Verifica preliminare. Utilizzo di un sistema informatico antifrode nell’ambito delle transazioni di commercio elettronico effettuate attraverso il sito web aziendale - 19 gennaio 2017 [6068256]

[doc. web n. 6068256]

Verifica preliminare. Utilizzo di un sistema informatico antifrode nell´ambito delle transazioni di commercio elettronico effettuate attraverso il sito web aziendale - 19 gennaio 2017

Registro dei provvedimenti
n. 14 del 19 gennaio 2017

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, in presenza del dott. Antonello Soro, presidente, della dott.ssa Augusta Iannini, vice presidente, della dott.ssa Giovanna Bianchi Clerici e della prof.ssa Licia Califano, componenti, e del dott. Giuseppe Busia, segretario generale;

VISTO il d.lgs. 30 giugno 2003, n. 196, recante il "Codice in materia di protezione dei dati personali" (di seguito "Codice");

VISTA la richiesta di verifica preliminare presentata ai sensi dell´art. 17 del Codice da Ikea Italia Retail s.r.l. (di seguito "Ikea" o la "Società");

VISTE le successive comunicazioni inviate dalla Società in data 13 novembre 2015, 29 febbraio e 17 ottobre 2016;

ESAMINATA la documentazione in atti;

VISTE le osservazioni formulate dal segretario generale ai sensi dell´art. 15 del regolamento del Garante n. 1/2000;

RELATORE la dott.ssa Giovanna Bianchi Clerici;

PREMESSO

1. La richiesta formulata dalla Società.

1.1. Ikea Italia Retail s.r.l., con la nota del 5 agosto 2015, ha presentato a questa Autorità una richiesta di verifica preliminare, ai sensi dell´art. 17 del Codice, relativa all´utilizzo di un sistema informatico antifrode nell´ambito delle transazioni di commercio elettronico effettuate attraverso il proprio sito web, www.ikea.com/it.

Il sistema proposto avrebbe l´obiettivo di "gestire e possibilmente bloccare le transazioni di pagamento relative ad ordini fraudolenti provenienti dalla piattaforma di e-commerce" e si inserirebbe all´interno dell´attuale sistema di controllo delle transazioni introducendo un ulteriore step alle verifiche attualmente già eseguite dai circuiti internazionali con il c.d. sistema 3D Secure (Verified By Visa e MasterCard SecureCode).

Il sistema informatico antifrode che Ikea vorrebbe implementare è di proprietà della società ACI Universal Payments (con sede in Florida), di seguito "ACI Universal". Nello specifico, la società contraente con Ikea Italia Retail sarebbe ACI Worldwide Emea Limited (con sede nel Regno Unito) di seguito "ACI Worldwide", controllata da ACI Universal.

A tal fine ACI Worldwide e ACI Universal verrebbero nominati responsabili del trattamento e il trasferimento dati negli USA avverrebbe sulla base delle clausole contrattuali standard.

2. Il sistema proposto.

2.1. Al termine della verifica 3D Secure, il sistema di vendita on line trasmetterebbe al sistema antifrode i dati della transazione (ammontare della somma autorizzata, identificativo della transazione), i dati del customer host (nome, cognome, indirizzo e-mail, indirizzo civico, indirizzo IP), i dati della spedizione, i dati relativi alla modalità di accesso (es. cliente registrato o ospite, privato o azienda), i dati dell´acquisto (nome e prezzo del prodotto).

Questi dati verrebbero poi verificati da ACI Worldwide, attraverso i software "Red Gateway" e "Red Shield" (residenti su server situati in USA), sulla base di taluni parametri, quali: congruità tra luogo di emissione della carta e indirizzo IP da dove giunge la richiesta di transazione, numero degli acquisiti eseguiti nella giornata dalla stessa carta, valore totale degli acquisti, nome dell´acquirente privo di vocali, provenienza da domini storicamente etichettati come non sicuri, controlli su indirizzi diversi usati per pagamenti con la stessa carta, coerenza fra i dati della carta e quelli relativi alle transazioni precedenti, numero di pagamenti in un periodo di tempo predeterminato, verifiche su eventuali tentativi di acquisto con numeri di carta sequenziali.

L´esito complessivo di tale operazione di controllo verrebbe poi comunicato al Payment Gateway nel Regno Unito e, successivamente, a Ikea con l´indicazione che la transazione è stata autorizzata o non autorizzata ovvero che è necessario un intervento manuale.

L´analisi automatica da parte del sistema per decidere se una transazione debba o meno essere accettata si baserebbe sulle "regole" con cui è stato configurato il sistema. Al riguardo, la Società ha dichiarato di avere intenzione di configurare il sistema antifrode attivando solo e soltanto le "regole" che il Gruppo Payment di Ikea - casa madre ha definito e già utilizzato in altre nazioni (Francia, Regno Unito, Germania, Austria, Canada, Svezia, Norvegia, Olanda).

