25 giugno 2018: ad un mese dal GDPR Start Day la PA è ancora ai blocchi di partenza?

Author : Leonardo Scalera

Date : 3 luglio 2018

E così dal fatidico GDPR START DAY (25 maggio 2018) è trascorso già un mese. Sia chiaro, si tratta di un lasso temporale troppo breve, anzi al limite del “ridicolo” per poter effettuare una qualsivoglia considerazione o valutazione sul “nuovo”, sui “cambiamenti”, sul “dopo” dall’entrata in vigore del nuovo Regolamento per la Protezione dei Dati Personali (Reg. UE – GDPR 2016/679), ma non è detto che in questo breve arco temporale qualcosa non sia effettivamente “cambiato”.

Nei mesi trascorsi dalla data di emanazione del GDPR (e parliamo dell’anno 2016), in quasi tutti i settori abbiamo assistito all’alternarsi di momenti di sconforto contrapposti a periodi di euforia, momenti di profonda frustrazione, di disfatta contrapposti a momenti di (quasi) certezza che “in Italia non cambierà nulla”, “tanto faranno la proroga” […], ma alla fine dei conti, trascorsi i 24 mesi concessi per gli adeguamenti ora bisogna guardare in faccia la realtà e guardarsi (tutti) allo specchio chiedendosi cosa è stato fatto, cosa andava, invece, realmente fatto e come dare un’accelerata su quello che ancora c’è da fare.

Il settore che, probabilmente, ha sofferto e continua a “soffrire” maggiormente per l’avvento della nuova normativa è, nel nostro bel paese, la Pubblica Amministrazione (nell’accezione più ampia possibile – amministrazioni centrali, locali, enti economici, aziende pubbliche, sanità …). Sulle motivazioni molto (forse anche troppo) è stato detto nel corso di questi mesi e, infatti, la PA è stata (nuovamente) oggetto di particolari attenzioni da parte di esperti, addetti ai lavori, osservatori, commissioni ecc… che, alla fine, hanno concordato nel riscontrare una serie di cause o concause responsabili della situazione in cui la PA italiana versa (come anche in passato versava) anche in ambito di Protezione dati Personali (e-Privacy):

- Mancanza di risorse finanziarie;
- Problematiche legate all’età e alla non specializzazione/preparazione del personale (legato al blocco del turn-over [ma non solo – ndr -])
- Scarsa (e a volte del tutto mancante) cultura nelle materie specifiche.

Va ricordato, non solo per dovere di cronaca, che la PA rientra fra quelle “categorie” di soggetti obbligati all’applicazione della nuova normativa, sui quali ricadono un numero maggiore di obblighi/adempimenti da effettuare proprio per le funzioni in essa incardinate.

Citiamo a titolo di esempio(non esaustivo) alcuni degli obblighi cui la PA deve comunque adempiere: l’art. 30 - Registi delle attività di trattamento - , l’art. 35 (e considerando 84 – 89 – 93 – 95) - Valutazione d’impatto sulla protezione dei dati -, l’art. 37 (e considerando 97) - Designazione del responsabile della protezione dei dati ; mentre per le aziende una serie di valutazioni preliminari in merito ai precedenti punti vanno fatte, per la PA non necessitano in quanto la stessa è OBBLIGATA ad adempiervi in toto.

A supporto va anche riportato quanto indicato dall’Autorità Garante per la Protezione Dati Personali nazionale quando, proprio in tema di GDPR e PA, ha indicato i tre punti fondamentali ai quali ogni PA doveva essere, quantomeno, conforme alla data del 25 maggio 2018 data la “consapevolezza” dell’Autorità di vigilanza e controllo delle “reali condizioni della PA italiana”:

1. Istituzione dei registri di trattamento;
2. Nomina del responsabile della protezione dei dati personali;
3. Procedura per la notifica in caso di violazione dei dati personali;

NB: Per il punto c) noto anche come “DATA BREACH” (art. 33) richiede anche per la PA una valutazione preliminare al fine di valutare la necessità di informare o meno gli interessati dell’avvenuta violazione così come previsto dall’art. 34 c. 1.

Trascorso un mese, come dicevano, dalla fatidica data del 25 maggio si è cercato di verificare se, e come, all’interno della PA (sia a livello centrale che locale) il cambiamento fosse percepibile o, quantomeno, se questo processo si sia almeno innescato.

Partendo dalle tre priorità fissate dall’autorità garante nazionale, senza dubbio, quella più facilmente verificabile risulta essere proprio la nomina del DPO (Data Protection Officer)/ RPD (Responsabile della Protezione dei Dati) in virtù di quanto previsto all’Art. 37 c. 7 [*il titolare del trattamento o il responsabile del trattamento pubblica i dati di contatto del responsabile della protezione dei dati e li comunica all’autorità di controllo*] e in previsione di quanto indicato al c. 4 dell’Art. 38 [*gli interessati possono contattare il responsabile della protezione dei dati per tutte le questioni relative al trattamento dei loro dati personali e l’esercizio dei loro diritti derivanti dal presente regolamento*].

Muovendosi nel web fra siti istituzionali di ministeri, dipartimenti, agenzie si ha effettivamente la sensazione del cambiamento, rispetto ad alcuni mesi fa in quanto è possibile rinvenire i “dati di contatto” del DPO (in molti casi), oppure (addirittura) i dati completi del DPO e dei suoi contatti con anche copia del provvedimento di nomina dello stesso.

