



FUMUS BONI IURIS Il Blog di Luigi De Valeri

[Home](#) [Profilo](#) [Pubblicazioni](#) [Contatti](#) [Archivio](#)

Postilla » Diritto » Il Blog di Luigi De Valeri » Diritto civile » GDPR is coming to town. Novità sulla privacy per imprese e professionisti

19 febbraio 2018

GDPR is coming to town. Novità sulla privacy per imprese e professionisti

[Tweet](#) [Mi piace 2](#) [Share](#)

La tua impresa, associazione, fondazione, clinica privata, studio professionale che deve trattare in sicurezza i dati personali di clienti, pazienti, fornitori e dipendenti si è effettivamente adeguata al nuovo Regolamento UE 2016/679 tra qualche mese in vigore in tutti gli Stati dell'Unione europea ?

Il **Regolamento (UE) 2016/679** del Parlamento europeo e del Consiglio, varato il 27 aprile 2016, prevede che ogni soggetto giuridico, tranne le persone fisiche che trattino dati per scopi esclusivamente personali ed alcune autorità pubbliche specificamente indicate, che debba trattare i dati personali di terzi, semplicemente identificativi oppure giudiziari o sensibili come quelli inerenti la salute, assuma, **entro il 25 maggio 2018, idonee misure organizzative e di sicurezza idonee a limitare i rischi derivanti dal trattamento medesimo adeguandosi alle nuove disposizioni del legislatore europeo.**

Pertanto meno di cento giorni ci separano da una svolta epocale in tema di **Data Protection** che avrà un evidente impatto in tutti gli stati europei in cui il regolamento sarà direttamente applicabile.

Il **General Data Protection Regulation (GDPR)** sostituisce in buona parte il nostro Codice Privacy **D. Lgs. 196/2003** ma soprattutto abroga la Direttiva 95/46/CE (Regolamento sulla protezione dei dati generali) ormai divenuta obsoleta quanto a contenuti visti gli evidenti sviluppi tecnologici intervenuti dal 1995.

Va subito detto a scanso di equivoci come il solo aggiornamento delle informative, seppur richiesto, non è sufficiente per mettersi in regola e chi si limiterà a questa minima iniziativa sarà esposto al rischio di sanzioni in caso di controlli scaturiti da contestazioni degli interessati come più volte verificatosi negli ultimi anni.

Ecco in sintesi i principi e i diritti di cui i titolari, persone fisiche o giuridiche, i responsabili della protezione dei dati personali e gli incaricati dovranno tener conto:

– il **principio di accountability** per cui è responsabilità dei titolari dei dati di clienti, dipendenti, fornitori, ecc. conformarsi alle nuove prescrizioni e dimostrare in caso di controlli di aver adottato informative chiare, misure

a.s.n. abilitazione scientifica nazionale, agente commercio, **agenzia**, art. 33 Costituzione, art. 2087 codice civile, art. 2229 codice civile, assemblea, banca, **Cassazione**, cassazione lavoro, commercio, commissione tributaria, contratto, D.Lgs. 81/08, **datore**, decreto sviluppo, **fisco**, geometri, idoneità, immobili, imprese, INAIL, **infortunio**, IRAP, jobs act, **lavoratore**, lavoro, legge 220/2012, mobbing, nomina, nullità, professionisti, **provvigione**, Rent to Buy, **ricorso**, riforma 2013, risarcimento, risarcimento danni, **sentenza**, **sicurezza lavoro**, società a

di sicurezza adeguate per proteggere i dati e aver effettuato la formazione di cui si dirà;

– the “**Data Protection Impact Assessment**” (DPIA) ovvero l’obbligo di “valutazione dell’impatto sulla protezione dei dati” in caso di rischi elevati nel trattamento, ad es. la profilazione, i dati biometrici e quelli riferiti ai minori;

– il titolare del trattamento deve pretendere dai fornitori l’uso di software conformi alle prescrizioni del Regolamento UE;

– the “**right to be forgotten**” il diritto all’oblio e “**the right to data portability**” il diritto alla portabilità dei dati a favore degli interessati;

– l’obbligo di comunicare entro settantadue ore agli interessati e al Garante le violazioni alla sicurezza che comportano l’accesso e la divulgazione dei dati personali non autorizzata, la perdita, ecc. (**data breaches notification**);

– il principio di “**privacy by design**” ovvero la necessità di tutelare il dato personale sin dalla progettazione dei sistemi informatici che ne prevedono l’utilizzo e il principio di “**privacy by default**” ovvero la tutela i dati personali come impostazione predefinita dell’organizzazione aziendale;

– l’obbligo di **trattare i dati personali c.d. “sensibili” in particolar modo quelli concernenti la salute in maniera totalmente sicura, utilizzando tecniche di cifrature dei dati e/o dei databases;**

– il **registro del trattamento dati**, in realtà saranno due considerando anche quello del responsabile della protezione dei dati, obbligo richiesto alle imprese con almeno duecentocinquanta dipendenti;

– la nomina di un **Data Protection Officer (D.P.O.)** che, ex art. 37 GDPR, è obbligatoria se le attività principali del titolare consistono in trattamenti che richiedono il monitoraggio regolare e sistematico di interessati su larga scala o riguardano categorie particolari di dati o di dati personali relativi a condanne penali e reati chi deve dovrà svolgere il trattamento dei dati su larga scala.

