Incubatore
Imprese
Innovative
Politecnico
Torino

Xenialab - GDPR

Corso di aggiornamento interno rivolto ai

programmatori ed analisti

sul regolamento di sicurezza in vigore dal 25 Maggio 2018

Cos'è il GDPR

- Regolamento che disciplina privacy
- Non solo i dati sensibili ma i dati personali

Perché il GDPR

- Evoluzione digitale
- Maggiore attenzione alla privacy rispetto ad alcuni anni fa
- Uniformità del regolamento a livello europeo
- Sanzioni importanti

Alcune definizioni

- DATO PERSONALE : qualsiasi informazione riguardante una persona fisica identificata o identificabile

Elenco dei principali esempi:

- nome cognome
- foto
- indirizzi email con nome e cognome
- conti correnti numero SSN
- firme digitali
- curricula
- istruzione e cultura
- luogo e data di nascita
- profilo medico
- ….

Alcune definizioni

- INTERESSATO: si intende la persona fisica a cui si riferiscono i dati trattati.

- TITOLARE DEL TRATTAMENTO: è la persona fisica (o l'impresa o altro) cui spettano le decisioni sugli scopi e sulle modalità del trattamento e sugli strumenti utilizzati.

- RESPONSABILE DEL TRATTAMENTO: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.

- SOGGETTI AUTORIZZATI AL TRATTAMENTO: la persona fisica che viene a contatto con i dati ma ne gestisce funzioni tipicamente operative (archiviazione , ecc).

- RISCHIO: la potenzialità che un'azione o un'attività scelta (includendo la scelta di non agire) porti a una perdita o ad un evento indesiderabile. Anche le perdite potenziali possono anche essere chiamate "rischi".

Differenze con la vecchia normative privacy

- **Cosa resta**
  - Protezione delle sole persone fisiche
  - Definizione di trattamento
  - Definizione dato personale
  - Principi relativi al trattamento dei dati
  - Liceità del trattamento
  - Obbligo di informative e consenso
  - Adozione di misure tecnico/organizzative adeguate

- **Cosa cambia**
  - Privacy by default e by design
  - Progetto di valutazione di impatto
  - Diritto all'oblio
  - Portabilità dei dati
  - Responsabilizzazione del titolare e responsabile
  - Registro trattamenti
  - Obbligo di notifica in caso di data-breach

Cosa dobbiamo fare noi, praticamente?

Privacy by default e by design

Developers

- Analisi e specifiche di progetti concepite sin dall'inizio per trattare le problematiche della privacy e della disponibilità delle informazioni
- L'approccio del progettista e dell'architetto deve essere inteso non come un aspetto legale da rispettare ma come una responsabilità da fare propria
- Gli ambienti di produzione contenenti dati effettivi devono essere protetti; sviluppo e test vanno eventualmente anonimizzati

Cosa dobbiamo fare noi, praticamente?

Privacy by default e by design

Developers

- I siti aziendali Xenialab, tramite I cookies raccolgono dati ed informazioni per i quali occorre chiedere l'autorizzazione al trattamento ed alle policies adottate ; il GDPR impone di informare gli utenti quali tipologie di cookie il sito utilizza
- Le autorizzazioni devono essere esplicite, richiesta chiara e consenso dell'interessato su domanda
- Tutte le gestioni di raccolta CV o altre informazioni personali vanno autorizzate con apposito modulo
- Il servizio di manutenzione e assistenza deve applicare il criterio di scegliere la strada di intervento e manipolazione del sw/hw che sia la meno impattante possibile sui dati
- **Qualsiasi azione proattiva che contribuisca a migliorare la protezione dei dati in possesso di Xenialab**

Cosa dobbiamo fare noi, praticamente?

Progetto di valutazione di impatto

Developers

- E’ caldamente consigliato (ove necessario) formulare un progetto di valutazione di impatto “PIA” ovvero la valutazione del rischio, composta da:
  - **Individuazione**: si mappano le possibili situazioni di rischio di violazione, della probabilità dell’evento e della gravità delle conseguenze.
  - **Rischi**: quali sono i rischi connessi al trattamento e quante le probabilità di accadimento
  - **Protezione**: quali sono le misure atte a ridurre la possibilità di accadimento di data-breach e discontinuità di disponibilità
  - **Rilevazione**: ci devono essere, secondo processi di qualità, dei sistemi di monitoraggio continuo in grado di segnalare tempestivamente eventi legati al rischio privacy.
  - **Ripristino:** prevedere piani di ripristino della normale operatività dopo un incidente.

Cosa dobbiamo fare noi, praticamente?

Developers

Diritto all'oblio

Portabilità dei dati

- Trovare sempre la possibilità di gestire la cancellazione dei dati personali
- I dati personali devono poter essere esportati (basta avere la possibilità di effettuare un export da DB)
- Devono essere disponibili in formato utilizzabile e leggibile

Cosa dobbiamo fare noi, praticamente?

