

Lavoro, vanno protetti i dati degli iscritti ai sindacati



Il datore di lavoro non può comunicare ad una organizzazione sindacale la nuova sigla alla quale ha aderito un suo ex iscritto. Per consentire al sindacato di espletare le procedure che seguono la revoca della affiliata sindacale e della relativa delega, il datore di lavoro avrebbe dovuto limitarsi a comunicare la sola scelta del lavoratore di non aderire più all'originaria sigla di appartenenza.

È quanto affermato dal Garante privacy a conclusione di un'istruttoria originata dai reclami di alcuni dipendenti di una Azienda socio-sanitaria territoriale che si erano rivolti all'Autorità affinché valutasse la correttezza del datore di lavoro nel trattamento dei loro dati sensibili, quale è l'appartenenza sindacale [doc. web n. [9065999](#)].

A giustificazione del proprio comportamento l'Azienda ha affermato, tra l'altro, di aver ritenuto necessario informare la Rappresentanza sindacale della variazione per evitare il rischio che senza questa comunicazione l'organismo avrebbe continuato ad operare in una composizione non più aderente alla realtà, con inevitabili ricadute sulla validità della contrattazione aziendale.

Le informazioni sull'adesione sindacale rientrano nella categoria dei dati sensibili - ha osservato l'Autorità - ai quali la disciplina di protezione dei dati riconosce particolari forme di tutela. Il datore di lavoro può lecitamente trattarli in base alla legge per adempiere agli obblighi derivanti dal rapporto di lavoro, ad esempio per effettuare il versamento delle quote di iscrizione ad associazioni o organizzazioni sindacali su delega e per conto del dipendente.

In questo caso invece l'amministrazione non si è limitata a comunicare alla Rappresentanza sindacale la revoca dell'affiliazione di alcuni lavoratori, ma ha inviato a tutti i componenti della sigla sindacale una e-mail cui erano allegati dei documenti nei quali era espressamente indicata l'iscrizione dei lavoratori che avevano aderito ad un altro sindacato. Ciò ha determinato una illecita comunicazione di dati personali sensibili dei reclamanti.

A conclusione dell'istruttoria il Garante ha ritenuto che dalla valutazione degli elementi acquisiti la condotta dell'Azienda, pur difforme dalla disciplina applicabile, abbia esaurito i suoi effetti e non sussistono quindi i presupposti per l'adozione di un provvedimento prescrivito o inibitorio.

L'Autorità si è riservata però di avviare un autonomo procedimento per valutare la contestazione di una eventuale violazione amministrativa per l'illecita comunicazione dei dati sindacali.

Gdpr e imprese extra Ue

Avviate a consultazione le Linee guida approvate dai Garanti Europei sull'ambito di applicazione



Quali società americane o asiatiche sono tenute a rispettare la normativa privacy europea? Un sito di e-commerce straniero può effettuare la profilazione di clienti italiani senza limitazioni? Se un datore di lavoro extra Ue ha assunto personale italiano o tedesco, deve applicare il Gdpr?

Queste sono alcune delle domande a cui rispondono le ["linee guida sull'applicazione dell'ambito territoriale del Gdpr"](#) approvate nel corso della quarta riunione plenaria del Comitato europeo per la protezione dei dati (Edpb), di cui fa parte anche il Garante privacy italiano.

Il testo chiarisce alcuni aspetti dell'articolo 3 del Gdpr, quello che obbliga molte imprese con sede in altri continenti, tra cui i giganti del mondo digitale, al rispetto della normativa privacy europea.

Se un sito di e-commerce, ad esempio, apre a Milano un ufficio per promuovere le proprie attività commerciali, esso può essere considerato al pari di uno stabilimento europeo della società stessa. E' tenuta ad adeguarsi alla normativa europea anche una start-up statunitense che propone "app" con servizi di geolocalizzazione a utenti che si trovano a Roma o Parigi, per offrire loro pubblicità mirata su luoghi da visitare, ristoranti e hotel. Al contrario, non è soggetta al Gdpr una banca di Taiwan che offre servizi a clienti che risiedono in quel Paese, anche se si tratta i dati di persone con cittadinanza tedesca o di un'altra nazione dell'Ue.

In considerazione del forte impatto che le linee guida possono produrre sull'attività di istituzioni e imprese - sia europee, sia straniere – con potenziali pesanti sanzioni per chi non rispettasse la normativa Ue, il Board europeo dei Garanti privacy ha sottoposto il testo a consultazione pubblica prima della sua definitiva approvazione. Ogni commento dovrà essere inviato direttamente all'indirizzo EDPB@edpb.europa.eu entro il 18 gennaio 2019.