In vista della prossima scadenza le imprese e tutti coloro che trattano i dati personali, associazioni e fondazioni ma anche le PMI e le ditte individuali del microcosmo commerciale italiano, i medici e altri professionisti sono chiamati ad adeguarsi alle prescrizioni del Regolamento e questo preferibilmente affidandosi all’ assistenza di **Data Protection Advisors, esperti del diritto della privacy, che dovranno agire in stretta collaborazione con il titolare del trattamento in azienda.**

Sarà ovviamente necessario analizzare caso per caso il soggetto implicato nel trattamento, la “**compliance**” aziendale alla normativa non solo del GDPR e della normativa italiana in tema I.C.T. ma anche considerando le prescrizioni del ben noto **D. Lgs 231/2001** sulla “responsabilità amministrativa degli enti”.

Rientra poi nel quadro delle attività di “compliance” e non va trascurato l’**obbligo di formazione** di tutti coloro che a vario titolo saranno chiamati a trattare i dati personali in azienda. L’art. 32.4 del GDPR dispone che chiunque “*abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento...*”

La formazione è vista dal legislatore sovranazionale come una decisiva misura di sicurezza per la protezione dei dati personali e quindi la prescrive a tutti i titolari del trattamento.

E ora il capitolo **sanzioni** che si prospetta assai scottante almeno sulla carta... del Regolamento.

La norma UE introduce un nuovo sistema punitivo a seguito dei controlli, in Italia della Guardia di Finanza che agisce per il Garante, sanzioni che, seppur erogate con gradualità, dalla semplice “*reprimand*” diffida amministrativa, potrebbero arrivare ad una pena pecuniaria di 20 milioni di euro oppure anche al 4% del fatturato totale annuo dell’esercizio precedente con la possibilità di limitare o addirittura vietare il trattamento dei dati personali.

responsabilità limitata, SOCIO, termine, tribunale, vittime

PER APPROFONDIRE [VAI ALLO SHOPWIKI](#) ▶



NOVITA'

[Commentario breve al Codice Civile](#)

Cian Giorgio

Cian Giorgio, Trabucchi Alberto

Editore: Cedam

Anno: 2018

Versione carta

€ 320,00 (-7%) € 298,00



[Collana "Formulari commentati del processo civile" \(3 volumi\)](#)

Consolo Claudio, Ferro Massimo,

Mariconda Vincenzo, Pototschnig Paolo

Editore: Ipsoa

€ 480,00 (-25%) € 360,00



NOVITA'

[Il Quotidiano Giuridico](#)

VV. AA.

Editore: Wolters Kluwer Italia

€ 250,00 +IVA (-52%) € 118,80 +IVA



[Ricorso civile per cassazione](#)

Cons. Domenico Chindemi

Editore: Altalex Editore

Anno: 2017

Versione carta

€ 49,00 (-15%) € 41,50



NOVITA'

[Agenda legale 2019](#)

Editore: Ipsoa

Anno: 2018

Le sanzioni se comminate all'azienda potrebbero causare evidenti ripercussioni nei rapporti tra i soci e aprire la porta alle azioni di responsabilità oltre che danneggiare l'immagine societaria.

Attenzione: va sottolineato che **le aziende inadempienti potranno poi rispondere anche ai sensi del D. Lgs. 231/2001 se non adottano misure idonee a prevenire i reati da illecito trattamento dei dati personali aggiornando per tempo i modelli organizzativi.**

Poi non andrà dimenticato il pericolo dei **risarcimenti a favore dei soggetti interessati che adducano un danno causato dal trattamento non conforme al GDPR**. Il regolamento UE contiene una serie di indicazioni che dovranno essere prese in considerazione ai fini della valutazione dell'impatto che può avere una violazione per gli eventuali danni agli interessati.

Si legge nel testo normativo che una violazione dei dati, se non affrontata in modo adeguato, può provocare danni fisici, materiali o immateriali alle persone fisiche tra cui la perdita del controllo dei dati personali che li riguardano o la limitazione dei loro diritti, la discriminazione, il furto o usurpazione d'identità, perdite finanziarie, la decifrazione non autorizzata degli pseudonimi utilizzati, il pregiudizio alla reputazione, la perdita di riservatezza dei dati personali protetti da segreto professionale e altro.

