Euroconference NEWS
L'INFORMAZIONE QUOTIDIANA DA PROFESSIONISTA A PROFESSIONISTA
Direttori: Sergio Pellegrino e Giovanni Valcarenghi

Edizione di mercoledì 16 Dicembre 2020

FINANZA AGEVOLATA

Accountability e formazione privacy

di **Giovanna Lipani – Gruppo Finservice**

Con l'introduzione del GDPR 2016/679 le organizzazioni devono rispettare uno dei principi più importanti del regolamento europeo: l'**Accountability**, ovvero la responsabilizzazione del Titolare del Trattamento dei dati, elemento centrale della compliance privacy e con un impatto ulteriormente incrementato in questa fase di emergenza sanitaria.

L'implementazione e la gestione dei protocolli sulla sicurezza Covid-19, hanno indotto le organizzazioni a considerare un **perimetro più ampio di attività da svolgere** e spesso anche **con modalità nuove**. Basti pensare allo sviluppo significativo di prestazioni lavorative erogate in modalità ***smart working***, esperienza che ha coinvolto una moltitudine di dipendenti sia nel settore privato sia in quello pubblico. In questo caso, ogni titolare del trattamento ha dovuto prontamente prendere in esame **nuove modalità organizzative** e di **sicurezza informatica** per mitigare i rischi connessi alla gestione del trattamento dei dati personali.

L'esempio citato è una delle tante attività a cui imprese e altre organizzazioni hanno dovuto far fronte, indirizzando verso la propria struttura e sotto la propria responsabilità **nuove regole e adempimenti connessi alla gestione dei dat**i.

Tuttavia, quest'ultimo passaggio necessità di un ulteriore approfondimento, per non rischiare di incorrere in una pura applicazione formale e non sostanziale di regole, contrariamente a quanto previsto dai principi espressi dal GDPR.

Il punto cardine che fa la differenza è rappresentato dal tema della **formazione**, elemento più

volte richiamato dagli articoli del GDPR:

- **art. 29**: **Trattamento sotto l'autorità del titolare del trattamento o del responsabile del trattamento**: "*Il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento…*"
- **art. 32: Sicurezza del Trattamento** "*…Il titolare del trattamento e 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…*"
- **art. 39: Compiti del responsabile della protezione dei dati: "-….***b) sorvegliare l'osservanza del presente regolamento, di altre disposizioni dell'Unione o degli Stati membri 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..".*

Il concetto base a cui sostanzialmente fanno riferimento gli articoli citati è il seguente: **i dipendenti e i collaboratori possono trattare i dati solo se autorizzati ed entro i limiti delle istruzioni ricevute.**

A questo punto si pone la questione sul come fare, ovvero come erogare una adeguata formazione ed essere nel contempo in grado di dimostrarne l'avvenuto ed efficace compimento della stessa.

Si consiglia sempre di prevedere che l'attività di formazione sia inserita all'interno di **una pianificazione più ampia** che abbia per oggetto una programmazione di interventi di miglioramento finalizzati al raggiungimento della ***compliance privacy.***

A questo punto la **valutazione del piano formativo più idoneo** è il primo passaggio da compiere. L'esame deve tenere conto della struttura dell'organizzazione a cui si rivolge e, più nello specifico, del target di utenti, delle modalità di erogazione (in aula e/o tramite e-learning) e di eventuali altre attività formative a supporto della gestione dei dati personali.

Ogni ente è dunque chiamato ad individuare, con l'eventuale collaborazione di società di consulenza specializzate nella gestione della privacy, quanto segue:

- **personale ed eventuali collaboratori** da coinvolgere nel percorso formativo;
- **prove finali** e percorsi dedicati;
- **documentazione attestante l'avvenuta formazione** (es: registri, test di validazione, attestati);
- **sessioni di aggiornamento**

Il **percorso formativo dovrà sempre essere adeguato ed aggiornato ai cambiamenti** che possono interessare la normativa privacy nella sua complessità, sia con riferimento al GDPR sia

con riferimento a provvedimenti nazionali, di settore e di altre norme che rivestono un maggior carattere di specificità.

Inoltre, in via generale, occorre sempre tener presente che **la formazione** rappresenta per l'azienda anche una **misura di sicurezza ed un obbligo normativo** da non sottovalutare, **se non si vuole incorrere in sanzioni**.

Sotto questo profilo il GDPR si è espresso chiaramente, prevedendo una **sanzione amministrativa fino a 10 milioni di euro o fino al 2% del fatturato mondiale annuo**, in caso di mancata formazione (art. 83 del GDPR)

Pertanto, in quest'ottica ricadono nell'ambito del potere ispettivo assegnato al garante privacy e all'apposito nucleo della Guardia di Finanza, **controlli** ed **acquisizioni di documenti** inerenti la formazione, la quale deve essere sempre dimostrabile tramite elementi certi e comprovati.

In conclusione, nel rispetto del principio dell'Accoutability, è opportuno che **ogni ente dimostri di avere consapevolezza e contezza dell'elenco degli incaricati al trattamento e delle relative attività svolte, dei test effettuati e di eventuali attestati finali, insieme di elementi utili per dimostrare oggettivamente e inequivocabilmente lo svolgimento dell'attività formativa.**