LA PROFESSIONALITÀ DEL DATA PROTECTION OFFICER E LA FORMAZIONE OBBLIGATORIA NEL NUOVO REGOLAMENTO

D.SSA LOREDANA BOSSI

CONSIGLIERE NAZIONALE AIFOS E DIRETTORE CENTRO DI FORMAZIONE AIFOS A&T AMBIENTE TECNOLGIA FORMAZIONE

ARGOMENTI TRATTATI

- Chi è il DPO
- Quando è obbligatorio nominare il DPO
- La formazione e l'esperienza del DPO
- La formazione a 360° nel nuovo Reg. 2016/679

CHI E' IL DPO

- **Tra le maggiori novità del Regolamento Europeo sulla protezione dei dati personali n. 2016/679 rientra sicuramente la previsione del Data Protection Officer (DPO) o responsabile della protezione dei dati, figura di indubbio rilievo.**

CHI E' IL DPO

L'art. 37 del Regolamento prevede che quando:

a) il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali, oppure

b) le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala, oppure

c) le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati di cui all'articolo 9 (dati sensibili) o di dati relativi a condanne penali e a reati di cui all'articolo 10

il titolare del trattamento e il responsabile del trattamento designano sistematicamente un responsabile della protezione dei dati (Data Protection Officer o DPO).

QUANDO E' OBBLIGATORIO NOMINARE IL DPO

- In data 13 Dicembre 2016, il WP29 (Article 29 Data Protection Working Party) ha pubblicato un documento denominato "*Guidelines on Data Protection Officers (DPO)*" con il quale ha meglio specificato le casistiche per le quali le aziende hanno l'obbligo di designare un Data Protection Officer.

QUANDO E' OBBLIGATORIO NOMINARE IL DPO

- In particolare il WP29 ha chiarito che i titolari del trattamento e i responsabili del trattamento (non appartenenti alla pubblica amministrazione) sono soggetti alla nomina del Data Protection Officer (DPO) quando le operazioni chiave necessarie per raggiungere i propri obiettivi istituzionali comportano:
- *il trattamento su larga scala di dati sensibili, genetici, giudiziari e biometrici*
- *il monitoraggio regolare e sistematico del comportamento di interessati su larga scala (es: tracciamento su internet, geolocalizzazione e profilazione per finalità di pubblicità comportamentale)*

QUANDO E' OBBLIGATORIO NOMINARE IL DPO

- Per valutare se un trattamento possa essere considerato su larga scala è necessario fare un'accurata analisi privacy dei processi aziendali tenendo in considerazione i seguenti parametri:
- *numero di interessati coinvolti*
- *volume e tipologia di dati trattati*
- *durata del trattamento*
- *estensione geografica del trattamento*

QUANDO E' OBBLIGATORIO NOMINARE IL DPO

- Per valutare se un'attività di monitoraggio possa essere considerata regolare e sistematica è, invece, necessario fare un'analisi privacy tenendo in considerazione i seguenti parametri:
- *durata, periodicità e ricorrenza*
- *sistematicità e pianificazione*
- *metodologia organizzativa*
- *strategia aziendale*

QUANDO E' OBBLIGATORIO NOMINARE IL DPO

- L'iter di valutazione che porta alla decisione di designare o meno un Data Protection Officer (DPO) deve essere, comunque, documentato per iscritto in modo da poter dimostrare, in caso di controlli, quali elementi sono stati presi in considerazione nel processo decisionale.
- Il WP29 suggerisce, inoltre, a tutte le persone fisiche o giuridiche di diritto pubblico o privato che prestano un pubblico servizio di provvedere, in ogni caso, alla designazione di un Data Protection Officer (DPO).

