L'esperto risponde
A CURA DELL'UFFICIO TECNICO-LEGISLATIVO DELL'UNIONE ITALIANA VINI
serviziogiuridico@uiv.it

PROTEZIONE DATI

COSA CAMBIA IN TEMA DI PRIVACY

Il 25 maggio è entrato finalmente in vigore il regolamento Ue 2016/679 (Regolamento Generale sulla Protezione dei Dati). L'aspetto cruciale non è più il possesso di dati, ma la loro corretta gestione

di **DUILIO CORTASSA**

È disponibile lo schema del decreto legislativo di armonizzazione dell'ordinamento italiano al regolamento Ue sulla protezione dei dati (n. 2016/679), che è diventato finalmente operativo lo scorso 25 maggio. Lo schema di decreto ha subito più di una stesura, ma l'ultima bozza sembra essere quella che sarà trasmessa in Parlamento per i pareri delle competenti commissioni parlamentari.
Punita l'acquisizione fraudolenta e la diffusione di ingenti dati personali; a 16 anni il consenso dei minori per la rete; la sanità perde l'obbligo del consenso e oblazione in vista per le violazioni amministrative del vecchio codice della privacy che, seppure amputato in larga parte, rimane in piedi, contrariamente a quanto previsto in precedenza. È, tra l'altro, abrogato integralmente l'allegato B sulle misure minime di sicurezza, anche alla luce del fatto che non sembrano rimanere in vita le sanzioni penali.
L'ultima bozza è decisamente diversa da quella circolata in precedenza e, in particolare, si passa dall'abrogazione totale del codice della privacy (dlgs 196/2003) a una abrogazione parziale, con un'operazione di sostituzione e integrazione di norme. Alcune di queste sono la riproposizione di analoghe disposizioni del codice della privacy, altre sono la trasposizione di norme europee.
Gli operatori e le aziende si trovano di fronte a un patchwork di norme che certo non renderanno maggiormente agile un lavoro interpretativo che negli anni è stato caratterizzato da continui "aggiustamenti di tiro" da parte del legislatore e del Garante per la protezione dei dati personali, soggetti che non sempre si sono trovati in perfetta sintonia sull'applicazione e sull'interpretazione delle norme. Avremo quindi un quadro di norme sparse, senza una fonte unificante, con le autorizzazioni generali del Garante tutte da verificare alla luce del RGPD e con una giurisprudenza del Garante, composta da provvedimenti adottati in 22 anni di privacy nazionale, che dovrà volta per volta essere riletta alla luce del RGPD.

La valutazione di impatto e il consenso

Per permettere alle aziende di comprendere come muoversi nell'ambito del mondo, in parte nuovo, della protezione dei dati personali, è bene riferirsi alle linee-guida del Gruppo Articolo 29 in materia di valutazione di impatto sulla protezione dei dati (WP248).
Quando un trattamento può comportare un rischio elevato per i diritti e le libertà delle persone interessate (a causa del monitoraggio sistematico dei loro comportamenti, o per il gran numero dei soggetti interessati di cui sono magari trattati dati sensibili, o anche per una combinazione di questi e altri fattori), il regolamento 2016/679 obbliga i titolari a svolgere una valutazione di impatto prima di darvi inizio, consultando l'autorità di controllo in caso le misure tecniche e organizzative da loro stessi individuate per mitigare l'impatto del trattamento non siano ritenute sufficienti, cioè quando il rischio residuale per i diritti e le libertà degli interessati resti elevato.
Si tratta di uno degli elementi di maggiore rilevanza nel nuovo quadro normativo, perché esprime chiaramente la responsabilizzazione (accountability) dei titolari nei confronti dei trattamenti da questi effettuati. I titolari sono infatti tenuti non soltanto a garantire l'osservanza delle disposizioni del regolamento, ma anche a dimostrare adeguatamente in che modo garantiscono tale osservanza; la valutazione di impatto ne è un esempio.
Quindi, entro lo scorso 25 maggio, anche le aziende del comparto vitivinicolo devono aver svolto un'analisi dettagliata del contesto aziendale in merito allo stato di applicazione della normativa in materia di protezione dei dati e vagliato la conformità della disciplina interna aziendale alle normative di recente introduzione, considerando che, nel RGPD, la definizione data protection ha sostituito la parola privacy; in altre parole, l'aspetto cruciale non è più il possesso di dati, ma la gestione corretta di questi.

