Regolamento Europeo 2016/679

COME PROMUOVERE LA PROPRIA IMMAGINE RISPETTANDO IL REGOLAMENTO EUROPEO 2016/679 COMUNICAZIONE E TUTELA DEI DATI PERSONALI NELL'ERA DIGITALE

SEMINARIO FORMATIVO SULLA PROTEZIONE DEI DATI PERSONALI

CENTRO CONGRESSI SGR RIMINI
18 Dicembre 2019

Luca Di Leo

Consulente in materia di privacy dal 2005

Associazione Protezione diritti e libertà privacy
(Vice presidente)

Studio Paci &C srl
(cda)

Responsabile della Protezione dei Dati

- certificazione **UNI 11697:2017** (Registro Accredia) – INTERTEK

Valutatore Privacy

- certificazione **UNI 11697:2017** (Registro Accredia) – INVEO

- Auditor - **ISDP@10003:2018** (Registro AICQ SICEV) – INVEO

- Lead Auditor ISO 27001

Aggiornamenti normativi e linee guida

Dei garanti europei per la protezione dei dati

nel mondo digitale correlato al web

---- COOKIES ----

Corte di giustizia dell'Unione europea

CGUE C-673/17 – Per l'installazione di cookie è necessario opt-in degli utenti
Decisione del Corte di Giustizia UE in tema di consenso all'installazione di cookie su Internet.

COMUNICATO STAMPA n. 125/19
Lussemburgo, 1° ottobre 2019 - Sentenza nella causa C-673/17

Per l'installazione di cookie è necessario il consenso attivo degli utenti di Internet
Una casella di spunta preselezionata è pertanto insufficiente

---- COOKIES ----

Guida all'uso dei cookies

AEPD – Agencia espanola protection datos

Novembre 2019

«…Inoltre, nel caso in cui un utente presti il tuo consenso all'uso dei cookie, le informazioni sul trattamento dovrebbero rimanere facilmente accessibili sulla pagina o nell'applicazione e **con non più di due clic, deve essere possibile recedere dal consenso…** »

---- COOKIES ----

Spagna:

Ikea riceve sanzione per violazioni sui cookie 5 Dicembre 2019

L'AEPD ha imposto una sanzione di 10.000 euro a Ikea Spagna per violazioni sui cookie. Infatti, in seguito a un reclamo, l'Autorità ha scoperto che ogni volta che un utente accedeva al sito, **venivano scaricati in automatico 23 cookie, per i quali non veniva richiesto il consenso dell'utente.**

---- COOKIES ----

Spagna:
AEPD sanziona **Vueling (compagnia aerea)** per non conformità dei cookie

22 Ottobre 2019 Il Garante spagnolo ha imposto una sanzione di 30.000 euro (riducibili a 18.000 con pagamento in un'unica soluzione) alla compagnia aerea Vueling per una non conformità dei cookie presenti sul suo sito web. Infatti, per gli utenti non era realmente possibile rifiutare i cookie, poichè la finestra di gestione, invece di permettere una loro accettazione granulare o rifiuto, rimandava alle impostazioni del browser utilizzato, senza dare informazioni sufficienti.

---- CONSERVAZIONE DEI DATI ----

DANIMARCA

Il garante danese ha aperto una procedura contro un'azienda di arredi per non avere cancellato i dati di 385 mila clienti, conservati in un vecchio sistema informativo, non più in uso, perché sostituito da altro aggiornato.

Il garante danese ha anche aperto un procedimento per l'applicazione di una sanzione di 160 mila euro alla compagnia di taxi, per mancata cancellazione dei dati della prenotazione delle corse. La società aveva la regola interna di distruzione dei dati dopo due anni. Ma questo non è avvenuto, in quanto la società cancellava solo i nomi, ma non i numeri di telefono dei clienti.

---- PROCEDURE PER L'ACCOUNTABILITY ----

INDAGINE INTERNAZIONALE SUL RISPETTO DELLA PRIVACY

SINTESI DEI RISULTATI ITALIANI
19 soggetti pubblici (Regioni e Provincie autonome) e 54 società in-house analizzate.

1. Politiche per la protezione dei dati personali

Un quinto delle regioni non ha ancora adottato una procedura interna per la gestione dei dati personali nell'organizzazione o non l'ha applicata correttamente nelle attività quotidiane. Quasi tutte, però, hanno incaricato una o più persone competenti in materia di governance e gestione della protezione dei dati personali, a un livello gerarchico sufficientemente elevato nell'organizzazione.

---- PROCEDURE PER L'ACCOUNTABILITY ----

2. Formazione, monitoraggio e consapevolezza

La maggior parte delle regioni e delle società in-house riconoscono l'importanza di un'adeguata formazione dei dipendenti in materia di protezione dei dati personali.

Nel 40% dei casi, però, le organizzazioni non hanno posto in essere alcun monitoraggio in merito all'attuazione di corrette pratiche nel trattamento dei dati personali.

