

VADEMECUM

GENNAIO 2018

GDPR PRIME NORME DI ADEGUAMENTO

GUIDA ALLE NOVITÀ IN TEMA DI PROTEZIONE DEI DATI PERSONALI



A CURA DEL TEAM PRIVACY
DEL DIGITAL&LAW DEPARTMENT -
STUDIO LEGALE LISI

INDICE

PREMESSE.....	3
IL “NUOVO” RESPONSABILE DEL TRATTAMENTO.....	4
RIUTILIZZO DEI DATI SENSIBILI SENZA CONSENSO: UNA NORMA CHE PROTEGGE I DATI PERSONALI O GLI INTERESSI DEI BIG DEL DIGITALE?	6
LE NOVITÀ INTRODOTTE DALLA LEGGE DI BILANCIO 2018 E NUOVI POTERI AL GARANTE PRIVACY	7
L’OBBLIGO DI COMUNICAZIONE PREVENTIVA DEL TRATTAMENTO BASATO SULL’INTERESSE LEGITTIMO E CIÒ CHE RESTA DELL’ <i>ACCOUNTABILITY</i>	8
COSA CAMBIA IN PRATICA CON L’OBBLIGO DI COMUNICAZIONE PREVENTIVA DEL TRATTAMENTO	11

PREMESSE

La cosiddetta “**Legge di bilancio**” 2018, n. 205 del 27 dicembre 2017, introduce diverse novità in tema di privacy, nell’ottica di **adeguare** la disciplina del nostro **Codice in materia di protezione dei dati personali (D. Lgs. n. 196/2003)** a quanto previsto dal **Regolamento UE 2016/679 (General Data Protection Regulation - GDPR)**, le cui norme – com’è noto - saranno direttamente applicabili nel nostro ordinamento dal 25 maggio 2018.

Ma tali novità **sono solo le ultime, in ordine di tempo**, con cui il nostro Legislatore si è recentemente occupato dell’adeguamento della normativa nazionale al Regolamento al GDPR. Ci si riferisce alla **Legge 25 ottobre 2017, n. 163 (c.d. Legge di delegazione europea 2016-2017)**¹ e alla **Legge 20 novembre 2017, n. 167 (c.d. Legge europea 2017)**, la prima contenente delega al Governo per l’adozione di uno o più decreti legislativi al fine di adeguare il quadro normativo nazionale alle disposizioni del Regolamento UE 2016/679 sulla protezione delle persone fisiche con riguardo al trattamento dei dati personali, la seconda direttamente modificativa del D. Lgs. 196/2003 (Codice per la protezione dei dati personali): entrambe emanate ai fini dell’armonizzazione della normativa nazionale al GDPR.

Ancora una volta, dunque, a distanza di poche settimane dai recenti interventi di coordinamento e modifica delle norme in materia protezione dei dati personali², **il Legislatore torna ad occuparsi dell’adeguamento al Regolamento UE 2016/679.**

¹ Questa, in particolare, ha previsto i princìpi e criteri direttivi specifici che il Governo dovrà seguire nell’esercizio della delega parlamentare. In particolare:

a) abrogare espressamente le disposizioni del codice in materia di trattamento dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196, incompatibili con le disposizioni contenute nel regolamento (UE) 2016/679;

b) modificare il codice di cui al decreto legislativo 30 giugno 2003, n. 196, limitatamente a quanto necessario per dare attuazione alle disposizioni non direttamente applicabili contenute nel regolamento (UE) 2016/679;

c) coordinare le disposizioni vigenti in materia di protezione dei dati personali con le disposizioni recate dal regolamento (UE) 2016/679;

d) prevedere, ove opportuno, il ricorso a specifici provvedimenti attuativi e integrativi adottati dal Garante per la protezione dei dati personali nell’ambito e per le finalità previsti dal Regolamento (UE) 2016/679.

Il piano di riordino previsto dal Parlamento dovrà essere portato a compimento entro sei mesi dalla data di entrata in vigore della Legge di delegazione europea.

