dal responsabile, alcuna istruzione per quanto riguarda l'esecuzione dei compiti affidati.
Inoltre **non** è soggetto a potere disciplinare o sanzionatorio per l'adempimento dei propri compiti (diversamente dal responsabile del trattamento che, al contrario, deve ricevere istruzioni scritte ed è soggetto al controllo e all'autorità del Titolare del Trattamento, ivi compresi i profili sanzionatori).
Il DPO è, in un certo senso, l'amministratore delegato della privacy, il front office con il mondo esterno per quanto riguarda la privacy. Proprio per questo, deve operare autonomamente senza influenze o conflittualità in azienda ed essere incaricato con un contratto o incarico formale.

D.P.O. ESTERNO o INTERNO?
Se il D.P.O. deve essere autonomo, non prendere ordini da nessuno e non avere conflittualità aziendale…

Quali sono allora i compiti del DPO?
- Adempiere a tutte le richieste di correzione, portabilità, modifica, cancellazione o diritto all'oblio dei dati.

- Redigere e inviare tutte le richieste e le comunicazioni al Garante (data breach, interpelli, ecc).

- Redigere con cadenza annuale una relazione di attività sulla privacy aziendale.

- Progettare assieme ai più alti vertici aziendali tutte le infrastrutture necessarie per i nuovi trattamenti (privacy by designe privacy by default).

- Vigilare sempre affinché le misure di sicurezza siano sempre attuali e proporzionate ai dati trattati.

- Verificare che tutti gli adempimenti normativi siano posti in essere.

In pratica il DPO fa da pungolo verso il titolare e da interfaccia verso le autorità.

Gestionale Toscana Srl
Per informazione chiama il 0574870700 oppure scrivi a info@gestionale.toscana.it

Registro dei trattamenti
Anche qui il Codice Europeo fa riferimento ad aziende oltre i 250 dipendenti, salvo poi allargare le maglie a chi tratta dati personali su larga scala e introducendo dei "considerando" che suggeriscono di far dotare tutte le aziende di un registro dei trattamenti come **best practice**.

Ma cos'è il Registro dei trattamenti?
Un registro documentale o elettronico in cui si riuniscono tutti i trattamenti e se ne descrive singolarmente: le finalità, il tipo di trattamento, le banche dati associate ad esso, il tipo di dati raccolti, i data Handler che sono incaricati, se vi sono trattamenti di minori, se i dati vengono esportati anche in extra UE ecc.…

E il PIA?
Acronimo di **Privacy Impact Assessment**, va di pari passo al registro dei trattamenti ed è una valutazione di impatto della privacy sui trattamenti, ovvero un altro registro documentale ragionato ove si specifichi, trattamento per trattamento, tutte le misure di sicurezza che sono state approntate per far fronte ai rischi di ogni banca dati di ogni trattamento, in che modo vengono realizzati i piani di disaster recovery e cosa si intende fare per aumentare la compliance alla privacy in futuro.

E il Data Breach?
Altro registro documentale dove vengono registrate tutte le intrusioni o perdite di dati che accadono nel quotidiano. Senza scomodare intrusioni di hacker peraltro poco diffuse nelle piccole e medie aziende soffermiamoci sulla più banale delle perdite di dati.

ESEMPIO:
Lo smarrimento di una penna USB. In questo caso inseriremo una serie di informazioni che vanno dall'origine dei dati che abbiamo perduto, la loro importanza, la data della perdita, tutte le operazioni che abbiamo svolto affinché questa perdita sia stata annullata e le operazioni che sono state fatte per mitigare o annullare il danno. In base alla gravità della perdita verrà generato un modulo interattivo per la comunicazione al Garante e dove il caso lo prevede anche comunicazione agli interessati.

E l'informativa?
Il Regolamento sancisce a carico dei titolari del trattamento obblighi di informativa rafforzati rispetto a quanto avviene ora con l'art. 13 del Codice della privacy, prevedendo numerose informazioni aggiuntive da fornire agli interessati in forma **concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro.**
L'Informativa va resa per iscritto o con altri mezzi, anche elettronici. Se richiesto dall'interessato, le informazioni possono essere fornite oralmente, purché sia comprovata con altri mezzi l'identità dell'interessato.
Rispetto agli elementi obbligatori da indicare nell'informativa privacy che già siamo abituati a conoscere in applicazione dell'art. 13 del Codice della privacy italiano (e che ovviamente non vengono meno), i titolari del trattamento dovranno inoltre inserire obbligatoriamente le informazioni aggiuntive sul trattamento (e ci si domanda come possa essere "concisa").