➔

LE NOVITÀ

1. L'applicazione del diritto dell'Ue anche ai trattamenti di dati personali non svolti nell'Ue, se relativi all'offerta di beni o sevizi a cittadini Ue o tali da comportare il monitoraggio dei comportamenti di cittadini Ue.
2. L'obbligo di trattare i dati e, di conseguenza, di tutelare i diritti dell'interessato nell'attività di trattamento, fin dalla fase della progettazione e per l'intera gestione del ciclo di vita dei dati, ponendo in essere misure di carattere tecnico e organizzativo, ove possibile, quali la minimizzazione e la pseudonimizzazione.
3. L'obbligo di trattare i dati partendo da configurazioni "chiuse" dei sistemi informatici, ampliabili dopo avere valutato l'impatto di eventuali aperture, adottando in via predefinita le impostazioni che garantiscono il maggior rispetto della privacy, affinché i dati personali non siano resi accessibili a un numero indefinito di persone senza l'intervento umano.
4. L'individuazione del Data Protection Officer (DPO, vedi pag. 14).
5. L'obbligo di svolgere il Data Protection Impact Assessment (DPIA), per i trattamenti ad alto rischio (come può essere un trattamento su larga scala) e di rispettare il data breach, cioè la segnalazione al Garante e all'interessato di eventuali fughe o compromissioni di dati.
6. La redazione del Registro delle attività di trattamento, nel quale saranno conservate numerose informazioni sul trattamento.
7. L'adozione di politiche e misure adeguate al fine di poter dimostrare che il trattamento dei dati personali effettuato è conforme (fin dalla fase embrionale) a tutte le disposizioni del Regolamento.

Il RGPD insiste sulla verifica che la richiesta di consenso sia chiaramente distinguibile da altre richieste o dichiarazioni rivolte all'interessato, per esempio all'interno di una modulistica prestampata; l'articolo 72 prevede che la formula sia comprensibile, semplice, chiara.

Intanto, in Europa...
Molti altri Paesi Ue, come la Germania (dove opera l'efficientissima Bundesbeauftragter für den Datenschutz und die Informationsfreiheit, "BfDI"), hanno emanato una nuova legge privacy in attuazione del RGPD o, comunque, hanno creato un raccordo tra la precedente e la nuova normativa. In Italia, la Camera dei Deputatati ha approvato in via definitiva, lo scorso 17 ottobre, la legge di delegazione europea 2016-2017, che rappresenta uno degli strumenti legislativi volti ad assicurare il periodico adeguamento dell'ordinamento nazionale a quello dell'Ue: tra le deleghe assegnate al Governo è prevista l'adozione di uno o più Decreti legislativi al fine di adeguare il quadro normativo nazionale alle disposizioni del RGPD sulla protezione delle persone fisiche con riguardo al trattamento dei dati personali, rinnovando in maniera significativa il sistema della disciplina in materia di privacy. Il piano di riordino previsto dal Parlamento dovrà essere portato a compimento entro sei mesi dalla data di entrata in vigore della legge.

La Commission Nationale de l'Informatique et des Libertés ("CNIL"), cioè l'autorità francese per la protezione dei dati, ha invece messo a disposizione un software di ausilio ai titolari in vista della effettuazione della valutazione d'impatto sulla protezione dei dati (DPIA). Il software è gratuito e liberamente scaricabile dal sito www.cnil.fr (https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil) e offre un percorso guidato alla realizzazione della DPIA, secondo una sequenza conforme alle indicazioni fornite dal WP29 nelle Linee-guida sulla DPIA.

IL DATA PROTECTION OFFICER

Il Garante per la protezione dei dati personali ha pubblicato le Faq relative al Responsabile della Protezione dei Dati (Data Protection Officer) in ambito privato, nuova figura introdotta dal Regolamento Ue 2016/679 e sulla quale le aziende di maggiori dimensioni, ma non solo quelle, dovranno fare una riflessione

1. Chi è il responsabile della protezione dei dati personali (RPD) e quali sono i suoi compiti?
Il responsabile della protezione dei dati personali (o Data Protection Officer - DPO) è una figura prevista dall'art. 37 del Regolamento (Ue) 2016/679.
Si tratta di un soggetto designato dal titolare o dal responsabile del trattamento per assolvere a funzioni di supporto e controllo, consultive, formative e informative relativamente all'applicazione del Regolamento medesimo. Coopera con l'Autorità (e proprio per questo, il suo nominativo va comunicato al Garante) e costituisce il punto di contatto, anche rispetto agli interessati, per le questioni connesse al trattamento dei dati personali (artt. 38 e 39 del Regolamento).

2. Quali requisiti deve possedere il responsabile della protezione dei dati personali?
Il responsabile della protezione dei dati personali, al quale non sono richieste specifiche attestazioni formali o l'iscrizione in appositi albi, deve possedere un'approfondita conoscenza della normativa e delle prassi in materia di privacy, nonché delle norme e delle procedure amministrative che caratterizzano lo specifico settore di riferimento. Deve poter offrire, con il grado di professionalità adeguato alla complessità del compito da svolgere, la consulenza necessaria per progettare, verificare e mantenere un sistema organizzato di gestione dei dati personali, coadiuvando il titolare nell'adozione di un complesso di misure (anche di sicurezza) e garanzie adeguate al contesto in cui è chiamato a operare. Deve inoltre agire in piena indipendenza (considerando 97 del Regolamento Ue 2016/679) e autonomia, senza ricevere istruzioni e riferendo direttamente ai vertici. Il responsabile della protezione dei dati personali deve poter disporre, infine, di risorse (personale, locali, attrezzature ecc.) necessarie per l'espletamento dei propri compiti.