² In argomento, si rinvia all’analisi sviluppata da Andrea Lisi [nell’editoriale della rivista scientifica KnowIT](#)

IL “NUOVO” RESPONSABILE DEL TRATTAMENTO

In ogni caso la Legge 167/2017, con il suo art. 28, ha modificato l'art. 29 del Codice, introducendo un nuovo comma (il comma 4 bis) e sostituendo il comma 5 dello stesso articolo. Il nuovo art. 29 del Codice, quindi, avrà questa nuova formulazione:

“Art. 29. Responsabile del trattamento

1. Il responsabile è designato dal titolare facoltativamente.

2. Se designato, il responsabile è individuato tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.

3. Ove necessario per esigenze organizzative, possono essere designati responsabili più soggetti, anche mediante suddivisione di compiti.

4. I compiti affidati al responsabile sono analiticamente specificati per iscritto dal titolare.

4-bis. Fermo restando quanto previsto ai commi 1, 2, 3 e 4, il titolare può avvalersi, per il trattamento di dati, anche sensibili, di soggetti pubblici o privati che, in qualità di responsabili del trattamento, forniscano le garanzie di cui al comma 2. I titolari stipulano con i predetti responsabili atti giuridici in forma scritta, che specificano la finalità perseguita, la tipologia dei dati, la durata del trattamento, gli obblighi e i diritti del responsabile del trattamento e le modalità di trattamento; i predetti atti sono adottati in conformità a schemi tipo predisposti dal Garante.

5. Il responsabile effettua il trattamento attenendosi alle condizioni stabilite ai sensi del comma 4-bis e alle istruzioni impartite dal titolare, il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni di cui al comma 2, delle proprie istruzioni e di quanto stabilito negli atti di cui al comma 4-bis.”

Il tentativo legislativo di coordinare la figura interna ed esterna di Responsabile del trattamento sembra evidente, ma il risultato lascia forse un po' a desiderare dal punto di vista della chiarezza e della sintesi³.

In effetti, circa la nuova formulazione dell'art. 29 del D. Lgs. 196/2003, relativamente alla **compatibilità della figura del Responsabile interno del trattamento**, occorre chiarire che questa risulta **attualmente ancora configurabile**, in astratto, anche in base alle nuove disposizioni, **sebbene le modifiche risultino delineare una figura più coerente con quella di Responsabile esterno**, e decisamente **più in linea con la figura di Responsabile del trattamento disciplinata nel GDPR**.

In argomento, inoltre, occorre considerare che la figura del Responsabile interno del trattamento dei dati (anche a seguito delle modifiche appena introdotte) risulta assumere – almeno in parte - dei connotati che nella prassi applicativa di molti soggetti privati e pubblici, nel nostro ordinamento, sembra avvicinarsi notevolmente a quanto il Regolamento 2016/679/EU prevede per la diversa (e delicata) figura del DPO (Data Protection Officer o Responsabile della protezione dei dati personali). In effetti, il DPO, contrariamente a quanto sembra delineare il GDPR per il ruolo del Responsabile del trattamento, innanzitutto può essere

³ In argomento, “GDPR, quanti pasticci nella legge europea 2017: ecco cosa rischia l'Italia”, di A. Lisi, su www.agendadigitale.eu

anche un dipendente del Titolare (e quindi essere individuato all'interno dell'organizzazione di riferimento)⁴, inoltre deve essere designato *“in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di cui all'articolo 39”* dello stesso GDPR (art. 37), similmente a quanto richiesto al comma 2 dell'art. 29 del D.Lgs. 196/2003 per il nostro Responsabile del trattamento. Ma è soprattutto in riferimento ad alcuni dei compiti elencati per il DPO all'art. 39 del GDPR, e in particolare alla lett. b)⁵, che si colgono le forti analogie con il ruolo del Responsabile interno al trattamento.

Tuttavia, è utile sgombrare il campo da ogni possibile equivoco e chiarire che **la figura del DPO deve essere tenuta ben distinta da quella del Responsabile del trattamento**, così come delineata dal Regolamento 2016/679/EU.

In effetti, il DPO (Data Protection Officer o Responsabile della protezione dei dati, da non confondere appunto con il Responsabile del trattamento) è una figura che assume un ruolo consultivo di supporto al Titolare o al Responsabile del trattamento. Diversamente da quest'ultimo, infatti, non ha margini decisionali in merito all'espletamento delle attività di trattamento (rimessi invece totalmente al Titolare o al Responsabile); il Responsabile del trattamento, in particolare, riceve sì le istruzioni dal Titolare, ma ha indubbiamente spazi di autonomia a cui il GDPR ricollega infatti eventuali profili di responsabilità, ai sensi dell'art. 82.

In tal senso, appare utile evidenziare che la verifica e il controllo del rispetto delle norme in materia di *data Protection* non comporta anche una responsabilità personale del DPO, in caso di non conformità dei trattamenti di dati personali posti in essere dal Titolare o dal Responsabile del trattamento. D'altronde, sempre nel Regolamento si chiarisce che è il Titolare - e non il DPO - il soggetto tenuto ad *“adottare misure tecniche e organizzative per garantire e per essere in grado di dimostrare che il trattamento viene eseguito in conformità del presente regolamento”* (art. 24).

⁴ Diversamente da quanto previsto dall'art. 28 del GDPR sul Responsabile del trattamento dei dati, la cui formulazione, al contrario di quella dell'art. 37 sul DPO, sembra non contemplare che tale ruolo possa essere ricoperto da un dipendente, ma disciplinato *“da un contratto o da altro atto giuridico”*.

⁵ *“Sorvegliare l'osservanza del presente regolamento, di altre disposizioni dell'unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e a formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo”*.

RIUTILIZZO DEI DATI SENSIBILI SENZA CONSENSO: UNA NORMA CHE PROTEGGE I DATI PERSONALI O GLI INTERESSI DEI BIG DEL DIGITALE?

Accanto a questa importante novità, nella c.d. nuova Legge europea 2017 (Legge 20 novembre 2017, n. 167) hanno fatto molto discutere⁶ le previsioni che modificano il Codice in materia di protezione dei dati e ricerca⁷. In particolare, viene introdotto l'art. 110 bis al D. Lgs. n. 196/2003, **prevedendo la possibilità, per scopi statistici e di ricerca scientifica, di riutilizzo dei dati personali, anche sensibili** (ad esclusione di quelli genetici), a condizione che siano adottate **forme preventive di minimizzazione e di anonimizzazione dei dati** ritenute idonee a tutela degli interessati, **previa autorizzazione del Garante**. Sinceramente la genericità di questa disposizione lascia sconcertati poiché gli scenari che essa sembra prefigurare appaiono piuttosto inquietanti. Se, infatti, i dati devono essere previamente anonimizzati non si comprende che senso abbia prevedere l'autorizzazione del Garante, visto che tali dati non dovrebbero essere più riconducibili ai singoli interessati (e quindi potenzialmente lesivi per i diritti fondamentali degli stessi).

Inoltre, non si specifica a chi spetti l'anonimizzazione di questi dati sensibili e in che punto del processo di riutilizzo debba essere effettuata, se *ex ante* o *ex post* rispetto all'autorizzazione del Garante. Non da ultimo, non è chiaro chi sia il soggetto sotto la cui responsabilità ricada l'onere di anonimizzazione di tali dati sensibili, se della struttura cedente (magari un'azienda sanitaria) o di una multinazionale IT che li riceve.

Infine, questa norma - nella sua formulazione poco chiara e troppo generica per non determinare un ventaglio interpretativo eccessivamente ampio per una materia così delicata - dimentica di citare i diritti fondamentali dell'individuo che costituiscono un presupposto di qualsiasi cessione senza consenso di dati sensibili (e ancor di più di quelli sanitari) per scopi scientifici.

⁶ Si veda, in proposito, l'articolo di A. Lisi nel suo [Blog per le pagine de Il Fatto Quotidiano](#)

⁷ Al capo III del titolo VII della parte II, dopo l'articolo 110 è aggiunto il seguente:

«Art. 110-bis. (Riutilizzo dei dati per finalità di ricerca scientifica o per scopi statistici). - 1. Nell'ambito delle finalità di ricerca scientifica ovvero per scopi statistici può essere autorizzato dal Garante il riutilizzo dei dati, anche sensibili, ad esclusione di quelli genetici, a condizione che siano adottate forme preventive di minimizzazione e di anonimizzazione dei dati ritenute idonee a tutela degli interessati.

2. Il Garante comunica la decisione adottata sulla richiesta di autorizzazione entro quarantacinque giorni, decorsi i quali la mancata pronuncia equivale a rigetto. Con il provvedimento di autorizzazione o anche successivamente, sulla base di eventuali verifiche, il Garante stabilisce le condizioni e le misure necessarie ad assicurare adeguate garanzie a tutela degli interessati nell'ambito del riutilizzo dei dati, anche sotto il profilo della loro sicurezza».

