Gianluca Amarù,
Alessandra Fava, Marco Fossi

Privacy in progress

Il trattamento dei dati personali dopo il GDPR con suggerimenti e template per predisporre la documentazione

MANAGEMENT

TOOLS

FrancoAngeli

FrancoAngeli
Edizioni La passione per le conoscenze

Informazioni per il lettore

Questo file PDF è una versione gratuita di sole 20 pagine ed è leggibile con **Adobe Acrobat Reader**

La versione completa dell'e-book (a pagamento) è leggibile **con Adobe Digital Editions**.

Per tutte le informazioni sulle condizioni dei nostri e-book (con quali dispositivi leggerli e quali funzioni sono consentite) consulta **cliccando qui** le nostre F.A.Q.

MANAGEMENT TOOLS

Visioni, esperienze, metodologie per potenziare competenze e capacità: proprie e dei collaboratori

---

Management Tools offre a tutti i professional (e agli imprenditori) testi precisi, puntuali, agili e innovativi. Scritti appositamente da consulenti qualificati, i volumi affrontano tutte le aree e i temi di rilievo per valorizzare le competenze e indirizzare al successo le organizzazioni.

Gianluca Amarù,
Alessandra Fava, Marco Fossi

Privacy in progress

Il trattamento dei dati personali dopo il GDPR con suggerimenti e template per predisporre la documentazione

FrancoAngeli
TOOLS

Progetto grafico di copertina di Elena Pellegrini

Indice

Parte terza – GDPR e nuove tecnologie

Parte quarta – *How to* i contenuti e i modelli dei documenti

Introduzione

Dopo tre anni dall'entrata in vigore nel maggio 2018 del Regolamento Europeo n. 679 del 2016, detto *General Data Protection Regulation* (GDPR), la parola privacy è diventata un termine di uso quotidiano. A fronte dell'inarrestabile sviluppo tecnologico, la protezione dei dati diventa un sistema dinamico, sollecitato anche da continui provvedimenti e nuove Linee Guida degli organi competenti.

Dopo le Linee Guida sui cookie del Comitato Europeo EDPB, le Linee Guida e le Faq del Garante per la protezione dei dati personali italiano in materia di videosorveglianza, di cookie e di microprofilazione, e ancora dopo l'abrogazione del Privacy Shield da parte della Commissione Europea a seguito della sentenza della Corte di Giustizia, è evidente la lotta quotidiana degli organismi nazionali ed europei per difendere i diritti in rete e garantire la protezione dei dati dei cittadini europei. Mentre scriviamo la Commissione Europea ha rilasciato ad aprile la bozza sull'uso dell'Intelligenza Artificiale (AI) e lavora ad altri due regolamenti che influiranno molto sui big del web, il commercio digitale e le piattaforme di marketing online, banalmente su tutte le aziende che fanno e-commerce: parliamo del Digital Services Act e del Digital Markets Act, previsti per il 2024.

Il volume offre uno spaccato di argomenti e temi recentissimi che impattano in maniera considerevole sul trattamento dei dati personali. Siccome la compliance al GDPR ed alle altre normative italiane si traduce anche nell'elaborazione di diversi documenti, abbiamo ritenuto utile fornire, nell'ultima parte del libro, i template di tutti i documenti privacy utili per un'azienda, dalle informative alle richieste di consenso, dalle lettere di nomina ad Incaricati e Responsabili, fino al modello del registro dei trattamenti del Titolare e del Responsabile, il contenuto di una DPIA e le indicazioni su come redigere le policy aziendali. Sono suggerimenti offerti nella consapevolezza che l'impegno per raggiungere la piena compliance debba essere continuo e costantemente "in progress".

Marco Fossi

Parte prima

1. Il GDPR 2016/679, i principi fondamentali e le novità rispetto alla disciplina preesistente

1.1. Premessa

Il GDPR (o Regolamento UE 2016/679 relativo alla protezione delle persone fisiche, con riguardo al trattamento dei dati personali e alla libera circolazione dei dati stessi) presenta alcune novità dirompenti rispetto alla precedente normativa contenuta nel Decreto Legislativo n. 196/2003 (il Codice della privacy). Già ad una prima lettura è possibile rilevare un approccio differente alla materia fondato sul principio dell'*accountability*, cioè il fatto che il Titolare del trattamento debba essere in grado di provare, dar contezza del suo adeguamento alla normativa. Un approccio basato sull'affidabilità del soggetto, sull'ottemperanza a disposizioni e sull'elaborazione della documentazione privacy. Troviamo però anche i concetti di *privacy by design* e *privacy by default,* l'introduzione della figura del *Data Protection Officer* (DPO), le sanzioni pecuniarie pesantissime in caso di violazioni o di irregolarità nel trattamento dei dati personali, una più forte tutela dei diritti degli Interessati, una miglior formulazione del diritto di cancellazione dei dati (vale a dire la possibilità per l'Interessato di chiedere l'eliminazione di dati che lo riguardano fino al diritto all'oblio sul web), l'introduzione del diritto alla portabilità dei dati.

