publika

Gli
approfondimenti
di Publika

Approfondimento n. 71 - Febbraio 2018

GDPR:
se non sai cosa significa, hai un problema

di Augusto Sacchi

Scopri i corsi di Publika
(tasto CTRL+clic per aprire il collegamento)

Publika S.r.l.
Sede legale
Via Pascoli 3
46049 Volta Mantovana (MN)
Sede operativa
Via Parigi 38
46047 Porto Mantovano (MN)
Telefono: 0376 1586860
Fax: 0376 1760102
Email: info@publika.it
Email PEC: info@pec.publika.it
Codice Fisc. e P. IVA
02213820208

1. GDPR: cos'è

Il regolamento generale sulla protezione dei dati (GDPR, *General Data Protection Regulation - Regolamento UE 2016/679)* è un REGOLAMENTO con il quale il Parlamento Europeo e il Consiglio dell'Unione Europea intendono rafforzare e rendere più omogenea la protezione dei dati personali di cittadini dell'Unione Europea e dei residenti nell'Unione Europea, sia all'interno che all'esterno dei confini della UE.

Il testo, pubblicato su Gazzetta Ufficiale Europea il 4 maggio 2016 ed entrato in vigore il 25 maggio dello stesso anno, inizierà ad avere efficacia il 25 maggio 2018.

Il Regolamento – *attenzione!* - non richiede alcuna forma di legislazione applicativa da parte degli Stati membri.

2. GDPR: finalità

Gli obiettivi principali perseguiti con l'approvazione del GDPR sono quelli di **restituire ai cittadini il controllo dei propri dati personali e di semplificare il contesto normativo che riguarda gli affari internazionali,** unificando e rendendo omogenea la normativa sulla *privacy* dentro la UE.

Dal 25 maggio 2018, il GDPR andrà a sostituire la direttiva sulla protezione dei dati (ufficialmente Direttiva 95/46/EC) istituita nel 1995 e abrogherà alcune norme del Codice per la protezione dei dati personali italiano (d.lgs. 30 giugno 2003, n. 196) che risulteranno con esso incompatibili. Ciò potrà generare confusione per alcuni aspetti, ma si attende – ed è auspicabile che venga emanata presto - una normativa italiana "di raccordo" che metta ordine e inserisca le norme del Codice *privacy* non incompatibili, all'interno dell'impianto normativo del Regolamento.

3. GDPR: a chi si applica

Il regolamento si applica ai dati personali delle persone residenti nell'Unione Europea. Inoltre, a differenza dell'attuale direttiva, il regolamento si applica anche a imprese ed enti, organizzazioni in generale, con sede legale fuori dall'UE, che trattano dati personali di residenti nell'Unione Europea (si pensi ai più importanti *social media*). Ciò anche a prescindere dal luogo o dai luoghi ove sono collocati i sistemi di archiviazione (*storage*) e di elaborazione (*server*).

Va sottolineato che il regolamento non riguarda la gestione di dati personali per attività di sicurezza nazionale o di ordine pubblico ("*le autorità competenti per gli scopi di prevenzione, indagine, individuazione e persecuzione di reati penali o esecuzione di provvedimenti penali*"). Per comprendere meglio il concetto di "dato personale" è bene ricordare che, secondo la Commissione Europea: "*i dati personali sono qualunque informazione relativa a un individuo, collegata alla sua vita sia privata, sia professionale o pubblica. Può riguardare qualunque dato personale: nomi, foto, indirizzi email, dettagli bancari, interventi su siti web di social network, informazioni mediche o indirizzi IP di computer.*" Il regolamento disciplina solo il trattamento di dati personali delle persone fisiche e non quello delle società (persone giuridiche).

4. GDPR: dati giudiziari

Tramite un'altra Direttiva collegata, la numero UE 2016/680, in aggiunta al regolamento di cui sopra, sarà applicata una disciplina speciale e, in parte derogatrice, per i trattamenti dei dati da parte dell'Autorità Giudiziaria e di tutte le forze di polizia. In ragione della caratteristica dell'istituto della direttiva europea tali trattamenti dei dati (Autorità Giudiziaria e forze di polizia) continueranno ad essere differenti da Stato a Stato ed oggetto di una legislazione separata di carattere nazionale.

