ASSIFACT
Associazione Italiana per il Factoring

Consiglio del 21 marzo 2018

Punto 11 all' ODG
Varie ed eventuali

ALLEGATO 11-3
Revisione procedura privacy

ASSIFACT
Associazione Italiana per il Factoring

REVISIONE PROCEDURE PRIVACY ASSIFACT

NUOVO REGOLAMENTO EUROPEO IN MATERIA DI PROTEZIONE DEI DATI PERSONALI ENTRATA IN VIGORE 25 MAGGIO 2018

E' stato avviato il processo di revisione delle procedure Assifact in materia di privacy per adeguare il sistema di regole attualmente adottate alle novità in materia di protezione delle persone fisiche con riguardo al trattamento dei dati personali introdotte dal Regolamento UE 2016/679 del 27 aprile 2016 (RGPD) e in vigore dal 25 maggio 2018, che abroga e sostituisce le attuali disposizioni previste dal D. Lgs. 196/2003 (c.d. Codice Privacy).

Si è proceduto in primo luogo all'analisi del RGPD per individuare le principali novità rispetto alla normativa in vigore, focalizzandosi su quelle d'interesse per l'attività associativa:

- la principale novità riguarda **l'approccio adottato nella nuova normativa** che si basa **sulla valutazione del rischio e sull'adozione di misure organizzative e di sicurezza ad esso commisurate** anziché su una serie di prescrizioni minime previste dalla normativa, con l'obiettivo di responsabilizzare il titolare e responsabile del trattamento. Ciò significa che è demandato ai titolari / responsabili di valutare e decidere in autonomia, fermo restando lo spirito del regolamento e i criteri indicati, le modalità e i limiti del trattamento nonché le misure di sicurezza da adottare. Tale autonomia decisionale si traduce in una serie di attività e valutazioni fatte a priori e dimostrabili che conducono a configurare le attività di trattamento adeguate al livello di rischio per i diritti e le libertà degli interessati. E' quindi necessario attribuire a ciascuno dei trattamenti che si intende porre in essere il relativo rischio. Se il trattamento presenta rischi elevati va effettuata una **Valutazione d'impatto sulla protezione dei dati.** Ai fini associativi, quest'ultima casistica non risulta ad oggi presente e, per la tipologia di attività svolta e di dati personali raccolti, sembra un'ipotesi assolutamente remota.
- Si rileva inoltre l'abolizione dell'adempimento inerente la notifica preventiva dei trattamenti. Per Assifact la notificazione (art. 37 codice privacy) non era più un adempimento obbligatorio già dalla revisione delle norme del codice privacy che circoscrivevano l'obbligo solo in alcuni casi espressamente previsti (es. trattamenti di dati genetici, biometrici, dati di geolocalizzazione, dati idonei a rivelare lo stato di salute e la vita sessuale, trattati a fini di procreazione assistita, prestazione di servizi sanitari, ecc.). Si è comunque proceduto ad eliminare dalla procedura privacy associativa i riferimenti e il paragrafo in tema notificazione che spiegava i motivi della mancata notifica. E' stata però introdotta l'obbligo di documentare tutte le violazioni di dati personali (comprese circostanze, conseguenze e provvedimenti adottati) e la **notifica all'Autorità di controllo e comunicazione agli interessati di eventuali violazioni dei dati personali** che presentino un rischio per i diritti e le libertà degli interessati.
- La notifica è stata "sostituita", nel regolamento, dalla tenuta di un **registro delle attività di trattamento** da parte del titolare/responsabile, che va tenuto in forma scritta anche elettronica a disposizione dell'Autorità di controllo e i cui contenuti minimi sono fissati dall'art. 30 RGPD. Seppure facoltativo in talune particolari circostanze (se il titolare non effettua alcun trattamento di dati sensibili o relativi al casellario giudiziale, le autorità di controllo lo hanno fortemente

raccomandato in quanto "parte integrante di un sistema di corretta gestione dei dati personali", "strumento indispensabile per ogni valutazione e analisi di rischio". Ai fini associativi, la tenuta del registro sarà parte integrante delle procedura privacy, "contenitore" della mappatura dei trattamenti di dati personali svolti nella complessiva attività associativa.

