Prontuario per professionisti della privacy: are you experienced?

Andrea Lisi - *Avvocato, Direttore Editoriale KnowIT, Coordinatore Digital&Law Department e Presidente ANORC Professioni*

Perdonerete l'apertura di questo intervento con il titolo di un album del 1967 di *Jimi Hendrix* (*Are you experienced?*), ma **è in fondo in questa domanda che si racchiude la portata realmente rivoluzionaria del Regolamento 2016/679/UE (General Data Protection Regulation),** che non risiede unicamente nel solo (temutissimo) apparato sanzionatorio.
Sul punto, è il caso di ribadire che **il D.Lgs. 196/2003, come modificato dal D.Lgs. 101/2018** (e adesso rubricato "Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 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"), **è pienamente applicabile dal 19 settembre 2018, sanzioni comprese. Precisazione tanto ovvia, quanto necessaria, sulla scorta di interpretazioni improvvisate e fuorvianti circolate negli ultimi tempi, sulla presunta sospensione delle sanzioni (definita improvvidamente "stato di grazia") nei primi otto mesi di applicazione**[1].

Ebbene in cosa risiede la vera novità? In cosa consiste la "rivoluzione" innescata ormai a livello europeo? A mio avviso, si tratta di un cambiamento radicale di "approccio": il nuovo framework europeo impone una presa di coscienza in termini di responsabilizzazione e ha inteso rendere consapevoli (non solo gli specialisti del settore) della complessità della "quarta dimensione", quella digitale, che pervade ogni nostra azione e interazione, possibile sempre e unicamente grazie al trattamento dei dati personali.
Occorre conoscersi, avere contezza della propria entità, per applicare correttamente i principi contenuti nel GDPR.

E in che modo si traduce questa responsabilizzazione? Con riferimento a un contesto sia pubblico sia privato corrisponde alla scelta documentata di ruoli, procedure e strumenti. Responsabilizzarsi significa anche (e soprattutto) fare i conti con una realtà professionale multidisciplinare, che necessita di essere alimentata dall'acquisizione delle giuste competenze e di crescere attraverso il confronto continuo e costante. Non è solo questione di applicazione (o di applicativi) quindi, ma anche e soprattutto di metodologie documentabili, in grado di farci capire (e di dimostrare che abbiamo capito) come procedere e con chi, per applicare i principi del GDPR (e quindi del "Codice della privacy" rinnovato e allineato alle nuove necessità del GDPR in modo che sia interpretabile in piena compatibilità con esse).

In uno scenario (quello italiano) in cui non si assiste spesso alla perfetta "quadratura del cerchio" tra norma e prassi, è quanto mai singolare per un giurista udire di strumenti (e termini) nuovi, quali: verifica delle procedure, check list, registri obbligatori, procedure di assessment e mappatura dei rischi, prevenzione e gestione del data breach, nonché monitoraggio e controllo; termini che rappresentano la traduzione reale di quanto previsto e "standardizzato" per tutto il continente europeo, e necessariamente tradotto a livello nazionale. A poco più di tre settimane dall'entrata in vigore del D. Lgs. 101/2018 di adeguamento UE, si avverte così da parte degli "addetti ai lavori" il bisogno di completare la selezione e l'adozione di quegli strumenti operativi pienamente conformi al principio di accountability, quintessenza del GDPR, e in grado di garantire lo sviluppo di processi armonizzati. Non a caso il Garante è recentemente intervenuto [2] per rendere disponibili delle **FAQ sul Registro delle attività di trattamento, corredate da modelli "semplificati" per Titolare e Responsabile**.