5. GDPR: regole e sportello unico

A tutti gli stati membri dell'Unione europea si applicherà un insieme unico di regole. Ciascun stato membro istituirà un'autorità sovrintendente indipendente per dare udienza ai reclami, effettuare indagini, sanzionare le infrazioni amministrative, eccetera. Le autorità sovrintendenti, in ciascuno stato membro, collaboreranno con le altre, fornendo assistenza reciproca e organizzando operazioni congiunte. Qualora una società abbia più stabilimenti nell'UE, avrà un'unica autorità sovrintendente come propria "autorità principale", sulla base dell'ubicazione del proprio "stabilimento principale", ossia il posto dove hanno luogo le principali attività di gestione. L'autorità principale agirà quale "sportello unico" per supervisionare tutte le attività di gestione dei dati di quella ditta nell'UE. Il Comitato europeo della

protezione dati (EDPB, *European Data Protection Board*) coordinerà le autorità sovrintendenti. L'EDPB andrà a sostituire il gruppo di lavoro dell'Articolo 29[1].
Saranno mantenute delle eccezioni nel caso di dati elaborati in un contesto di impiego e di dati trattati a scopo di sicurezza nazionale, che potrebbero ancora essere soggetti ai regolamenti delle singole nazioni.

6. GDPR: responsabilità

Il principio di responsabilità legato al trattamento dei dati personali resta ancorato – come già oggi nel Codice per la protezione dei dati personali, d.lgs. 196/2003 - ad un concetto di responsabilità per esercizio di attività pericolosa, con una valutazione *ex ante* in concreto ed una sostanziale inversione dell'onere della prova. Per non rispondere del danno commesso, derivante dal trattamento dei dati personali, occorre dimostrare di aver fatto, in concreto, tutto il possibile per evitarlo. Il Regolamento aggancia e sviluppa questo tipo di responsabilità verso il concetto di *ACCOUNTABILITY*[2]. In altri termini, si può affermare che i soggetti coinvolti sono tenuti ad osservare i principi applicabili al trattamento dei dati personali, adempiendo alle relative obbligazioni ed essere in grado di comprovarlo, qualora venga richiesto.

7. GDPR: obblighi di informazione

I requisiti per le informative agli interessati sul trattamento dei dati, in parte rimangono confermate e, in parte, vengono ampliati. Essi devono includere il tempo di mantenimento dei dati personali e occorre fornire i contatti di chi controlla i dati e del funzionario preposto alla protezione dei dati (RPD-DPO).
È stato introdotto, inoltre, il diritto di contestazione delle decisioni automatizzate, compresa la *profilazione*[3]. I cittadini hanno, ora, il diritto di contestare e contrastare decisioni che impattano su di loro e che sono state realizzate unicamente in base ai risultati di un algoritmo.
Tale diritto - fatta eccezione per dati personali intesi ad identificare in modo univoco una persona fisica - non si applica nel caso in cui la decisione:

a) sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento;
b) sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, che precisa inoltre misure adeguate a tutela dei diritti, della libertà e dei legittimi interessi dell'interessato;
c) si basi sul consenso esplicito dell'interessato.

I principi di *Privacy by Design and by Default*[4] richiedono che la protezione dei dati faccia parte del progetto di sviluppo dei processi aziendali per prodotti e servizi.
Le impostazioni di *privacy* devono essere configurate su un livello alto di trattamento e di protezione, in modo predefinito.

8. GDPR: valutazione dell'impatto

Una delle novità più significative del GDPR è la valutazione d'impatto sulla protezione dei dati. Una misura preventiva inerente il cosiddetto *Risk assessment*[5], che ciascun titolare del trattamento dei dati è tenuto ad effettuare, nei casi in cui si verifichino rischi specifici per i diritti e le libertà dei soggetti dei dati. La valutazione e la riduzione del rischio sono richieste insieme ad

