DATA BREACH

Significa: Violazione della sicurezza dei dati. Definizione molto generale.
Il 196/2003 Decreto sulla privacy è il precursore del trattamento della violazione dei dati personali in ambito nazionale.
All'interno della Comunità Europea si profilavano normative e sanzioni differenti tra gli stati a seconda delle rispettive normative .
La volontà del legislatore comunitario è stata quella di armonizzare ed uniformare la disciplina (sia la normativa, sia l'applicazione della normativa)
Anche un testo normativo univoco corre il rischio di essere interpretato ed applicato in modo diverso tra stato e stato.
I garanti europei hanno costituito un organismo collegiale che prende decisioni su linee guida circa l'applicazione delle normative negli stati membri.
E' il WP (Working Party) , organo collegiale delle autorità garanti europee che ha emanato le linee guida sulla notifica delle violazioni dei dati (SLIDE 5).
l **Gruppo dell'articolo 29 per la tutela dei dati**[1] (in inglese ***Article 29 Working Party*** o WP29) era il gruppo di lavoro comune della autorità nazionali di vigilanza e protezione dei dati.

Era un organismo consultivo indipendente, composto da un rappresentante della varie autorità nazionali, dal Garante europeo della protezione dei dati e da un rappresentante della Commissione. Il presidente era eletto dal Gruppo al suo interno ed ha un mandato di due anni, rinnovabile una sola volta. Il Gruppo adottava le sue decisioni a maggioranza semplice dei rappresentanti delle autorità di controllo.

L'articolo 29 della direttiva europea 95/46 prevede, vari compiti da affidare ai membri dei Garanti nazionali, che quindi si riunivano per garantire regole comuni in tema di privacy.

Le sue principali missioni erano:

•Fornire un parere esperto agli Stati in merito alla protezione dei dati;
•Promuovere l'applicazione coerente della direttiva sulla protezione dei dati in tutti gli Stati membri dell'UE, nonché in Norvegia, Liechtenstein e Islanda;
•Dare alla Commissione un parere sulle leggi comunitarie (primo pilastro) che riguardano il diritto alla protezione dei dati personali,
•Fornire raccomandazioni al pubblico su questioni relative alla protezione delle persone con riguardo al trattamento dei dati personali e alla privacy nella Comunità europea.

SLIDE 6
Cosa deve fare il Titolare in caso di violazione dei dati personali.
Parametri fondamentali sono:
"da quando è venuto a conoscenza (parallelismo con la PEC e con l'ISP)
"senza giustificato ritardo"
"quando sia probabile che la violazione comporti etc, etc,……)

SLIDE 7
Si sottolinea che in caso di 1 notifica per più violazioni il titolare sarà sottoposto ad una sola istruttoria che si potrà eventualmente concludere con la comminazione di 1 sola sanzione (pecuniaria) nel caso in cui si siano riscontrati comportamenti illeciti.
Per contro in caso di più notifiche per più violazioni il titolare sarà sottoposto a più istruttorie con il rischio di più sanzioni.

SLIDE (

c) principio di proporzionalità tra rischio dell'interessato e rimedio da porre in essere da tarte del titolare
si può scegliere una modalità di comunicazione massiva nel caso in cui la comunicazione individuale sia particolarmente onerosa

CASO INPS
SLIDE 10
Stiamo parlando di dati ex art. 9 – dati sensibili.

La notifica dell'INPS al garante avviene il 3 aprile.
Primo problema: non è ancora chiaro se la violazione sia scaturita da un attacco hacker piuttosto che da un malfunzionamento interno. (seee, hacker, come no.....)

SLIDE 14
punto c) viene individuato un indirizzo Email a cui poter inviare richieste di informazioni e chiarimenti (in aggiunta o in alternativa al DPO?? non ho capito.)

SLIDE 20
Il garante della privacy ha individuato tempi e modalità con cui INPS dovrà informare gli interessati nonché le sanzioni.

SANZIONI

3 tipologie /metodologie sanzionatorie

1. correttive (SLIDE 22-23)
2. economiche – sanzioni pecuniarie (in seguito a comportamenti illeciti – penale)
3. civili (perché secondo l'art 2050 del c.c. si ravvisa una responsabilità per l'esercizio da attività pericolosa).
   L'onere della prova di aver fatto tutto il possibile è a carico del titolare per dimostrare la mancanza del nesso di causalità tra la negligenza ed il danno del soggetto interessato.

Sono previste sanzioni con gradualità crescente (dalla più leggera alla più pesante)
Tavola edittale: quadro di sanzioni in corrispondenza di vari illeciti.