CAMMINO DIRITTO
Rivista di informazione giuridica
https://rivista.camminodiritto.it

IL G.D.P.R. E LA TUTELA DELLA RISERVATEZZA DEI DATI PERSONALI

Il nodo delle modifiche organizzative con l'entrata in vigore del Regolamento U.E. sulla protezione dei dati personali. La nuova figura del data protection officer e la valutazione dell'impatto del trattamento di dati personali

di **Pietro Cucumile**
IUS/15 - DIRITTO PROCESSUALE CIVILE
Articolo divulgativo - ISSN 2421-7123

Direttore responsabile
Raffaele Giaquinto

Pubblicato, Mercoledì 1 Agosto 2018

CamminoDiritto.it
ISSN 2421-7123

Sommario: 1. Inquadramento normativo; 2. Esegesi della struttura normativa; 3. Violazione dei dati personali; 4. Valutazione dell'impatto del trattamento di dati personali.

1. Inquadramento normativo.

Dal 25 maggio 2018, gli enti pubblici e le imprese, come è noto, hanno dovuto iniziare un impervio percorso di avvicinamento agli adempimenti degli obblighi previsti dal nuovo Regolamento europeo sulla riservatezza e tutela dei dati personali U.E. 2016/679 del 27 aprile 2016. Il G.D.P.R. riconosce un particolare valore ai **dati** così definendoli: "asset fondamentale", beni non riproducibili, parzialmente riacquistabili, difficilmente ricostruibili, che riguardano l'individuo ma che sono integrati con le organizzazione che li trattano per erogare un servizio (piattaforme tecnologiche di intermediazione, es. piattaforme di e-commerce) e che li detengono attraverso un "rapporto fiduciario" con l'individuo. I dati personali sono le informazioni che identificano o rendono identificabile una persona fisica e che possono fornire dettagli sulle sue caratteristiche, le sue abitudini, il suo stile di vita, le sue relazioni personali, il suo stato di salute e la sua situazione economica. A tutela dei diritti dell'individuo sono stati scolpiti alcuni principi orientanti una corretta azione: **liceità,** ovvero si riferiscono solo alcune informazioni ed ad un determinato scopo; **accesso,** ovvero è possibile accedere alle proprie informazioni in tempi e costi certi; **rettifica,** possibilità di modificare i propri dati quando ciò è necessario e voluto; **oblio,** ovvero è possibile cancellare i propri dati in qualunque momento. Si consideri che la liceità è un principio che riguarda tutto l'ordinamento giuridico per cui rappresenta il grimaldello con cui l'Autorità garante o un giudice, nell'esercizio dell'attività interpretativa, possono far ricorso "ai combinati disposti", innestandosi su normative di settore o specialistiche quali quelle giuslavoristiche (si pensi allo Statuto dei lavoratori), anche in forza della matrice e cogenza europea di tali enunciazioni. Per essere concreti, si pensi a quanti profili di tutela dei dati personali dei lavorati possa attivare il controllo a distanza da parte di "droni", in uso nei complessi penitenziari nei cambi turno del personale o per la vigilanza perimetrale di strutture a rischio.

Il pacchetto di riforma in materia di protezione dei dati è costituito dal Regolamento generale sulla protezione dei dati personali, Regolamento 2016/679/U.E., nonché dalla Direttiva «Polizia» 2016/680 sul trattamento dei dati personali delle persone fisiche a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio. Altre riforme normative sono in corso di approfondimento quali la revisione della Convenzione 81/108, della direttiva 2002/58/CE, c.d. e-privacy directive: e-privacy regulation, del Regolamento 2001/45 relativo al trattamento dei dati personali da parte delle istituzioni, degli organi e uffici dell'Unione europea.

CamminoDiritto.it
ISSN 2421-7123

Il nuovo G.D.P.R. ha perseguito l'esigenza di costituire un mercato unico digitale a livello europeo in grado di far fronte alle sfide di un mondo globalizzato ed in grado di rispondere agli utenti in termini di maggiore fiducia a fronte dello sviluppo tecnologico, della costituzionalizzazione del diritto fondamentale alla protezione dei dati personali (l'art. 16 T.F.U.E. dopo il Trattato di Lisbona) nonché della frammentazione del quadro normativo per la trasposizione disomogenea della Direttiva 95/46 nei diritti nazionali. A tal fine, in relazione alla costituzionalizzazione del diritto fondamentale alla protezione dei dati personali, l'art. 16 T.F.U.E. così recita «1. Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano».