Procedendo con ordine, proviamo a ricostruire una sorta di "prontuario" di metodi e strumenti necessari per titolari, responsabili, DPO (Data Protection Officer) e non ultimo "consulenti privacy", che scelgono di "fare per bene" il loro lavoro:

Una, nessuna, centomila check list

Una "check list" con domande specifiche da fare è il primo passo per entrare in contatto con la nostra realtà professionale, aziendale e/o amministrativa. Il primo identikit da tracciare è quello del reparto già impegnato ad

occuparsi direttamente della materia (in genere quello amministrativo o informatico, o legale...sperando che questo reparto realmente esista!) allargando il tratto ad altri uffici più “delicati”, sulla base dei trattamenti di dati posti in essere al loro interno (ad esempio il reparto risorse umane, o l’ufficio marketing e comunicazione, quello IT e così via).
Durante questo primo audit (che può richiedere anche più check list, in rapporto all’organizzazione di riferimento) è possibile riuscire a ottenere quanto meno una mappatura completa (pur se generica) del modus operandi adottato, individuando e analizzando l’appropriatezza di:

- lettere di nomina degli incaricati e degli amministratori di sistema;
- clausole contrattuali con gli eventuali responsabili del trattamento;
- informative (dipendenti, clienti, utenti/pazienti ecc.);
- modelli di consenso;
- DPS se adottato e mantenuto aggiornato;
- policy e/o regolamenti interni in materia di trattamento dei dati personali;
- registri/elenchi hardware e software;
- eventuali procedure certificate
- etc.

Le check list consentono di effettuare un primo screening delle criticità e degli eventuali gap da colmare e, quindi, di avviare la successiva pianificazione degli interventi necessari. In questa fase, si può già riconoscere se la realtà con cui si ha a che fare debba dotarsi obbligatoriamente di un DPO (Data Protection Officer) o se per natura e dimensioni è in grado di auto regolamentarsi.

Adottare ed implementare il registro obbligatorio del trattamento dati

L’introduzione di un registro obbligatorio delle attività svolte è prevista espressamente dall’art. 30 del GDPR ed è stata più volte ribadita e caldeggiata del Garante,.
Obbligatorietà che si fa duplice, poiché oltre a riguardare il possesso dello stesso, a essere obbligatoria è soprattutto la sua corretta, aggiornata e puntuale compilazione. Le disposizioni sono chiare e precise e lasciano poco ai margini di errore, infatti l’art 30 del GDPR[3] stabilisce che: *ogni titolare del trattamento e, ove applicabile, il suo rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità.*
Tale registro contiene tutta **una serie di indicazioni che permettono da un lato di adeguarsi alla norma, dall’altro di creare delle procedure (sartoriali) rispetto ai sistemi di gestione interni**. Le disposizioni in merito, pressoché intuitive e di facile applicazione a tutti i livelli di trattamento, si riferiscono essenzialmente a:

a. il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;
b. le finalità del trattamento;
c. una descrizione delle categorie di interessati e delle categorie di dati personali;
d. le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
e. ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;
f. ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
g. ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.

I registri **non vanno mai considerati come documenti finiti**, **ma pensati come schema di riferimento** che può per esigenze dinamiche e temporali essere plasmato senza snaturarsi della propria natura di raccolta e conservazione.

Definire i principali attori e loro responsabilità

Dopo aver compiuto questi passi, ci troviamo in una fase intermedia del nostro processo di assessment, un punto cruciale dell’intera attività. Un momento questo, in cui abbiamo a disposizione una mappatura completa dei flussi dei dati personali sia all’interno che all’esterno dell’organizzazione e quindi, da adesso fino alla fine del processo di adeguamento, **saranno le scelte del “professionista della privacy” a fare la differenza**. Scelte che vertono essenzialmente sulle dinamiche procedurali come:

- l’individuazione dei responsabili del trattamento in linea con i principi sanciti dall’art. 28 del GDPR e la definizione dei contenuti vincolanti del contratto o di altro atto giuridico;
- la profilazione di eventuali referenti interni per la gestione delle politiche aziendali in materia di protezione dei dati personali;
- la definizione di un sistema di controllo periodico (audit interno) che consenta il costante monitoraggio del livello di compliance con il GDPR;
- la definizione di un piano formativo in grado di armonizzare le competenze interne delle diverse funzioni coinvolte.

Non ci resta che avviarci così a un indispensabile check generale del lavoro svolto fino ad ora, così da poter rilevare e correggere eventuali gap (normativi e applicativi) tra quanto svolto (compreso la redazione della documentazione obbligatoria) e lo spirito (funzionale) del GDPR.