1.2. La precedente normativa in materia di trattamento dei dati personali e la nascita del GDPR

In materia di trattamento dei dati personali l'Italia era da tempo dotata di una disciplina capace di garantire i diritti degli Interessati: la **prima legge sul trattamento dei dati personali risale al 1996, la n. 675**. Quest'ultima era a sua volta stata emanata in adempimento alle disposizioni di una **Direttiva Europea (95/46/CE)** che imponeva agli stati membri della Comunità di adottare delle norme a tutela ed a garanzia dei dati personali.

Al momento dell'entrata in vigore la legge 675/96 generò qualche allarme. Si trattava di una normativa molto tecnica e precisa che introduceva principi innovativi. Molti si chiedevano se chiunque avesse detenuto dati personali (anche la classica "rubrica telefonica"), avrebbe dovuto rispettare tutti gli obblighi previsti dalla legge. La legge 675/96 subì nel corso degli anni modificazioni e semplificazioni che condussero, nell'anno 2003, alla nascita del **Decreto Legislativo n. 196, chiamato anche *Testo Unico o Codice della privacy***. Il "Codice" raccoglieva l'eredità della vecchia 675/96 con le modifiche e correzioni che nel frattempo si erano andate stratificando ed incorporava i principi enunciati dal Garante ovvero quelli rintracciabili nella giurisprudenza formatasi dall'anno 1996 all'anno 2003.

In realtà l'utilizzo del termine *privacy* è improprio. Lo era già nel 1996, così nel 2003 e lo è ancora di più col nuovo Regolamento Europeo n. 679 del 2016. Improprio perché la parola *privacy* viene immediatamente ricondotta al concetto di riservatezza personale, concetto spesso collegato a un comportamento di diniego: non si può dare una data informazione "perché c'è la privacy". Quindi, se convenzionalmente facciamo riferimento alla Normativa sulla privacy, più correttamente si dovrebbe parlare di Normativa in materia di tutela del dato personale e con il Regolamento Europeo anche di libera circolazione del dato personale. Tanto è vero che il Garante Privacy italiano all'inizio del 2021 ha mutato il suo nome in Garante per la Protezione dei Dati Personali (GPDP), anche se il sito web continua ad essere garanteprivacy.it per economia.

Già dopo pochi anni dall'entrata in vigore del D.Lgs. 196/2003 (Codice della privacy), si era avvertita l'esigenza di superare la normativa italiana ed offrire un *corpus* di norme che garantisse la tutela del dato personale in modo uniforme in ogni Paese della Comunità Europea. Infatti a questo proposito il Trattato firmato a Lisbona il 13 dicembre 2007, composto dal Trattato dell'Unione Europea (TUE) e dal Trattato sul Funzionamento dell'Unione Europea (TFUE), aveva riconosciuto la protezione dei dati personali come diritto fondamentale dei cittadini meritevole di uguale tutela in ogni territorio dell'Unione.

Tutto ciò ha condotto all'**abrogazione della direttiva 95/46/CE**, che aveva dato origine alla prima legge sulla privacy del 1996, ed ha determinato la nascita del **nuovo Regolamento (679/2016) del Parlamento Europeo e del Consiglio (GDPR)**, che ha previsto – per tutti gli Stati dell'Unione Europea – regole comuni per assicurare nei Paesi dell'Unione un livello adeguato e uniforme di tutela dei dati personali, ma anche la loro libera circolazione, similmente a quanto era accaduto per la libera circolazione delle persone prevista dal Trattato di Schengen.

Il Regolamento Europeo n. 679 del 2016, chiamato GDPR, entrato in vigore in tutti i Paesi europei il 25 maggio del 2018, riguarda esclusivamente i dati personali relativi a persone fisiche. Quindi non si interessa dei dati delle

persone giuridiche, delle imprese, delle società, degli enti, delle associazioni, dei professionisti. Sebbene, questi ultimi siano elementi meritevoli di tutela e di rilievo da qualsiasi punto di vista (non ultimo quello della sicurezza aziendale), sono estranei al GDPR che ha come scopo di tutelare solo i dati personali delle persone fisiche.