- Il RGPD introduce nuove figure e ruoli coinvolti nel trattamento dei dati (es. contitolari, sub responsabili), fra cui in particolare il **Responsabile della protezione dei dati** (RPD - DPO), soggetto designato in funzione delle qualità professionali e competenze specialistiche per supportare il titolare e il responsabile del trattamento nella corretta applicazione del regolamento, sorvegliarne l'osservanza e fornire un parere in merito alle valutazioni d'impatto. La nomina del RPD è obbligatoria in alcune fattispecie espressamente previste dal regolamento e facoltativa/consigliata nelle altre. Tenuto conto che l'Associazione non rientra nei casi previsti dall'art. 37 RGPD di designazione obbligatoria, valutate le finalità dei trattamenti, la natura sostanzialmente comune dei dati trattatati e le dimensioni/struttura organizzativa associative, non si ritiene opportuno designare un Responsabile della protezione dei dati (RPD). L'Associazione infatti non tratta dati particolari (dati sensibili e dati giudiziari) sul larga scala né effettua trattamenti che richiedono il monitoraggio regolare e sistematico degli interessati su larga scala. Il regolamento non cita più la figura dell' "**incaricato**" del trattamento ma fa riferimento a "persone autorizzate al trattamento dei dati sotto l'autorità diretta del titolare o del responsabile", figura del tutto assimilabile; pertanto ai fini associativi non dovrebbero essere previste modifiche.
- Il trattamento dei dati deve fondarsi sul principio di liceità (art.6 RGPD). In linea di massima la base giuridica idonea a "consentire" i trattamenti non ha subito sostanziali cambiamenti (il primo luogo il consenso seguito da obbligo legale, adempimento contrattuale, ecc.). Il RGPD enfatizza però il concetto di perseguimento di "**interesse legittimo prevalente" del titolare**, che in un'ottica di bilanciamento fra interessi del titolare e diritti e libertà fondamentali degli interessati rende possibile il trattamento in assenza di consenso. E' lo stesso titolare che valuta, in relazione alla natura dei dati personali, alle finalità per cui i dati sono stati raccolti rispetto alle finalità di ulteriori trattamenti e alle conseguenze possibili derivanti da ulteriori trattamenti, se non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato. Ai fini associativi, ad esempio, dovrebbe configurare interesse legittimo dell'Associazione la raccolta, l'utilizzo e la comunicazione dei dati identificativi e di contatto dei membri delle Commissioni Tecniche / gdl dipendenti degli Associati in quanto il trattamento avviene nell'ambito del rapporto di associazione con l'Associato per la realizzazione degli scopi statutari.
- Il trattamento dei dati personali deve essere sempre "informato". Le novità introdotte dal RGPD in ordine **all'informativa** da fornire agli interessati sono numerose e riguardano tutti i profili: **contenuto, modalità e tempistica**. Il contenuto è arricchito e definito in modo tassativo. Il regolamento fornisce indicazioni sulle modalità di stesura dell'informativa, che deve essere scritta con un linguaggio chiaro e semplice, conciso, trasparente e facilmente intelligibile. Inoltre, in caso di raccolta dati presso terzi, deve essere fornita tempestivamente e al massimo entro un mese. L'informativa va data, in linea generale, per iscritto e preferibilmente in formato elettronico. Non è più previsto di poter fornire l'informativa al terzo presso cui sono raccolti i dati; ai fini associativi questo significa fornire informativa diretta ai dipendenti degli Associati che partecipano alle attività associative con la partecipazione alle Commissioni tecniche e ai gdl per i quali vengono raccolti, utilizzati e comunicati i dati identificativi e i contatti.

- Il regolamento introduce novità anche in relazione ai diritti degli interessati e alle modalità di esercizio dei medesimi. Fra le novità si citano il diritto alla limitazione del trattamento (diverso dal precedente blocco del trattamento) e il diritto alla portabilità dei dati.

TIMING DI ADEGUAMENTO

ATTIVITA'	DESCRZIONE	TEMPISTICA 2018
PROCEDURA PRIVACY	• Analisi delle novità introdotte dal RGPD • Adeguamento della procedura privacy associativa e, se necessario, delle misure organizzative e di sicurezza • Verifica mappatura delle attività associative e valutazione rischi • Verifica nomina ruoli / incarichi in relazione ai trattamenti • Verifica contratti per attività in outsourcing. Conformità delle clausole contrattuali alle previsioni normative e valutazione eventuali necessarie modifiche / integrazioni.	FEBBRAIO / APRILE
REGISTRO DEI TRATTAMENTI	• Implementazione del Registro dei trattamenti	MARZO / APRILE
INFORMATIVA INTERESSATI	• Verifica della rispondenza delle informative in uso alle nuove previsioni del regolamento, con particolare riguardo ai contenuti obbligatori e alle modalità di redazione.	MARZO / APRILE
	• invio diretto a tappeto dell'informativa ai membri delle commissioni tecniche / gdl / ecc	• APRILE / MAGGIO
	• Pubblicazione sul sito associativo – area riservata	• APRILE / MAGGIO
	• invio diretto dell'informativa ai membri delle commissioni tecniche / gdl / utenti corsi / …..	• AL MOMENTO DELLA RICHIESTA DI PARTECIPAZIONE AI LAVORI ASSOCIATIVI / DI CONTATTO CON L'ASSOCIAZIONE
COOKIE POLICY	• Verifica aggiornamento e rispondenza alle nuove previsioni del regolamento	APRILE / MAGGIO
FORMAZIONE	• formazione dipendenti Assifact sulla nuova procedura privacy e relativi adempimenti nello svolgimento dei singoli incarichi	MAGGIO