---

1 http://www.garanteprivacy.it/home/attivita-e-documenti/attivita-comunitarie-e-internazionali/cooperazione-in-ambito-ue/gruppo-di-lavoro-ex-articolo-29
2 Traduzione in italiano "*il rendere conto del proprio operato*".
3 Significato di *profilazione*: analisi ed elaborazione di dati relativi a utenti o clienti, al fine di suddividere l'utenza in gruppi omogenei di comportamento;
4 Significato: *Privacy by default*: necessità di tutelare la vita privata dei cittadini di default, ovvero come impostazione predefinita dell'organizzazione aziendale. *Privacy by design*: la protezione dei dati deve avvenire fin dal disegno o progettazione di un processo aziendale.
5 In italiano: valutazione del rischio;

un'approvazione preventiva da parte delle autorità per la protezione dei dati (DPA, *Data Protection Authority*) per rischi elevati. I Responsabili per la protezione dei dati (DPO-RPD) sono tenuti a verificare l'osservanza delle norme del Regolamento, da parte dei titolari e, nel caso di valutazioni di impatto, se richiesto dal titolare, sono tenuti a consultarsi con esso.

9. GDPR: consenso

Un valido consenso deve essere **esplicitamente dato** per la raccolta dei dati e per i propositi per i quali vengono usati. Pertanto, se la richiesta viene inserita nell'ambito di altre dichiarazioni, essa va distinta e formulata con linguaggio **semplice e chiaro**. Condizione di validità del consenso è che le finalità per cui viene richiesto siano **esplicite, legittime, adeguate e pertinenti**.
Nel caso in cui il consenso al trattamento dei propri dati personali, per una o più specifiche finalità, sia stato **espresso da minori** esso è valido solo se il minore ha almeno sedici anni. L'età viene ridotta a tredici anni, solo se lo stato membro ha previsto, con legge, una diversa età purché non inferiore a questa.
Qualora il minore abbia un'età inferiore ai 16 o 13 anni, il consenso al trattamento deve essere dato da un genitore o da chi eserciti la potestà, e deve essere verificabile. I controllori dei dati devono essere in grado di provare il consenso (*opt-in*) e il consenso può essere ritirato o modificato con l'introduzione di limitazioni nel trattamento.
Per ciò che riguarda le pubbliche amministrazioni, sulla base della legislazione vigente, è bene ricordare che i soggetti pubblici, fatta eccezione per le istituzioni che operano in ambito sanitario, "*non devono richiedere il consenso dell'interessato*" (art.18, comma 4, d.lgs. 196/2003) e possono trattare dati diversi da quelli sensibili e giudiziali, "*anche in mancanza di una norma di legge o di regolamento*" che preveda il trattamento (art.19, comma 1).

10. GDPR: sicurezza dei dati

La sicurezza dei dati raccolti **è garantita dal titolare del trattamento e dal responsabile del trattamento** chiamati a mettere in atto le misure tecniche e organizzative idonee per garantire un livello di sicurezza adeguato al rischio. A tal fine, il titolare e il responsabile del trattamento, garantiscono che chiunque acceda ai dati raccolti lo faccia nel rispetto dei poteri da loro conferiti e dopo essere stato appositamente istruito, salvo che lo richieda il diritto dell'Unione o degli Stati membri.
A tutela e garanzia degli interessati, il Regolamento UE 2016/679, disciplina anche il caso di trasferimento dei dati personali verso un paese terzo o un'organizzazione internazionale e prevede che l'interessato venga prontamente informato in presenza di una violazione che metta a rischio i suoi diritti e le sue libertà.

11. GDPR: responsabile per la protezione dei dati (cosiddetto DPO, Data Protection Officer)

Senza alcun dubbio, una delle principali novità del Regolamento europeo è l'obbligo – non previsto prima in Italia - di individuare e nominare un Responsabile per la Protezione dei Dati (RPD). La designazione del RPD è obbligatoria quanto "*il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali*".
Le Pubbliche amministrazioni devono, quindi, individuare e nominare una persona esperta di legislazione e pratiche relative alla protezione dei dati, che avrà il compito di assistere colui che li controlla o li gestisce, al fine di verificare l'osservanza interna al regolamento.
Il responsabile per la protezione dei dati (RPD-DPO) è una figura simile - ma non identica - al preposto all'osservanza, in quanto ci si aspetta che il primo abbia una buona padronanza dei processi informatici, della sicurezza dei dati (inclusa la gestione dei *ciber*-attacchi) e di altre questioni di coerenza aziendale riguardanti il mantenimento e l'elaborazione di dati personali e sensibili.
Per ulteriori approfondimenti sulla figura del RPD, è possibile consultare le FAQ del Garante della privacy, reperibili al link: http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/7322110.

