I 15 errori da evitare nell'applicare il Reg. UE 2016/679 Privacy europea

Autore: Dr. Matteo Rapparini

www.consulenzaprivacy.org

Edirama Viale dei Gelsi 17
40068 San Lazzaro di Savena BO
P.I. 04200180372

7429537411418

Introduzione

Il nuovo regolamento privacy UE 2016/679 presenta numerose novità che richiedono per essere applicate una pianificazione dettagliata delle attività e delle relative risorse. E' importante altresì definire tempistiche entro le quali devono concludersi le varie attività.

Ricordiamo che l'aggiornamento deve essere fatto correttamente, in quanto sono previste sanzioni fino al 4% del fatturato dell'intero gruppo aziendale.

Per questo motivo la mancata compliance anche in una piccola azienda che appartiene a un gruppo industriale o internazionale, può avere gravi ripercussioni.

La preparazione e l'adeguamento al nuovo regolamento europeo richiede la riorganizzazione di numerose procedure interne che devono essere per tempo ri-aggiornate.

Dal punto di vista operativo l'adeguamento e l'applicazione del Reg. Ue 2016/679 presenta numerose insidie e trappole che possono creare problemi nella corretta applicazione delle prescrizioni richieste.

Tipicamente sono 15 gli errori da evitare nell'applicazione del Reg. UE 2016/679.

Vediamoli insieme.

1) **Mancanza consapevolezza del management sulla applicabilità del nuovo Regolamento europeo**. Questo errore potrebbe verificarsi nelle realtà meno complesse e di dimensioni minori, mentre in quelle dove esiste già una struttura dedicata alla privacy, con la presenza di vari responsabili, tale problematica è minore.
   Cosa fare
   Verificare che le persone chiave delle struttura organizzativa del Titolare siano consapevoli dell'impatto che avrà il Regolamento, mappare le aree di rischio, individuare quelle che saranno maggiormente interessate dai cambiamenti e i ruoli decisionali; potrebbe essere necessario introdurre nuovi documenti (si pensi ad esempio al Registro dei trattamenti), interfacciarsi con nuove figure professionali (si pensi al Data Protection Officer), o intervenire sulla contrattualistica.

2) **Non costituire da subito una squadra multidisciplinare** (giurista, informatico, esperto di organizzazione, esperto di processi).

In molte aziende l'aggiornamento e l'applicazione della privacy è spesso stata fatta dall'azienda informatica che seguiva il sistema IT.

Cosa fare

Con il nuovo Reg. UE 2016/679 sono invece richieste ulteriori competenze che coinvolgono aspetti più specifici che vanno dall'organizzazione aziendale, alla gestione e monitoraggio dei processi aziendali, per passare da aspetti legali che non possono essere omessi e non valutati.

3) **Non mappare tutti i trattamenti in corso o programmati e non documentare quali dati si trattano, da dove si originano, e a chi vengono comunicati.**

Cosa fare

Occorre individuare dati e informazioni, riconoscendo i dati personali.

Occorrerà anche fare attenzione alla tipologia di dati trattati: il Regolamento definisce all'articolo 4 «dati genetici», «dati biometrici», «dati relativi alla salute», mentre all'articolo 9 disciplina e definisce quelli a noi noti come "dati sensibili", ossia "dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona" che, sottoposti alla

medesima disciplina prevista per i dati genetici, e i dati biometrici intesi a identificare in modo univoco una persona fisica, vengono (tutti) rubricati come "Trattamento di categorie particolari di dati personali" (si tratta quindi di un aggiornamento dell'articolo 8 della Direttiva 95/46/CE)
La nostra normativa prevede già che il titolare tenga traccia di tali elementi e molte realtà continuano ad adottare documenti che "fotografano" i trattamenti anche dopo che è venuto meno l'obbligo di redigere o aggiornare il DPS

4) **Non verificare origine e flussi dei dati personali**
Cosa fare
Documentare i dati personali trattati, da dove arrivano e con chi vengono condivisi. Organizzare procedure di verifica, se necessarie.