---- PROCEDURE PER L'ACCOUNTABILITY ----

3. Trasparenza

E' garantita un'adeguata trasparenza nel trattamento dei dati, attraverso specifiche informative agli interessati sul trattamento dei dati personali. Tali informative, di solito, sono costantemente aggiornate e facilmente accessibili, sebbene alcune organizzazioni appaiono limitarsi a presentare la sola privacy policy del sito web.

---- PROCEDURE PER L'ACCOUNTABILITY ----

4. Capacità di risposta e gestione degli incidenti di sicurezza

Appare grave che il 24% delle società e il 48% delle Regioni non abbiano definito policy e procedure per la gestione delle richieste e dei reclami da parte degli interessati, o delle stesse Autorità.

Si evidenziano ancora carenze in merito alla gestione degli incidenti di sicurezza – i cosiddetti Data Breach – tanto che un quinto delle organizzazioni non ha ancora implementato una procedura di risposta agli incidenti di sicurezza che includa, tra l'altro, la notifica all'Autorità e, in caso di alto rischio per le libertà e i diritti degli interessati, anche la comunicazione a questi ultimi. Un quarto delle organizzazioni, inoltre, sembra non disporre di un registro per documentare le violazioni subite.

---- PROCEDURE PER L'ACCOUNTABILITY ----

5. Valutazione e monitoraggio dei rischi

Il 24% delle società in-house,

ma addirittura il 58% delle Regioni,

non hanno processi documentati per la valutazione dei rischi sulla protezione dei dati personali (DPIA), in relazione all'utilizzo di nuovi prodotti, tecnologie o servizi.

La maggior parte dei soggetti analizzati ha creato un registro dei trattamenti effettuati. Un quinto delle Regioni, però, dovrebbe fare uno sforzo maggiore per tenere traccia anche dei dati personali comunicati o trasmessi a terzi.

PROCEDURE PER L'ACCOUNTABILITY IMPLEMENTAZIONE

Politica di sicurezza e procedure per la protezione dei dati personali

- L'organizzazione dovrebbe documentare la propria politica in merito al trattamento dei dati personali come parte della sua politica di sicurezza delle informazioni.

- La politica di sicurezza dovrebbe essere revisionata e rivista, se necessario, su base annuale.

- La policy di sicurezza dovrebbe almeno riferirsi a**: i ruoli e le responsabilità del personale**, **le misure tecniche e organizzative** di base adottate per la sicurezza dei dati personali, **i responsabili del trattamento** dei dati o altre terze parti coinvolte nel trattamento dei dati personali.

- Dovrebbe essere creato e mantenuto **un inventario di policy / procedure specifiche** relative alla sicurezza dei dati personali, **basato sulla policy generale di sicurezza.**

PROCEDURE PER L'ACCOUNTABILITY IMPLEMENTAZIONE

Ruoli e responsabilità

- I ruoli e le responsabilità relativi al trattamento dei dati personali devono essere chiaramente definiti e assegnati in conformità con le politiche di sicurezza

- Dovrebbe essere effettuata una chiara nomina delle persone incaricate di compiti specifici di sicurezza, compresa la nomina di un responsabile della sicurezza.

Politica di controllo degli accessi

- I diritti specifici di controllo degli accessi dovrebbero essere assegnati **a ciascun ruolo** (coinvolto nel trattamento di dati personali) in base al principio della stretta pertinenza e necessità per il ruolo di accedere e conoscere i dati.

PROCEDURE PER L'ACCOUNTABILITY IMPLEMENTAZIONE

Gestione risorse/asset

- L'organizzazione dovrebbe disporre di un registro/censimento delle risorse e degli apparati IT utilizzati per il trattamento dei dati personali (hardware, software e rete).

- Il registro dovrebbe includere almeno le seguenti informazioni: risorsa IT, tipo (ad es. Server, workstation), posizione (fisica o elettronica). Dovrebbe essere assegnato ad una persona specifica il compito di mantenere e aggiornare il registro (ad esempio, il responsabile IT).

PROCEDURE PER L'ACCOUNTABILITY IMPLEMENTAZIONE

Gestione degli incidenti / Violazione dei dati personali (Personal data breaches)

- È necessario definire un piano di risposta agli incidenti (Incident Response Plan) con procedure dettagliate per garantire una risposta efficace e ordinata al verificarsi di incidenti o violazioni di dati personali.

- Gestione degli incidenti / Personal data breaches

Il piano di risposta degli incidenti (Incident Response Plan) dovrebbe essere documentato, compreso un elenco di possibili azioni di mitigazione e una chiara assegnazione dei ruoli.

PROCEDURE PER L'ACCOUNTABILITY IMPLEMENTAZIONE

Gestione degli incidenti / Violazione dei dati personali (Personal data breaches)

- È necessario definire un piano di risposta agli incidenti (Incident Response Plan) con procedure dettagliate per garantire una risposta efficace e ordinata al verificarsi di incidenti o violazioni di dati personali.

- Gestione degli incidenti / Personal data breaches

Il piano di risposta degli incidenti (Incident Response Plan) dovrebbe essere documentato, compreso un elenco di possibili azioni di mitigazione e una chiara assegnazione dei ruoli.

THANKS
And Bob's your Uncle