Si ricorda, infine, che il nominativo e i dati di contatto del RPD (recapito postale, telefono, email) devono essere resi disponibili nella intranet dell'Ente e comunicati al Garante per la protezione dei dati personali. I dati di contatto saranno, altresì, pubblicati sul sito internet istituzionale.

A completamento informativo, in fondo al presente articolo, viene riportato uno *Schema di atto di designazione del Responsabile della Protezione dei Dati personali (RPD),* ai sensi dell'art. 37 del Regolamento UE 2016/679, da adottarsi, anche nelle P.A., entro il 25 maggio 2018.

12. GDPR: Violazione dei dati (cd Data Breach)

Il titolare del trattamento dei dati avrà l'obbligo legale di rendere note le fughe di dati all'autorità nazionale e di comunicarle entro 72 ore da quando ne è venuto a conoscenza. I resoconti delle fughe di dati non sono soggetti ad alcun standard *de minimis* e debbono essere riferite all'autorità sovrintendente (Garante della *privacy* nazionale) non appena se ne viene a conoscenza e comunque entro il termine suindicato (72 ore). In alcune situazioni, le persone di cui sono stati sottratti i dati, dovranno essere avvertite.

13. GDPR: Sanzioni

Il GDPR, all'articolo 83, prevede una serie di sanzioni che devono avere carattere di effettività, proporzionalità e dissuasività.
Le sanzioni amministrative pecuniarie riportate nell'elenco "A", possono essere **integrative**, oppure **completamente sostitutive** delle sanzioni correttive indicate nell'elenco "B" e si distinguono in sanzioni di carattere economico e sanzioni correttive.
La decisione sull'applicazione delle sanzioni spetta all'autorità di controllo (in Italia: l'Autorità Garante per la Protezione dei Dati Personali), la quale, nella sua valutazione, terrà conto delle circostanze del singolo caso, ossia:

- ✓ della natura, gravità e durata della violazione;
- ✓ del carattere doloso o colposo della violazione;
- ✓ delle misure adottate per attenuare il danno subito dagli interessati;
- ✓ delle eventuali precedenti violazioni commesse dal titolare del trattamento;
- ✓ del grado di cooperazione con l'autorità di controllo;
- ✓ degli eventuali altri fattori aggravanti.

"A" - Le **SANZIONI DI CARATTERE ECONOMICO,** sono le seguenti:

- inosservanza degli obblighi del titolare e del responsabile del trattamento; inosservanza degli obblighi dell'organismo di certificazione; inosservanza degli obblighi dell'organismo di controllo: fino a 10 milioni di Euro, o per le imprese, fino al 2% del fatturato annuo mondiale dell'esercizio precedente;
- inosservanza dei principi base del trattamento; inosservanza dei diritti degli interessati; inosservanza delle disposizioni sul trasferimento dei dati personali in paesi terzi o verso organizzazioni internazionali; inosservanza di un ordine, limitazione provvisoria o definitiva o di un ordine di sospensione dei flussi da parte dell'autorità di controllo: fino a 20 milioni di Euro, o per le imprese, fino al 4% del fatturato annuo mondiale dell'esercizio precedente.
- inosservanza di un ordine correttivo dell'autorità di controllo: fino a 20 milioni di Euro, o per le imprese, fino al 4% del fatturato annuo mondiale dell'esercizio precedente.

"B" - Le **SANZIONI CORRETTIVE** sono connesse ai poteri dell'Autorità di controllo. Essi consistono nel:

- rivolgere avvertimenti al titolare del trattamento o al responsabile del trattamento sul fatto che i trattamenti previsti possono violare il GDPR;

