LA GUIDA

Formazione privacy obbligatoria, col Gdpr: che c’è da sapere

Il nuovo regolamento privacy introduce l’obbligo della formazione a tutti i livelli, all’interno di società e P.A. Chi non si adegua rischia grosse sanzioni. Vediamo impatti, soluzioni e opportunità

30 Gen 2018

Mauro Alovisio

avvocato, docente corso di formazione del data protection officer - Università degli Studi di Torino

Costanza Mottino

avvocato, esperto data protection

Il Regolamento privacy europeo 679/16 (Gdpr) prevede **l’obbligo della formazione per le pubbliche amministrazioni** ed imprese in materia di protezione dei dati personali per tutte le figure presenti nell’organizzazione (sia dipendenti che collaboratori).

La base normativa

Si tratta di una novità rilevante in quanto il decreto legge 9 febbraio 2012, n. 5, convertito, con modificazioni, dalla legge 4 aprile 2012, n. 35. aveva abrogato nel 2012 l’obbligo di formazione previsto al punto 19.6 del Disciplinare tecnico in materia di misure minime (allegato B al D.Lgs, 196 del 2004 “Codice della privacy) che prevedeva: “*interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare”.*

La formazione privacy **restava e resta obbligatoria nel settore sanitario v. art. 83 del Codice della Privacy** che prevede l’obbligo delle strutture di attivare *“ la messa in atto di procedure, anche di formazione del personale,*

*dirette a prevenire nei confronti di estranei un'esplicita correlazione tra l'interessato e reparti o strutture, indicativa dell'esistenza di un particolare stato di salute"**[1]*** e di prevedere "*la sottoposizione degli incaricati che non sono tenuti per legge al segreto professionale a regole di condotta analoghe al segreto professionale**[2]***.

L'art. 29 del sopra citato regolamento prevede, infatti, che "*il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso ai dati personali* ***non può trattare tali dati se non è istruito in tal senso dal titolare*** *…*".

Il Gruppo di lavoro ex 29 nel parere n. 3/2010 aveva individuato tra le misure comuni concernenti la responsabilità "*un'adeguata formazione ed istruzione del personale in materia di protezione dei dati. Il personale in questione dovrebbe includere gli incaricati (o responsabili) del trattamento dei dati personali, ma anche dirigenti e sviluppatori in campo informatico e direttori di unità commerciali".*

La centralità della formazione[3] è confermata anche dall'art. 32 "Sicurezza del trattamento" paragrafo 4 che prevede che *"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 del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri****".*

Come sarà la formazione

La formazione costituisce, pertanto, **un prerequisito per potere operare all'interno delle organizzazioni, imprese e pubbliche amministrazioni.** Essa dovrebbe, alla luce dell'impianto del Regolamento, presentare un taglio **interdisciplinare** (con sessioni sia informatiche sia giuridiche sia sui profili organizzativi dell'Ente o Società) e pragmatico (come si evince dal termine "istruito" previsto all'art 29 e 32 del Regolamento) e riguardare tutti i soggetti.

La formazione dovrebbe essere **finalizzata ad illustrare i rischi generali e specifici dei trattamenti di dati, le misure organizzative, tecniche ed informatiche adottate, nonché le responsabilità e le sanzioni.**

L'obbligo formativo non deve essere in alcun modo sottovalutato da parte delle pubbliche amministrazioni e delle imprese: nel caso di mancata erogazione della formazione **scatta, infatti, ai sensi dell'art. 83 par 4 del Regolamento privacy europeo, la rilevante sanzione**amministrativa pecuniaria **fino a 10 milioni di euro o, per le imprese, fino a 2 % del fatturato mondiale annuo dell'anno precedente se superiore.**

L’adempimento degli obblighi formativi è sovente oggetto anche di accertamenti ispettivi da parte dell’Autorità Garante privacy e da parte della Guardia di Finanza che ha rinnovato nel 2016 il protocollo di intesa con l’Autorità.

Il Garante, in diversi casi, in sede ispettiva ha richiesto, infatti, di acquisire il programma ed il piano di formazione, le dispense, i materiali erogati, il test finale ed ha analizzato il profilo delle istruzioni agli incaricati al trattamento connesse all’accesso, alla consultazione delle banche dati, i livelli di autorizzazione e policy aziendali (ad esempio in materia di password aziendali e di videosorveglianza).

La formazione costituisce, pertanto, una misura di sicurezza per le organizzazioni, un onere a carico del titolare, un diritto e dovere per i dipendenti e i collaboratori.

