Il nuovo regolamento europeo sulla privacy (GDPR): i nuovi adempimenti per la pubblica amministrazione, le imprese e le strutture sanitarie

La gestione degli incidenti informatici (violazioni dati) connessi ai dati personali: il nuovo obbligo di notificazione.

Relatore: Avv. Emiliano Vitelli

Casistica di data breach

FURTO NOTTURNO SCOPERTO STAMATTINA

Ladri nel palazzo comunale di Aprilia: rubate anche le carte di identità

A+ | A− | 24 febbraio 2017, ore 08:52 Condividi

Casistica di data breach

CORRIERE DELLA SERA

ROMA / CRONACA

3

367

LITORALE

Fiumicino, attacco hacker al Comune Cancellati i database del «sociale»

Il virus giunto per mail con richiesta di soldi in cambio dei dati. Sparite le graduatorie delle case popolari e i back-up. Gonnelli: caso sospetto. Montino: danni gravi

Casistica di data breach

Albano, furto in Comune: rubate 970 carte d'identità

Ennesimo colpo grosso all'ufficio Anagrafe del Comune di Albano dove, in nottata, sono state portate via 970 carte di identità, 500 euro in contanti e un cospicuo numero di valori bollati. Dopo l'analogo furto che ai primi di agosto fruttò un

Casistica di data breach

Articolo pubblicato sull'Unione Sarda 02 febbraio 2017.

PULA

Attacco hacker al Comune: colpa degli antivirus gratis

«Ci chiediamo perché il Comune non protegga in maniera adeguata il sistema informatico dei propri uffici: è inaccettabile affidarsi ad antivirus scaricati gratuitamente da internet». Nei giorni scorsi un potente virus ha attaccato la rete informatica comunale, creando non pochi disagi. L'attacco sarebbe partito da un computer del settore ragioneria: un con- dei dati dei computer comunali, composta da dati e documenti sensibili, ci siano solo antivirus *freeware* - dice Emanuele Olla, del gruppo Libertas - vorremmo sapere perché non è stata presa in considerazione l'ipotesi di acquistarne altri capaci di mettere al riparo la rete da spiacevoli soprese. A volte si utilizza il denaro per iniziative di cui si potrebbe fare a meno e

Casistica di data breach

Home › Aprilia › Aprilia, gruppo di hacker attacca pc di un'azienda e chiede il riscatto...

APRILIA CRONACA LATINA

Aprilia, gruppo di hacker attacca pc di un'azienda e chiede il riscatto per restituire i file

Le nuove frontiere del rapimento 2.0

23 gennaio 2017

Casistica di data breach

Il Mattino > Salerno >

Attacco hacker a un'azienda alterata la gamma di prodotti

Continua a mietere vittime, nel Salernitano, il potente virus informatico "Cryptlocker", in grado di inibire pc e server dell'ignaro utente di turno. Per sbloccare il tutto, il "ransomware", letteralmente "riscatto della merce", chiede una somma di denaro da pagare entro un termine perentorio, spesso accompagnato da un conto alla rovescia sul desktop. Ma, il più delle volte – avvertono gli esperti di sicurezza informatica – pur pagando, non si è certi di rientrare in possesso dei propri archivi.

Casistica di data breach

Patient records stolen in computer breach at Torrance Memorial Medical Center

Torrance Memorial Medical Center reported that a data breach occurred in April 2017. File photo. (Thomas R. Cordova/Daily Breeze/SCNG)

Casistica di data breach

Ladri senza scrupoli. Furto all'ospedale di Siena, rubato supporto con dati di pazienti e di ricerca

By **Redazione** - 05/06/2017 182 0

SHARE Facebook Twitter G+

Casistica di data breach

Yahoo violata ancora: trafugati i dati di un miliardo di account

L'azienda ha svelato un altro massiccio data breach, identificato grazie al lavoro delle forze dell'ordine. Gli hacker avrebbero prelevato nomi, indirizzi email, numeri di telefono, date di nascita, password crittografate, domande e risposte di sicurezza. I pirati avrebbero inoltre creato cookie speciali per entrare nei profili personali senza utilizzare chiavi d'accesso.

Pubblicato il 15 dicembre 2016

Non c'è pace per Yahoo. Dopo aver svelato solo a settembre un attacco hacker vecchio di almeno due anni, che aveva portato alla compromissione di circa 500 milioni di account, ieri l'azienda ha confermato un'altra intrusione nei propri sistemi informatici. A essere trafugate, questa volta, sarebbero le informazioni

Definiamo «data breach»

La trasmissione, comunicazione o comunque l'apprensione non autorizzata di informazioni [sensibili] ad una parte non è autorizzata.

Il regolamento definisce violazione dei dati personali (art. 4):

La violazione di sicurezza che comporta <u>accidentalmente</u> o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

Il Regolamento Europeo n. 679/2016

Dal Considerando 86

Il titolare del trattamento dovrebbe comunicare la violazione dei dati personali qualora questa violazione sia suscettibile di presentare **un rischio per i diritti e le libertà della persona fisica**.