Qualora, invece, la transazione necessitasse di essere revisionata, l´operazione verrebbe eseguita manualmente da un incaricato del Customer Service Center (dislocato presso la sede di Carugate - MI), identificato come IKEA CSI Fraud user, che contatterebbe direttamente il compratore per ottenere ulteriori informazioni e, al termine della revisione, deciderebbe se accettare la transazione o rifiutarla, inserendo quindi la sua decisione nel sistema (tramite il "Case Manager").

In questo modo le potenziali vittime di furti di identità avrebbero la possibilità di prendere cognizione della frode sostanzialmente in tempo reale.

Anche nel caso in cui il sistema dovesse automaticamente rifiutare una transazione, gli interessati avrebbero, comunque, la possibilità di contattare (attraverso il numero verde, la chat o la email) gli operatori di Ikea per segnalare il problema e proseguire nell´operazione di acquisto.

L´obiettivo di Ikea, infatti, non è solo quello di bloccare una procedura di acquisto fraudolenta ma soprattutto quello di tutelare i propri clienti e garantire la massima sicurezza durante le fasi di acquisto e di pagamento.

Terminata la verifica da parte del sistema antifrode, i dati delle transazioni non andate a buon fine verrebbero inseriti in una apposita black list. Al riguardo la Società ha precisato che all´interno della black list non confluirebbero tutti i dati identificativi degli acquirenti precedentemente enumerati ma solo alcuni dati delle transazioni rifiutate e, in particolare, il numero della carta di credito, l´indirizzo email e il device id.

2.2. Il fornitore ACI garantirebbe non solo il rispetto delle misure minime di sicurezza richieste dal Codice ma anche di misure di sicurezza aggiuntive così sintetizzate:

- general requirements (designazione di un Data Privacy Officer, formazione dei coworker relativamente al trattamento di informazioni confidenziali, adozione di policies relative alla data privacy);

- misure tecnico-organizzative (misure per l´accesso ai locali sensibili, videosorveglianza, sistemi di logging, procedure per la rimozione di privilegi d´accesso in caso di venuta meno dei requisiti);

- misure per l´autenticazione degli utenti e degli amministratori di sistema;

- misure per la trasmissione dei dati;

- misure per la gestione dei trattamenti secondo le istruzioni del committente;

- misure per garantire la disponibilità del dato (backup, piano di emergenza, mirroring degli hard-disk ed altre misure supplementari);

- misure per il rispetto dei tempi di conservazione.

3. Le valutazioni dell´Autorità.

3.1. La verifica preliminare presentata all´Autorità ha ad oggetto il trattamento di dati personali degli utenti/clienti di Ikea Italia Retail s.r.l. nell´ambito delle transazioni di commercio elettronico effettuate sul portale della Società.

Occorre in primo luogo osservare che il sistema descritto si inserirebbe "nell´ambito della standardizzazione dei metodi di pagamento sulla piattaforma e-commerce IKEA", richiesta dal Gruppo Payment di Ikea casa madre (avente sede in Svezia).

In disparte tale premessa, si rileva, inoltre, che la specifica attenzione posta dal fornitore ACI rispetto all´osservanza di elevati standard di sicurezza, unitamente alla riconosciuta idoneità del sistema prescelto nel contribuire al contrasto di eventuali tentativi di frode, valgono a giustificare l´utilizzo dello strumento proposto e il correlato trattamento dei dati. Al riguardo, la Società ha, tra l´altro, segnalato che la piattaforma e-commerce italiana (solo nel bimestre aprile-maggio 2015) ha rilevato 71 tentativi di pagamento fraudolenti bloccati e che, considerati i parametri definiti dai circuiti internazionali relativi al numero dei tentativi di pagamento fraudolenti rilevati sui siti di e-commerce (che non deve superare il 7,5% delle transazioni totali provenienti dall´Europa e il 2,5% per le transazioni provenienti da tutto il mondo), il sistema proposto consentirebbe di rispettare questa soglia.

Occorre, altresì, valutare la conformità del sistema antifrode ai principi richiamati dal Codice.

A fronte della documentazione prodotta e delle dichiarazioni rese, il trattamento dei dati che Ikea intende effettuare per la finalità antifrode risulta soddisfare i requisiti di cui all´art. 11, comma 1, lett. a) e b), del Codice.

Per quanto attiene all´osservanza dei principi di necessità e proporzionalità (artt. 3 e 11, comma 1, lett. d), del Codice), il sistema descritto risulta preordinato all´acquisizione delle informazioni strettamente necessarie al perseguimento della finalità antifrode.

Con particolare riferimento ai tempi di conservazione dei dati, la Società ha dichiarato che i dati delle transazioni non andate a buon fine (conservati nel CSI Fraud database) verrebbero mantenuti per due anni e durante questo lasso temporale sarebbero utilizzati solo da Ikea per finalità di controllo antifrode.

Analogamente, i dati delle transazioni sarebbero conservati (nel CSI Payments database) per due anni. Tale termine è stato prescelto da Ikea anche in ragione del fatto che le condizioni contrattuali di vendita on line prevedono una garanzia di due anni.

