Ordine Ingegneri Genova

DotNet Liguria

GDPR – Approfondimento sulla security

22 Febbraio 2018

Agenda

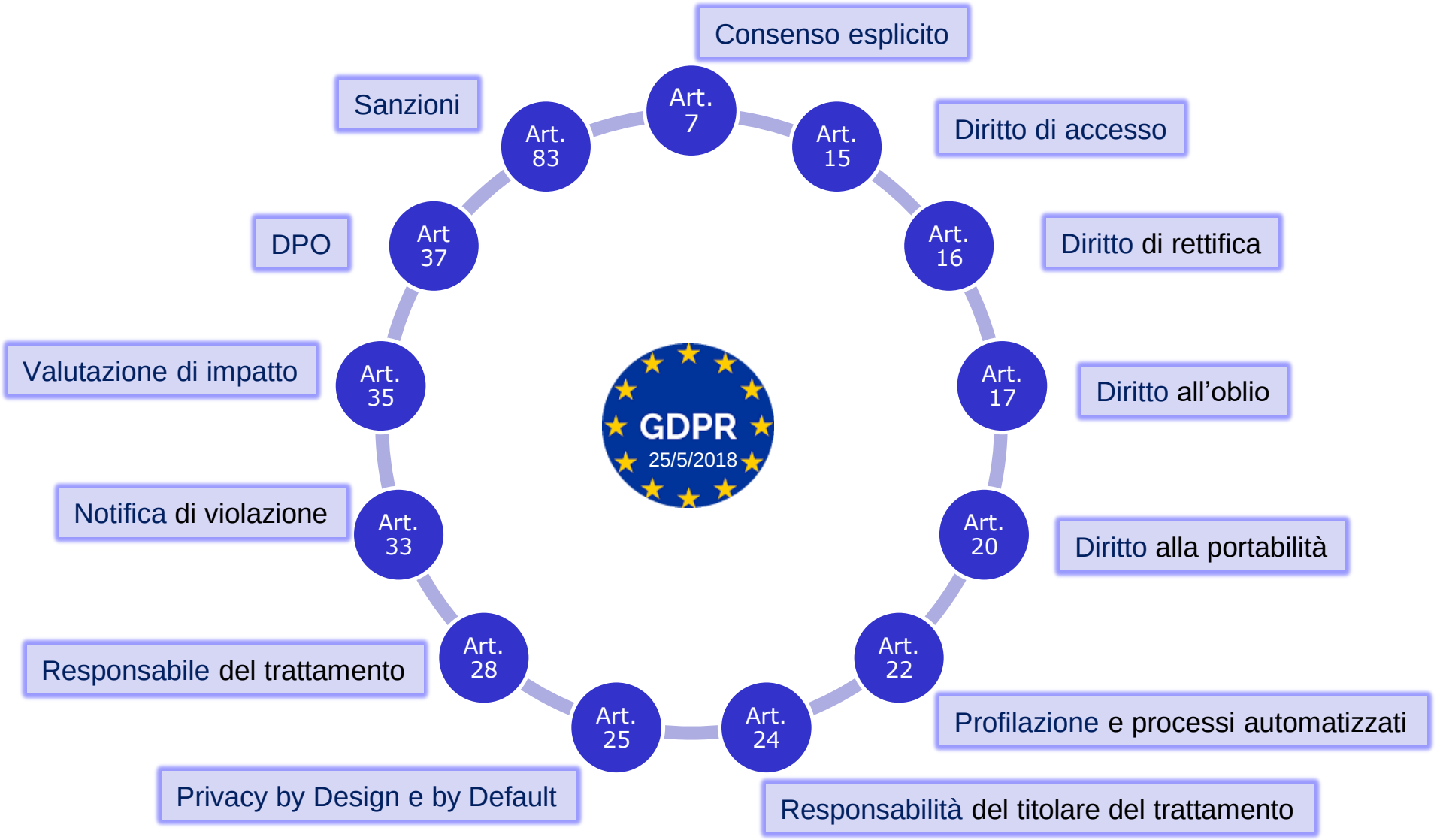
- Presentazione e Introduzione
  Matteo Gentile *– Ordine degli Ingegneri Genova*
- Progettare software in linea con il nuovo regolamento GDPR
  Raffaele Rialdi *- DotNet Liguria | Microsoft .NET MVP*
- SQL Server & GDPR
  Gianluca Hotz *- Presidente UGISS | Microsoft SQL Server MVP | Mentor at SolidQ*
- Ritorno ai fondamenti
  Raffaele Rialdi *- DotNet Liguria | Microsoft .NET MVP*

