Olingo Consulting & Advokatfirman Vinge

CIO hotspot´16

EU:s Dataskyddsförordning

Olingo Consulting
Ammi Södergård, Konsult (kvalitet & Informationssäkerhet)
Ammi.sodergard@olingo.se
Tel: 070 990 77 47

Advokatfirman Vinge
Nicklas Thorgerzon, Advokat (IT, Teknik & Integritetsskydd)
nicklas.thorgerzon@vinge.se
Tel: 070 714 31 55

olingo

EU:s dataskyddsförordning

GDPR - General Data Protection Regulation

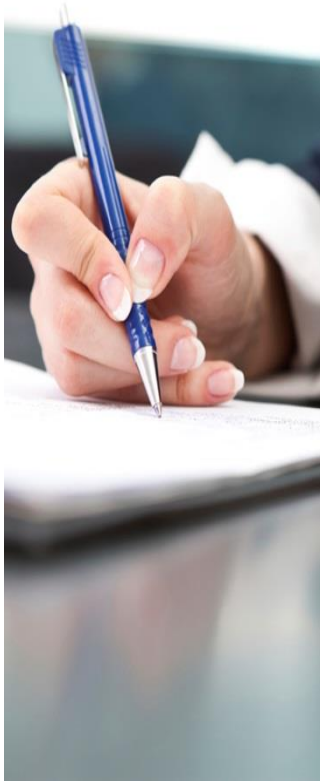
- Övergripande bild av EU:s dataskyddsförordning
- Inblick i hur det kommer påverka organisationen
- Förslag på vägen till anpassning

olingo

GDPR - NÄR / VARFÖR

- NÄR?
  - Förslag av EU-kommissionen 25 januari 2012
  - Formellt antagen under våren 2016
  - Direkt tillämplig våren 2018

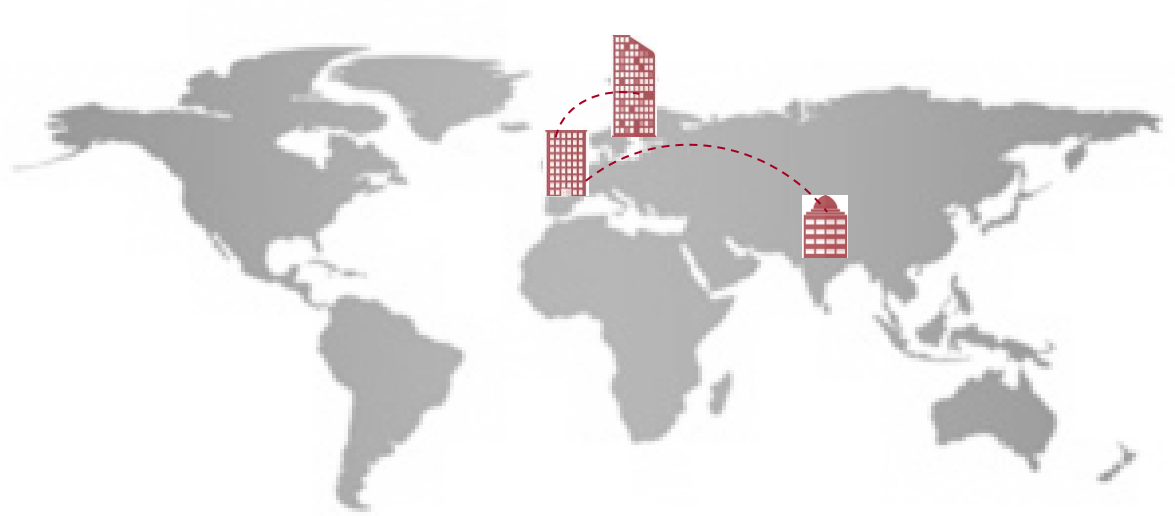
- VARFÖR?
  - Harmonisering
  - Anpassning till ny teknik
  - Stärka integritetsskyddet



olingo

GDPR – omfattar

- Personuppgiftsansvariga etablerade i EU
- Personuppgiftsbiträden etablerade i EU
- Personuppgiftsansvariga utanför EU som behandlar uppgifter om EU medborgare