CHI E' IL DPO

- È sicuramente un'importante figura professionale, fortemente voluta, i cui compiti e responsabilità, però, non sono particolarmente chiari, specialmente avuto riferimento ai rapporti con le altre figure soggettive in ambito privacy. È indubbio però che il responsabile della protezione dei dati sia una figura chiave nell'ambito del trattamento automatizzato dei dati personali.
- Proprio per tali motivi il WP 29 istituito dalla Direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995 ha adottato recentemente in data 13 dicembre 2016 delle linee guida al fine di chiarire quali debbano essere i requisiti ed i compiti di un Data Protection Officer e quale dovrà essere in concreto il suo apporto nel campo della protezione dei dati personali di un'unità organizzativa.

LA FORMAZIONE E L'ESPERIENZA DEL DPO

- **Lo stesso DPO deve godere di ampia autonomia e non riceve alcuna istruzione per quanto riguarda l'esecuzione dei propri compiti.** Inoltre il Regolamento specifica (art. 38) che il responsabile della protezione dei dati non è rimosso o penalizzato dal titolare del trattamento o dal responsabile del trattamento per l'adempimento dei propri compiti, ma riferisce direttamente ai massimi superiori gerarchici del titolare del trattamento o del responsabile del trattamento.

LA FORMAZIONE E L'ESPERIENZA DEL DPO

- Per il WP29 la nomina di un DPO è importante in quanto **questa figura rappresenta un elemento fondante ai fini della responsabilizzazione.** La stessa presenza del DPO può facilitare l'osservanza della normativa e aumentare il margine competitivo delle imprese, nel rispetto del principio di *accountability*.
- **Si ricorda, inoltre, che il DPO svolge un ruolo chiave nel promuovere la cultura della protezione dei dati all'interno dell'azienda o dell'organismo**, e contribuisce a dare attuazione a elementi essenziali del Regolamento quali i principi fondamentali del trattamento, i diritti degli interessati, la protezione dei dati sin dalla fase di progettazione e per impostazione predefinita, i registri delle attività di trattamento, la sicurezza dei trattamenti e la notifica e comunicazione delle violazioni di dati personali.

LA FORMAZIONE E L'ESPERIENZA DEL DPO

- **Le linee guida ribadiscono un altro aspetto molto importante e cioè che i DPO non rispondono personalmente in caso di inosservanza del Regolamento.** Quest'ultimo chiarisce che spetta al titolare o al responsabile del trattamento garantire ed essere in grado di dimostrare che le operazioni di trattamento sono conformi alle disposizioni del Regolamento stesso (articolo 24, primo paragrafo). L'onere di assicurare il rispetto della normativa in materia di protezione dei dati ricade, quindi, sul titolare o sul responsabile.
- Inoltre, al titolare o al responsabile del trattamento spetta il compito fondamentale di consentire lo svolgimento efficace dei compiti cui il DPO è preposto. La nomina di un DPO è solo il primo passo, perché il DPO deve disporre anche di autonomia e risorse sufficienti a svolgere in modo efficace i compiti cui è chiamato.

LA FORMAZIONE E L'ESPERIENZA DEL DPO

- E' però inutile nascondere che nel caso in cui il titolare o responsabile del trattamento dovessero prendere decisioni non conformi al Regolamento comunitario con il configurarsi di conseguenti danni a soggetti terzi e tali decisioni siano dovute a pareri fuorvianti del DPO, quest'ultimo potrà sicuramente essere chiamato a responsabilità, seppur in sede di rivalsa.

LA FORMAZIONE E L'ESPERIENZA DEL DPO

- In ambito nazionale bisogna inoltre riconoscere che a seguito dei lavori congiunti UNI – UNINFO per la redazione dello standard sui Profili professionali relativi al trattamento e alla protezione dei dati personali è stato redatto un progetto di norma UNI attualmente in pubblica consultazione che sicuramente avrà riflessi importanti per il DPO ed in generale in tutto il settore privacy.
- Il progetto prevede, infatti, diverse figure professionali competenti nel campo della protezione dei dati personali. **Oltre al DPO previsto dal Regolamento Comunitario sono previste altre figure professionali come il manager privacy, lo specialista privacy ed il valutatore privacy.**