Il Regolamento (U.E.) 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, abroga, quindi, la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) e si affianca alla normativa italiana di cui al D. Lgs. n° 196/2003 che il Legislatore italiano ha in animo di abrogare o modificare. L'esigenza di intervento del legislatore europeo nasce da un'esigenza di armonizzazione delle varie normative statali vigenti in tema di privacy e dalla considerazione dei molteplici luoghi dove si trovino i dati personali: dati comunicati, dati raccolti leggendo le azioni di ciascuno, dati elaborati su ognuno attraverso strumenti vari come la videosorveglianza, le rilevazioni biometriche, gli R.F.I.D., i sistemi di localizzazione, le applicazioni e così via. Si può affermare, infatti, che, nella nuova logica dei big data, ognuno è le tracce che lascia, anche alla luce del valore economico dei dati acquisiti, ad esempio, attraverso una penetrante profilazione.

Il **cyberspazio** e la **globalizzazione** hanno evidenziato l'obsolescenza dei sistemi giuridici tradizionali fondati su strumenti e regole di diritto che si arrestano ai confini nazionali o europei; il **web è ormai uno spazio virtuale senza frontiere per cui si sono resi necessari strumenti normativi sovranazionali.** Si è avvertita forte l'esigenza di costituire una normativa unica europea in tema di privacy e di mercato unico digitale per far fronte alle sfide di un mondo globalizzato al fine di rispondere agli utenti in termini di maggior fiducia. Si pensi che, dal punto di vista delle fonti normative, era avvenuta la **costituzionalizzazione del diritto fondamentale alla protezione dei dati** personali (ex art. 16 T.F.U.E. dopo il Trattato di Lisbona) ma si presentava un quadro normativo frammentato a causa della trasposizione disomogenea della Direttiva 95/46 nei diritti nazionali. Il Trattato di Lisbona, infatti, accanto al diritto alla riservatezza ha introdotto il diritto alla protezione dei dati che prescinde dalle interferenze nella vita privata.

2. Esegesi della struttura normativa.

CamminoDiritto.it
ISSN 2421-7123

Volendo procedere secondo un metodo ricostruttivo e analitico, il Regolamento europeo 2016/679/C.E. presenta la seguente struttura normativa:

capo I disposizioni generali – artt. da 1 a 4; capo II principi – artt. da 5 a 11; capo III diritti dell'interessato – artt. da 12 a 23; capo IV titolare del trattamento e responsabili – artt. da 24 a 43; capo V trasferimento di dati verso paesi terzi o organizzazioni internazionali – artt. da 44 a 50; capo VI autorità di controllo – artt. da 51 a 59; capo VII cooperazione e coerenza – artt. da 60 a 76; capo VIII mezzi di ricorso, responsabilità e sanzioni – artt. da 77 a 84; capo IX disposizioni relative a specifiche situazioni di trattamento – artt. da 85 a 91; capo X atti delegati e atti di esecuzione – artt. da 92 a 93; capo XI disposizioni finali – artt. da 94 a 99. Inoltre, cercando di confezionare un riepilogo delle novità **in tema di informativa** secondo il vigente G.D.P.R. l'esito potrebbe essere il seguente:

sui dati di contatto del DPO (non necessario il nome: requisito di conoscibilità esterna del DPO); sul periodo di conservazione; sulla portabilità dei dati; sul diritto di proporre il reclamo; sulle icone standardizzate; sulla revoca del consenso; sulla intenzione di trasferire i dati fuori dall'UE/SEE; sulla specificazione se il trattamento sia necessario per perseguire il legittimo interesse del titolare o da terzi (marketing diretto anche tramite terzi o prevenzione frodi) (cfr. considerandi nn. 47, 48, 50, 111); su eventuali destinatari o categorie di destinatari. Anche in materia di informativa non si potranno utilizzare tutte le informazioni raccolte a seguito dell'uso delle attrezzature lavorative per ogni finalità possibili; non è conforme allo spirito della normativa raccogliere indistintamente ogni sorta di informazione sull'attività di un lavoratore per, poi, utilizzare quei dati per finalità diverse: ad esempio, la rilevazione elettronica degli accessi al luogo di lavoro ha una finalità precisa e l'utilizzo delle informazioni sull'accensione della postazione del personal computer di assegnazione ad un lavoratore ne ha un'altra.