L'onere della prova, si noti bene, non è a carico del danneggiato ma incomberà sull'impresa titolare e sul responsabile del trattamento, responsabili in via solidale, che saranno tenuti a risarcire il danno se non dimostrano che esso non è "in alcun modo" loro imputabile.

Ecco le prime riflessioni sul tema GDPR, certamente non esaustive delle svariate problematiche che interessano la prossima rivoluzione della Data Protection, rimando i lettori ad ulteriori commenti sull'iter che porterà quest'anno all'entrata in vigore di principi e norme del nuovo Regolamento UE.

Studio Legale DE VALERI Law Firm Rome
GDPR Legal Check-up & Advice

studiolegaledevaleri@hotmail.com

Lecture: 3478 | Commenti: 5 |



5 Commenti a "GDPR is coming to town. Novità sulla privacy per imprese e professionisti"

1.  **Avv. Luigi DE VALERI** scrive:
Scritto il 27-2-2018 alle ore 07:28

La Carta dei diritti fondamentali dell'UE all'art. 8 afferma che "Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano".

2.  **Avv. Luigi DE VALERI** scrive:
Scritto il 15-3-2018 alle ore 12:18

A causa di un refuso nella scrittura a beneficio dei lettori propongo alcune precisazioni per la parte relativa al DPO. Il GDPR, considerando 97 e articoli 37,38 e 39, tra l'altro prevede, salvo interventi del

Versione carta

€ 50,00 (-50%) € 25,00



eBook - GDPR: il nuovo regolamento europeo sulla Privacy.

Marini Paolo

Editore: Ipsoa

Anno: 2018

Versione eBook

€ 14,90 +IVA

legislatore nazionale più ampi, che la nomina del DPO sia obbligatoria nei seguenti casi:

- a) amministrazioni ed enti pubblici, fatta eccezione per le autorità giudiziarie;
- b) tutti i soggetti la cui attività principale consiste in trattamenti che, per la loro natura, il loro oggetto o le loro finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala;
- c) tutti i soggetti la cui attività principale consiste nel trattamento, su larga scala, di dati sensibili, relativi alla salute o alla vita sessuale, genetici, giudiziari e biometrici. Pertanto al di fuori di questi casi pur non essendovi obbligatorietà di nomina consiglio di valutare con l'ausilio di un giurista esperto di Data Protection il caso particolare che riguarda i dati personali trattati l'opportunità di nominare COMUNQUE un Data Protection Officer interno all'impresa o meglio giovare di un professionista esterno. La sua certificazione, qualunque essa sia, ad oggi non è richiesta dalla normativa.



3. **Monica scrive:**

Scritto il 28-4-2018 alle ore 08:04

Quindi non è più sufficiente il classico foglio da far firmare per il trattamento dei dati personali?



4. **Avv. Luigi DE VALERI scrive:**

Scritto il 2-5-2018 alle ore 14:04

Nota del Garante privacy 19 aprile 2018. "Con riferimento a notizie circolanti in Internet è necessario precisare che non è vero che il Garante per la protezione dei dati si sia pronunciato sul differimento dello svolgimento delle funzioni ispettive e sanzionatorie né il provvedimento richiamato nei siti attiene a tale materia.

Nessun provvedimento del Garante, peraltro, potrebbe incidere sulla data di entrata in vigore del Regolamento europeo fissata al 25 maggio 2018."

Info adeguamento e formazione GDPR mail studiolegaledevaleri@gmail.com mob. 347.8013774



5. **Avv. Luigi DE VALERI scrive:**

Scritto il 11-5-2018 alle ore 02:42

Schema di decreto legislativo recante disposizioni per l'adeguamento della normativa nazionale alle disposizioni del 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).

La nuova bozza di decreto del 5 maggio 2018 sostituisce quella precedente del 21 marzo e invece di abrogare il Codice in materia di protezione dei dati personali, come previsto dalla precedente versione, propone alcune modifiche al codice.

Scrivi il tuo commento!

Nome (obbligatorio)

E-mail - non verrà pubblicata - (obbligatorio)

Sito web

Avvisami dei nuovi commenti tramite e-mail

Invia commento

HOME | FISCO | DIRITTO | LAVORO | IMPRESA | SICUREZZA | AMBIENTE
Chi è postilla | I blogger | Blog Policy | Diventa Blogger | Chi siamo | Contatti | Privacy | Note Legali | Policy cookie | Pubblicità
P.I. 10209790152

Postilla è promossa da:  IPSOA Gruppo Wolters Kluwer  il fisco Gruppo Wolters Kluwer CEDAM  UTET  INDICIALIA Gruppo Wolters Kluwer