STUDIO ANSALDI & ASSOCIATI
Marco Ansaldi - Antonella Bolla
CONSULENZA FISCALE E DEL LAVORO
SEGUICI SU
www.ansaldiassociati.it
www.marcoansaldicommercialista.it

14.10.2018

DECRETO DI ADEGUAMENTO DEL CODICE *PRIVACY* AL GDPR

Il 19 settembre 2018 è entrato in vigore il D.Lgs. 101/2018, recante disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati. Il trattamento dei dati personali deve avvenire secondo le norme del GDPR e del D.Lgs. 196/2003 (come da ultimo modificato), nel rispetto della dignità umana, dei diritti e delle libertà fondamentali della persona.

Posto quanto sopra, si forniscono, qui di seguito, le prime indicazioni di massima con riferimento alla *privacy* nelle aziende.

Occorre subito precisare che il decreto non prevede alcun periodo di non applicazione delle sanzioni amministrative, bensì un periodo in cui il Garante terrà conto della difficoltà di applicazione delle nuove norme. Questo potrebbe consentire di applicare solo i poteri correttivi che l'articolo 58, paragrafo 2, GDPR, assegna al Garante.

Lo stesso paragrafo consente, però, al Garante di infliggere una sanzione amministrativa pecuniaria ai sensi dell'articolo 83, Regolamento UE 2016/679, in aggiunta alle misure correttive, o in luogo di tali misure, in funzione delle circostanze di ogni singolo caso. Quindi, il Garante potrebbe applicare le sanzioni amministrative pecuniarie che, si rammenta, sono di 2 tipologie:

- fino a 10 milioni di euro o, per le imprese, fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore;
- fino a 20 milioni di euro o, per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

A tal proposito si ricorda che, ai sensi dell'articolo 83, Regolamento UE 2016/679, al momento di decidere se infliggere una sanzione amministrativa pecuniaria e di fissare l'ammontare della stessa in ogni singolo caso, il Garante *privacy* dovrà tenere in debito conto i seguenti elementi:

a) la natura, la gravità e la durata della violazione, tenendo in considerazione la natura, l'oggetto o la finalità del trattamento in questione nonché il numero di interessati lesi dal danno e il livello del danno da essi subito;

b) il carattere doloso o colposo della violazione;
c) le misure adottate dal titolare del trattamento o dal responsabile del trattamento per attenuare il danno subito dagli interessati;
d) il grado di responsabilità del titolare del trattamento o del responsabile del trattamento, tenendo conto delle misure tecniche e organizzative da essi messe in atto;
e) eventuali precedenti violazioni pertinenti commesse dal titolare del trattamento o dal responsabile del trattamento;
f) il grado di cooperazione con l'autorità di controllo al fine di porre rimedio alla violazione e attenuarne i possibili effetti negativi;
g) le categorie di dati personali interessate dalla violazione;
h) la maniera in cui l'autorità di controllo ha preso conoscenza della violazione, in particolare se e in che misura il titolare del trattamento o il responsabile del trattamento ha notificato la violazione;
i) qualora siano stati precedentemente disposti provvedimenti nei confronti del titolare del trattamento o del responsabile del trattamento in questione relativamente allo stesso oggetto, il rispetto di tali provvedimenti;
j) l'adesione ai codici di condotta approvati o ai meccanismi di certificazione approvati;
k) eventuali altri fattori aggravanti o attenuanti applicabili alle circostanze del caso, ad esempio i benefici finanziari conseguiti o le perdite evitate, direttamente o indirettamente, quale conseguenza della violazione.

I Titoli dal II al VII della parte I del vecchio Codice *privacy* sono stati abrogati, per cui:

- per i diritti degli interessati occorre fare riferimento agli articoli dal 12 al 23, Regolamento UE 2016/679 e agli articoli da 2-*undecies* a 2-*terdecies*, nuovo Codice *privacy*;
- per i principi occorre riferirsi agli articoli 5-11, GDPR, e agli articoli da 2-*ter* a 2-*decies*, nuovo Codice *privacy*.

Per quanto concerne le figure del trattamento (titolare, contitolare, responsabile esterno e rappresentante non stabilito nell'Unione) occorre rifarsi alle figure di cui al Regolamento UE, tenendo comunque presente che il titolare o il responsabile del trattamento:

- possono prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità;
- individuano le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta;

per cui è ancora possibile nominare responsabili interni del trattamento e incaricati, anche se non previsti del GDPR.

Per l'informativa l'azienda dovrà riferirsi agli articoli 13 e 14, Regolamento, e anche per il consenso è il GDPR a dettare le disposizioni da applicare, così come per il trattamento delle categorie particolari di dati personali *ex* articolo 9, Regolamento UE 2016/679.

Si segnala che, ai sensi dell'articolo 111, Codice *privacy*, come da ultimo modificato, il Garante è tenuto a promuovere l'adozione di regole deontologiche per i soggetti pubblici e privati interessati al trattamento dei dati personali effettuato nell'ambito del rapporto di lavoro, prevedendo anche specifiche modalità per le informazioni da rendere all'interessato.

La ricezione dei *curricula*

Con riferimento ai *curricula* spontaneamente trasmessi dagli interessati al fine dell'instaurazione di un rapporto di lavoro, il nuovo articolo 111-*bis*, Codice *privacy*, prevede che vada fornita l'informativa di cui all'articolo 13, Regolamento UE 2016/679, al momento del primo contatto utile e non è dovuto il consenso al trattamento dei dati personali ivi presenti.

Le sanzioni penali

Il D.Lgs. 101/2018 ha previsto l'applicazione di sanzioni penali nel caso di:

- trattamento illecito dei dati;
- comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala;
- acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala;
- falsità nelle dichiarazioni al Garante e interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante;
- inosservanza di provvedimenti del Garante;
- violazioni delle disposizioni in materia di controlli a distanza e indagini sulle opinioni dei lavoratori.

Violazioni delle disposizioni in materia di controlli a distanza e indagini sulle opinioni dei lavoratori

Le modifiche apportate al Codice privacy dal D.Lgs. 101/2018 non apportano cambiamenti degni di nota in materia di "Impianti audiovisivi e altri strumenti di controllo" e "Divieto di indagini sulle opinioni", questioni disciplinate rispettivamente dagli articoli 4 e 8, L. 300/1970. Pertanto, salvo che il fatto non costituisca più un grave reato, i rei saranno ancora puniti con l'ammenda da 154 a 1.549 euro o l'arresto da 15 giorni a un anno e, nel caso di specie, è ammessa la prescrizione *ex* articolo 15, D.Lgs. 124/2004.

Infine, si rammenta che, nei casi più gravi, le pene dell'arresto e dell'ammenda sono applicate congiuntamente e, inoltre, quando, per le condizioni economiche del reo, l'ammenda può presumersi inefficace anche se applicata nel massimo, il giudice ha facoltà di aumentarla fino al quintuplo.

Misure di sicurezza

In ultimo, si rileva che è stato abrogato anche l'allegato B al D.Lgs. 196/2003, che prevedeva le misure minime di sicurezza; questo perché il GDPR prevede l'applicazione di misure di sicurezza "adeguate" nel rispetto del principio della responsabilizzazione.

Spetta, quindi, al titolare del trattamento, o al responsabile esterno del trattamento, valutare quando una misura di sicurezza sia da considerarsi "adeguata" ai sensi del Regolamento.