Particolare attenzione andrà prestata al test dell'interesse legittimo: "l'esistenza di legittimi interessi richiede un'attenta valutazione anche in merito all'eventualità che l'interessato, al momento e nell'ambito della raccolta dei dati personali, possa ragionevolmente attendersi che abbia luogo un trattamento a tal fine". Si ricordi quanto veniva espresso sull'interesse legittimo dal Codice della privacy: "art. 24. Casi nei quali può essere effettuato il trattamento senza consenso: g) con esclusione della diffusione, è necessario, nei casi individuati dal Garante sulla base dei principi sanciti dalla legge, per perseguire un legittimo interesse del titolare o di un terzo destinatario dei dati, qualora non prevalgano i diritti e le libertà fondamentali, la dignità o un legittimo interesse dell'interessato [...]".

Costituisce, parimenti, **legittimo interesse del titolare del trattamento** il caso in cui si

CamminoDiritto.it
ISSN 2421-7123

trattino dati personali strettamente necessari per la prevenzione di frodi. Può essere, inoltre, considerato un legittimo interesse trattare dati personali per finalità di marketing diretto, o di sicurezza delle reti e dell'informazione per possibili reati o minacce alla sicurezza pubblica o per un trattamento dei dati personali all'interno di un gruppo di imprese per finalità contabili e/o amministrative.

Un modello di informativa dovrà, quindi, esprimersi, almeno, su queste informazioni minime:

sui dati di contatto del D.P.O. senza la necessità di inserire il nome in quanto è richiesto il requisito di conoscibilità esterna del D.P.O.; sul periodo di conservazione; sulla portabilità dei dati; sul diritto di proporre il reclamo; sulle icone standardizzate; sulla revoca del consenso; sulla intenzione di trasferire i dati fuori dall'U.E./S.E.E.; sulla specificazione se il trattamento sia necessario per perseguire il legittimo interesse del titolare (cfr. considerandi nn. 47, 48, 50, 111); su eventuali destinatari o categorie di destinatari. Inoltre, qualora l'informativa riguardi i minori si deve utilizzare un linguaggio chiaro e semplice adatto a loro.

3. Violazione dei dati personali.

Sotto un diverso punto di vista, la trasmissione, comunicazione o comunque l'apprensione non autorizzata di informazioni ad una parte non è autorizzata; a tal fine, il Regolamento definisce **la violazione dei dati personali** (art. 4): "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 personali trasmessi, conservati o comunque trattati".

Inoltre, il Regolamento prevede **un sistema di notifica** a seconda del rischio associato alla violazione: ovvero all'autorità di controllo, ex art. 33 del G.D.P.R. o ai soggetti interessati dalla violazione, ex art. 34 del G.D.P.R.. Di più. Secondo il "Considerando 85" il titolare del trattamento dovrebbe comunicare all'Autorità di controllo il caso in cui la violazione presenti rischi per i diritti e libertà dell'interessato; invece, ai sensi dell'art. 33, comma 1, è esclusa la notificazione quando si possa dimostrare che il rischio è improbabile. Occorre, quindi, documentare tale valutazione nell'inventario delle violazioni dei dati.

In forza, poi, del "Considerando 86" il titolare del trattamento deve comunicare all'interessato la violazione dei dati personali qualora questa violazione sia suscettibile di presentare **un rischio elevato** di pregiudizio per i diritti e le libertà della persona fisica, **secondo il criterio dell'impatto significativo**.

CamminoDiritto.it
ISSN 2421-7123

Si ponga l'attenzione sulla circostanza che una violazione dei dati personali, se non affrontata in modo adeguato e tempestivo, può provocare una perdita del controllo dei dati personali, una limitazione dei diritti delle persone, una discriminazione, un furto o usurpazione d'identità, perdite finanziarie, un pregiudizio alla reputazione, qualsiasi altro danno economico o sociale significativo alla persona fisica interessata.

Inoltre, il termine per informare l'Autorità di Controllo dell'avvenuta violazione o dei motivi di ritardo è di 72 ore; **il contenuto minimo della notifica** deve contenere almeno una descrizione della natura della violazione, del numero e delle categorie dei dati interessati, se disponibili, del nome del responsabile della protezione dei dati, delle probabili conseguenze della violazione e delle misure adottate per porvi rimedio e/o attenuarne gli effetti negativi.

Nell'art. 34 che tratta la notifica all'interessato, non si menziona un termine preciso entro il quale adempiere, ma il legislatore prevede che questo adempimento debba avvenire "senza ingiustificato ritardo". L'obbligo di comunicazione all'interessato si attiva nei casi più gravi, in cui dalla violazione possano derivare **rischi elevati** per i diritti e le libertà delle persone fisiche.