Che devono fare PA e aziende

Gli Enti pubblici le imprese, pertanto, devono:

– pianificare quanto prima un percorso ed un piano di formazione;

– accantonare adeguate risorse in sede di approvazione di bilancio, al fine di arrivare preparati alla scadenza del 25 maggio 2018, data in cui il Regolamento, già in vigore, esplicherà i suoi effetti;

– prevedere prove finali[4] nel percorso formativo, e sessioni di aggiornamento alla luce delle modifiche normative, organizzative e tecniche;

– individuare un percorso formativo alternativo, in caso di mancato superamento del test finale, ed un nuovo esame di verifica;

Nella progettazione dei corsi di formazione, occorre esaminare ed individuare: i fabbisogni formativi, la struttura dell’Ente o dell’impresa, i profili organizzativi, il target, i prerequisiti, le finalità generali e specifiche di ciascuna sessione formativa nonché le relative modalità di erogazione (in aula o a distanza) ed i precedenti corsi predisposti in materia.

Occorrerebbe, inoltre, stabilire aree di priorità di intervento, a titolo esemplificativo ma non esaustivo le figure apicali, gli amministratori di sistema, i nuovi assunti ed infine le persone autorizzate al trattamento.

Queste ultime, corrispondono agli ex incaricati del codice privacy e sono, sostanzialmente, tutti coloro che trattano dati personali. Essi dovranno essere appositamente nominati mediante una lettera di designazione contenete le istruzioni sui trattamenti che dovranno svolgere.

Nelle previsioni di budget è necessario considerare anche risorse specifiche per la formazione de Data protection Officer[5] e dei componenti del team.

Il data protection officer, figura obbligatoria nelle pubbliche amministrazioni e organo di presidio e di controllo deve anch'esso, ai sensi dell'art. 39 del regolamento, occuparsi della "***formazione del personale*** *che partecipa ai trattamenti ed alle connesse attività di controllo"*.

La previsione di tale compito a carico del DPO costituisce un ulteriore elemento di garanzia della centralità e dell'effettività della formazione che potrà nella logica del regolamento anche essere oggetto di specifici audit.

La formazione costituisce essa stessa una misura essenziale al fine di garantire un livello di sicurezza adeguato a garanzia del Titolare del trattamento[6], la pietra angolare del trattamento e sul quale ricade ogni responsabilità.

La previsione di eventi formativi diretti al personale e ai collaboratori concretizza il principio di "accountability[7]" ossia di responsabilizzazione del Titolare del trattamento, previsto dal Regolamento europeo n. 679/16.

Ed invero, il titolare deve dimostrare[8] che il trattamento dei dati sia lecito, corretto, trasparente, pertinente, adeguato, legittimo e che vengano, inoltre, rispettati i principi di minimizzazione, di conservazione dei dati e siano previste misure di sicurezza adeguate.

I dipendenti e i collaboratori potranno, infatti, trattare i dati solo se autorizzati ed entro i limiti delle istruzioni impartite dal titolare, il quale potrà comunque avvalersi come intermediario di altro soggetto debitamente autorizzato.

Il programma ed il piano formativo costituiscono, pertanto, dei tasselli rilevanti del cd sistema di gestione privacy in grado di concretizzare il principio di accountability inteso come capacità di dimostrare di avere adottato misure di sicurezza adeguate. Si suggerisce, per tale ragione, di pubblicare il piano ed i relativi materiali formativi nella sezione intranet aziendale al fine di costituire un presidio di informazione e aggiornamento a beneficio di tutta l'organizzazione e di inserire i sopra citati atti come allegati al registro del trattamento.

In ambito pubblico la formazione sulla protezione dei dati non potrà non integrarsi con la digitalizzazione dei processi, con la riforma del Codice di Amministrazione digitale[9], con i codici di comportamento degli enti e con le ultime recenti novità normative in materia di trasparenza, prevenzione della corruzione, Foia e whistleblowing.

Nell'ottica di un miglioramento continuo e di una gestione in qualità del sistema privacy, sarebbe consigliabile, come alcuni enti stanno progettando, prevedere sessioni informative on line per sensibilizzare anche gli utenti sul valore della protezione dei dati personali, come diritto collettivo e sull'utilizzo consapevole e responsabile di Internet.[10]

La formazione non deve essere considerata, pertanto, un mero adempimento burocratico ma come un'opportunità per rendere consapevoli gli operatori dei rischi connessi al trattamento dei dati, delle misure di sicurezza, per migliorare i processi organizzativi e i servizi erogati, evitare danni reputazionali, ridurre i rischi di sanzioni amministrative e rendere più competitiva l'organizzazione.