1.3. Il concetto di "dato personale" e di "trattamento dei dati" nel GDPR

È opportuno, a questo punto, definire che cosa sia un **dato personale**. Il GDPR all'articolo 4 (comma 1) dice che: *"dato personale: è qualsiasi informazione riguardante una persona fisica identificata o identificabile ("Interessato") e si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento ad un identificativo come un nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale"*.

Le norme del GDPR devono essere applicate a ogni **trattamento di dati personali** che riguardano appunto persone fisiche. A questo punto ci si può chiedere che cosa sia un trattamento: è qualsiasi operazione o un insieme di operazioni che possono essere compiute sia con strumenti automatizzati che non automatizzati, quindi anche un trattamento cartaceo, che riguardano la raccolta di dati personali, la registrazione, la conservazione, l'estrazione, la consultazione, la trasmissione e anche la cancellazione. Se ad esempio ho una banca dati che mi viene messa a disposizione da terzi e provvedo a cancellare dei dati, anche questa sola attività è un'operazione di trattamento dei dati, per cui deve essere regimentata dal GDPR. Anche le immagini che ritraggono una persona costituiscono dati personali, così anche gli web cookie.

Possiamo concludere come il GDPR sia una produzione normativa e sovranazionale dell'Unione Europea, uguale per tutti gli stati membri, che disciplina il trattamento dei dati personali di persone fisiche, fornendo regole per la tutela degli stessi, al fine di consentire sia il trattamento che la circolazione dei dati in maniera sicura.

1.4. Le novità del GDPR rispetto alla precedente normativa italiana

a) Misure di sicurezza

Le novità del GDPR rispetto alla normativa italiana preesistente, quindi rispetto al Codice, sono molteplici: la prima e forse quella che balza meno agli

occhi, ma è la più importante dal punto di vista organizzativo per le aziende, è quella che riguarda **le misure di sicurezza**. Con il Codice 196/2003 l'approccio era diverso: allora il Titolare del trattamento era guidato "*per mano*" da una normativa che disciplinava anche gli aspetti tecnici, perché indicava, ad esempio, all'interno dell'allegato B del D.Lgs. 196/2003, quelle che erano le misure di sicurezza **minime***,* sotto le quali non si poteva scendere, misure che venivano considerate un *minimum* per garantire un'adeguata o sufficiente tutela. Con l'adozione del Regolamento Europeo si registra un cambio di mentalità e di approccio: il legislatore europeo non impone più misure di sicurezza minime, ma **misure di sicurezza "*adeguate*" rispetto alle finalità che persegue il Titolare e rispetto alla tipologia di dati trattati** (ad esempio se si tratta di dati particolari come quelli sanitari o genetici o relativi a condanne penali, i cosiddetti *ex-dati sensibili* della precedente normativa, o atti giudiziari, devono essere attivate misure di sicurezza di rango più elevato). Quindi, mentre prima era possibile osservare le misure minime di sicurezza utilizzando regole preconfezionate e codificate, ora invece le misure di sicurezza di qualsiasi rango, sia quelle fisiche (come le porte chiuse a chiave, gli archivi o gli scaffali chiusi a chiave, la separazione dei dati particolari da quelli ordinari) o le misure di tipo logico- informatico (quindi la sicurezza delle reti, delle connessioni internet etc), o le misure di sicurezza di tipo organizzativo, non sono più codificate ma sono rimesse a un giudizio di adeguatezza che viene fatto *ex ante* dal Titolare del trattamento, in qualità di '*proprietario*' della banca dati. In buona sostanza è il Titolare del trattamento il soggetto che deve stabilire se le misure che ha adottato siano o meno adeguate rispetto ai trattamenti che sta realizzando. Successivamente potrebbe essere realizzata anche una valutazione *ex post;* ad esempio qualora vi sia un'ispezione o un'attività di accertamento da parte dell'Autorità di Controllo, vale a dire il Garante per la protezione dei dati personali. Ovviamente alle aziende diamo l'antico consiglio: *meglio prevenire che curare*.