LE NOVITÀ INTRODOTTE DALLA LEGGE DI BILANCIO 2018 E NUOVI POTERI AL GARANTE PRIVACY

Alcune delle innovazioni di maggiore interesse recentemente introdotte sono sicuramente ravvisabili nei commi da 1020 a 1025, art. 1, della Legge di bilancio 2018, che definiscono – tra l'altro - i compiti e i poteri spettanti all'Autorità Garante per la protezione dei dati personali nel quadro della disciplina europea e in vista della sua diretta applicazione, a partire dal 25 maggio prossimo.

Questa (ennesima) serie di previsioni è introdotta dal richiamo espresso al Regolamento 2016/679, che rappresenta (o dovrebbe rappresentare) la **cornice normativa destinata a circoscrivere l'esercizio dei poteri attribuiti al Garante**, confermando il ruolo chiave dell'Autorità nell'assicurare la **tutela dei diritti e delle libertà fondamentali dei cittadini** in materia di trattamento dei dati personali e la libera circolazione degli stessi.

Inoltre, sono state stilate una serie di indicazioni operative destinate all'Autorità Garante, da cui derivano, peraltro, ricadute non indifferenti sul Titolare del trattamento, come definito all' articolo 4, paragrafo 7 del GDPR.

In particolare, nella Legge di bilancio 2018 viene dato mandato all'Autorità di adottare, nel termine di due mesi dall'entrata in vigore della Legge di bilancio⁸, un provvedimento che disciplini le modalità atte alla verifica, da parte della stessa Autorità, della corretta applicazione del GDPR, anche attraverso un costante scambio di informazioni con il Titolare del trattamento. Le verifiche dell'Autorità dovranno essere particolarmente permeanti, specialmente con riferimento ai **dati personali trattati per via automatizzata o tramite tecnologie digitali** – ossia, in pratica, circa la quasi totalità dei trattamenti – e all'**adeguatezza delle infrastrutture per l'interoperabilità dei formati** utilizzati dal Titolare per mettere a disposizione i dati ai soggetti interessati, in linea con quanto disposto dall'art. 20 GDPR ("*Diritto alla portabilità dei dati*") e, in generale, per adempiere tempestivamente al rinnovato scenario normativo.

A prescindere dalla coerenza con il GDPR, per l'espletamento dei compiti assegnati all'Autorità Garante è stabilito uno stanziamento pari a 2 milioni di euro annui, a partire dal 2018, a cui si aggiunge l'incremento del fondo destinato alle spese di funzionamento del Garante (ex art. 156, comma 10, D. Lgs. 196/2003) per un importo pari a 4 milioni di euro, finalizzati all'attuazione del GDPR (comma 1162). Entrambi gli stanziamenti, comunque si interpretino le norme da cui traggono giustificazione, appaiono sicuramente più in linea con uno spirito votato all'evoluzione digitale, rispetto alla tristemente nota "clausola di invarianza finanziaria", sistematicamente inserita in chiusura dei più recenti testi normativi in materia di digitalizzazione e privacy: la realizzazione degli obiettivi di crescita digitale, nel settore pubblico e in quello privato, è di importanza vitale sia per il progresso del Paese, ma altresì per andare di pari passo con gli standard europei. Per questo, è da accogliere con favore lo **stanziamento di risorse finanziarie che diano impulso alla digitalizzazione**, per mezzo della Legge di bilancio⁹.

⁸ Ossia, entro il 28 febbraio 2018.

⁹ Risulta pregevole, in particolare, la presenza di stanziamenti destinati alla digitalizzazione delle amministrazioni statali, mediante il rifinanziamento del fondo ex art.1, comma 140, della legge 11 dicembre 2016, n. 232, il cui ammontare, tuttavia, non appare ben chiaro secondo la formulazione del comma 1072: il finanziamento, infatti, viene inserito in un "calderone", contenente voci di spesa estremamente eterogenee,

L'OBBLIGO DI COMUNICAZIONE PREVENTIVA DEL TRATTAMENTO BASATO SULL'INTERESSE LEGITTIMO E CIÒ CHE RESTA DELL'ACCOUNTABILITY

Nell'ambito delle attribuzioni demandate al Garante nella Legge di bilancio 2018, assume particolare rilievo **il trattamento dei dati personali fondato sull'interesse legittimo del Titolare**: spetta all'Autorità Garante, in relazione ai trattamenti fondati su tale specifico presupposto di liceità (ex art. 6, par. 1, lett. f) GDPR), la **definizione di linee-guida o buone prassi e la predisposizione di un modello di informativa**.

