STUDI PERUZZI
Commercialisti Associati
Via Dante, 34 - 40125 Bologna
tel +39 051 331220 - fax +39 051 333913
P.Iva - Cod. Fisc. 03453211207
peruzzi@studioperuzzi.info - www.peruzzicommercialisti.it

Speciale: Privacy

OGGETTO: Privacy

Gentile Cliente,

con la stesura del presente documento informativo, intendiamo informarla che con Provvedimento del Direttore dell'Agenzia delle Entrate n. 29190/2018, pubblicato ieri 5 febbraio sono state modificate le specifiche tecniche delle informazioni da trasmettere e delle modalità per la comunicazione dei dati delle fatture emesse e ricevute.

Privacy – dal 25 maggio 2018

GDPR:
Il nuovo Regolamento (UE) sulla protezione dei dati, che entrerà in vigore dal 25 maggio 2018, apre le porte ad un profondo cambiamento culturale perché richiede un nuovo approccio all'uso che si fa dei dati personali, ossia l'approccio basato sull'analisi del rischio e sulle misure da adottare in maniera preventiva da parte di responsabili e titolari, vale a dire sull'adozione di comportamenti proattivi e tali da dimostrare la concreta attuazione di misure finalizzate ad assicurare l'applicazione del regolamento.

Cos'è il GDPR?
GDPR sta per General Data Protection Regulation.
Il nuovo Regolamento (Ue) 2016/679 relativo alla libera circolazione e alla protezione del trattamento dei dati personali delle persone fisiche (che abroga la direttiva 95/46/CE - regolamento generale sulla protezione dei dati). Pubblicato nella Gazzetta Ufficiale europea il 4 maggio 2016 è entrato in vigore il 24 maggio 2016, ma la sua piena attuazione è stata prevista per il 25 maggio 2018.

Non dovrò più attenermi in nessun punto al Codice della privacy (il D.Lgs. 196 del 2003)?
Ebbene sì! Non bisognerà più far riferimento al vecchio Codice della privacy.
In data 21 marzo, infatti, il Consiglio dei Ministri ha approvato, in via preliminare, un Decreto Legislativo che manda in soffitta l'attuale codice della riservatezza (il D.Lgs. 196 del 2003) lasciando campo libero al Regolamento (Ue) 679/2016, che diventerà operativo a partire dal 25 maggio.

Quali sono gli obiettivi del nuovo Regolamento? Perché è stato adottato?
I pilastri del nuovo cambiamento sono da un lato la protezione dei dati personali e dall'altro la libera circolazione dei medesimi all'interno dei confini dell'Unione Europea.

STUDI PERUZZI
Commercialisti Associati
Via Dante, 34 - 40125 Bologna
tel +39 051 331220 - fax +39 051 333913
P.Iva - Cod. Fisc. 03453211207
peruzzi@studioperuzzi.info - www.peruzzicommercialisti.it

I vantaggi vanno quindi dall'avere un'unica autorità per la protezione dei dati (anche per attività svolte all'estero) e norme univoche che troveranno applicazione anche per i soggetti extra-europei che operano nell'Unione europea, innalzando e uniformando i gradi di tutela di protezione di tali dati entro i confini comunitari, considerando che le imprese nei loro percorsi di crescita e di espansione sono volte sempre più verso l'internalizzazione e che i big data, il digital single market e la fabbrica 4.0 si stanno sempre più affermando come un importante investimento per le imprese.

Chi dovrà applicare il nuovo Regolamento?
Entro il 25 maggio tutti dovranno applicare le nuove norme, in tutto il territorio dell'Ue, dai grossi colossi quali google alle banche, alle farmacie, le PA, le Pmi e le organizzazioni no profit, ovvero tutti coloro i quali, per lo svolgimento delle proprie mansioni, maneggiano dati degli utenti, anche quelli più basilari.
Il Regolamento 679/2016 prevede, alla lettera c) del primo comma dell'articolo 2 "Ambito di applicazione materiale", l'esclusione dell'applicazione esclusivamente ai trattamenti di dati personali:
(...) effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico".

Cosa cambia per professionisti e imprese?
Con l'avvento del nuovo Regolamento europeo in materia di protezione dei dati le imprese e i liberi professionisti dovranno metter mano al tema privacy con uno sguardo non solo al quadro giuridico nazionale ma in un'ottica comunitaria, il fine ultimo infatti è quello di applicare le medesime norme in tutto il continente, per garantire la certezza giuridica per le imprese e lo stesso livello di protezione dei dati in tutta l'UE.

Quali sono le novità?
Sostanzialmente cambia l'approccio a tutto il sistema. Precedentemente l'obiettivo principale da parte delle aziende era quello di svolgere una serie di adempimenti a cui le stesse dovevano provvedere, ora si pone l'attenzione sul principio di sensibilizzazione delle imprese. L'approccio sarà basato infatti sul rischio e sulle misure di accountability (responsabilizzazione) di titolari e responsabili, ossia, sull'adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del regolamento.