Diritti e doveri. Due facce della stessa medaglia

La richiesta di normalizzazione alle specifiche del Decreto di adeguamento 101/2018 ha messo in difficoltà, almeno in prima istanza, gran parte degli attori coinvolti: le criticità applicative sono però meno invasive di quanto si possa credere. **Quello che la Comunità Europea ha regolamentato (e il nostro Garante ha ribadito) non è altro che la formalizzazione di un'esigenza di tutela resa urgente dalla liquidità che caratterizza il transito di ingenti quantitativi di dati personali, nell'era della "quarta rivoluzione" industriale. Il GDPR ha solo definitivamente chiarito gli obblighi incombenti sul titolare, rafforzando il complesso di garanzie e procedure da osservare minuziosamente nel rapporto con gli interessati, attraverso l'implementazione di procedure finalizzate ad agevolare l'osservanza degli obblighi stabiliti per i responsabili del trattamento dei dati e l'esercizio dei diritti da parte degli interessati** [4].

Si ha spesso una percezione distorta delle procedure, concepite generalmente come qualcosa di rigido e poco funzionale al naturale decorso di vita operativo delle organizzazioni, più o meno complesse. Il GDPR esorta invece a ridisegnare queste procedure, in maniera sartoriale rispetto alle esigenze della propria organizzazione di riferimento, sulla base delle reali necessità esistenti, in modo che esse consentano proattivamente di rispettare i principi previsti dall'art. 5 del GDPR, verificando anche se – pur in caso di assenza di obbligo – non sia utile dotarsi comunque di un DPO (Data Protection Officer o Responsabile per la protezione dei dati personali). **Il DPO, infatti, è un professionista (sia esso soggetto interno o esterno all'organizzazione di riferimento) che deve svolgere una funzione con competenze multidisciplinari e trasversali tra loro, rispetto alle materie trattate.** La sua responsabilità principale è quindi quella di osservare, valutare e organizzare la gestione del trattamento di dati personali (e dunque la loro protezione) all'interno di un'azienda (sia essa pubblica che privata), affinché questi siano trattati nel rispetto delle normative privacy europee e nazionali [5].

Mappatura dei rischi, misure di prevenzione e gestione *data breach*

Come in qualsiasi processo di assessment efficace ed efficiente, non si può prescindere dalla mappatura dei rischi (ex artt. 24 e 32 del GPPR) intesa come strumento di prevenzione e cura da possibili attacchi. Sarà assolutamente necessario (ex artt. 24 e 32 del GPPR):

- individuare i possibili ambiti di rischio che dovranno essere oggetto di valutazione;
- definire la metodologia di analisi dei rischi più adatta alla realtà organizzativa aziendale con particolare riferimento ai sistemi informativi;
- analizzare (per ogni trattamento o per trattamenti simili) sia i rischi connessi ai trattamenti effettuati senza l'utilizzo di strumenti elettronici, che quelli relativi alla configurazione dei sistemi informativi e ai software utilizzati;
- censire le attuali misure di sicurezza organizzative, fisiche e logiche;
- definire le misure di sicurezza necessarie a ridurre il rischio entro un livello di accettabilità (es. pseudonimizzazione, cifratura ecc.);
- verificare tutti gli applicativi adottati e da adottare e avviare politiche di controllo in linea con i principi di privacy by design e privacy by default (art. 25 GDPR);
- etc.

In questa fase è opportuno concentrarsi anche sulle possibili violazioni nel trattamento di dati personali (artt. 33 e 34 GDPR), quindi:

- definire e integrare le procedure di incident management per la gestione dei data breach, in modo da ridurre il più possibile il termine che intercorre tra la violazione e il momento in cui ci si accorge della violazione
- implementare un sistema di file log che consenta la raccolta di tutte le necessarie informazioni a supporto delle violazioni e delle opportune indagini sottostanti;
- impostare il registro delle violazioni;
- definire la modulistica per le notificazioni all'autorità di controllo (art. 33) e le comunicazioni agli interessati (art. 34).