Il Regolamento Europeo n. 679/2016

Il Considerando n. 85

Una violazione dei dati personali può, **se non affrontata in modo adeguato e tempestivo**, provocare:

1. perdita del controllo dei dati personali;
2. limitazione dei diritti delle persone;
3. discriminazione;
4. furto o usurpazione d'identità;
5. perdite finanziarie;
6. pregiudizio alla reputazione;
7. o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata.

Il Regolamento Europeo n. 679/2016

La valutazione concreta del Considerando n. 88

Ai fini della notifica occorre tenere debitamente conto delle circostanze della violazione, ad esempio:

- stabilire se i dati personali fossero o meno protetti con misure tecniche adeguate di protezione;
- verificare i legittimi interessi delle autorità incaricate dell'applicazione della legge, qualora una divulgazione prematura possa ostacolare inutilmente l'indagine.

Il Regolamento Europeo n. 679/2016

Il Regolamento prevede un sistema di notifica a seconda del rischio associato alla violazione:

1) all'autorità di controllo (art. 33 del GDPR);

2) ai soggetti interessati dalla violazione (art. 34 del GDPR).

Il Regolamento Europeo n. 679/2016

Art .33 – Notifica di violazioni dei dati all'autorità di controllo (1)

Termine di 72 ore per informare l'Autorità di Controllo dell'avvenuta violazione (o motivi di ritardo)

Contenuto minimo della notifica:

1) La descrizione della natura della violazione;
2) Il numero e le categorie dei dati interessati (se disponibili);
3) Il nome del responsabile della protezione dei dati;
4) Le probabili conseguenze della violazione;
5) Le misure adottate per porvi rimedio e/o attenuarne gli effetti negativi.

Il Regolamento Europeo n. 679/2016

Art .34 – Comunicazione di una violazione dei dati personali all'interessato (1)

Non si menziona un termine preciso entro il quale adempiere, ma il legislatore prevede che questa debba avvenire "**senza ingiustificato ritardo**".

L'obbligo di comunicazione all'interessato scatta nei casi più gravi, in cui dalla violazione possano derivare **rischi elevati per i diritti e le libertà delle persone fisiche**.

Il Regolamento Europeo n. 679/2016

Art .34 – Comunicazione di una violazione dei dati personali all'interessato (2)

La notifica delle violazioni deve almeno:

a) comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;

b) descrivere le probabili conseguenze della violazione dei dati personali;

c) descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

La comunicazione all'interessato deve essere formulata con un linguaggio semplice e chiaro e deve descrivere la natura della violazione dei dati personali.

Evito il data breach o vi pongo rimedio?

E' importante che i Titolari del trattamento procedano a un'adeguata pianificazione adottando e attuando misure tecniche ed organizzative adatte per garantire un livello di sicurezza appropriato rispetto ai rischi individuati.

Quindi sarà necessario:

1) idoneo quadro di gestione dei rischi (valutazione di impatto);
2) corretta tenuta del Registro dei trattamenti (anche se non obbligatorio);
3) istituire preventivamente piani appropriati per il trattamento (reazione e mitigazione) delle violazioni dei dati personali;

Sanzioni…

Fatto salvo ogni altro ricorso amministrativo o giurisdizionale, l'interessato che ritenga che il trattamento che lo riguarda violi il presente regolamento ha il diritto di proporre reclamo ad un'autorità di controllo.

Ogni autorità di controllo provvede affinché le sanzioni amministrative pecuniarie inflitte siano in ogni singolo caso effettive, proporzionate e dissuasive.

Sanzioni…

L'art. 83 stabilisce espressamente che la violazione degli obblighi del titolare del trattamento e del responsabile del trattamento a norma degli articoli 8, 11, **da 25 a 39**, 42 e 43 è soggetta a sanzioni.

…e responsabilità

Chiunque subisca un danno materiale o immateriale causato da una violazione del presente regolamento ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento.

La valutazione delle danno

(Il Considerando 75) (1)

La responsabilità conseguente alle violazioni può determinare un danno fisico, materiale o immateriale, in particolare se il trattamento può comportare:

1) discriminazioni, furto o usurpazione d'identità;
2) perdite finanziarie;
3) pregiudizio alla reputazione;
4) perdita di riservatezza dei dati personali protetti da segreto professionale;
5) decifratura non autorizzata della pseudonimizzazione;

…

La valutazione delle danno

(Il Considerando 75) (2)

…

6) qualsiasi altro danno economico o sociale significativo;
7) se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o venga loro impedito l'esercizio del controllo sui dati personali che li riguardano;
8) se sono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza;

…

La valutazione delle danno

(Il Considerando 75) (3)

…

9) in caso di valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali;
10) se sono trattati dati personali di persone fisiche vulnerabili, in particolare minori;
11) se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati.

Grazie per l'attenzione

EPCE

European Privacy Centre

La gestione degli incidenti informatici (violazioni dati) connessi ai dati personali: il nuovo obbligo di notificazione.

Relatore: Avv. Emiliano Vitelli