LA FORMAZIONE E L'ESPERIENZA DEL DPO

- Tenuto conto della complessità dell'iter decisionale, infine, risulta buona prassi, anche per i soggetti non direttamente obbligati dal Regolamento Europeo Privacy, nominare sempre un Data Protection Officer, in quanto il GDPR considera il DPO, un attore chiave del sistema di gestione privacy.
- La violazione degli obblighi di nomina del Data Protection Officer è sanzionata dal Regolamento Europeo Privacy con una sanzione amministrativa pecuniaria fino a € 10.000.000 o fino al 2 % del fatturato mondiale totale annuo dell'esercizio precedente (ove superiore).

LA FORMAZIONE A 360° NEL NUOVO REG. 2016/679

- Il Nuovo Regolamento Europeo Privacy (GDPR) ha introdotto nuovi e specifici obblighi di formazione privacy in capo a tutti i Titolari del Trattamento e Responsabili del Trattamento.
- L'art. 39.1.b del Regolamento Europeo Privacy (GDPR), infatti, prevede espressamente che rientri tra i compiti del Data Protection Officer (DPO o Privacy Officer) "*[…] sorvegliare l'osservanza […] delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi […] la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo*".

LA FORMAZIONE A 360° NEL NUOVO REG. 2016/679

- Inoltre, l'art. 32 . 4 del Regolamento Europeo Privacy (GDPR), dispone che chiunque " *[…] abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento* […]".
- Da una semplice e veloce lettura dei suddetti articoli, si evince chiaramente che il Regolamento Europeo Privacy (GDPR) considera la formazione privacy una importante misura di sicurezza per la protezione dei dati personali, che deve essere obbligatoriamente adottata da tutti i Titolari del Trattamento e Responsabili del Trattamento.

LA FORMAZIONE A 360° NEL NUOVO REG. 2016/679

- Al fine di garantire il rispetto di tali obblighi di formazione privacy, l'art. 39.1.a del Regolamento Europeo Privacy (GDPR), infine, affida al Data Protection Officer (DPO o Privacy Officer) anche il compito di "*informare […] i dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal […] regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati*"
- Il compito del Data Protection Officer (DPO o Privacy Officer), è dunque, quello di concordare annualmente con il Titolare del Trattamento e con il Responsabile del Trattamento un piano di formazione privacy, che preveda corsi privacy periodici per tutto il personale incaricato al trattamento di dati personali.

LA FORMAZIONE A 360° NEL NUOVO REG. 2016/679

- Il piano di formazione privacy deve essere approvato per iscritto dal Titolare del Trattamento e dal Responsabile del Trattamento e i corsi privacy previsti devono essere svolti, in aula o in modalità e-learning, avvalendosi di personale docente esperto e specializzato in protezione dei dati personali.
- Al termine del corso privacy, è necessario, poi, che venga somministrato a tutti i partecipanti un test finale di apprendimento al fine di poter dimostrare il raggiungimento degli obiettivi didattici e l'effettivo efficacia della formazione privacy, quale misura di sicurezza per la protezione dei dati personali.

LA FORMAZIONE A 360° NEL NUOVO REG. 2016/679

- In caso di violazione degli obblighi di formazione privacy, il Regolamento Europeo Privacy (GDPR), prevede per il Titolare del Trattamento e per il Responsabile del Trattamento pesanti sanzioni amministrative pecuniarie, che possono arrivare fino a € 10.000.000 o fino al 2 % del fatturato mondiale totale annuo dell'esercizio precedente (ove superiore).

Centro Congressi Galileo
meeting . congressi . eventi

A&T
Ambiente Tecnologia Formazione

AiFOS
Associazione Italiana Formatori ed Operatori della Sicurezza sul Lavoro

GRAZIE PER L'ATTENZIONE