- rivolgere ammonimenti al titolare e del trattamento o al responsabile del trattamento ove i trattamenti abbiano violato le disposizioni del GDPR;
- ingiungere al titolare del trattamento o al responsabile del trattamento di soddisfare le richieste dell'interessato di esercitare i relativi diritti;
- ingiungere al titolare o al responsabile del trattamento di conformare i trattamenti alle disposizioni del GDPR, anche specificando in che modo ed entro quale termine;
- ingiungere al titolare del trattamento di comunicare all'interessato una violazione dei dati personali;
- imporre una limitazione provvisoria o definitiva al trattamento, incluso il divieto di trattamento;
- ordinare la rettifica, la cancellazione di dati personali o la limitazione del trattamento e la notificazione di tali misure ai destinatari cui sono stati comunicati i dati personali;
- revocare la certificazione o ingiungere all'organismo di certificazione di ritirare la certificazione, oppure ingiungere all'organismo di certificazione di non rilasciare la certificazione se i requisiti per la certificazione non sono o non sono più soddisfatti;
- infliggere una sanzione amministrativa pecuniaria in aggiunta alle presenti misure (vedi capitolo precedente);
- ordinare la sospensione dei flussi di dati verso un destinatario in un paese terzo o un'organizzazione internazionale.

14. GDPR: Diritto alla cancellazione, limitazione e rettifica

Il cosiddetto *diritto all'oblio* è stato sostituito da un più limitato *diritto alla cancellazione* nella versione del GDPR. Il Regolamento (art. 17) stabilisce che il soggetto a cui i dati si riferiscono ha il diritto di richiedere la cancellazione dei propri dati personali, sulla base di una serie di giurisdizioni che comprendono – tra le altre - la mancata osservanza della legalità. Tra le varie casistiche rientra anche il caso in cui gli interessi o i diritti fondamentali del soggetto dei dati, richiedente la loro protezione, prevalgono sui legittimi interessi del controllore. L'interessato deve poter esercitare questo suo diritto **con la stessa facilità** con cui ha espresso il consenso al trattamento dei suoi dati. Il responsabile del trattamento, dietro richiesta dell'interessato, dovrà comunicare all'interessato i destinatari a cui ha trasmesso la sua richiesta di cancellazione. Sul responsabile del trattamento grava lo stesso onere in caso di richiesta di limitazione o di rettifica dei dati, presentata dall'interessato.

15. GDPR: portabilità dei dati

Una persona deve essere in grado di trasferire i propri dati personali da un sistema di elaborazione elettronico a un altro senza che il controllore dei dati possa impedirlo. Inoltre, i dati devono essere forniti dal controllore in un formato strutturato e di uso comune. Il diritto alla portabilità dei dati è sancito dall'art. 18 del GDPR. Gli esperti legali vedono nella versione finale di questa misura, la creazione di un "nuovo diritto" che "si estende oltre l'ambito della portabilità dei dati tra due controllori, così come stipulato dall'articolo 18"

16. GDPR: come si compone:

Si riportano alcune informazioni generali, più specifiche, sulla composizione del nuovo regolamento europeo.
Il documento è diviso in due parti:

- la prima definita "CONSIDERANDO" che va da pagina 9 a 73, dove vengono definiti i principi e le motivazioni dell'atto. I *Considerando* sono 173;
- la seconda parte è quella del "REGOLAMENTO" che va da pagina 74 a 187, dove sono definiti i Capi (11), le Sezioni e gli Articoli (n. 99).

Come già sottolineato sopra, il Regolamento non necessita di «recepimenti» da parte degli Stati membri, ma questi hanno/avevano DUE ANNI (sino al 25 maggio 2018) per adeguare le proprie normative interne e, gli enti che trattano i dati hanno due anni per essere sensibilizzati sulle novità introdotte.

La Commissione europea potrà adottare atti delegati e di esecuzione al fine di rendere operativa la disciplina, ma lascia ai legislatori nazionali la facoltà di introdurre, a seconda delle circostanze, norma nazionali *ad hoc*.
Il regolamento nasce dalla necessità di adattare la legislazione dell'Unione Europea (in vigore da 19 anni) alle **nuove tecnologie e all'uso sempre più disparato di internet e social media**. Per come il regolamento è strutturato e per la sua valenza generale applicabile a tutti gli stati dell'Unione europea, si ritiene di poter escludere la possibilità che venga prorogato il termine ultimo di applicazione, già fissato, sin dall'aprile 2016, al 25 maggio 2018.