Quali sono le informazioni aggiuntive:
- I dati di contatto della nuova figura del **Data Protection Officer** (Responsabile della protezione dei dati personali) ove prevista;

- La base giuridica del trattamento a corredo dell'illustrazione delle finalità del trattamento (contratto di lavoro, di fornitura, ecc.);

- Qualora il trattamento si basi sulla necessità di perseguire un legittimo interesse (condizione del codice alternativa al consenso) del Titolare del Trattamento o di terzi, la specificazione di quali siano i legittimi interessi perseguiti dal Titolare del Trattamento o da terzi;

- L'ambito del trasferimento all'estero (ovviamente extra UE) o a un'organizzazione internazionale dei dati personali;

- Il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;

- La specifica esistenza del diritto alla portabilità dei dati;

- L'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità basata sul consenso prestato prima della revoca;

- Il diritto di proporre reclamo al Garante privacy

- La eventuale esistenza di un processo decisionale automatizzato, compresa la profilazione e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza
e le conseguenze previste di tale trattamento per l'interessato;

- Le categorie di dati personali oggetto del trattamento (tale informazione è obbligatoria) la fonte da cui hanno origine i dati personali.

Le informazioni da rendere agli interessati possono essere fornite anche in combinazione con icone standardizzate per dare, in modo facilmente visibile, intelligibile e chiaramente leggibile, un quadro d'insieme del trattamento previsto. Se presentate elettronicamente, le icone devono essere leggibili da qualsiasi dispositivo.
Quindi attenzione all'inidonea informativa. E' sparito il consenso verbale perché, introducendo il concetto di accountability, si va verso la documentabilità, ovvero "*dimostrami che il consenso lo hai ottenuto*".

E il consenso?
Il Regolamento fonda sul «consenso dell'interessato» la principale precondizione (salve le deroghe) di liceità del trattamento. Il titolare del trattamento deve poter dimostrare che l'interessato ha prestato il consenso al trattamento dei propri dati personali. La richiesta di consenso deve essere presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro, pena l'invalidità del consenso prestato.

Gestionale Toscana Srl
Per informazione chiama il 0574870700 oppure scrivi a info@gestionale.toscana.it

L'interessato ha poi il diritto di revocare il proprio consenso (e tale informazione è uno dei nuovi elementi obbligatori dell'informativa privacy) in qualsiasi momento, **con modalità di esecuzione della revoca del consenso, facili come la sua prestazione originaria**.
Pensate ai siti internet che acquisiscono dati come e-commerce, prenotazioni hotel, ecc.: non devono solo dimostrare di avere i consensi differenziati per operazione (tanti consensi quanti sono le modalità di trattamento) ma dare la possibilità all'interessato in modo analogo di poter accedere in un area privata per restringere, allargare o negare il consenso.
E il tutto in modo dimostrabile (**accountability**).

Portabilità del dato?
Il nuovo **diritto alla portabilità dei dati personali** consiste nel diritto dell'interessato di trasmettere tali dati ad un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti.
Esempio:
il gestore di posta elettronica che mi deve garantire la portabilità dei messaggi e dei contatti del mio dominio. Tale diritto è esercitabile quando il trattamento è effettuato con mezzi automatizzati. In questo specifico caso l'interessato, fermo restando comunque il suo diritto alla cancellazione dei dati, ha il diritto di ottenere la trasmissione diretta dei dati personali da un titolare del trattamento all'altro, "se tecnicamente fattibile".

E il diritto all'oblio?
Il Regolamento codifica compiutamente il diritto ad essere dimenticati (quale specifico esercizio del diritto alla cancellazione dei dati personali). L'interessato esercita questo diritto chiedendo al titolare del trattamento che siano cancellati e non più sottoposti a trattamento i propri dati personali.
Tuttavia, rimane lecita l'ulteriore conservazione dei dati personali in caso di diritto alla libertà di espressione e di informazione, per adempiere un obbligo legale o un compito di interesse pubblico, per motivi di interesse pubblico nel settore della sanità pubblica, a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, per accertare, esercitare o difendere un diritto in sede giudiziaria. Ci sono moduli direttamente sui motori di ricerca (Google) oppure prestampati per rivolgersi al Garante in caso di diniego del motore di ricerca. Per esperienza il consiglio che vi posso dare è un'istanza di esercitazione del diritto all'oblio direttamente agli editori.

Privacy by Design?
L'articolo 25 del Regolamento ("Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita") impone vincoli che impattano sulle stesse fasi produttive e di operatività di apparati e/o servizi che implicano il trattamento di dati personali.
Con riferimento a questo principio, il Regolamento prescrive che il titolare del trattamento, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse, debba applicare misure tecniche adeguate (es: anonimizzazione) volte ad attuare in modo efficace i principi di protezione dei dati e a integrare nel trattamento le necessarie garanzie per tutelare i diritti degli interessati.
Tale adempimento va effettuato sia al momento di determinare i mezzi del trattamento (es: progettazione di device) sia all'atto del trattamento stesso.

Privacy by Default?

Con riferimento al principio cosiddetto della privacy by default, il Regolamento stabilisce che il titolare del trattamento deve mettere in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita (cioè by default), solo i dati personali necessari per ogni specifica finalità del trattamento.

Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità.

In particolare, dette misure devono garantire che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche.