IPSOA

CORRIERE TRIBUTARIO

11 GIUGNO
2018
23

IVA
- Soggetti tenuti allo split payment
- Detrazione tardiva dell'imposta

STUDI DI SETTORE
Definizione di correttivi e modelli

OPERAZIONI STRAORDINARIE
Aggregazioni aziendali under common control

REDDITI D'IMPRESA
Contributi a titolo di liberalità nelle procedure concorsuali

RISCOSSIONE
Intervento dell'agente della riscossione nell'esecuzione forzata

PROCESSO TRIBUTARIO
Esecutività retroattiva delle sentenze pro contribuente

ACCERTAMENTO
Modifiche e integrazioni al Codice dell'amministrazione digitale

PRIVACY
Entrata in vigore del GDPR

DI PROSSIMA PUBBLICAZIONE
- Transfer pricing
- Interessi negativi
- Ne bis in idem
- Cancellazione società dal registro imprese

Anno XLI - Direzione e Redazione: Via dei Missaglia, n. 97, Edificio B3 - 20142 Milano (MI)
Tariffa R.O.C.: Poste Italiane Spa - Spedizione in abbonamento Postale - D.L. 353/2003 (conv. in L. 27/02/2004 n. 46) art. 1, comma 1, DCB Milano

ON-LINE
www.edicolaprofessionale.com

Wolters Kluwer

La rivoluzione GDPR

di Tommaso D'Onofrio (*) e Carlo Macculi (**)

Il 14 aprile 2016 il Parlamento e il Consiglio Europeo hanno approvato in via definitiva il **Reg. UE 2016/679** in materia di **protezione** dei **dati personali** ("**GDPR**"). Il Regolamento esplica i propri **effetti** dal **25 maggio 2018** e abroga la Direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali. A livello nazionale, pone l'esigenza di operare una rilettura in chiave GDPR del D.Lgs. n. 196/2003 (Codice in materia di protezione dei dati personali).

Dopo oltre 20 anni dalla Direttiva-madre 95/46 in materia di *privacy*, è stato emanato, con effetto abrogativo della Direttiva precedente, il Reg. UE 2016/679 in materia di protezione dei dati personali (di seguito, "Regolamento" o "GDPR"), che sostanzialmente rivoluziona l'approccio alla *privacy* in ambito comunitario. Si passa da un sistema orientato su un modello autorizzatorio ad una nuova visione legata all'introduzione del principio di responsabilizzazione (*accountability*). Il nuovo Regolamento impone, quindi, una radicale rilettura dei comportamenti in materia di *privacy*, adottati sino ad oggi, in quanto comporta una responsabilizzazione sostanziale del Titolare del trattamento, che non può più limitare la propria azione ad una valutazione puramente formale.

Il principio della responsabilizzazione richiede l'adozione, anche per il trattamento dei dati personali, dell'approccio tipico dei sistemi di gestione, collocandosi all'interno di un Regolamento che risponde all'esigenza di armonizzare le regole in materia di trattamento di dati personali in tutti gli stati dell'Unione Europea. La dimostrazione della conformità dell'organizzazione, nel trattamento dei dati personali, alla nuova disciplina regolamentare passa oggi per l'implementazione di misure tecniche ed organizzative adeguate, ma soprattutto disegnate sulle specifiche caratteristiche dell'organizzazione.

Il nuovo Regolamento si applica ai trattamenti realizzati da Titolari stabiliti in ambito UE o da Titolari non stabiliti in ambito UE, ma che offrono beni e servizi anche gratuiti ai cittadini UE o ne monitorano il comportamento. In particolare, il Regolamento si riferisce esclusivamente ai trattamenti di dati relativi a persone fisiche identificate o identificabili (interessati) e non anche a quelle giuridiche.

Due sono i passaggi chiave di questa rivoluzione, generata senza dubbio dall'esigenza di fronteggiare la complessità dello scenario socio-tecnologico che accompagna la nostra epoca. In primo luogo il rafforzamento del concetto di interesse legittimo pone sul tavolo l'esigenza, in ogni trattamento dati, di pervenire ad un sostanziale equilibrio tra la necessità di trattare dati personali in modo sempre più rapido ed efficiente e le legittime aspettative di ciascun terzo interessato. Non è quindi l'Autorità a determinare l'esistenza di un bilanciamento fra il legittimo interesse del Titolare o del terzo, ma sarà compito dello stesso Titolare.

L'interesse legittimo del Titolare per avere un fondamento di liceità deve prevalere sui diritti e le libertà fondamentali dell'interessato.

Il principio della responsabilizzazione si lega strettamente ad un secondo elemento chiave: l'obbligo di tenuta del registro dei trattamenti, documento che deve essere redatto in forma scritta, anche su formato elettronico e su richiesta deve essere posto a disposizione dell'Autorità di controllo. Questo strumento per-

(*) *Vicepresidente Aiscris (Associazione Italiana società di consulenza per la ricerca l'innovazione e lo sviluppo), Dottore commercialista e Revisore legale*

(**) *Esperto di sistemi di gestione. Ingegnere*

mette di dimostrare la capacità del Titolare e del Responsabile (se nominato) di conformarsi al GDPR e di conservare in maniera ordinata, ricostruibile *ex post* e verificabile da terzi, le considerazioni svolte in merito alla mappatura ed analisi di tutti i trattamenti attuati dall'organizzazione. Il registro dimostra, altresì, l'adozione di misure adeguate ed efficaci volte ad attuare la piena *compliance* al GDPR. Indipendentemente dagli obblighi di tenuta, previsti sulla carta solo per le organizzazioni che presentino talune caratteristiche (imprese o organizzazioni con oltre 250 dipendenti, nonché quelle che effettuano trattamenti che possono presentare un rischio per i diritti e le libertà dell'interessato, o abbiano ad oggetto dati sensibili, biometrici, genetici, relativi alla salute o a reati e condanne penali) (1), il registro rappresenta uno strumento efficace per qualsiasi tipologia di organizzazione per dimostrare ai terzi la corretta applicazione del principio di *accountability* (responsabilizzazione). Da qui nasce l'invito dell'Autorità Garante, rivolto a tutte le organizzazioni, all'adozione del registro indipendentemente da un obbligo specifico.

LA NOVITÀ NORMATIVA

Registro dei trattamenti

Il registro dei trattamenti, indipendentemente dagli obblighi giuridici, rappresenta lo strumento chiave per la dimostrazione del rispetto del **principio** di **responsabilizzazione**. La stessa **Autorità Garante** per la Privacy, auspicando l'adozione di questo strumento per tutte le organizzazioni coinvolte, all'interno delle raccomandazioni delle linee guida al GDPR, afferma che la tenuta del registro dei trattamenti **non** costituisce un **adempimento formale**, bensì parte integrante di un **sistema** di **corretta gestione** dei **dati personali**. Per tale motivo l'Autorità invita tutti i titolari di trattamento e i responsabili, a prescindere dalle dimensioni dell'organizzazione, a compiere i passi necessari per dotarsi di tale registro e, in ogni caso, a compiere un'accurata ricognizione dei trattamenti svolti e delle rispettive caratteristiche, ove già non condotta.

Le nuove norme in materia di *privacy* hanno spinto molti Paesi, fin dal 2016, a porre in essere azioni concrete e finalizzate ad adeguare il quadro normativo al GDPR. Il nostro Consiglio dei Ministri, solo il 21 marzo 2018, circa due mesi prima dell'entrata in vigore del Regolamento, ha adottato uno schema di Decreto. La delega prevedeva un generale riassetto normativo con l'abrogazione delle norme del D.Lgs. n. 196/2003 (T.U. *privacy*) incompatibili con il GDPR. In merito, il legislatore delegato sarebbe dovuto intervenire entro il 21 maggio 2018 con opportuno Decreto, ma lo schema di Decreto è stato assegnato alla Commissione del Senato in data 14 maggio 2018 e alla Commissione della Camera dei Deputati in data 15 maggio 2018, date dalle quali sono scattati i 40 giorni per l'espressione dei prescritti pareri. Alla luce dei predetti avvenimenti, il termine per l'esercizio della delega si intende prorogato di ulteriori tre mesi e quindi fissato al 21 agosto 2018 per effetto della Legge n. 234/2012. Solo al termine dell'*iter* completo di approvazione del Decreto si potrà conoscere in forma definitiva la legge italiana di adeguamento al GDPR. Al momento, sono stati mantenuti in vita, transitoriamente in attesa di un successivo riesame, ove compatibili con il GDPR, i precedenti provvedimenti dell'Autorità, le autorizzazioni precedentemente rilasciate e i codici deontologici.

Una nuova visione di responsabilizzazione

All'interno di questa nuova visione regolamentare si collocano due principi di grande rilievo: la *privacy by design* e la *privacy by default* (2). La *privacy by design* comporta che le attività, i prodotti e i servizi che prevedono il trattamento di dati personali debbano essere progettati, impostati e sviluppati in modo da assicurare il rispetto dei principi e delle garanzie a tutela della *privacy*. Nella progettazione bisogna adottare misure per minimizzare l'utilizzo di dati personali, consentire all'interessato il controllo dei propri dati, garantire trasparenza e sicurez-

(1) Art. 30, comma 5, Reg. UE 2016/679.

(2) Art. 25, Reg. UE 2016/679.

za. Ciò rappresenta una delle espressioni più elevate del principio di responsabilizzazione in quanto impone alle organizzazioni, fin dalla fase di progettazione, di disegnare le azioni in una logica ben lontana da qualunque processo di standardizzazione dei processi di gestione della *privacy*.

La *privacy by default* comporta che il trattamento, per impostazione predefinita, debba avere ad oggetto solo i dati necessari al perseguimento della specifica finalità prefissata in termini di quantità, di portata del trattamento, di periodo di conservazione e di accessibilità. Questo principio, pur in una lettura estensiva, si muove nella stessa logica del c.d. principio di pertinenza, già presente in passato all'interno delle normative nazionali.

LA NOVITÀ NORMATIVA

Privacy by design e privacy by default
La **privacy by design** comporta che le **attività**, i **prodotti** e i **servizi** che prevedono il trattamento di dati personali debbano essere progettati, impostati e sviluppati in modo da assicurare il rispetto dei **principi** e delle **garanzie** a tutela della **privacy**. Nella progettazione bisogna adottare misure per minimizzare l'utilizzo di dati personali, consentire all'interessato il controllo dei propri dati, garantire trasparenza e sicurezza. La privacy **by default** comporta che il trattamento, per impostazione predefinita, debba avere ad oggetto solo i **dati** necessari al perseguimento della specifica finalità prefissata in termini di **quantità**, di **portata** del trattamento, di **periodo** di **conservazione** e di **accessibilità**. Questo principio, pur in una lettura estensiva, si muove nella stessa logica del c.d. principio di **pertinenza**, già presente in passato all'interno delle normative nazionali.

Rispetto al passato il ruolo di Responsabile del trattamento, il soggetto esterno all'organizzazione che tratta i dati per conto del Titolare viene descritto in modo molto più specifico. Il Regolamento, difatti, introduce il contenuto del processo di nomina (obbligatorio e documentato con un contratto o altro atto giuridico) e le relative responsabilità, anche dirette, nei confronti degli interessati. Il Responsabile del trattamento deve presentare garanzie professionali sufficienti per attuare misure tecniche e organizzative adeguate (art. 28 GDPR).

È importante sottolineare che i Titolari, ovvero il Titolare e il Responsabile, ovvero i Responsabili coinvolti nel medesimo trattamento, rispondono in solido per l'intero ammontare del danno cagionato dalla violazione. Il Regolamento introduce anche la possibilità di inserire ulteriori soggetti, definiti Contitolari del trattamento, i quali determinano congiuntamente le finalità e i mezzi del trattamento.

Anche in questo caso appare necessario un accordo interno che delinei in modo specifico ruoli e responsabilità. Il Regolamento non prevede, al contrario di quanto avveniva nel T.U. *privacy*, la figura dell'incaricato al trattamento quale soggetto che tratta dati operando sotto l'autorità del Titolare e del Responsabile, tuttavia la nomina di tale soggetto non è espressamente esclusa.

Un importante elemento di novità del Regolamento è costituito da quanto disciplinato all'interno dell'art. 17 del Regolamento in riferimento al c.d. diritto all'oblio. In pratica l'interessato ha il diritto di ottenere dal Titolare del trattamento la cancellazione dei dati personali che lo riguardano e il Titolare del trattamento ha l'obbligo di cancellare, senza ingiustificato ritardo, i dati personali, se sussiste uno dei motivi seguenti:

a) i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;

b) l'interessato revoca il consenso su cui si basa il trattamento conformemente all'art. 6, paragrafo 1, lett. a), o all'art. 9, paragrafo 2, lett. a), e se non sussiste altro fondamento giuridico per il trattamento;

c) l'interessato si oppone al trattamento ai sensi dell'art. 21, paragrafo 1, e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si oppone al trattamento ai sensi dell'art. 21, paragrafo 2;

d) i dati personali sono stati trattati illecitamente;

e) i dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il Titolare del trattamento;

f) i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione di cui all'art. 8, paragrafo 1.

Importante sottolineare che il Titolare del trattamento, se ha reso pubblici dati personali ed è obbligato a cancellarli, tenendo conto della tecnologia disponibile e dei costi di attuazione, adotta le misure ragionevoli, anche tecniche, per informare i Titolari del trattamento che stanno trattando i dati personali della richiesta dell'interessato di cancellare qualsiasi *link*, copia o riproduzione dei suoi dati personali.

La lettura del nuovo Regolamento comunitario lascia emergere due ulteriori importanti novità: il c.d. principio della *data portability* (3) e quello relativo al *Data breach notification* (4). Il principio di *data portability* sancisce che l'interessato ha il diritto di ricevere dal Titolare del trattamento in un formato strutturato, di uso comune e leggibile da dispositivo automatico, i dati personali che lo riguardano e ha il diritto di trasmettere tali dati a un altro Titolare del trattamento, senza impedimenti da parte del precedente Titolare del trattamento, qualora il trattamento si basi sul consenso precedentemente rilasciato o si basi su un contratto o su trattative precontrattuali in corso. Nell'ambito di questo principio, l'interessato ha anche il diritto di ottenere la trasmissione diretta dei dati personali da un Titolare del trattamento all'altro, se tecnicamente fattibile. Anche in questo caso il Regolamento, evidenziando la giusta attenzione alla concreta possibilità di attuare le azioni richieste, vincola la trasmissione diretta dei dati tra diversi titolari alla fattibilità tecnica.

LA NOVITÀ NORMATIVA

Responsabile del trattamento

Il T.U. privacy identificava con la figura del Responsabile del trattamento un soggetto che, sotto le dirette dipendenze del Titolare, rappresentava l'organizzazione in ambito privacy. Oggi la figura del Responsabile del trattamento viene ricoperta da tutti **coloro, esterni all'organizzazione**, che **trattano dati personali** per **conto** del **Titolare**. Si pensi, in via meramente esemplificativa, ai consulenti del lavoro o ai professionisti contabili che assistono l'organizzazione trattando dati personali di persone fisiche per conto del Titolare. Per queste figure non sarà più sufficiente un generico atto di nomina, ma sarà necessaria la condivisione e sottoscrizione di un **contratto specifico** che ne delinei compiti e responsabilità.

Ponendo l'attenzione sul principio del *data breach notification*, viene previsto che, in caso di violazione dei dati personali, il Titolare effettui una notifica dell'accaduto all'Autorità di controllo senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione presenti un rischio per i diritti e le libertà degli interessati. La comunicazione deve contenere la natura della violazione, la descrizione delle possibili conseguenze e delle misure adottate per rimediare e ridurre gli effetti negativi. Vige altresì un obbligo di implementazione e conservazione di documentazione di qualsiasi violazione dei dati personali (circostanze, conseguenze e azioni poste in essere per porvi rimedio) per permettere all'Autorità di controllo il rispetto delle prescrizioni in tema di *data breach*.

La valutazione preliminare e la nomina del Data protection Officer

Una corretta disamina del Reg. 2016/679 deve soffermarsi sugli altri due aspetti innovativi. Ci si riferisce all'obbligo per alcune organizzazioni di redigere il DPIA (*Data Protection Impact Assessment*) (5), che rappresenta una novità nel nostro Paese (6), e alla nomina del DPO (*Data Protection Officer*) (7), rinominato in ambito nazionale come RPD (Responsabile Protezione Dati).

La stesura del DPIA è obbligatoria in tutte le ipotesi di rischio elevato (trattamento automatizzato e destinata a produrre effetti giuridici e/o trattamento su larga scala di dati sensibili o giudiziari). Il documento in oggetto descrive in modo sistematico: i trattamenti, le finalità, la proporzionalità dei trattamenti in relazione alle

(3) Art. 20, Reg. UE 2016/679.
(4) Art. 34, Reg. UE 2016/679.
(5) Art. 35, Reg. UE 2016/679.
(6) Uno dei primi esempi di DPIA lo ritroviamo nel 2002 negli USA all'interno dell'E-Government Act.
(7) Art. 37, Reg. UE 2016/679.

finalità, esprimendo la valutazione dei rischi e le misure previste per affrontarli. Si tratta in pratica di una vera e propria fase di *risk assessment* che ricorda quella posta in essere preventivamente alla redazione dei modelli di organizzazione e controllo *ex* D.Lgs. n. 231/2001.

È opportuno soffermarsi, in conclusione, sulla nuova figura del *Data Protection Officer* (DPO). Qui si utilizzerà la denominazione anglosassone al fine di evitare confusione interpretativa tra il Responsabile della Protezione Dati (traduzione dell'Autorità italiana del DPO), e il Responsabile del Trattamento Dati, che, come abbiamo visto, ricopre un ruolo del tutto differente rispetto a quello del DPO, che invece assiste e riferisce al Titolare in merito al rispetto degli obblighi *privacy* e all'implementazione delle *policies* cooperando con l'Autorità di controllo e fungendo da punto di contatto per tutte le questioni connesse al trattamento anche verso gli interessati.

La designazione del DPO è obbligatoria per la PA, nei casi nei quali le attività principali del Titolare consistono in trattamenti che richiedono il monitoraggio regolare e sistematico degli interessati su larga scala (8) o se le attività principali del Titolare consistono in trattamenti su larga scala di dati "sensibili".

Può trattarsi di un soggetto interno o esterno (anche persona giuridica) all'organizzazione designato in funzione delle sue qualità professionali e munito di prerequisiti di autonomia e indipendenza. Deve avere una conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati e la capacità di assolvere i propri compiti. I dati del DPO devono essere comunicati all'Autorità Garante.

Due parole finali merita il sistema sanzionatorio previsto per le violazioni delle norme contenute nel Regolamento. Le sanzioni amministrative pecuniarie possono arrivare fino a 20.000.000 euro o, per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore. L'entità delle sanzioni ha suscitato in questi mesi una crescente preoccupazione, da parte delle organizzazioni e degli operatori. Tuttavia, è necessario precisare, pur confermando i soprapprecisati livelli massimi, che le predette sanzioni amministrative possono essere inflitte congiuntamente o in luogo di: avvertimenti, ammonimenti, ingiunzioni, limitazioni, divieti e sono dimensionate in funzione della natura, gravità, durata, carattere doloso o colposo della violazione, grado di responsabilità e comportamenti precedenti del Titolare, adozione delle misure di prevenzione, grado di cooperazione con l'Autorità di controllo per rimediare alla violazione.

L'attuazione del principio di responsabilizzazione deve essere vissuta dalle organizzazioni con l'obiettivo di garantire un ritorno di efficienza e di crescita di reputazione. Al contrario, l'implementazione di singole e semplicistiche risposte ai diversi adempimenti e prescrizioni del Regolamento, scevra da una lettura di sistema, comporterebbe un inutile investimento di tempo e danaro senza produrre alcun risultato efficace in termini di *compliance* con il GDPR.

LA NOVITÀ NORMATIVA

Data portability e data breach notification

I due nuovi principi, introdotti dal GDPR, di data portability e data breach notification sono strettamente correlati alla nuova visione di **responsabilizzazione** e si allineano perfettamente al concetto di **privacy by design**. Le organizzazioni, difatti, al fine di porre in essere celermente le azioni richiamate dai due principi, non potranno che dotarsi di una struttura snella, conforme al Regolamento e in grado di gestire con rapidità i dati personali relativi a singoli interessati (data portability) e reagire prontamente ad eventuali attacchi informatici ai propri sistemi di gestione dei dati (data breach notification). I due aspetti impongono una radicale **rilettura** della **progettazione** dei propri **sistemi informativi** e della **formazione** del proprio **personale**, soprattutto all'interno delle strutture che trattano dati in forma massiva e con continue azioni di monitoraggio.

(8) Utilizzo di una notevole quantità di dati personali a livello regionale, nazionale o sovranazionale che incidono su un elevato numero di interessati.