La privacy guarda ai modelli «231»

a cura diLuigi Ferrajoli


La privacy guarda ai modelli «231»
Le imprese devono adeguare l'organigramma e procedere alla valutazione dei rischi
Avvocati-consulenti per ricoprire il ruolo di responsabile dati
NUOVO STATUTO COMIECO
Più spazio alle alternative al carcere

Revisione dell' organigramma e ripartizione delle funzioni, valutazione dei rischi e individuazione degli strumenti per tutelare la riservatezza. La realizzazione del "modello organizzativo privacy" - con cui sono alle prese in questo periodo le imprese per prepararsi al debutto delle prescrizioni del regolamento Ue 679/2016, che entrerà in vigore il 25 maggio 2018 - presenta molti punti di contatto e somiglianze con le disposizioni del decreto legislativo 231/2001 in materia di responsabilità amministrativa delle persone giuridiche. Il regolamento Ue 679/2016 rivoluziona la normativa sulla privacy, abrogando, tra l' altro, la direttiva 95/46, da cui "discende" l' attuale Codice italiano sulla privacy (decreto legislativo 196/2003). Per adeguarsi alle nuove norme, le imprese devono quindi rivedere la compliance interna finalizzata a garantire la protezione dei dati e delle informazioni personali che trattano e conservano. Precisamente è il titolare del trattamento che ha il compito di attuare gli adempimenti previsti dalla normativa e a cui devono essere rimproverate eventuali violazioni o omissioni rispetto ai divieti e alle prescrizioni introdotte. Ed è sempre il titolare del trattamento a dover provare di aver posto in essere le iniziative necessarie per assicurare l' adeguamento delle policy interne alla nuova disciplina. La necessità di provare l' avvenuto adeguamento della compliance aziendale alle nuove prescrizioni privacy ha portato le imprese a introdurre una sorta di "dossier privacy" o per alcuni altrimenti detto "modello organizzativo privacy", che racchiuda tutti gli adempimenti necessari ad assicurare la riservatezza e il più elevato grado di tutela per i dati personali trattati nelle società. Un modello che ricorda da vicino quello che va predisposto (e aggiornato) per rispettare il decreto legislativo 231/2001. Si parte con la revisione dell' organigramma, prestando cioè attenzione alla presenza delle nomine esistenti e alla descrizione dei nuovi compiti assegnati al titolare, al responsabile del trattamento, agli incaricati al trattamento. A ciò si accompagna la verifica circa l' obbligatorietà, per i casi espressamente indicati dalla normativa, o la mera

opportunità, negli altri casi, di nominare un Data protection officer (Dpo). Quanto detto sembra pienamente rispondere al criterio della segregation of duties (Sod) che già governa il sistema 231, secondo cui occorre individuare le distinte responsabilità in capo a ciascuna funzione descrivendone nel dettaglio i compiti affidati. In questa chiave di lettura, di notevole impatto è l' obbligo di provvedere alla valutazione dei rischi privacy (una sorta di risk assessment privacy), destinata inevitabilmente a confluire in un documento riepilogativo delle analisi effettuate. In esso sono individuati i possibili rischi associati alle distinte attività svolte, passaggio che presuppone la previa disamina dei rispettivi processi aziendali nell' ambito dei quali sono trattati i dati. In questa valutazione si deve tener conto dell' identità dei soggetti interessati al trattamento (ad esempio, dipendenti o fornitori), delle finalità del trattamento nonché delle tipologie (ad esempio, dati sanitari, anagrafici o altri) e delle categorie di trattamento entro le quali sono compresi i dati gestiti dall' azienda. Sarà necessario, inoltre, garantire un costante aggiornamento a questo documento in occasione di possibili mutamenti sia organizzativi che normativi in grado di incidere sul trattamento dei dati messi a disposizione delle imprese. Riecheggiando la recente normativa sul whistleblowing (legge 179/2017, in vigore dal 29 dicembre 2017), è infine richiesta l' introduzione di specifiche modalità di presentazione delle comunicazioni circa eventuali violazioni riscontrate sui dati personali (data breach): sarà utile predisporre moduli distinti a seconda della tipologia di violazione riscontrata, individuare un ufficio responsabile per ricevere le segnalazioni oltre che individuare le eventuali iniziative da intraprendere, a livello organizzativo e tecnico, capaci di porre rimedio alle irregolarità che si sono verificate. Infine, allo scopo di sensibilizzare tutto il personale dipendente nonché le funzioni aziendali impiegate a ogni livello nell' assessment societario, è prevista l' implementazione di un codice di condotta per garantire la corretta osservanza delle prescrizioni del regolamento Ue, da elaborare tenuto conto delle peculiarità settoriali e delle esigenze specifiche delle micro, piccole e medie imprese.