Tale strumento mira all'adempimento di un **obbligo di "comunicazione preventiva"** che il Legislatore ha posto **in capo al Titolare che effettui un trattamento basato sull'interesse legittimo, qualora questo dovesse prevedere l'utilizzo di nuove tecnologie o di strumenti automatizzati**¹⁰.

Per come articolato, questo *iter* comunicativo, introdotto nelle pieghe della Legge di bilancio, **evoca schemi e cadenze tipici del Codice per la protezione dei dati personali, ma assai distanti** – per non dire incompatibili – **rispetto ai principi che reggono l'impianto del GDPR**. La stessa – ondivaga - formulazione della norma, rende infatti non poco faticosa la ricerca di una *ratio* univoca e conciliabile con lo spirito del GDPR.

Una delle possibili letture di tale disposizione potrebbe suggerire l'intenzione del Legislatore di snellire le attività di monitoraggio del Garante: l'informativa suddetta, predisposta dal Garante e compilata dal titolare del trattamento, con indicazione dell'oggetto, delle finalità e del contesto del trattamento, **instaura un procedimento di verifica ad impulso dello stesso Titolare**, a cui compete un **ruolo essenzialmente referente**, che si risolve nel **riportare all'Autorità Garante le informazioni necessarie a valutare la liceità del trattamento e il rispetto del GDPR**. Una volta ricevuta l'informativa, infatti, il Garante dovrà avviare un'**istruttoria** basata

senza meglio specificare le modalità dell'effettivo frazionamento dell'importo, abbastanza cospicuo, di 800 milioni per l'anno 2018 e maggiorato di anno in anno, fino alla soglia dei 2.500 milioni di euro nel 2033.

¹⁰ Legge 27 dicembre 2017, n. 205, art. 1:

1022. Il titolare di dati personali, individuato ai sensi dell'articolo 4, numero 7), del regolamento RGPD, ove effettui un trattamento fondato sull'interesse legittimo che prevede l'uso di nuove tecnologie o di strumenti automatizzati, deve darne tempestiva comunicazione al Garante per la protezione dei dati personali. A tale fine, prima di procedere al trattamento, il titolare dei dati invia al Garante un'informativa relativa all'oggetto, alle finalità e al contesto del trattamento, utilizzando il modello di cui al comma 1021, lettera c). Trascorsi quindici giorni lavorativi dall'invio dell'informativa, in assenza di risposta da parte del Garante, il titolare può procedere al trattamento.

1023. Il Garante per la protezione dei dati personali effettua un'istruttoria sulla base dell'informativa ricevuta dal titolare ai sensi del comma 1022 e, ove ravvisi il rischio che dal trattamento derivi una lesione dei diritti e delle libertà dei soggetti interessati, dispone la moratoria del trattamento per un periodo massimo di trenta giorni. In tale periodo, il Garante può chiedere al titolare ulteriori informazioni e integrazioni, da rendere tempestivamente, e, qualora ritenga che dal trattamento derivi comunque una lesione dei diritti e delle libertà del soggetto interessato, dispone l'inibitoria all'utilizzo dei dati.

1024. Il Garante per la protezione dei dati personali dà conto dell'attività svolta ai sensi del comma 1023 e dei provvedimenti conseguentemente adottati nella relazione annuale di cui all'articolo 154, comma 1, lettera m), del codice in materia di protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196.

su quanto deducibile dal documento ricevuto e, in mancanza di riscontro entro il termine di quindici giorni¹¹, il trattamento si intenderà consentito.

Quali siano gli **effetti attribuibili al silenzio dell'Autorità Garante, tuttavia, non è del tutto chiaro**: l'inerzia protratta per quindici giorni dall'invio dell'informativa, giustificherebbe il convincimento, anzitutto in capo al Titolare, dell'assenza di elementi ostativi al trattamento oggetto di comunicazione e, pertanto, della sua liceità. Il procedimento in questione, dunque, consentirebbe al Titolare del trattamento di **conseguire, per silentium, un titolo abilitativo tacito**, secondo lo schema del silenzio assenso.