Monitoraggio e controllo

Il principio di *accountability* non prevede più la verifica preliminare da parte dell'autorità di controllo (richiesta in passato prevista dall'art. 17 - oggi abrogato - del nostro Codice), ma diviene indispensabile (ex art. 35 del GDPR):

- individuare, i trattamenti per i quali è necessario effettuare la valutazione d'impatto;
- individuare la metodologia più appropriata da utilizzare per la valutazione d'impatto;
- effettuare la valutazione d'impatto per singoli trattamenti (o per gruppi simili di trattamenti che

presentino rischi analoghi) nonché le necessarie misure tecniche ed organizzative per attenuarli;
- predisporre e conservare la documentazione relativa alla DPIA (Data Privacy Impact Assessment);
- definire le modalità per il monitoraggio e l'eventuale revisione della DPIA.

Ovvio anche che, nel momento in cui le nostre azioni ci sembrano non bastare per minimizzare i rischi di carattere elevato evidenziati nella DPIA, allora si potrà (eccezionalmente) avviare un processo di consultazione preventiva con l'Authority (art. 36 GDPR).

Conclusioni

Le azioni descritte in questo (breve) prontuario sono certamente da accompagnare a letture approfondite del "nuovo" Codice per la protezione dei dati, che dovremo tutti fare. A prescindere da tutto occorre però non dimenticare l'aspetto più importante per la corretta applicazione della normativa europea e cioè: conoscersi e dimostrare di aver provato a mappare con serietà la propria organizzazione, al fine di avviare un percorso sostanziale e non solo formale di adeguamento. La ricetta del perfetto adeguamento può richiedere settimane o mesi o anche anni (a seconda della complessità dell'organizzazione di riferimento) per la sua riuscita, ma l'importante è tener presente che la semplificazione della norma si può raggiungere solo attraverso un'intesa pratica di conoscenza della propria realtà.
Resta solo da chiedersi: avremo tutti il coraggio (o purtroppo anche solo la voglia) di essere "experienced" ossia, di conoscerci davvero fino in fondo?

[1] Questa *famigerata* sospensione di cui si è tanto parlato e scritto prima che il decreto di adeguamento al GDPR venisse finalmente pubblicato in Gazzetta Ufficiale, è stata, effettivamente, suggerita da Camera e Senato, nei rispettivi pareri sullo schema di Decreto di adeguamento, invitando il Governo a valutare la possibilità che il Garante, in una fase transitoria, in ogni caso non inferiore a 8 mesi, successiva all'entrata in vigore del decreto legislativo, non irroghi sanzioni alle imprese, ma disponga ammonimenti o prescrizioni di adeguamento alla nuova disciplina. Raccomandazione, questa, mai tradotta in atto nella redazione del testo definitivo del Decreto (né, peraltro, sarebbe stato diversamente ipotizzabile, data l'evidente antinomia di una eventuale sospensione delle sanzioni rispetto al GDPR, che è fonte sovraordinata al diritto nazionale). Ad alimentare l'equivoco, peraltro, ha contribuito l'ambigua formulazione dell'art. 22 del D.Lgs. 101/2018 che, al comma 13, dispone che per i primi otto mesi dalla data di entrata in vigore del presente decreto, il Garante per la protezione dei dati personali tiene conto, ai fini dell'applicazione delle sanzioni amministrative e nei limiti in cui risulti compatibile con le disposizioni del Regolamento (UE) 2016/679, della fase di prima applicazione delle disposizioni sanzionatorie. La sospensione evidentemente non c'è e le sanzioni amministrative saranno applicate senza alcuna esenzione. Ciò che si raccomanda al Garante, nei primi otto mesi dall'entrata in vigore del Decreto di adeguamento, è, piuttosto, l'impiego di un criterio di bilanciamento nella graduazione delle sanzioni amministrative, attenuandone, eventualmente, la severità, nella misura in cui il disvalore della violazione risulti attenuato dalla complessità del percorso di adeguamento della propria organizzazione al nuovo quadro normativo in materia di protezione dei dati personali. Un percorso che dovrà essere, comunque e necessariamente, avviato, senza ulteriori indugi.