17. Prima Guida Applicativa Emanata Dal Garante Privacy Italiano

L'Autorità Garante per la Protezione dei Dati Personali (cd. *Garante privacy*) ha realizzato una prima Guida applicativa sul DGPR, pubblicata con comunicato del 28 aprile 2017 e successivamente aggiornata. La Guida traccia un quadro generale delle principali innovazioni introdotte dalla normativa e fornisce indicazioni utili sulle prassi da seguire e gli adempimenti da attuare per dare corretta applicazione alla normativa, efficace dal 25 maggio 2018.

L'obiettivo della Guida è duplice:

a) offrire un primo "strumento" di ausilio ai soggetti pubblici e alle imprese che stanno affrontando il passaggio alla nuova normativa *privacy*;
b) far crescere la consapevolezza sulle garanzie rafforzate e sui nuovi importanti diritti che il Regolamento riconosce alle persone.

Il testo della Guida è articolato in SEI sezioni tematiche che trattano:

1. Fondamenti di liceità del trattamento;
2. Informativa;
3. Diritti degli interessati;
4. Titolare, responsabile, incaricato del trattamento;
5. Approccio basato sul rischio del trattamento e misure di *accountability* di titolari e responsabili;
6. Trasferimenti internazionali di dati.

Ogni sezione illustra in modo semplice e diretto **cosa cambierà e cosa rimarrà immutato** rispetto all'attuale disciplina del trattamento dei dati personali, aggiungendo raccomandazioni pratiche per una corretta implementazione delle nuove disposizioni introdotte dal Regolamento.
La guida è disponibile sul sito del Garante in formato ipertestuale navigabile, al link:
http://www.garanteprivacy.it/guida-all-applicazione-del-regolamento-europeo-in-materia-di-protezione-dei-dati-personali

18. Formazione obbligatoria in materia di GDPR

Il nuovo Regolamento sulla *privacy* prevede un obbligo di formazione a tutti i livelli, comprese, ovviamente, le Pubbliche amministrazioni. L'obbligo riguarda tutte le figure presenti nell'organizzazione degli enti e comprende sia i dipendenti che i collaboratori. Più in particolare, la centralità della formazione è prevista nell'art. 32, paragrafo 4, del Regolamento che, testualmente recita:

> *"il titolare del trattamento ed il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare dei dati, salvo che lo richieda il diritto dell'Unione o degli Stati membri".*

La formazione, pertanto, diventa un prerequisito per poter operare sui dati all'interno delle P.A. e la stessa dovrebbe avere un taglio pratico e operativo, di natura interdisciplinare e riguardare tutti i soggetti, a vario titolo, coinvolti.
La formazione deve essere finalizzata a contrastare i rischi general e specifici dei trattamenti, comprese le misure organizzative, tecniche ed informatiche adottate, nonché i vari livelli di responsabilità e le relative sanzioni, come meglio illustrate al precedente Paragrafo 13.
Le Pubbliche amministrazioni, per quanto sopra, sin da subito, dovranno:

a) pianificare un percorso di formazione di tutte le figure coinvolte, inserendolo nel Piano Formativo annuale, tenendo conto della struttura dell'ente, i profili organizzativi, le finalità di ciascun corso, la possibilità di associare, con altri enti, l'attività formativa;
b) prevedere idonee risorse in sede di approvazione del bilancio;
c) prevedere prove finali di verifica del percorso formativo e sessioni di aggiornamento sulla base delle modifiche normative, organizzative e tecniche che interverranno;
d) stabilire aree di priorità nell'attività formativa partendo – ad esempio – dal Responsabile Protezione dei Dati (RPD) e dai suoi collaboratori; dalle figure apicali presenti nell'ente; i neo assunti; gli amministratori di sistema e tutto il personale autorizzato al trattamento.

Una efficace attività formativa, in definitiva, costituisce un tassello rilevante del sistema di gestione della tutela dei dati personali, in grado di dare concretezza al principio di *accontuability*, inteso come capacità di dimostrare di aver adottato misure di sicurezza idonee ed efficaci.
Alla luce di quanto sopra illustrato, va aggiunto che l'attività di formazione e aggiornamento sul trattamento dei dati DEVE necessariamente integrarsi con la formazione – anch'essa obbligatoria - in materia di prevenzione della corruzione, codici di comportamento per i dipendenti delle P.A., la recente normativa in materia di FOIA (o accesso civico generalizzato), il *whistleblowing* e soprattutto, con la normativa sugli obblighi di pubblicità e pubblicazione dei dati, documenti e informazioni, nei siti *web* delle Pubbliche amministrazioni. Le correlazioni tra Trasparenza e *Privacy*, non da oggi, sono una delle questioni più spinose e complesse per gli operatori degli enti pubblici. Solo una formazione specifica e mirata, interdisciplinare e concreta, con fornitura di esempi pratici, può evitare pericolosi (e costosi) errori, pesantemente sanzionati dal Garante *Privacy*.