Azioni preventive e quotidiane

Developers

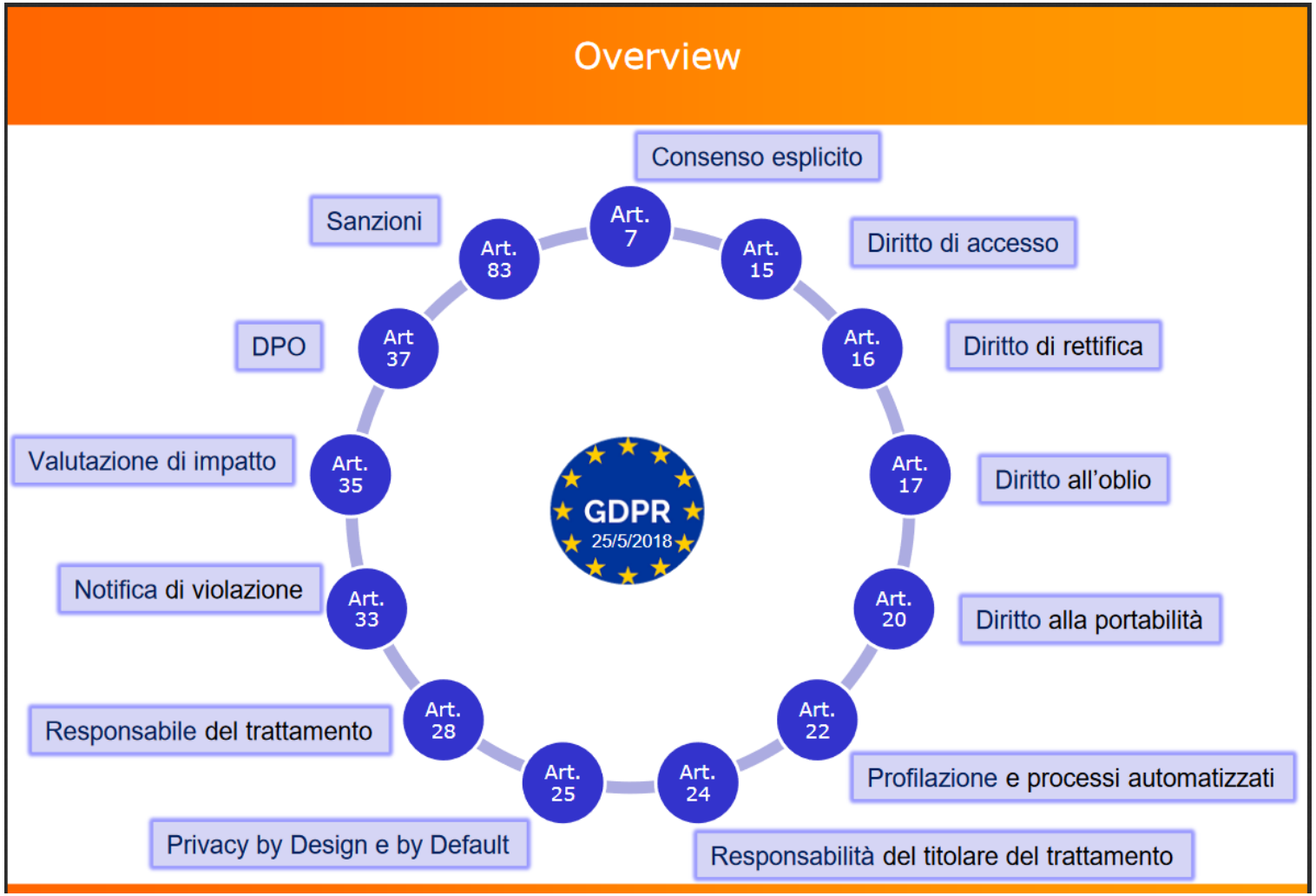
- Gestione sicura e riservata delle proprie mail e di quelle in arrivo (password, backup); riservatezza nelle fasi di lettura e scrittura
- In caso di possesso di dati personali:
  - PC non accessibile in caso di assenza; protezione con password
  - Backup regolare dei dati
  - Protezione dell'hard disk per i casi di furto o smarrimento (encryption ?)
  - Uguali criteri del notebook da usare per il cellulare
  - Scrivanie senza fogli con informazioni o appunti significativi così come l'accesso alle cassettiere

Cosa dobbiamo fare noi, praticamente?

Azioni preventive e quotidiane

Developers

- Applicare il GDPR: by default and by design
- Aggiornamenti periodici da seguire
- Ulteriori riferimenti:
  - http://www.xenialab.it/meo/web/white/oracle/db_lex.htm#gdpr (GDPR)
  - http://www.xenialab.it/meo/web/white/oracle/db_enc.htm (crittografia con i DB)
  - http://www.xenialab.it/meo/web/white/oracle/my_fix.htm (sicurezza con MySQL)
  - http://www.xenialab.it/meo/web/white/oracle/my_mixen.htm (anonimizzazione con MySQL)
  - http://www.xenialab.it/meo/web/white/varie/xcally_sat.htm (controlli sicurezza xCally)


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

XENIALAB™
WEB AND MOBILE COMMUNICATIONS

Xenialab - GDPR

Corso di aggiornamento interno rivolto ai

programmatori ed analisti

sul regolamento di sicurezza in vigore dal 25 Maggio 2018

Incubatore Imprese Innovative Politecnico Torino