3. Chi sono i soggetti privati obbligati alla sua designazione?
Sono tenuti alla designazione del responsabile della protezione dei dati personali il titolare e il responsabile del trattamento che rientrino nei casi previsti dall'art. 37, par. 1, lett. b) e c), del Regolamento (Ue) 2016/679. Si tratta di soggetti le cui principali attività (in primis, le attività c.d. di "core business") consistono in trattamenti che richiedono il monitoraggio regolare e sistematico degli interessati su larga scala o in trattamenti su larga scala di categorie particolari di dati personali o di dati relative a condanne penali e a reati (per quanto attiene alle nozioni di "monitoraggio regolare e sistematico" e di "larga scala", v. le "Linee guida sui responsabili della protezione dei dati" del 5 aprile 2017, WP 243). Il diritto dell'Unione o degli Stati membri può prevedere ulteriori casi di designazione obbligatoria del responsabile del trattamento dei dati personali (art. 37, par. 4).

4. Chi sono i soggetti per i quali non è obbligatoria la designazione del responsabile della protezione dei dati personali?
Nei casi diversi da quelli previsti dall'art. 37, par. 1, lett. b) e c), del Regolamento (UE) 2016/679, la designazione del responsabile del trattamento non è obbligatoria (ad esempio, imprese individuali o familiari; piccole e medie imprese, con riferimento ai trattamenti dei dati personali connessi alla gestione corrente dei rapporti con fornitori e dipendenti: v. anche considerando 97 del Regolamento, in relazione alla definizione di attività "accessoria"). In ogni caso, resta comunque raccomandata, anche alla luce del principio di "accountability" che permea il Regolamento, la designazione di tale figura (v. in proposito le menzionate linee guida), i cui criteri di nomina, in tale evenienza, rimangono gli stessi sopra indicati.

5. È possibile nominare un unico responsabile della protezione dei dati personali nell'ambito di un gruppo imprenditoriale?
Il Regolamento (UE) 2016/679 prevede che un gruppo imprenditoriale (v. definizione di cui all'art. 4, n. 19) possa designare un unico responsabile della protezione dei dati personali, purché tale responsabile sia facilmente raggiungibile da ciascuno stabilimento (sul concetto di "raggiungibilità", v. punto 2.3 delle linee guida in precedenza menzionate). Inoltre, dovrà essere in grado di comunicare in modo efficace con gli interessati e di collaborare con le autorità di controllo.

6. Il responsabile della protezione dei dati personali deve essere un soggetto interno o può essere anche un soggetto esterno? Quali sono le modalità per la sua designazione?
Il ruolo di responsabile della protezione dei dati personali può essere ricoperto da un dipendente del titolare o del responsabile (non in conflitto di interessi) che conosca la realtà operativa in cui avvengono i trattamenti; l'incarico può essere anche affidato a soggetti esterni, a condizione che garantiscano l'effettivo assolvimento dei compiti che il Regolamento (Ue) 2016/679 assegna a tale figura. Il responsabile della protezione dei dati scelto all'interno andrà nominato mediante specifico atto di designazione, mentre quello scelto all'esterno, che dovrà avere le medesime prerogative e tutele di quello interno, dovrà operare in base a un contratto di servizi.

Nell'esecuzione dei propri compiti, il responsabile della protezione dei dati personali (interno o esterno) dovrà ricevere supporto adeguato in termini di risorse finanziarie, infrastrutturali e, ove opportuno, di personale. Il titolare o il responsabile del trattamento che abbia designato un responsabile per la protezione dei dati personali resta comunque pienamente responsabile dell'osservanza della normativa in materia di protezione dei dati e deve essere in grado di dimostrarla (art. 5, par. 2, del Regolamento; v. anche i punti 3.2 e 3.3. delle linee guida sopra richiamate).
I dati di contatto del responsabile designato dovranno essere infine pubblicati dal titolare o responsabile del trattamento. Non è necessario - anche se potrebbe rappresentare una buona prassi - pubblicare anche il nominativo del responsabile della protezione dei dati: spetta al titolare o al responsabile e allo stesso responsabile della protezione dei dati, valutare se, in base alle specifiche circostanze, possa trattarsi di un'informazione utile o necessaria. Il nominativo del responsabile della protezione dei dati e i relativi dati di contatto vanno invece comunicati all'Autorità di controllo. A tal fine, è possibile utilizzare il modello disponibile scaricabile dal sito del Garante.