Tuttavia, se così fosse, d'altra parte (e al netto di ogni giudizio sulla sostenibilità, alla luce del GDPR, di una simile opzione interpretativa), lo spirare del termine di quindici giorni coinciderebbe con il limite temporale previsto per l'esercizio dei poteri di verifica dell'Autorità Garante, decorso il quale l'operato del Titolare diventerebbe incontestabile, almeno rispetto alla sussistenza dei requisiti di liceità del trattamento riferiti nell'informativa. **Ma a ben vedere, un termine finale per lo svolgimento dell'attività di verifica spettante al Garante, non c'è affatto**¹². Ai sensi del comma 1023, infatti, l'Autorità può disporre una **moratoria del trattamento**, della durata di massimo trenta giorni, nel caso in cui, alla luce dell'informativa, ravvisi **il rischio di una lesione dei diritti e delle libertà dei soggetti interessati**. Durante questo lasso di tempo, il Garante ha la facoltà di richiedere al titolare ulteriori informazioni e integrazioni, che dovranno essere *"tempestivamente"* rese. Qualora, nonostante le nuove informazioni, l'Autorità ritenga che dal trattamento *"derivi comunque una lesione dei diritti e delle libertà del soggetto interessato"*, allora, disporrà l'**inibitoria all'utilizzo dei dati**.

Decorso il termine ostativo al trattamento, quindi, l'Amministrazione rimarrebbe titolare di un **potere inibitorio esercitabile sine die**: o, meglio, fino a quando non rilevi *una lesione*, prodotta ai danni di *un soggetto interessato* al trattamento. **Sarebbe logico pensare**, se non altro per evitare di sovvertire i principi dell'affidamento legittimo¹³, della certezza dei rapporti giuridici e della trasparenza amministrativa in un colpo solo, **che questi poteri di integrazione istruttoria e di inibizione del trattamento** (intrapreso dal Titolare in assenza di contraria indicazione del Garante nei tempi previsti) **non siano espressione di una funzione di controllo preventivo sulla sussistenza dei presupposti di liceità del trattamento oggetto di informativa ma, piuttosto, della più generale funzione di vigilanza e garanzia sulla corretta applicazione del GDPR, a tutela dei diritti dei singoli soggetti interessati**.

¹¹ È quantomeno criticabile, peraltro, la scelta di far decorrere il termine di quindici giorni *"dall'invio dell'informativa"*, a prescindere, cioè, dalla sua ricezione (che potrebbe, in ipotesi, verificarsi in prossimità, se non proprio successivamente allo spirare del termine, vanificando ogni seria funzione di verifica e tutela affidata all'Autorità Garante).

¹² A parte il dato letterale, comunque, difficilmente potrebbe giudicarsi sufficiente un termine variabile a seconda del tempo intercorrente tra l'invio dell'informativa da parte del Titolare del trattamento e la sua ricezione all'indirizzo del Garante, e pari, nella migliore delle ipotesi, a quindici giorni, per definire la mole di istruttorie (che si immagina formidabile, dati i presupposti) affidate all'Autorità Garante. E non si può fare a meno di pensare che *"l'assenza di risposta"* sia esattamente l'esito procedimentale atteso dallo stesso Legislatore, tanto da non richiedere al Garante di dar conto di quanto posto in essere in relazione alla ricezione dell'informativa, nell'ambito della relazione annuale sull'attività svolta e sullo stato di attuazione del codice in materia di protezione dei dati personali *ex art. 154 comma 1, lettera m)*, D.lgs. 196/2003, così come previsto, invece, con riferimento all'attività di istruzione integrativa di cui al comma 1023 e ai provvedimenti conseguentemente adottati.

¹³ Considerando, inoltre, i potenziali danni derivanti al Titolare dalla vanificazione di investimenti e di risorse nel caso in cui il trattamento di dati personali debitamente comunicato al Garante sia inibito solo una volta decorso il termine di 15 giorni entro cui l'Autorità avrebbe dovuto tempestivamente esprimere osservazioni o parere contrario, come previsto dalle nuove norme.

In ogni caso, il risultato è quello di aver reso assai più confuso il sistema delle norme a tutela dei dati personali, che andrebbe invece semplificato e coordinato, imponendo un obbligo di comunicazione di dubbia applicabilità, per consentire all'Autorità Garante di esercitare i poteri connaturati alla sua stessa vocazione istituzionale.