5) **Non aggiornare le informative**
Il Regolamento europeo 2016/679 aggiunge nuovi elementi alle informative attuali.
Cosa fare
Occorre spiegare all'interessato la base giuridica del trattamento, informarlo dell'esistenza di un processo decisionale automatizzato, compresa la profilazione, e dovranno essere fornite informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze di

tale trattamento previste per l'interessato.
Si dovrà informare l'interessato circa la durata della conservazione dei suoi dati.
Occorrerà informare l'interessato circa il suo diritto di proporre reclamo a un'Autorità di controllo; quindi dire all'interessato anche dove si trova e qual è l'Autorità alla quale si può rivolgere.
Le informazioni dovranno essere date in maniera semplice: occorrerà eliminare dalle informative inutili contenuti poco comprensibili, inserendo forme schematiche di facile e immediata comprensione.

6) **Non aggiornare e verificare i diritti degli interessati**

Il Regolamento formalizza un ampio catalogo di diritti che spettano all'interessato. Si tratta del diritto di accesso, del diritto di rettifica, del diritto alla cancellazione (più noto come diritto all'oblio), diritto di limitazione del trattamento, diritto alla portabilità dei dati, diritto di opposizione al trattamento, con gli eventuali connessi obblighi di notifica/comunicazione gravanti sul titolare.

Cosa fare

E' necessario controllare le procedure, e verificare come l'ente si pone di fronte all'esercizio dei diritti da parte dell'interessato: come sono gestite le richieste di cancellazione da parte dell'interessato? I sistemi informatici

in uso aiutano a reperire e cancellare i dati? Chi decide in ordine alla cancellazione? Il nuovo “diritto all’oblio”, riconosciuto all’interessato dall’articolo 17 del Regolamento, deve essere soddisfatto tempestivamente o come dice il Regolamento “senza ingiustificato ritardo”. Anche il diritto alla portabilità dei dati è nuovo, e quindi si dovrà definire una procedura per gestire la richiesta di portabilità avanzata dall’interessato. Nei casi in cui si debbano fornire i dati personaliall’interessato occorrerà farlo in formato elettronico di uso comune.

7) **Non aggiornare o predisporre le procedure per garantire e facilitare l’esercizio dei diritti degli interessati.**
Il termine per la risposta all'interessato è, per tutti i diritti (compreso il diritto di accesso), 1 mese, estendibili fino a 3 mesi in casi di particolare complessità; il titolare deve comunque dare un riscontro all'interessato entro 1 mese dalla richiesta, anche in caso di diniego.
Cosa fare
Spetta al titolare valutare la complessità del riscontro all'interessato e stabilire l'ammontare dell'eventuale contributo da chiedere all'interessato, ma soltanto se si tratta di richieste manifestamente infondate o eccessive (anche ripetitive) (art. 12.5), a differenza di quanto

prevedono gli art. 9, comma 5, e 10, commi 7 e 8, del Codice, ovvero se sono chieste più "copie" dei dati personali nel caso del diritto di accesso (art. 15, paragrafo 3); in quest'ultimo caso il titolare deve tenere conto dei costi amministrativi sostenuti. Il riscontro all'interessato di regola deve avvenire in forma scritta anche attraverso strumenti elettronici che ne favoriscano l'accessibilità; può essere dato oralmente solo se così richiede l'interessato stesso (art. 12, paragrafo 1; si veda anche art. 15, paragrafo 3). La risposta fornita all'interessato non deve essere solo "intelligibile", ma anche concisa, trasparente e facilmente accessibile, oltre a utilizzare un linguaggio semplice e chiaro.

8) **Non individuare correttamente la base giuridica dei trattamenti**

Il regolamento conferma che ogni trattamento deve trovare fondamento in un'idonea base giuridica; i fondamenti di liceità del trattamento sono indicati all'art. 6 del regolamento e coincidono, in linea di massima, con quelli previsti attualmente dal Codice (consenso, adempimento obblighi contrattuali, interessi vitali della persona interessata o di terzi, obblighi di legge cui è soggetto il titolare, interesse pubblico o esercizio di pubblici poteri, interesse legittimo prevalente del titolare o di terzi cui i dati vengono comunicati).

Cosa fare

Fare una ricognizione dei diversi trattamenti, individuandone la base giuridica per poterla comunicare (quando richiesto dalla normativa) e documentarla.
Il consenso raccolto precedentemente al 25 maggio 2018 resta valido se ha tutte le caratteristiche sopra individuate. In caso contrario, è opportuno adoperarsi prima di tale data per raccogliere nuovamente il consenso degli interessati secondo quanto prescrive il regolamento, se si vuole continuare a fare ricorso a tale base giuridica.

