BROGLIA
_STUDIO LEGALE | SLB

SLB_News#01

Newsletter Garante Privacy

Linee Guida Confindustria 231

L’importanza del controllo sui fornitori

Sicurezza informatica: il phishing

Newsletter Garante Privacy

Online la newsletter n. 481 del 10 settembre del GP
https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9698442

Tre i temi affrontati:

- **Bodycam e riconoscimento facciale**
- **Roma Capitale, parcheggi e mancata tutela degli automobilisti**
- **Regione Lombardia, divieto di diffusione di dati che rivelino disagio economico.**

Bodycam

L'Autorità ha dato il via libera all'utilizzo di **particolari telecamere** per documentare situazioni critiche durante eventi o manifestazioni.
Sia la Polizia sia i Carabinieri potranno utilizzare questi strumenti **a condizione che non consentano l'identificazione univoca o il riconoscimento facciale** degli interessati.

Le telecamere potranno essere attivate **solo in presenza di concrete e reali situazioni di pericolo** di turbamento dell'ordine pubblico o di fatti di reato.

Non è ammessa la registrazione continua delle immagini e tantomeno quella di episodi non critici.

Roma Capitale

Il Garante ha irrogato una **sanzione di oltre 1 milione di euro** a Roma Capitale, alla società di servizi Atac Spa e a un subfornitore **per non aver tutelato i dati degli automobilisti che parcheggiano nel territorio del Comune**.

Atac, incaricata anche per la gestione dei parcheggi, aveva messo in atto un aggiornamento tecnologico dei parcometri per offrire nuovi servizi (ad esempio per il pagamento di sanzioni e tributi, l'acquisto dei biglietti) e introdurre nuove modalità di pagamento, inserendo anche il numero di targa del veicolo.

Le informazioni erano gestite anche attraverso un fornitore mediante un sistema centralizzato e una apposita app alla quale potevano accedere anche gli addetti al controllo dell'avvenuto pagamento della sosta.

Il Garante ha rilevato numerose violazioni della normativa privacy, tra le quali:

- la **mancata informazione degli interessati**
- la **mancata contrattualizzazione del fornitore** e l'assenza di precise istruzioni e indicazioni in ordine alle misure da adottare per il trattamento dei dati degli automobilisti
- la **mancata adozione del registro delle attività** di trattamento
- la **mancata individuazione delle tempistiche di conservazione** dei dati personali
- la **mancata adozione di adeguate misure di sicurezza**.

Regione Lombardia

Il Garante ha **sanzionato** la Regione per un importo di **200 mila euro**.

Il motivo è dato dalla mancata adeguata **protezione dei dati** personali relativi al **disagio economico e sociale** di coloro che avevano **presentato richiesta di ottenere benefici** economici connessi a tale situazione di difficoltà.

Poiché per ottenere borse di studio, sussidi per l'acquisto di libri e materiale tecnologico era necessario presentare una dichiarazione ISEE non superiore a 15 mila euro e che l'elenco di coloro che avevano presentato tali istanze era **pubblicamente disponibile**, ne è derivato il mancato rispetto degli obblighi di minimizzazione dei dati personali trattati.

Il rispetto degli obblighi di trasparenza cui i soggetti pubblici sono tenuti, infatti, impone di verificare sempre se la diffusione di dati personali sia prevista da una norma di legge o di regolamento: nel caso di specie, oltre a non essere previsto un tale obbligo, dalla pubblicazione era **derivata la possibilità indistinta di ricavare informazioni sulla situazione di disagio** degli interessati che avevano presentato domanda.

Linee Guida Confindustria per l'adozione dei Modelli Organizzativi 231

Pubblicate le nuove indicazioni alle imprese per la predisposizione dei Modelli Organizzativi di Gestione di Controllo ai sensi del D.Lgs. 231/2001

Parte generale
Parte speciale

Novità importante rispetto alla precedente versione la rilevanza dell'adeguamento dei Modelli al GDPR.

Oltre a costituire un efficace strumento di di controllo da tenere in considerazione nelle diverse aree e processi, la compliance alla protezione dei dati diviene una esimente in diverse ipotesi di commissione dei reati presupposto.

Altro aspetto di interesse quello della necessità della conformità dei sistemi di segnalazione cc.dd. whistleblowing dei Modelli al Regolamento Europeo, che dovrà tutelare la riservatezza dei soggetti segnalanti.

Vale la pena evidenziare l'importanza che le Linee Guida conferiscono all'adozione di sistemi di certificazione in materia di sicurezza delle informazioni e anticorruzione.

L’importanza del controllo sui fornitori

I provvedimenti del Garante Privacy richiamati nella newsletter che abbiamo citato all’inizio di queste news (n. 292, 293 e 294 del 22 luglio 2021) fanno particolare riferimento alla **“filiera” dei fornitori** e ribadiscono con fermezza la necessità, in tutti i casi in cui si demandino operazioni su dati personali (nonché laddove i fornitori abbiano, comunque, accesso agli stessi):

- innanzi tutto di **mettere “per iscritto”** ciascuno di questi rapporti;
- di indicare con precisione e accuratezza **le misure di sicurezza** cui la supply chain deve adottare e, inoltre,
- di precisare con dovizia di particolari **le istruzioni** nonché
- **i limiti** che, in base all’art. 28 del GDPR devono essere fissati in tali rapporti perché il responsabile tratti conformemente alle finalità e modalità demandate i dati che gli sono affidati.
- Tale **obbligo ricade, inoltre, anche sul Responsabile** che, a propria volta, deve fare altrettanto con i propri sub-responsabili.

Sicurezza informatica: il phishing

Il phishing, così come anche il social engineering, è una tecnica di attacco informatico tesa a **carpire informazioni sensibili o riservate** di un utente.

Un classico caso di phishing è quello del **messaggio email con caratteristiche grafiche o testuali pressoché identiche a quelle di istituzioni, aziende o operatori molto noti** (la nostra Banca, la Posta, per esempio): cliccando su un link contenuto nel messaggio si viene indirizzati, però, non al vero sito dell'azienda, ma ad un sito artefatto, in tutto e per tutto simile all'originale nel quale si è invitati a **inserire** le proprie credenziali, ossia **username e password**.

E' un attacco basato sul fattore umano (come anche il citato e "antico" *social engineering*, da sempre utilizzato per esempio, dagli agenti segreti 😃), spesso dovuto a fretta, stanchezza, stress o semplice distrazione.

In tal modo l'attaccante viene in possesso delle informazioni utili a inserirsi in un sistema, in un sito, in una applicazione, gestendola poi per le proprie finalità, per lo più illegali.

Si parla di **smishing** quando l'attacco viene effettuato tramite messaggi SMS o di **vishing** quando si utilizzano messaggi vocali.

BROGLIA
_STUDIO LEGALE SL3

SL3 _AVV. ANDREA BROGLIA

via della Brunella, 4 - 21100 Varese VA - Italy
Tel +39.0332.811.238 - info@studiolegalebroglia.com
www.studiolegalebroglia.com