Il **25 Maggio 2018** inizierà ad avere efficacia il nuovo **Regolamento Generale sulla Protezione dei Dati - RGPD**, meglio noto con l'acronimo "***GDPR – General Data Protection Regulation***", una normativa approvata dal Parlamento Europeo nell'Aprile 2016 (Regolamento UE 2016/679).

L'obiettivo è quello di armonizzare le leggi sulla riservatezza delle informazioni e sulla privacy di tutti i Paesi Europei e tenere al sicuro i dati sensibili degli utenti processati dalle aziende.

Il testo è stato pubblicato sulla Gazzetta Ufficiale Europea il **4 maggio 2016** ed è entrato in vigore il **25 maggio** dello stesso anno.

Overview


Consenso esplicito
Art. 7
Diritto di accesso
Art. 15
Diritto di rettifica
Art. 16
Diritto all'oblio
Art. 17
Diritto alla portabilità
Art. 20
Profilazione e processi automatizzati
Art. 22
Responsabilità del titolare del trattamento
Art. 24
Privacy by Design e by Default
Art. 25
Responsabile del trattamento
Art. 28
Notifica di violazione
Art. 33
Valutazione di impatto
Art. 35
DPO
Art 37
Sanzioni
Art. 83
GDPR
25/5/2018

Alcune recenti linee guida

European Commission

- Il 6/2/2018 è uscita l'ultima revisione del **testo** delle Linee guida elaborate e adottate dal Gruppo Art. 29 in materia di **processi decisionali automatizzati e profilazione**, definite in base alle previsioni del **Regolamento (UE) 2016/679.**

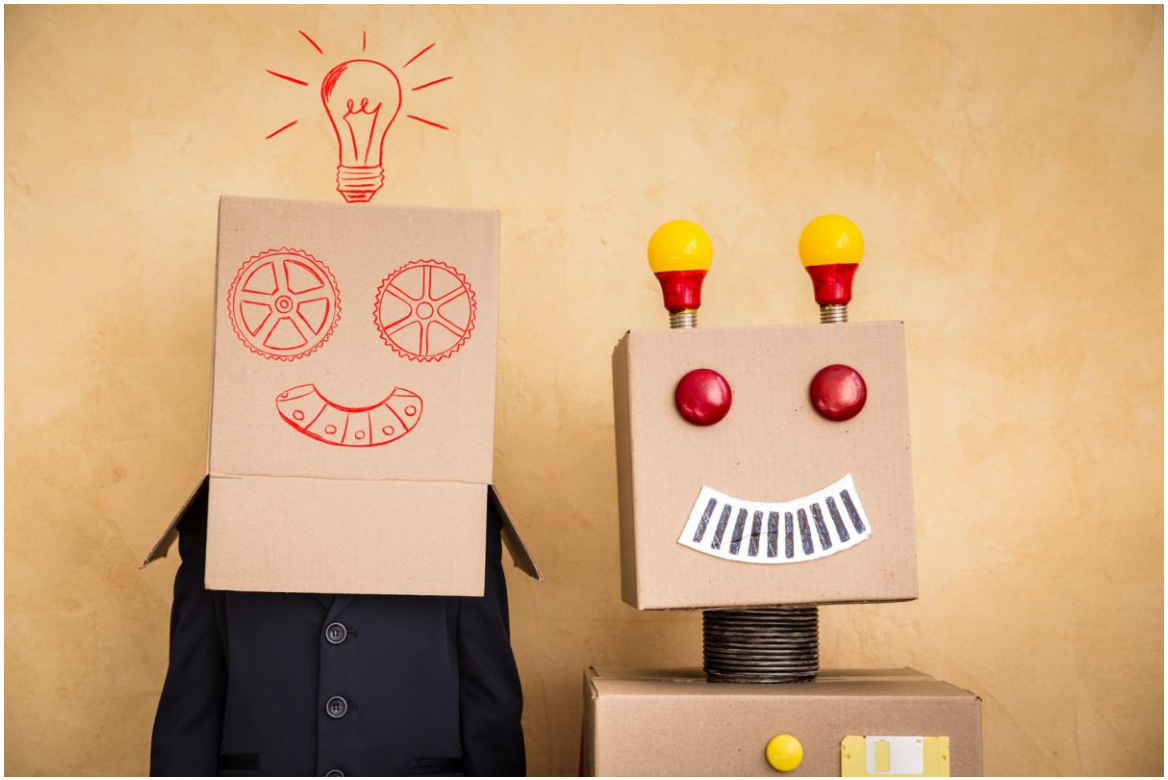
- Il 6/2/2018 è uscita l'ultima revisione del **testo** delle Linee guida elaborate e adottate dal Gruppo Art. 29 in materia di **notifica delle violazioni di dati personali (data breach notification)**, definite in base alle previsioni del **Regolamento (UE) 2016/679.**