In particolare, occorre verificare che la richiesta di consenso sia chiaramente distinguibile da altre richieste o dichiarazioni rivolte all'interessato (art. 7.2), per esempio all'interno di modulistica. Prestare attenzione alla formula utilizzata per chiedere il consenso: deve essere comprensibile, semplice, chiara (art. 7.2). I soggetti pubblici non devono, di regola, chiedere il consenso per il trattamento dei dati personali (art. 9, altre disposizioni del Codice: artt. 18, 20).

9) Non verificare come i consensi siano chiesti, ottenuti e registrati.

Per i dati "sensibili" (si veda art. 9 regolamento) il consenso DEVE essere "esplicito"; lo stesso dicasi per il consenso a decisioni basate su trattamenti automatizzati (compresa la profilazione – art. 22).

- NON deve essere necessariamente "documentato per iscritto", né è richiesta la "forma scritta", anche se questa è modalità idonea a configurare l'inequivocabilità del consenso e il suo essere "esplicito" (per i dati sensibili); inoltre, il titolare (art. 7.1) DEVE essere in grado di dimostrare che l'interessato ha prestato il consenso a uno specifico trattamento.
- Il consenso dei minori è valido a partire dai 16 anni; prima di tale età occorre raccogliere il consenso dei genitori o di chi ne fa le veci.

Cosa fare

Rivedere in quali casi e con quali modalità vengono richiesti, ottenuti e registrati i consensi, in modo da valutare se sia necessario operare modifiche. Valutare il valore probatorio della registrazione dei consensi in caso di controversie.

10) Non realizzare o realizzare in modo approssimativo la valutazione rischi impatti trattamenti dati.

Il rischio inerente il trattamento è da intendersi come rischio di impatti negativi sulle libertà e i diritti degli interessati ; tali impatti dovranno essere analizzati attraverso un apposito processo di valutazione (si vedano artt. 35-36) tenendo conto

dei rischi noti o evidenziabili e delle misure tecniche e organizzative (anche di sicurezza) che il titolare ritiene di dover adottare per mitigare tali rischi. All'esito di questa valutazione di impatto il titolare potrà decidere in autonomia se iniziare il trattamento (avendo adottato le misure idonee a mitigare sufficientemente il rischio) ovvero consultare l'autorità di controllo competente per ottenere indicazioni su come gestire il rischio residuale; l'autorità non avrà il compito di "autorizzare" il trattamento, bensì di indicare le misure ulteriori eventualmente da implementare a cura del titolare e potrà, ove necessario, adottare tutte le misure correttive ai sensi dell'art. 58: dall'ammonimento del titolare fino alla limitazione o al divieto di procedere al trattamento.

Non è sempre necessario condurre una PIA: la valutazione di impatto privacy é richiesta in situazioni che presentano rischi elevati, ad esempio quando si sviluppa una nuova tecnologia o quando operazioni di profilazione possano incidere significativamente sugli interessati. Saranno le Autorità nazionali, anche in coordinamento tra loro, a definire le tipologie di trattamenti da sottoporre o sottrarre alla valutazione di impatto sulla protezione dei dati.

Cosa fare

La valutazione rischi impatti trattamenti dati deve essere svolta in un ambito di approccio di privacy by design, ovvero all'inizio

della definizione e della progettazione del trattamento dati. E' necessario quindi apprendere le modalità di risk management.

11) Non definire le procedure che consentano di individuare, riportare e investigare le violazioni di dati personali.

L'art. 33 del Regolamento Europeo 679/2016 introduce una grossa novità nello scenario della sicurezza dei dati: la necessità di notificare la violazione dei propri sistemi informatici (ossia un data breach) al Garante. Inoltre, l'art. 34 estende, in alcuni casi, tale notifica a tutti gli interessati! Scatta, quindi, un obbligo di autodenuncia: entro 72 ore da cui si viene a conoscenza di una violazione dei propri sistemi informatici è necessario seguire una procedura che notifichi la violazione all'autorità Garante della Privacy.

Cosa fare

Occorre definire procedure efficaci che consentano di individuare, documentare investigare e (se necessario) comunicare, come per legge, le violazioni di dati personali.

12) Non formare gli incaricati

Il nuovo Regolamento europeo 2016/679 richiede tutta una serie di nuovi adempimenti e l'applicazione di nuove procedure, che necessitano di essere comunicati in modo corretto e completo agli incaricati. Per cui è fondamentale realizzare la formazione a queste importanti figure della gestione privacy

Cosa fare

Definire un piano di formazione sul nuovo Reg. UE 2016/679 agli incaricati e formarli anche sulle nuove procedure applicate in azienda.