19. Conclusioni

Come spesso (ci) capita, la scadenza del 25 maggio 2018 è stata un po' sottovalutata dalle pubbliche amministrazioni, intorpidite da trent'anni di *decreti Milleproroghe*. Le procedure da sistemare, verificare, individuare, nominare, formare, analizzare e predisporre, prima di tale data, sono numerose e, non sempre, di facile declinazione. Bisognerà anche decidere se la nuova figura – già prevista in altri paesi dell'Unione europea – denominata Responsabile dei Dati Personali (RDP) o, in inglese, *Data Protection Officer* (DPO), debba essere un dipendente dell'ente o, come previsto nel comma 6, dell'art. 37 del regolamento[6], affidare i compiti a un soggetto esterno, mediante stipula di un contratto di servizio.
Certamente, tra le cose da sistemare, con urgenza, ci sono le informative sul trattamento dei dati personali, ora previste dall'art. 13 del d.lgs. 196/2003. Si tratta di quelle "informative" che troviamo, ormai da anni, in fondo alla modulistica utilizzata dai cittadini/utenti, per accedere a delle procedure o attivare procedimenti amministrativi di qualsiasi genere.
Un ultima riflessione va utilizzata per specificare che il Regolamento UE non incide per nulla, al momento, sulle disposizioni in materia di diritto di accesso civico e obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni, che resta disciplinato dal d.lgs. 14 marzo 2013, n. 33 e successive modificazioni ed integrazioni (d.lgs. 97/2016).

[6] 6. Il responsabile della protezione dei dati può essere un dipendente del titolare del trattamento o del responsabile del trattamento oppure assolvere i suoi compiti in base a un contratto di servizi.

NOTA:
Per la stesura del presente articolo ci si è avvalsi delle seguenti fonti informative:

- *REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE* (regolamento generale sulla protezione dei dati);
- G*uida all'applicazione del Regolamento europeo in materia di protezione dei dati personali,* predisposta dal Garante della Privacy italiano;
- *Linee guida sui responsabili della protezione dei dati*, predisposte da Gruppo di Lavoro Articolo 29 per la Protezione dei dati, adottate il 13/12/2016, Versione emendata e adottata in data 5 aprile 2017;
- https://it.wikipedia.org/wiki/Regolamento_generale_sulla_protezione_dei_dati;
- Avv. Mauro Alovisio *"Formazione privacy obbligatoria, con GDPR; che c'è da sapere"*; https://www.agendadigitale.eu/cittadinanza-digitale/la-formazione-privacy-obbligatoria-nelle-pa-ed-imprese-come-pietra-angolare-del-sistema/
- FAQ del Garante Privacy sul GDPR: http://www.garanteprivacy.it/regolamentoue

Allegato A alle Nuove Faq sul Responsabile della Protezione dei dati (RPD) in ambito pubblico (in aggiunta a quelle adottate dal Gruppo Art. 29 in Allegato alle Linee guida sul RPD

Schema di

Atto di designazione del Responsabile della Protezione dei Dati personali (RDP) ai sensi dell'art. 37 del Regolamento UE 2016/679

Premesso che:

- Il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 *«relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati)»* (di seguito *RGPD*), in vigore dal 24 maggio 2016, e applicabile a partire dal 25 maggio 2018, introduce la figura del Responsabile dei dati personali (RDP) (artt. 37-39);
- Il predetto Regolamento prevede l'obbligo per il titolare o il responsabile del trattamento di designare il *RPD «quando il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali»* (art. 37, paragrafo 1, lett a);
- Le predette disposizioni prevedono che il RPD *«può essere un dipendente del titolare del trattamento o del responsabile del trattamento oppure assolvere i suoi compiti in base a un contratto di servizi»* (art. 37, paragrafo 6) e deve essere individuato *«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»* (art. 37, paragrafo 5) *e «il livello necessario di conoscenza specialistica dovrebbe essere determinato in base ai trattamenti di dati effettuati e alla protezione richiesta per i dati personali trattati dal titolare del trattamento o dal responsabile del trattamento»* (considerando n. 97 del RGPD);