Quali sono le sanzioni?
Ignorare il nuovo regolamento o commettere errori nella sua applicazione comporterà pesanti conseguenze, alcune violazioni del regolamento, infatti, sono punibili con sanzioni pecuniarie fino al 4% del fatturato totale annuo o fino ad un massimo di 20 milioni di euro. Sarà il titolare del trattamento a dover dimostrare, in caso di controversie, di aver adottato tutte le precauzioni previste per ridurre al minimo i rischi.
Mentre le sanzioni amministrative vengono inasprite nella bozza del Decreto Legislativo decade interamente la parte riferita agli illeciti penali.

Cosa dovranno fare, in sintesi, le aziende o i professionisti?
Secondo il nuovo regolamento europeo ogni impresa e libero professionista dovrà:

- effettuare un controllo interno;
- verificare il proprio livello di esposizione ai rischi;
- svolgere una serie di interventi per mitigare i rischi;
- innalzare il livello di tutela;
- documentare le scelte prese secondo un processo di accountability che caratterizza l'intero regolamento.

Quali sono le priorità?
Le prime linee guida arrivate dal Garante, avevano suggerito in via obbligatoria per le Pubbliche Amministrazioni e in maniera facoltativa in alcuni casi per imprese e studi professionali, tre priorità:

STUDI PERUZZI
Commercialisti Associati
Via Dante, 34 - 40125 Bologna
tel +39 051 331220 - fax +39 051 333913
P.Iva - Cod. Fisc. 03453211207
peruzzi@studioperuzzi.info - www.peruzzicommercialisti.it

- la designazione in tempi stretti del Responsabile della protezione dei dati (oDPO–Data Protection Officer);
- l'istituzione del Registro delle attività del trattamento, dove sono descritti i trattamenti effettuati e le procedure di sicurezza adottate;
- la definizione di tutti gli adempimenti da adottare per ogni evento che potrebbe accadere in azienda dalla notifica delle violazioni dei dati personali, i cosiddetti Data Breach, alla valutazione di impatto, fino all'eventuale consultazione preventiva con il Garante ecc...

Tutte le persone "attive" del processo dovranno conoscere le varie azioni da adottare e sapere come comportarsi in tutti gli eventi che potrebbero imbattersi all'interno di un'azienda o in uno studio professionale.
Va effettuata, in sintesi, la formazione del personale.

Quali gli step necessari per adeguarsi?
Sarà di fondamentale importanza la Compliance alla nuova normativa.
Ma sintetizziamo di seguito gli step da seguire per adeguarsi ed essere conformi:

1. L'Individuazione dei ruoli e delle responsabilità attraverso la designazione in tempi stretti del Responsabile della protezione dei dati (o DPO–Data Protection Officer) che in alcuni casi è obbligatoria e l'individuazione, sensibilizzazione e formazione di tutte le persone "attive" del processo - Individuare anche le singole responsabilità;
2. L'istituzione del Registro delle attività del trattamento, dove sono descritti i trattamenti effettuati e le procedure di sicurezza adottate;
3. Analizzare e fissare gli adempimenti previsti nel caso ad esempio di un data breach, ossia la notifica delle violazioni dei dati personali, (perdita, violazione ecc. di dati sensibili, protetti o riservati) o la valutazione d'impatto sulla protezione dei dati personali da effettuare i caso dal trattamento dei dati ne derivi un rischio elevato (consente di valutare gli aspetti relativi alla protezione dei dati, prima che questi vengano trattati);
4. Definizione delle politiche di sicurezza e valutazione dei rischi (determinazione del valore quantitativo o qualitativo dei rischi connessi ad una situazione concreta o minaccia conosciuta);
5. Implementazione dei processi per l'esercizio dei diritti dell'interessato (al fine di assicurarsi di aver adottato tutte le procedure idonee alla tutela dei diritti dell'interessato);
6. Stesura/modifica della documentazione (Tutta la documentazione deve essere necessariamente sempre aggiornata e completa);
7. Adottare tutte le misure necessarie per la cyber security (crittografia, pseudonimizzazione dati, backup dati, sicurezza password ecc.).

Ci sarà una moratoria?
Nessuna moratoria in vista, nessun periodo di grazia dunque in relazione alle sanzioni e alla diretta applicazione del Regolamento, anche se richiesto a gran voce da Confindustria e in generale da tutti gli operanti nel settore, sul modello - ad esempio - di quanto già fatto in Francia.
È direttamente il Garante con un comunicato pubblicato sul suo sito istituzionale a specificarlo, a seguito di informazioni non corrette circolanti sul web che lasciavano intendere a un differimento di sei mesi.
Il Regolamento è entrato in vigore il 24 maggio 2016 e aveva lasciato per l'appunto ben due anni dalla sua pubblicazione in G.U. a tutti gli Stati membri e quindi a enti pubblici, imprese ecc. per l'effettivo adeguamento e applicazione.

Lo studio rimane a disposizione per ulteriori chiarimenti.

Distinti saluti

Studio Peruzzi Commercialisti Associati