13) Non nominare il Data Protection Officer quando previsto.
L'articolo 37 del Reg. UE 2016/679 indica i casi in cui è obbligatorio nominare il DPO:
a) se il trattamento è svolto da un'autorità pubblica o da un organismo pubblico;
b) se le attività principali del titolare o del responsabile consistono in trattamenti che richiedono il monitoraggio regolare e sistematico di interessati su larga scala; oppure
c) se le attività principali del titolare o del responsabile consistono nel trattamento su larga scala di categorie particolari di dati di dati personali relativi a condanne penali e reati

Cosa fare

Valutare se si rientra nei casi previsti dalla normativa per cui occorre designare un DPO al fine di dimostrare la conformità ai requisiti di sicurezza previsti dal Regolamento, e valutare come questo ruolo potrà collocarsi in rapporto alla propria struttura, considerando le necessarie modifiche anche in ordine alla governance.

14) In caso di trattamenti transfrontalieri non definire correttamente l'Autorità sotto la quale si ricade

Se si opera a livello internazionale occorre comprendere sotto quale Autorità nazionale si ricade.

Il Regolamento elabora in maniera piuttosto complessa il modo in cui una Autorità (quella nel cui territorio ricade lo stabilimento principale del Titolare) diviene "capofila", nel caso di controlli su trattamenti transfrontalieri, ad esempio quando operazioni di trattamento incidano su interessati di diversi Stati membri. L'Autorità capofila si individua sulla base dello stabilimento principale del titolare. Quello di "stabilimento principale" è un concetto nuovo, introdotto dal Regolamento; con la direttiva era sufficiente l'individuazione dello stabilimento ai soli fini dell'applicazione delle diverse normative nazionali.

Lo stabilimento principale di un titolare del trattamento è il luogo in cui ha sede la sua amministrazione centrale nell'Unione, a meno che le decisioni sulle finalità e i mezzi del trattamento di dati personali siano adottate in un altro stabilimento del titolare del trattamento nell'Unione, nel qual caso lo stabilimento principale è quello in cui vengono prese le decisioni.

Nelle realtà più complesse non è sempre agevole individuare o stabilimento principale, dato che i diversi trattamenti possono essere effettuati e decisi in luoghi diversi: sarà utile, in questi casi, mappare dove vengono prese le decisioni più importanti in ordine alla protezione dei dati,

in modo da risalire all'Autorità capofila**.**

15) Non garantire un presidio continuativo sia legale che informatico

Le difficoltà dell'applicazione corretta del Reg. UE 2016/679 fanno sì che, soprattutto nelle aziende più strutturate e con una operatività multinazionale, sia necessario attivare un gruppo di lavoro permanente che comprenda profili ed esperienze di carattere legale e informatico

Cosa fare

La direzione aziendale deve instaurare un gruppo di lavoro interdisciplinare con profili qualificati legali e informatici

Web Bibliografia

_ Linee-guida sui responsabili della protezione dei dati (RPD) - WP 243.pdf
http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/5930287

_ Reg. UE 2016/679
http://eur-lex.europa.eu/legal-content/IT/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ITA&toc=OJ:L:2016:119:TOC

_ Il nuovo "pacchetto protezione dati" - Pagina informativa
http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/4443361

_ Guida sintentica a nuova Reg. UE 2016/679
http://194.242.234.211/documents/10160/5184810/Guida+al+nuovo+Regolamento+europeo+in+materia+di+protezione+dati

SOFTWARE E STRUMENTI PER AZIENDE E CONSULENTI PER APPLICARE IL REG. UE 2016/679

Sul sito www.consulenzaprivacy.org sono disponibili i seguenti prodotti per realizzare la formazione e tutti gli adempimenti richiesti dal Reg. UE 2016/679

1) Corso on line esperto privacy europea reg. UE 2016/679
2) Kit software privacy europea – raccolta di 4 software specifici per realizzare tutti gli adempimenti previsti dalla privacy europea: compliance, analisi rischi impatti trattamenti, aggiornamento informative privacy, mappatura trattamenti e registro trattamenti
3) Raccolta informative privacy in formato MS Word già aggiornate al Rge. 2016/679
4) Software Project privacy, per realizzare e gestire i progetti di implementazione privacy europea