La notifica delle violazioni deve almeno comunicare:

il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni; descrivere le probabili conseguenze della violazione dei dati personali; descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi. La comunicazione all'interessato deve essere formulata con un linguaggio semplice e chiaro, oltre a descrivere la natura della violazione dei dati personali.

Ciò detto, per un'organizzazione, mettere in piedi un progetto di adeguamento al G.D.P.R. non è una banalità, anche perché occorre rivedere l'organizzazione, l'informatica, la sicurezza, la modulistica, la formazione interna, l'informazione interna ed esterna, gli aspetti legali per il rapporto con i clienti/utenti/cittadini e così via. L'entità stessa del progetto può variare molto a seconda della tipologia di organizzazione in termini di dimensione e di attività svolta.

Sicuramente è necessario procedere alla **revisione** delle attuali **figure** attraverso l'istituzione del titolare del trattamento, del/dei responsabile/i del/dei trattamento/i e del

CamminoDiritto.it
ISSN 2421-7123

sub responsabile/i e del D.P.O., data protection officer, con la stesura di contratti ad hoc per disciplinare la distribuzione delle responsabilità; occorrerà **revisionare** anche le **procedure** e la **modulistica** per i rapporti con il cliente/utente, prevedendo la richiesta del consenso al trattamento dei dati, attivando la gestione delle procedure di reclami, con l'accesso ai dati. Un occhio particolare andrà prestato alle procedure di notifica di violazione dei dati personali e di gestione del registro di data breach.

La nomina del data protection officer, D.P.O., è obbligatoria per un ente pubblico e tale figura dovrà essere designata per un determinato periodo ed in funzione delle qualità professionali, della conoscenza specialistica della materia e in condizioni da assicurare l'esercizio del proprio ruolo senza conflitti di interesse. Il D.P.O. può essere un dipendente dell'ente o un incaricato esterno che assolva al servizio sulla base di uno specifico contratto. Inoltre, il D.P.O., per gli enti pubblici, può essere designato per più autorità pubbliche o organismi pubblici tenuto conto della loro struttura organizzativa; in conseguenza, il titolare del trattamento pubblicherà i dati di contatto del D.P.O. e li comunicherà all'autorità di controllo.

Particolare attenzione andrà posta alla predisposizione di guide e moduli formativi per titolari e responsabili: si tratta di un apposito "corpus" formativo che accompagni i titolari e i responsabili all'uso dei documenti, dei dati e delle procedure nel rispetto della normativa sulla privacy. Andranno definiti e documentati i processi ispettivi (auditing interno) sull'utilizzo del prodotto in conformità alla nuova normativa, procedendo alla reingegnerizzazione dei processi per trattamento "data protection by default and by design". Un altro focus andrà garantito per **l'analisi dei rischi** inerente il trattamento dei dati che significa impostare un sistema di valutazione dei processi e delle tecnologie utilizzate, con documentazione e relativa manutenzione: tutti i processi realizzati con un software devono essere ben documentati, in particolare per gli aspetti relativi alla privacy. La manutenzione dei processi deve prevedere una costante e parallela manutenzione della relativa documentazione, oltre ad un supporto agli interessati sui documenti gestiti (help desk, reclami, richieste di portabilità, ecc.) ed un accompagnamento alla migrazione della raccolta dei consensi precedente alla data di avvio del nuovo Codice ovvero una nuova richiesta per il completamento dei dati.

Il **registro delle attività di trattamento** svolte da un comune, quale titolare del trattamento, deve recare almeno le seguenti informazioni minime:

il nome ed i dati di contatto del comune, eventualmente del contitolare del trattamento e del R.P.D.; le finalità del trattamento; la sintetica descrizione delle categorie di interessati (cittadini, residenti, utenti, dipendenti, amministratori, parti, altro), nonché le categorie di dati personali (dati identificativi, dati genetici, dati biometrici, dati relativi alla salute); le

CamminoDiritto.it
ISSN 2421-7123

categorie di destinatari a cui i dati personali sono stati o saranno comunicati: persona fisica o giuridica, autorità pubblica o altro organismo destinatario; l'eventuale trasferimento di dati personali verso un paese terzo od organizzazione internazionale; ove stabiliti, i termini ultimi previsti per la cancellazione delle diverse categorie di dati; il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate. Il **registro delle categorie di attività** trattate da ciascun responsabile del trattamento dovrà recare almeno le seguenti informazioni minime:

il nome ed i dati di contatto del responsabile del trattamento e del R.P.D. ; le categorie di trattamenti effettuati da ciascun responsabile: raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, uso, comunicazione, raffronto, interconnessione, limitazione, cancellazione, distruzione; l'eventuale trasferimento di dati personali verso un paese terzo od organizzazione internazionale; il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate. **4. Valutazione dell'impatto del trattamento di dati personali.**

Nel caso in cui un tipo di trattamento, specie se preveda, in particolare, l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare, prima di effettuare il trattamento, deve effettuare una **valutazione dell'impatto** del medesimo trattamento ai sensi dell'art. 35, G.D.P.R., considerati la natura, l'oggetto, il contesto e le finalità dello stesso trattamento.