Nel caso in cui si opti per la designazione di un RPD condiviso si dovrà aggiungere

- Le disposizioni prevedono inoltre che *«un unico responsabile della protezione dei dati può essere designato per più autorità pubbliche o organismi pubblici, tenuto conto della loro struttura organizzativa e dimensione»* (art. 37, paragrafo 3);

Considerato che *l'Ente X:*

- è tenuto alla designazione obbligatoria del RPD nei termini previsti, rientrando nella fattispecie prevista dall'art. 37, par. 1, lett a) del RGPD;

Nel caso in cui si opti per la designazione di un RPD condiviso si dovrà aggiungere

- ha ritenuto di avvalersi della facoltà, prevista dall'art. 37, paragrafo 3, del Regolamento, di procedere alla nomina condivisa di uno stesso RPD con gli *Enti X, Y, Z,* sulla base delle valutazioni condotte di concerto con i predetti Enti in ordine a … (es. dimensioni, affinità tra le relative strutture organizzative, funzioni (attività) e trattamenti di dati personali, razionalizzazione della spesa);

- all'esito di … (*indicare la procedura selettiva interna o esterna, gara, altro*) ha ritenuto che il la/il ....., sia in possesso del livello di conoscenza specialistica e delle competenze richieste dall'art. 37, par. 5, del RGPD, per la nomina a RPD, e non si trova in situazioni di conflitto di interesse con la posizione da ricoprire e i compiti e le funzioni da espletare;

DESIGNA

(*generalità della persona individuata*), Responsabile della protezione dei dati personali (RPD) per l'*Ente X*,

Il predetto, nel rispetto di quanto previsto dall'art. 39, par. 1, del RGPD è incaricato di svolgere, in piena autonomia e indipendenza, i seguenti compiti e funzioni:

a) informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal RGPD, nonché da altre disposizioni nazionali o dell'Unione relative alla protezione dei dati;
b) sorvegliare l'osservanza del RGPD, di altre disposizioni nazionali o dell'Unione 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 la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35 del RGPD;
d) cooperare con il Garante per la protezione dei dati personali;
e) fungere da punto di contatto con il Garante per la protezione dei dati personali per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione;

(*è possibile inserire di seguito anche ulteriori compiti, purché non incompatibili, quali ad es.:*

f) tenere il registro delle attività di trattamento sotto la responsabilità del titolare o del responsabile ed attenendosi alle istruzioni impartite...)

I compiti del Responsabile della Protezione dei Dati personali attengono all'insieme dei trattamenti di dati effettuati dall' Ente X.

L'*Ente X* si impegna a:

a) mettere a disposizione del RPD le seguenti risorse al fine di consentire l'ottimale svolgimento dei compiti e delle funzioni assegnate ... (*specificare, ad es. se è stato istituito un apposito Ufficio o gruppo di lavoro, le relative dotazioni logistiche e di risorse umane, nonché i compiti o le responsabilità individuali del personale*);
b) non rimuovere o penalizzare il RPD in ragione dell'adempimento dei compiti affidati nell'esercizio delle sue funzioni;
c) garantire che il RPD eserciti le proprie funzioni in autonomia e indipendenza e in particolare, non assegnando allo stesso attività o compiti che risultino in contrasto o conflitto di interesse;

DELIBERA

di designare ..... come Responsabile dei dati personali (RPD) per *l'Ente X*

Data .....

Il nominativo e i dati di contatto del RPD (recapito postale, telefono, email) saranno resi disponibili nella intranet dell'Ente (url...., ovvero bacheca) e comunicati al Garante per la protezione dei dati personali. I dati di contatto saranno, altresì, pubblicati sul sito internet istituzionale.
n inadempimento ai danni dell'interesse del datore di lavoro[7].

[7] Cass .lav. n. 17625/2014