[2] Faq del Garante sul Registro delle attività di trattamento

[3] Dalle già citate Faq del Garante troviamo conferma della generale opportunità di questo adempimento. Chi è tenuto a redigerlo? Tutti i titolari e i responsabili del trattamento sono tenuti a redigere il Registro delle attività di trattamento (v. art. 30, par. 1 e 2 del RGPD). In particolare, in ambito privato, i soggetti obbligati sono così individuabili: imprese o organizzazioni con almeno 250 dipendenti; qualunque titolare o responsabile (incluse imprese o organizzazioni con meno di 250 dipendenti) che effettui trattamenti che possano presentare un rischio – anche non elevato – per i diritti e le libertà dell'interessato; qualunque titolare o responsabile (incluse imprese o organizzazioni con meno di 250 dipendenti) che effettui trattamenti non occasionali; qualunque titolare o responsabile (incluse imprese o organizzazioni con meno di 250 dipendenti) che effettui trattamenti delle categorie particolari di dati di cui all'articolo 9, paragrafo 1 RGPD, o di dati personali relativi a condanne penali e a reati di cui all'articolo 10 RGPD.
Si precisa che le imprese e organizzazioni con meno di 250 dipendenti obbligate alla tenuta del registro potranno comunque beneficiare di alcune misure di semplificazione, potendo circoscrivere l'obbligo di redazione del registro alle sole specifiche attività di trattamento sopra individuate (es. ove il trattamento delle categorie particolari di dati si riferisca a quelli inerenti un solo lavoratore dipendente, il registro potrà essere predisposto e mantenuto esclusivamente con riferimento a tale limitata tipologia di trattamento). Al di fuori dei casi di tenuta obbligatoria del Registro, anche alla luce del considerando 82 del RGPD, il Garante ne raccomanda la redazione a tutti i titolari e responsabili del trattamento, in quanto strumento che, fornendo piena contezza del tipo di trattamenti svolti, contribuisce a meglio attuare, con modalità semplici e accessibili a tutti, il principio di accountability e, al contempo, ad agevolare in maniera dialogante e collaborativa l'attività di controllo del Garante stesso. Si invita altresì a consultare il documento interpretativo del 19 aprile 2018 del Gruppo ex art. 29 (ora Comitato europeo per la protezione dei dati) reperibile al seguente link.

[4] Del resto come ribadito dalla Commissione al Parlamento il regolamento non ha modificato in modo sostanziale i concetti e i principi fondamentali della legislazione in materia di protezione dei dati introdotta nel 1995. La grande maggioranza dei titolari del trattamento e dei responsabili del trattamento che rispettano già le attuali disposizioni dell'UE non dovrà quindi introdurre importanti modifiche nelle proprie operazioni di trattamento dei dati per conformarsi al regolamento (Comunicazione della Commissione al Parlamento Europeo e al Consiglio - Bruxelles, 24.1.2018 COM(2018) - Maggiore protezione, nuove opportunità – Orientamenti della Commissione per l'applicazione diretta del regolamento generale sulla protezione dei dati a partire dal 25 maggio 2018).

[5] E proprio in merito alla figura del DPO, credo sia doveroso richiamare la recente sentenza del TAR Friuli Venezia Giulia n. 287/2018, che ha con autorevolezza affermato il principio della non obbligatorietà (e oserei dire superfluità) delle certificazioni per svolgere questa delicata funzione, sottolineandone la necessaria competenza anche in ambito giuridico. È utile ricordare che al coro di voci negative sulle certificazioni del DPO si è aggiunta anche quella altrettanto autorevole del Comitato europeo per la protezione dei dati (ex art. 68 del GDPR), che già da tempo ha tenuto a precisare in modo lapalissiano nelle Linee guida sulle certificazioni quanto segue: *To further specify what may be certified under the GDPR, the GDPR contains additional guidance. It follows from Article 42.7 that certifications under the GDPR are issued only to data controllers and data processors, which rule out for instance the certification of natural persons, such as data protection officers for example.*