



XENIALABTM

WEB AND MOBILE COMMUNICATIONS



Xenialab - GDPR

Corso di aggiornamento interno rivolto al
personale amministrativo

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

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

Amministrazione.

- Tutte le attività che si compiono, tecnologiche o “manuali” devono tener conto di questo principio basilare
- Segregazione e separazione dei ruoli per la consuntivazione (kimai , mail o altro)
- Riservatezza delle informazioni per il provisioning elettronico e la documentazione cartacea (CV, lettere al personale ecc.)
- I siti aziendali Xenialab, tramite i cookies raccolgono dati ed informazioni per i quali **occorre chiedere l'autorizzazione al trattamento**; il GDPR impone di informare gli utenti quali tipologie di cookie il sito utilizza.
- 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

Amministratz.

- Tutte le gestioni di raccolta CV o altre informazioni personali vanno autorizzate con apposito modulo, anche per i dipendenti e collaboratori attuali
- 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
- I documenti elettronici e cartacei utili alla compliance di Xenialab per il GDPR saranno conservati in luoghi sicuri e aggiornati periodicamente o a fronte di eventi significativi
- **Qualsiasi azione proattiva che contribuisca a migliorare la protezione dei dati in possesso di Xenialab**





Cosa dobbiamo fare noi, praticamente?

Amministrare.

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

Amministratz.

- 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
 - Raccoglitori di documenti non accessibili in assenza di personale amministrativo, per esempio chiuso a chiave in armadio o stanza
 - Raccolta di password o localizzazione chiavi armadi in busta chiusa per emergenze





Cosa dobbiamo fare noi, praticamente?

Azioni preventive e quotidiane

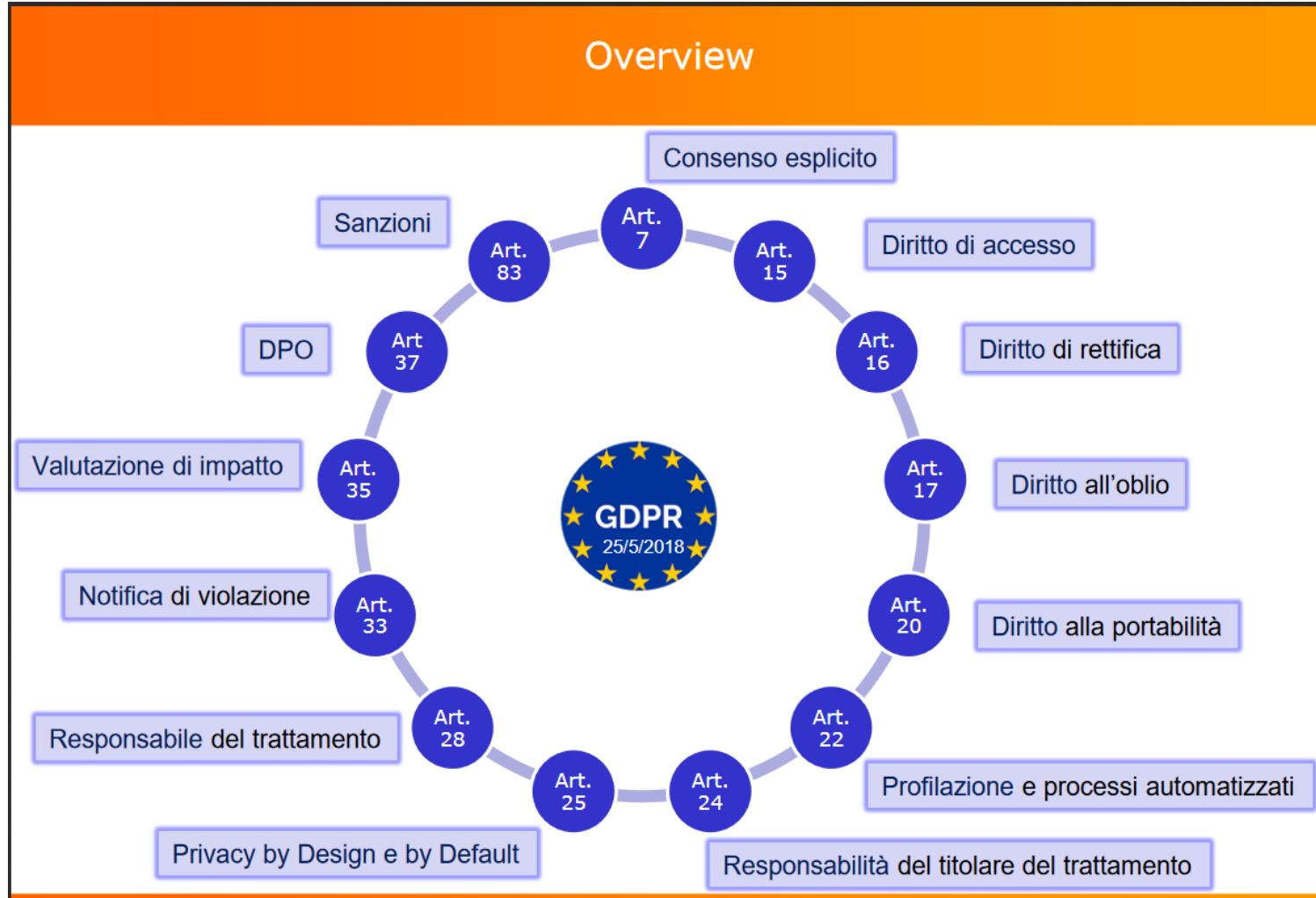
Amministratz.

- Seguire le procedure previste
- Aggiornamenti periodici da seguire
- Ulteriori informazioni:

http://www.xenialab.it/meo/web/white/oracle/db_lex.htm#gdp

<https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:32016R0679&from=IT>







Xenialab - GDPR

Corso di aggiornamento interno rivolto al
personale amministrativo
sul regolamento di sicurezza in vigore dal 25 Maggio 2018