In effetti, un meccanismo così definito risulta assimilabile a un **metodo di controllo generalizzato sull'attività dei Titolari del trattamento**, un incrocio tra verifica preliminare e notificazione del trattamento¹⁴, ma con latitudine applicativa non altrettanto circoscritta, che **riaccredita, di fatto, all'Autorità Garante la titolarità del giudizio di bilanciamento tra diritti e libertà dell'interessato e legittimo interesse del titolare del trattamento.**

Esattamente il contrario dei principi che reggono la normativa europea del GDPR.

Nella logica del Regolamento 2016/679, infatti, la protezione dei diritti e delle libertà fondamentali delle persone fisiche, con riguardo alla protezione dei dati personali, non è assicurata dalla pedissequa osservanza di misure dettagliatamente somministrate dal Legislatore, ma – com'è noto - dal **raggiungimento effettivo di livelli adeguati di tutela**, tenendo conto *“della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché del rischio per i diritti e le libertà delle persone fisiche”* (cfr. Considerando n. 74): il giudizio di bilanciamento tra diritti, la valutazione del rischio e la traduzione in atto dei precetti normativi, competono, in primo luogo, **al Titolare del trattamento, “responsabilizzato” a rispettare i principi di corretto trattamento dei dati personali e a dimostrarne la conformità al Regolamento (principio di “accountability”).**

In questa prospettiva, l'Autorità di controllo dismette il ruolo paternalistico assegnato dal Codice in materia di protezione dei dati personali al nostro Garante e assume una funzione consultiva, allorché un tipo di trattamento presenti un rischio elevato per i diritti e le libertà delle persone fisiche e non siano adottate misure idonee ad attenuarlo (cfr. art. 36 GDPR): qui, però, il parere dell'Autorità **non si sostituisce alla valutazione di impatto svolta dal Titolare in adempimento all'art. 35 GDPR, ma la presuppone**, restando in capo al Titolare stesso la responsabilità di stabilire se e in che misura intraprendere un trattamento ad elevato grado di rischio, assicurando (e, se necessario, provando) il rispetto del Regolamento.

Vero è che ad ogni Stato membro è riservata la possibilità di prevedere, per legge, che la rispettiva Autorità di controllo abbia poteri ulteriori rispetto a quelli previsti dal GDPR (art. 58, pag. 6), a condizione, si intende, di rispettare la lettera e lo spirito del Regolamento europeo, condividendo e favorendo la realizzazione degli obiettivi che ne sono alla base, tra i quali *“quello di **garantire un livello equivalente di tutela delle persone fisiche e la libera circolazione dei dati personali nell'Unione**”* (art. 1, par. 1).

¹⁴ Rispettivamente regolate dagli artt. 17 e 37 del D. Lgs. 196/20013.

COSA CAMBIA IN PRATICA CON L'OBBLIGO DI COMUNICAZIONE PREVENTIVA DEL TRATTAMENTO

Il procedimento in sintesi:

- 1) **Il Garante predispone un modello di informativa la cui compilazione è di competenza dei Titolari del trattamento** dei dati personali che effettuano un trattamento fondato sull'interesse legittimo, qualora sia previsto l'uso di nuove tecnologie o di strumenti automatizzati;
- 2) **Il Titolare**, prima di procedere al trattamento, **invia l'informativa** di cui al punto 1) **al Garante**, indicando l'oggetto, le finalità e gli ulteriori dati inerenti al contesto del trattamento, **utilizzando il modello predisposto dal Garante stesso**;
- 4) Se il Garante non fornisce riscontro, **trascorsi quindici giorni lavorativi dall'invio dell'informativa, il Titolare può procedere con il trattamento** secondo le modalità comunicate;
- 5) **Il Garante**, sulla base dell'informativa, **avvia un'istruttoria**;
- 6) **Il Garante**, alla luce dell'istruttoria, qualora rintracci il rischio di una lesione dei diritti e delle libertà dei soggetti interessati, derivante dal trattamento, **dispone la moratoria del trattamento per un periodo massimo di trenta giorni**;
- 7) **Durante i trenta giorni di moratoria, il Garante può richiedere ulteriori informazioni e integrazioni al Titolare del trattamento**;
- 8) **Il Titolare deve fornire tempestivamente le informazioni** richieste dal Garante;
- 9) **Il Garante**, valutata la questione tenendo conto delle ulteriori informazioni ricevute, **qualora ritenga comunque presente una lesione derivante dal trattamento, dispone l'inibitoria all'utilizzo dei dati**.