[1] art. 83 del Codice privacy" Altre misure per il rispetto dei diritti degli interessati, secondo comma, lett. h); per approfondimenti v Garante Privacy. **Strutture sanitarie: rispetto della dignità – 9 novembre 2005** (web n. 1191411) **dove si prevede all'art. 3, comma h "*regole di condotta per gli incaricati (art. 83, comma 2, lett. i) che:* "*A tal fine, anche avvalendosi di iniziative di formazione del personale designato, occorre mettere in luce gli obblighi previsti dalla disciplina in materia di protezione dei dati personali con particolare riferimento all'adozione delle predette misure organizzative (artt. 30 e 35 del Codice e punto 19.6 del disciplinare tecnico allegato B) al Codice), evidenziando i rischi, soprattutto di accesso non autorizzato, che incombono sui dati idonei a rivelare lo stato di salute e le misure disponibili per prevenire effetti dannosi".*art. 3 comma g), "correlazione fra paziente e reparto o struttura" (art. 83, comma 2, lett. h)) dove si prevede che *" Gli organismi sanitari devono mettere in atto specifiche procedure, anche di formazione del personale, per prevenire che soggetti estranei possano evincere in modo esplicito l'esistenza di uno stato di salute del paziente attraverso la semplice correlazione tra la sua identità e l'indicazione della struttura o del reparto presso cui si è recato o è stato ricoverato".*

[2] art. 83 del Codice privacy *"Altre misure per il rispetto dei diritti degli interessati",* secondo comma, lett. h);

[3] L'importanza della formazione è ribadita, nell'ambito aziendale dall'art 47 rubricato "Norme vincolanti d'impresa" che prevede che le norme, che verranno applicate a gruppi d'impresa che trattano dati in più Stati, dovranno specificare "l'appropriata formazione in materia di protezione dei dati al personale che ha accesso permanente o regolare ai dati personali".

[4] Le prove finali consentono di dimostrare il grado di conoscenza della normativa, delle istruzioni privacy all'interno dell'organizzazione.

[5] V. art. 38 del Regolamento privacy ad oggetto: "Posizione del responsabile della protezione dei dati " che prevede che " Il titolare e del trattamento e il responsabile del trattamento sostengono il responsabile della protezione dei dati nell'esecuzione dei compiti di cui all'articolo 39 fornendogli le risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica".

[6] Per approfondimenti v. il considerando n. 74 che prevede che "*è opportuno stabilire la responsabilità generale del titolare del trattamento per qualsiasi trattamento di dati personali che quest'ultimo abbia effettuato direttamente o che altri abbiano effettuato per suo conto…***".**

[7] v. art. 5, paragrafo 2 del regolamento privacy europeo

[8] v.art. 5 paragrafi 1 e 2 del regolamento privacy europeo

[9] Per approfondimenti v. art 13 del Decreto Legislativo 7 marzo 2005, n. 82 ad oggetto*: "Formazione informatica dei dipendenti* pubblici "che prevede che: 1*. Le pubbliche amministrazioni nella predisposizione dei piani di cui all'articolo 7-bis, del decreto legislativo 30 marzo 2001, n. 165, e nell'àmbito delle risorse finanziarie previste dai piani medesimi, attuano anche politiche di formazione del personale finalizzate alla conoscenza e all'uso delle tecnologie dell'informazione e della comunicazione, nonché dei temi relativi all'accessibilità e alle tecnologie assistive, ai sensi dell'articolo 8 della legge 9 gennaio 2004, n. 4. (comma così modificato dall'art. 9, comma 6, lettera b), legge n. 221 del 2012)*

1-bis. Le politiche di formazione di cui al comma 1 sono altresì volte allo sviluppo delle competenze tecnologiche, di informatica giuridica e manageriali dei dirigenti, per la transizione alla modalità operativa digitale.

[10] Per approfondimenti v. art. 8 Decreto Legislativo 7 marzo 2005, n. 82 ad oggetto; " *Alfabetizzazione informatica dei cittadini " che prevede* che: *1. Lo Stato e i soggetti di cui all'articolo 2, comma 2, promuovono iniziative volte a favorire la diffusione della cultura digitale tra i cittadini con particolare riguardo ai minori e alle categorie a rischio di esclusione, anche al fine di favorire lo sviluppo di competenze di informatica giuridica e l'utilizzo dei servizi digitali delle pubbliche amministrazioni con azioni specifiche e concrete, avvalendosi di un insieme di mezzi diversi fra i quali il servizio radiotelevisivo.*