Al riguardo, il Garante ritiene tale arco temporale congruo e proporzionato rispetto alle finalità e alla tipologia dei dati trattati.

Infine, considerato che, ai sensi degli artt. 23 e 24 del Codice, il trattamento di dati da parte di soggetti privati può essere lecitamente effettuato se è stato acquisito il consenso preventivo dell´interessato ovvero se sussistono i c.d. presupposti di liceità equipollenti al consenso, il Garante, ritenendo che il trattamento descritto sia correlato al perseguimento di un legittimo interesse della Società, con il presente provvedimento intende dare applicazione all´istituto del bilanciamento di interessi (art. 24, comma 1, lett. g), del Codice), individuando nello specifico trattamento di dati per finalità antifrode descritto in premessa un´ipotesi in cui il consenso non deve essere richiesto.

4. Ulteriori adempimenti.

4.1. Ai sensi dell´art. 17 del Codice, si ritiene opportuno prescrivere a Ikea le seguenti ulteriori misure a garanzia degli interessati.

Ferma restando la condizione che i dati dei clienti/utenti non siano utilizzati in operazioni di trattamento non compatibili con le

finalità originarie della raccolta (art. 11, comma 1, lett. b), del Codice) e che, alla scadenza dell´indicato periodo di conservazione, siano cancellati automaticamente, ovvero resi anonimi in modo permanente e non reversibile, è necessario che il titolare del trattamento fornisca agli interessati, ai sensi dell´art. 13 del Codice, le indicazioni relative alle caratteristiche del sistema proposto, integrando l´informativa attualmente presente sul sito web. Anche con riguardo al periodo di conservazione dei dati, la Società dovrà specificare nell´informativa che gli stessi saranno conservati per finalità antifrode per il periodo massimo di due anni.

4.2. Per quanto riguarda le misure tecniche da adottare, si ritiene necessario che la Società, nel garantire il rispetto di tutte le altre misure minime di sicurezza previste dal Codice, oltre a quelle aggiuntive di cui al par. 2.2., preveda anche l´utilizzazione di un sistema di autorizzazione (cfr. art. 34, comma 1, lettera c); regg. 12 – 14 del Disciplinare tecnico in materia di misure minime di sicurezza) per la gestione dei differenti ruoli degli incaricati delle diverse fasi di trattamento.

Inoltre, in ragione della delicatezza dei trattamenti antifrode, si richiede alla Società l´utilizzo di protocolli di comunicazione sicuri sia nella fase di interazione dei clienti con il portale web, sia nella fase di trasmissione dei dati in backoffice tra la Società stessa e i fornitori che intervengono nel trattamento antifrode in qualità di responsabili.

In aggiunta, considerato che l´analisi antifrode è attivata dalla "accettazione a procedere al pagamento", si ritiene necessario che anche la fase di gestione del "carrello", comprendente la raccolta degli articoli da acquistare e l´inserimento delle informazioni anche personali richieste (destinatario della merce, indirizzo, recapiti telefonici ed email), debba essere protetta con protocolli crittografici SSL (Secure Socket Layer), garantendo una migliore sicurezza a fronte dei rischi di furto di identità sempre presenti nell´interazione web con normali protocolli http "in chiaro".

Infine, allo scopo di valutare la reale efficacia del sistema antifrode in oggetto e delle correlate misure organizzative e di sicurezza, si richiede alla Società di fornire all´Autorità una relazione sul funzionamento del sistema riferito ai primi 12 mesi di sua effettiva implementazione, con particolare riguardo al numero dei tentativi di frode effettivamente sventati, nonché all´eventuale rilevazione di falsi positivi e di falsi negativi.

Si ricorda che, ai sensi degli artt. 17, 162, comma 2-bis e 167, comma 2, del Codice, chiunque, essendovi tenuto, non osserva il presente provvedimento è punito in sede amministrativa con la sanzione del pagamento di una somma da diecimila a centoventimila euro.

TUTTO CIÒ PREMESSO IL GARANTE

1) ai sensi dell´art. 17 del Codice, accoglie la richiesta di verifica preliminare presentata da Ikea Italia Retail s.r.l., nei termini di cui in motivazione e, a tal fine, prescrive al titolare del trattamento l´adozione delle misure di cui al punto 4 del presente provvedimento;

2) ai sensi dell´art. 24, comma 1, lett. g), del Codice, individua nel trattamento di dati per finalità antifrode un´ipotesi in cui non è richiesto il consenso degli interessati.

Ai sensi degli artt. 152 del Codice e 10 del d.lgs. n. 150 del 2011, avverso il presente provvedimento può essere proposta opposizione all´autorità giudiziaria ordinaria, con ricorso depositato al tribunale ordinario del luogo ove ha la residenza il titolare del trattamento dei dati, entro il termine di trenta giorni dalla data di comunicazione del provvedimento stesso, ovvero di sessanta giorni se il ricorrente risiede all´estero.

Roma, 19 gennaio 2017

IL PRESIDENTE
Soro

IL RELATORE
Bianchi Clerici

IL SEGRETARIO GENERALE
Busia