b) ***Accountability***

Altro elemento di novità del GDPR è l'introduzione del principio dell'***accountability***, tradotto in italiano con il termine Principio di responsabilizzazione. Anche questa, come tante traduzioni operate dal testo originario del GDPR, non è molto felice perché fa riferimento solamente alla responsabilizzazione: cioè è il Titolare ad essere responsabile di qualsiasi conseguenza che derivi dal trattamento dei dati, ma anche di qualsiasi scelta, sia la scelta della nomina dei propri collaboratori interni ed esterni, sia la scelta delle misure di sicurezza, della finalità, della durata della conservazione dei dati. Il Titolare è responsabile praticamente di tutto, come vedremo in seguito. In realtà il termine inglese è un po' più ricco di sfumature. *Accountability* è anche dare contezza in qualsiasi momento a chiunque lo richieda di quello che si sta facendo. Non è più tollerabile l'atteggiamento del Titolare del trattamento

che, interpellato su qualche aspetto dell'attività di trattamento di dati personali che sta realizzando, non sia in grado di rispondere in tempi brevi, non sappia neanche quali misure di sicurezza abbia attivato o come sia strutturato il suo "sistema privacy", che, – come previsto dal Regolamento Europeo – è stato da lui creato. *Accountability* ha dunque anche un'accezione positiva nel senso di affidabilità e credibilità del Titolare. Infatti il GDPR introduce l'esortazione a ricorrere a certificazioni di qualità per chi realizzi trattamenti di raccolta di dati personali.

c) *Privacy by design* e *privacy by default*

Parlando di sistema privacy, introduciamo la terza novità del GDPR che è quella della ***privacy by design* e *privacy by default***. Anche in questo caso nella traduzione si perde qualcosa, a causa del solito *lost in translation*. Il principio è che il Titolare del trattamento quando si trovi a realizzare qualsiasi attività commerciale, organizzativa, strutturale che comporti un trattamento di dati personali, deve preoccuparsi delle ricadute e delle conseguenze sul trattamento dei dati *by design*, quindi sin dalla fase di progettazione. Il sistema privacy non deve essere qualcosa di posticcio che viene appiccicato dopo, o analizzato in coda. Il Titolare del trattamento virtuoso, o meglio a norma, allorquando introduca dei nuovi prodotti o servizi – ad esempio una nuova app o un nuovo software o voglia offrire un prodotto commerciale a una tipologia di clientela privata ed abbia necessità di entrare in contatto e raccogliere dati di persone fisiche – deve aver preventivamente valutato e garantito la sicurezza dei dati personali che andrà a trattare ed aver espletato tutte le attività necessarie a questo fine. Quindi il Titolare deve anche pianificare le regole e le misure di protezione, verificando la compatibilità delle stesse con il sistema privacy già attuato, affinché tutto sia rispettoso conforme (*compliant)* alle norme.

Dopo che si è fatto questo, si procede *by default* cioè con regole che il Titolare ha predefinito già in fase di progettazione secondo il Regolamento Europeo. In pratica il Titolare non può improvvisare all'ultimo momento, magari correndo ai ripari avendo già iniziato un'attività di trattamento dei dati senza averla normata. Il Titolare è tenuto invece a valutare in fase di progettazione anche l'impatto che avrà il nuovo progetto sui dati personali e quindi fare verifiche periodiche al sistema.

d) *Data breach*

Un'altra novità è il ***data breach*** dell'articolo 4 (comma 12): *"violazione dei dati personali: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati trasmessi, confermati o comunque trattati"*.

Il legislatore specifica che si può verificare una violazione della sicurezza accidentale per colpa o per dolo. Anche qui ci imbattiamo in un altro termine anglosassone che in italiano si traduce come *violazione dei dati* e qualcosa si perde anche in questo caso. Il *data breach* non è semplicemente una violazione, una perdita di dati, è piuttosto la perdita della sicurezza di quel dato, è una **breccia** in quella banca dati, in quella raccolta di dati o in quel dato particolare, che potrebbe essere corrotto, modificato, distrutto, cancellato, oppure rivelato a soggetti terzi o diffuso a un pubblico indefinito.

La norma sull'eventualità di un *data breach* si è resa necessaria dopo gli scandali internazionali relativi a violazioni di banche dati e non era prevista dalla vecchia normativa. Si è voluto disciplinare in maniera cogente questo aspetto per evitare che il dato personale, che ha una particolare importanza anche dal punto di vista economico, possa essere oggetto di attacchi o comunque di finalità illecite. Il dato è diventato nell'ultimo decennio un bene prezioso anche dal punto di vista economico, non solo giuridico, qualcuno lo definisce l'oro del XXI secolo. Basti pensare a tutti i *data breach* che hanno coinvolto multinazionali, piattaforme social, banche, assicurazioni, o agli scandali per l'utilizzo illecito di dati che sono stati usati per finalità diverse da quelle per le quali erano stati raccolti o senza un'adeguata informazione dell'utente.