In relazione agli **impatti informatici**, andranno comunque garantiti alcuni processi quali:

un'analisi dei rischi e la revisione dei piani di sicurezza (D.p.i.a.); un adeguamento ai regolamenti sulla sicurezza; un adeguamento alle disposizioni del C.A.D. (codice dell'Amministrazione digitale di cui al d.lgs. n° 82/2005 e ss.mm.ii.); un adeguamento al piano triennale per l'I.C.T. della p.A. (Circolare Agid 24/6/2016, n. 216 di razionalizzazione dei C.E.D.); un'analisi delle basi di dati aziendali; un'accelerazione nell'adozione di banche dati nazionali (A.N.P.R., C.I.E.) e di strumenti e servizi di livello nazionale (ad esempio S.U.A.P., NOIPA, centrali di committenza COMPROPA, PAGOPA); adeguamenti del software di gestione documentale quale orchestratore dei processi informativi dell'ente; una "profilazione" degli utenti per un'assegnazione dei diritti di accesso ai dati; un'automazione del registro dei trattamenti attraverso la gestione dei metadati; una gestione dei diritti di accesso, di oblio, di limitazioni del trattamento, di portabilità; l'adozione di sistemi di conservazione, a norma, dei dati e dei documenti; l'adesione ai poli archivistici regionali. Inoltre, l'articolo 83 del G.D.P.R. stabilisce «le condizioni generali per infliggere sanzioni amministrative pecuniarie» all'ente o impresa che disattenda le disposizioni del regolamento. L'autorità di controllo provvede affinchè le sanzioni amministrative pecuniarie inflitte ai sensi dell'articolo 83 del G.D.P.R. siano,

CamminoDiritto.it
ISSN 2421-7123

in ogni singolo caso, **effettive, proporzionate e dissuasive**. Le sanzioni amministrative amministrative sono inflitte in ragione delle circostanze di ogni singolo caso tenendo conto degli elementi indicati nel comma 2 del citato articolo 83 (natura, gravità, carattere doloso e grado di responsabilità). Inoltre, la violazione delle disposizioni è soggetta a sanzioni amministrative pecuniarie fino a 10.000.000 euro e, per le imprese, fino al 2% del fatturato mondiale totale e annuo dell'esercizio precedente.

E', poi, importante che i titolari del trattamento procedano ad un'adeguata pianificazione adottando e attuando misure tecniche ed organizzative adatte per garantire un livello di sicurezza appropriato rispetto ai rischi individuati. Quindi, sarà necessario predisporre almeno:

un idoneo quadro di gestione dei rischi (una valutazione dei rischi e una valutazione di impatto); una corretta tenuta del registro dei trattamenti; una corretta tenuta di dell'inventario delle violazioni dei dati; una istituzione preventiva di piani appropriati per il trattamento (c.d. mitigazione dei rischi) delle violazioni dei dati personali. In caso di data breach, in base all'art. 83 del G.D.P.R., come sopra accennato, la sanzione pecuniaria è fino a 10 milioni di o fino al 2% del fatturato mondiale annuo dell'impresa. A tal fine, si ricordi che, nel Codice della privacy, all'art. 32 bis è prevista, al comma 3, un'esenzione delle comunicazione dei dati se i dati sono resi inintelligibili tramite misure di protezione secondo un bilanciamento tra l'impatto sensibile e i concreti rischi di arrecare pregiudizio. Il G.D.P.R. alla lettera a) del comma terzo dell'art. 34 ha un contenuto analogo e garantisce un'esenzione anche in caso di violazione dei dati, compreso il caso di cui alla lett. b) comma 2 dell'art. 34: "il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e libertà fondamentali".

In conclusione, non sfugga che la materia della tutela della privacy dei dati personali richiede complessi bilanciamenti fra opposti interessi e principi e che il diritto alla riservatezza accompagna le persone, nelle più svariate espressioni della sua personalità e non si ferma certo all'ingresso delle sedi di imprese e enti pubblici.