- Il 3 Ottobre 2017 sono state emanate le **Linee guida riguardanti l'applicazione e la previsione delle sanzioni amministrative pecuniarie ai fini del regolamento (UE) n. 2016/679 - WP253**

Informazioni personali …

How companies learn your secrets

Smart toys: i suggerimenti del Garante per giochi a prova di privacy



http://www.garanteprivacy.it/iot/smarttoys

Performance di vendita & privacy

Secondo il Cisco 2018 Privacy Maturity Benchmarch Study (performance di vendita in relazione alla gestione dei dati personali dei clienti, che ha analizzato le risposte di 3000 professionisti di sicurezza in 25 Paesi del mondo) **le aziende che non gestiscono la privacy nel modo migliore accusano ritardi di vendite medi di circa 7,8 settimane, mentre chi segue una metodologia appropriata si attesta a 3,4 settimane**.
Il peso della gestione dei dati nei tempi di conclusione degli affari varia molto in rapporto alla posizione geografica e alla tipologia di business.

http://www.ilsole24ore.com/art/tecnologie/2018-01-26/alle-aziende-privacy-costa-ritardi-vendite-fino-8-settimane--165406.shtml

Costi medi per impresa di un Data Breach

Ponemon Institute - 2017

Errori umani o negligenza

$ 3,85 M
per incidente

$ 137 per record

Problemi tecnici espongono dati

$ 3,99 M
per incidente

$ 142 per record

Hacker & Insiders

$ 4,77 M
per incidente

$ 170 per record

Un sondaggio PwC rileva che il 40% dei manager di società con elevata automazione IT è conscia che un attacco possa portare al collasso dell'attività, e **il 44% degli intervistati ha ammesso che la propria impresa non possiede una strategia complessiva di sicurezza informatica**.

Data Breach

Il 4 febbraio 2018 il Gruppo attivista *AnonPlus*, affiliato ad *Anonymous Italia*, ha trafugato un database del Partito Democratico Italiano contenente informazioni personali sugli appartenenti al Partito registrati a Firenze.

I dati trafugati sono costituiti da 2.652 file di informazioni personali tra cui nome e cognome, indirizzo e-mail, data di nascita, città di nascita e numero di telefono (linea fissa e cellulare).

Il 5 febbraio il sito del Partito Democratico di Firenze mostrava un messaggio di errore relativo al database SQL quando si provava ad accedere al sito; questa è una potenziale indicazione di un attacco di **SQL injection**.

It’s time to start !