Attraverso le norme sul *data breach* si vogliono tutelare i dati nel caso di un'eventualità nefasta. Prima di tutto ci dovrebbero essere misure di sicurezza per evitare possibili violazioni, ma sappiamo che i sistemi non sono mai del tutto e per sempre sicuri – anche la Nasa viene sottoposta ad attacchi – non esiste per definizione la **sicurezza assoluta** di un sistema: vi è l'obsolescenza, sia dell'hardware che del software, e la nascita di nuovi strumenti in grado potenzialmente di aggirare anche le migliori misure di sicurezza.

Qualora si verifichi un *data breach* e qualcuno riesca a superare le nostre misure di sicurezza e vengano colpiti dei dati personali, il Titolare del trattamento è obbligato a notificare questa violazione al Garante **entro 72 ore** dall'evento. Se l'evento ha anche impatto sugli Interessati del trattamento, quindi i soggetti a cui i dati si riferiscono, la norma richiede che anche questi soggetti Interessati siano messi al corrente dell'avvenuto *data breach* con modalità adeguate. Se abbiamo un largo pubblico di Interessati, potrebbe non bastare una comunicazione con email, ma essere necessaria la pubblicazione di una pagina su un quotidiano.

e) Sanzioni

Altra novità è il **sistema delle sanzioni**. In ipotesi di inosservanza degli obblighi previsti dal Regolamento, le sanzioni amministrative sono molto più onerose del passato. Si va da sanzioni fino a 10 milioni di euro o fino al 2 per cento del fatturato mondiale dell'anno precedente quando sono violati obblighi come ad esempio l'inosservanza del principio della *privacy by de-*

sign oppure le norme in materia di *data breach* ad esempio se accade una violazione della banca dati e non viene comunicata al Garante. Queste sono le sanzioni più lievi. Altre sanzioni arrivano anche a 20 milioni di euro o al 4 per cento del fatturato mondiale dell'anno precedente, quando vengono violati i principi fondamentali del trattamento, ad esempio quello di dare l'informativa per ogni trattamento dei dati che faccio, acquisire il consenso nei casi in cui sia necessario; quando non soddisfo le richieste dell'Interessato, magari mi chiede o la cancellazione dei dati o semplicemente un riscontro o si vuole sapere quali dati si stanno trattando come Titolare del trattamento e non venga data risposta entro 30 giorni. Oppure quando si violino le disposizioni in materia di trasferimento dei dati verso Paesi terzi. Sul punto si ricorda al lettore come la Corte di Giustizia dell'Unione Europea – con la sentenza nella causa C-311/18 del 16 luglio 2020 – abbia invalidato il Privacy Shield, ovvero l'accordo largamente diffuso con cui grandi organizzazioni e multinazionali potevano – fino a quel momento – legittimare il trasferimento di dati personali tra Europa e Stati Uniti.

f) Diritti degli Interessati

Sempre nell'ambito di questo nuovo assetto dato dal Regolamento UE, è stato codificato o meglio precisato il **diritto degli Interessati**. Anche questo è frutto dell'esperienza, quindi di situazioni che si sono verificate nella vita di tutti i giorni allorquando persone che avevano commesso reati, anche a distanza di molti anni venivano citati in rete in documenti o articoli reperibili da un qualunque motore di ricerca. Quindi a corollario del diritto degli Interessati si è dato maggior risalto al **diritto all'oblio e/o alla cancellazione dei dati personali** che significa procedere anche alla deindicizzazione delle ricerche sui motori web**,** quando un Interessato lo richieda. È opportuno specificare che questi ultimi due diritti non possono essere sempre esercitati integralmente, ad esempio non possono essere esercitati quando sia presente un obbligo di conservazione dei dati previsto da disposizioni normative di qualunque autorità oppure l'argomento sia giudicato ancora di attualità. In ogni caso, ogni dato personale deve essere conservato per il tempo necessario a soddisfare la finalità per il quale è stato raccolto o trattato e non può pertanto essere conservato in eterno. Infatti il principio generale da osservare è che, venute meno le finalità della conservazione, salvo sussistano obblighi normativi, amministrativi, fiscali o sia necessario conservare l'informazione perché sto esercitando un diritto o mi sto difendendo in giudizio, si debba cancellare il dato o renderlo anonimo.

Dalla lettura integrale dell'articolo 4 del Regolamento (UE) 2016/679, uno dei più importanti del GDPR, si vede come la limitazione del trattamento sia un aspetto importante. In pratica in qualsiasi momento il soggetto Interessato dal trattamento può intervenire per limitarne l'uso.