Cristina Vicarelli
Avvocato

GDPR: le utilità gratuite per implementarlo

Il 25 maggio 2018 è alle porte, ma ancora mancano molti tasselli, a titolari e responsabili, per orientarsi con sicurezza nel mare magno della compliance alla nuova normativa di matrice europea; mancanze che vanno dalla attesa legislazione nazionale allo stillicidio della pubblicazione delle linee guida del Gruppo di lavoro articolo 29, in netto ritardo sulle tempistiche inizialmente promesse. Le lacune, tuttavia, non fermeranno il Regolamento 679/2016 che diverrà inesorabilmente applicabile indipendentemente dalla completezza del quadro normativo nazionale o dalla esaustività delle indicazioni dei Garanti che si attendevano a corredo del regolamento stesso. Ciò che diverrà più complesso sarà l'impegno di chi è chiamato ad applicare il regolamento, che si troverà a dover valutare con i pochi mezzi a disposizione la conformità alle nuove norme, sopperendo alle inattese difficoltà con una buona dose di creatività e lungimiranza.

Tuttavia è vero che molte Autorità nazionali per la protezione dei dati hanno fornito non solo indicazioni ma anche strumenti gratuiti per aiutare i titolari e i responsabili a gestire il passaggio al meglio.

Se si consultano i siti delle principali Autorità per la protezione dei dati è possibile trovare strumenti, pensati per le piccole e medie imprese, che coprono quasi tutte le aree del Regolamento e che possono rivelarsi molto utili quantomeno per una prima fase di adeguamento.

Sono tutti gratuiti e di facile implementazione, anche se a volte subiscono l'influenza delle normative nazionali e possono richiedere qualche aggiustamento. Ne ho selezionati alcuni, che mi paiono particolarmente interessanti, sperando di poter aggiornare questo post se

dovessero uscirne altri parimenti validi, sperando di poter essere d'ausilio a titolari e responsabili che non possono contare su ampie risorse.

Riporterò gli strumenti che ho reperito divisi per argomento, in modo da facilitare la loro collocazione nell'ambito del Regolamento, con l'avvertenza che molte aree restano scoperte, quindi l'uso di questi strumenti non soddisfa tutti gli adempimenti necessari per la compliance.

Designazione del Data protection officer (DPO o responsabile per la protezione dei dati o RPD)

La designazione del Data protection officer non è obbligatoria per tutti i titolari e i responsabili, ma solo per:

1. amministrazioni ed enti pubblici, fatta eccezione per le autorità giudiziarie;
2. 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;
3. 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.

Ulteriori casi di designazione obbligatoria possono essere individuati dal legislatore statale.

Se non si è sicuri di ricadere nell'obbligo, il Gruppo di lavoro articolo 29 suggerisce di operare una valutazione seguendo i parametri dell'articolo 24 del Regolamento, che deve essere documentata e conservata per essere messa a disposizione dell'Autorità competente in caso di controlli.

Il Garante italiano nelle Nuove Faq sul Responsabile della Protezione dei dati (RPD) in ambito pubblico, ha precisato che il GDPR prevede all'art. 37, par. 1, che il titolare e il responsabile del trattamento **designino** il DPO; "**da ciò deriva, quindi, che l'atto di designazione è parte costitutiva dell'adempimento**".

Ha successivamente evidenziato che occorrerà anche adeguata contrattualistica (sul punto si vedano le linee guida del Gruppo di lavoro ex art. 29), ma ha mostrato di ritenere essenziale l'atto di designazione e ha fornito un modello di designazione e anche un modello di comunicazione al Garante. Si tratta di atti che, sebbene inseriti in delucidazioni destinate a soggetti pubblici, e pensati per i soggetti pubblici, con qualche necessario aggiustamento potranno essere facilmente utilizzati anche da soggetti privati, almeno sino a che non verrà fornito un modello speculare e apposito anche per questi ultimi.

Registro dei trattamenti

L'Autorità belga ha fornito una serie di chiarimenti pratici (in francese) in ordine al Registro dei trattamenti ex art. 30 GDPR, per poi fornire direttamente il modello di registro in excel disponibile in lingua francese.

Del modello su foglio di calcolo fornito dal Garante belga è possibile trovare online una traduzione non ufficiale in lingua inglese

Valutazione di impatto sulla protezione dei dati

La CNIL, che è l'autorità di protezione dei dati francese, ha fornito un software open source che aiuta i titolari a redigere una valutazione di impatto sulla protezione dei dati completa e congrua.

Il tool è disponibile in diverse lingue, tra cui l'italiano, ed è anche liberamente scaricabile in versione compatibile con diversi sistemi operativi (Linux, Windows e MacOS).

Protezione dei dati sin dalla progettazione

L'Autorità per la protezione dei dati norvegese (Il GDPR si applica anche alla Norvegia, dato che fa parte dello Spazio Economico Europeo) ha fornito una interessante guida sulla privacy by design . Si tratta di una guida destinata principalmente allo sviluppo di software, quindi destinata principalmente a sviluppatori, software architects ecc., ma non solo: spiega

l'Autorità che è pensata anche per i data protection officer e gli esperti di sicurezza. La guida è disponibile in lingua inglese.

Sicurezza e GDPR

In occasione del Data protection day del 18 gennaio 2018 l'ENISA (Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione) ha reso disponibili due pubblicazioni in lingua inglese dedicate alla sicurezza nei trattamenti di dati personali e alla privacy e protezione dei dati nelle app. Si tratta di utilità anch'esse destinate alle piccole e medie imprese, che attraverso esempi, casistica e buone pratiche aiutano districarsi nella gestione del rischio connesso all'utilizzo di apparecchiature informatiche.