A questo punto, però, nascono delle domande, forse ovvie, ma necessarie (a parere di chi scrive):

- Può bastare come “dati di contatto del DPO” esclusivamente una casella di posta

elettronica al limite “dell’anonimato” (es. amministrazione@amministrazione.it)?
- Perché non seguire le indicazioni dell’Autorità Garante Nazionale che nelle FAQ in merito al DPO in ambito pubblico consigliava la pubblicazione del nominativo del DPO sul sito web del soggetto pubblico, nonché l’inserimento di tutti i dati all’interno della sezione “Amministrazione Trasparente” e non solo in quella “Privacy”(se esistente)?
- E’ sufficiente indicare esclusivamente una “mail generica” di riferimento al DPO all’interno dell’informativa privacy del sito web?

E ancora …

- Come è possibile che all’interno di diversi siti web di amministrazioni centrali, dipartimenti, agenzie, non vi sia traccia alcuna non solo dei dati del DPO, ma anche di modifiche all’interno dell’informativa privacy del sito web?

Scendendo ancora di più in profondità e tenendo conto di quanto recita il c. 6 dell’Art. 38 [*il responsabile della protezione dei dati può svolgere altri compiti e funzioni. Il titolare del trattamento o il responsabile del trattamento si assicura che tali compiti e funzioni non diano adito a conflitto di interessi]* sarebbe interessante conoscere il parere dell’autorità di controllo in merito al rilascio, in sede di nomina, da parte di alcuni nominandi DPO di “autodichiarazioni” di assenza di conflitto di interessi in merito ad altre/i funzioni/incarichi ricoperti, fatto salvo poi verificare che gli stessi ricoprono incarichi in una certa rilevanza all’interno dell’Amministrazione/ente (es. dirigenti area personale, dirigenti area controlli amministrativi, segretari generali, dirigenti uffici legali..).

Una menzione a parte va fatta per il settore Istruzione Pubblica e Enti/Amministrazioni locali che, nonostante la sempre più cronica mancanza di risorse finanziarie, a causa della non reperibilità di figure “interne” con adeguato profilo professionale fra i dipendenti, si stanno, in maniera sempre maggiore, rivolgendo al “mercato” per reperire soggetti preparati/professionisti che possano ricoprire l’incarico di DPO.

In questi casi i sistemi più utilizzati sono quelli delle “reti di scuole” o del bando unico per unioni di comuni. Anche in questi casi, però, è possibile riscontrare delle “storture” che possono essere riassunte col famoso detto del “cane che si morde la coda” (requisiti richiesti non proprio “in linea” con la normativa), remunerazione per l’incarico che sfiora il paradossale, offerte economiche (in diversi casi) al massimo ribasso (che solitamente non collima con la richiesta di elevata professionalità – ndr -), fermo restando i casi in cui a causa della mancanza di candidati, pur di “adempiere” sempre e comunque alla nomina (spesso nel lasso di tempo che va dal 24 a 26 maggio [!!!]) la scelta è ricaduta su personale interno all’ente/organizzazione privo di requisiti (necessari oltre che obbligatori) o addirittura nell’autonomina da parte dei vertici delle strutture (dirigenti scolastici, segretari comunali, dirigenti sanitari/amministrativi di aziende sanitarie ecc).

In merito alle altre priorità indicate dall’Autorità garante, ma anche a riguardo di tutti gli altri punti inseriti nella normativa, risulta difficile avere contezza del reale stato dell’arte o quantomeno entrare in possesso di un crono programma che possa fornire dati certi sul cammino del processo di adeguamento,quando, al contrario, sarebbe auspicabile mettere a

disposizione di Amministrazioni/Enti maggiormente in ritardo procedure e best practies già disponibili e rodate (vedasi ad es. Ministero dell'Economia e Finanze).

Questo piccolo spaccato non vuole, ovviamente, "buttare alle ortiche" tutto il buon lavoro e le buone prassi che sono state messe in campo da una buona parte del settore pubblico (seppur con ritardo, con mille difficoltà e con responsabilità che andrebbero imputati ad altri e temporalmente spostate su altri periodi "storici"), ma si propone solamente (ahimè) di evidenziare paure e timori che già da tempo serpeggiavano fra i tavoli degli addetti ai lavori, esperti, studiosi della materia, pienamente consapevoli delle difficoltà che la PA italiana avrebbe dovuto affrontare nel rapporto con la nuova normativa europea.

Sarebbe auspicabile, proprio per "correggere il tiro" il prima possibile che si innescasse una inversione di tendenza magari grazie ad una spinta congiunta fra Autorità Garante Nazionale, e Amministrazioni centrali, Associazione dei Comuni italiani affinché quantomeno in questa prima fase di piena operatività la "BASE" su cui si poggerà tutta la macchina della protezione dati personali sia costruita a regola d'arte e non (ancora una volta) "ad occhio".

SITOGRAFIA

- Regolamento (UE) 2016/679, http://eur-lex.europa.eu/legal-content/IT/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ITA&toc=OJ:L:2016:119:TOC;
- https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/7322110
- https://www.garanteprivacy.it/regolamentoue/formazione/
- https://www.garanteprivacy.it/regolamentoue/rpd
- https://www.agendadigitale.eu/sicurezza/privacy/gdpr-il-piano-di-adeguamento-per-le-pubbliche-amministrazioni/

A cura di: **Leonardo Scalera**