5 steg till anpassning

1. Information och medvetande
2. Bedöma påverkan på den egna organisationen
3. Nulägesanalys
4. Verifiera framkomna bedömningar samt prioritera åtgärderna
5. Starta projektet – Anpassning till GDPR

olingo

Steg 1. Information och medvetande

- Vilka bör få information ?
  - CEO, CFO, CIO, Företagsjurist, Informationssäkerhetsansvarig, HR-chef, Dataskyddsombud, operativa chefer
  - Ansvariga för verksamhet med personuppgifter, Personer med bred kompetens om företaget
- Hur blir rätt personer medvetna?
  - Övergripande information som följs av workshops där man blandar specialister och ansvariga för att öka medvetenheten och ta fram konkreta exempel.
- Hur går man vidare?
  - Skapa en organisation samt fastställa en budget
  - Utser en ansvarig (projektledare/programledare för den fortsatta planeringen och anpassningen)

olingo

Steg 2. Första bedömning om påverkan

- Workshops
  - Diskutera risker vid företagets hantering av personuppgifter
    - Skickas lösenord via mail?
    - Skickas/hämtas material via sftp-server och hur verifieras att allt kommit fram?
    - Ligger persondata framme vid på bord/vid skrivare
    - Har vi rätt intervall på backuperna?
    - Behörigheterna för läs och skriv rättigheter?
    - Hanteras information om nära anhöriga?
    - Har vi helt klart hur vi tar bort personligt data när lagringstiden går ut?
  - Ex. kund-profilering
    - Vilken data samlas in?
    - Vilken data behövs?
    - Vilka verktyg används?
    - Var sparas data och vilka har åtkomst?
    - Hur används data och hur påverkas kunderna?

olingo

Steg 3. Nulägesanalys

- Dokumentera
  - Identifiera vilken information som hanteras, för vilket syfte, vilka risker som finns samt vilka konsekvenser riskerna kan innebära
- Konsekvensanalys – Privacy Impact Assessment, PIA
  - Krav för bolag som har för avsikt att hantera personuppgifter som kan medföra stora integritetsrisker
- Regelefterlevnad idag
  - Uppfylls kraven i PUL?
- Avtal
  - Se över reglering i leverantörsavtal
- Policy och guidelines
  - Hur informeras berörda personer?
  - Vilka interna riktlinjer finns?

olingo

Steg 4. Verifiera och prioritera

- Verifiera
  - Granska informationsflöde
  - GAP-analys i förhållande till GDPR
  - Sammanställ allt material
- Prioritera
  - Skapa åtgärdsplan
  - Skapa underlag för beslut
  - Vad bör man tänka på – vilket går först
- Exempel
  - Ändra rutiner för att inhämta samtycke från kunder
  - Bygga in integritet vid utveckling av nya IT-system
  - Utveckla nya interna rutiner och processer för registerutdrag och radering

olingo

Steg 5. Projekt - Implementation

- Underlag från tidigare steg
  - Resultat från konsekvensanalys
  - Resultat från GAP-analys
  - Resultat från prioritering och åtgärdsplan

- Ex – Ny anmälningsprocess vid säkerhetsincident
  - Vad händer om det dagen innan julafton kl 15:30 inträffar en läcka av personuppgifter?
  - Informera
    - Tillsynsmyndigheten inom 72 timmar
    - Den Registeransvarige om du är registerförare
    - Den enskilde – tex kontonummer och lösenord – utan onödigt dröjsmål vid
- Ex. förhandla nya avtal med leverantörer
  - Skyldigheter för leverantören
  - Ansvar om GDPR inte uppfylls
- Ex. implementera nya policys
  - Ändra villkor/policy på hemsida
  - Uppdatera ledningsinformation

olingo

Vad blir det för påföljder om man inte gör något?

- Datainspektionen kräver rättelse
- Administrativa sanktionsavgifter
  - Upp till 20 MEUR eller 4% av global omsättning
    - Tex. Inte återkopplar till enskilds krav om rättelse, radering eller registerutdrag
  - Myndigheter?
- Skadestånd
- Böter och fängelse