

# Ný Evrópureglugerð um persónuvernd: *Breytingar á skyldum og ábyrgð fyrirtækja*

Málstofa SFF um persónuvernd  
7. júní 2016

Alma Tryggvadóttir  
skrifstofustjóri upplýsingaöryggis  
Persónuvernd

Rauðárstíg 10  
105 Reykjavík | Ísland  
Sími 510 9600 | Fax 510 9606  
postur@personuvernd.is  
www.personuvernd.is

# Yfirlit

- Umfangsmiklar endurbætur á gildandi persónuverndarlöggjöf
- Víðtækt gildissvið
- Aukinn réttur einstaklinga
- Breyttar kröfur til fyrirtækja og stofnana
- Breytt eftirlitshlutverk persónuverndarstofnana
- Aðferðir til að sína fram á reglufylgni
- Næstu skref?

# Umfangsmiklar endurbætur

- Aðdragandi og undirbúningur
- Endurbæturnar settar fram með:
  - Reglugerð um vernd einstaklinga í tengslum við vinnslu persónuupplýsinga og frjálst flæði slíkra upplýsinga („Reglugerð um persónuvernd“)
  - Tilskipun um vernd einstaklinga í tengslum við vinnslu persónuupplýsinga hjá löggæsluaðilum („Löggæslutilskipunin“)
- Markmið
- Taka formlega gildi **25. maí 2018**

# Víðtækt gildissvið

- Hugtakið „persónuupplýsingar“
- Landfræðilegt gildissvið
  - Allir sem vinna upplýsingar innan EES-svæðisins óháð landfræðilegri staðsetningu
- Nær til ábyrgðar- og vinnsluaðila
  - Tilnefna fulltrúa ef utan ESB/EES
  - Sjálfstæð skylda á vinnsluaðilum m.a.:
    - Tryggja öryggi persónuupplýsinga
    - Ítarlegri ákvæði um vinnslusamning
    - Tryggja að undirvinnsluaðilar fari einnig að lögnum
    - Halda skrá yfir vinnslu

# Aukinn réttur einstaklinga

- Breyttar kröfur til samþykkis
- Fela einstaklingum betri stjórn á upplýsingum sínum
  - Aukið gagnsæi vinnslu
  - Einfaldari aðgang að upplýsingum
  - Réttur til flutnings milli þjónustuveitenda (e. Data portability)
  - Vitneskja um öryggisbrot
- Rétturinn til að gleymast
- Gerð persónusniða

# Breyttar kröfur til fyrirtækja og stofnana

- Skrá yfir vinnsluaðgerðir
- Breytt tilkynningarskylda vegna öryggisbrests
  - Tilkynna til persónuverndarstofnunar innan 72 klst.
  - Tilkynna til hinna skráðu án tafar
- Mat á áhrifum vinnslu (PIA)
  - Fyrirframveitt ráðgjöf
- Tilnefning persónuverndarfulltrúa (DPO)
- Innbyggð og sjálfgefin friðhelgi (Privacy by design / Privacy by default)

# Breytt eftirlitshlutverk persónuverndarstofnana

- Einn afgreiðslustaður (e. One stop shop)
- „Samræmingar-kerfi“ (e. Consistency mechanism)
  - Evrópska persónuverndarráðið (EDPB)
- Úrræði, skaðabætur og viðurlög
- Nýjar og stórauknar sektarheimildir
  - Allt að 4% af árlegri heildarveltu eða 20 milljón evrum

# Aðferðir til að sína fram á reglufylgni

- Aðferðir til að sína fram á reglufylgni
  - Vottun (e. Certification)
  - Sjálfstæðir vottunaraðilar
  - Starfsreglur (e. Codes of Conduct)
- Næstu skref?



# Hverju þarf að huga að?

1. Fellur starfsemi undir gildissvið reglugerðarinnar
2. Vitundarvakning
  - Meðal stjórnenda og starfsmanna
3. Persónuupplýsingar
  - Hverjar, hver, hvers vegna o.fl.
4. Persónuverndarstefna og fræðsla
  - Setja/uppfæra
5. Réttindi einstaklinga
  - Yfirfara verkferla/starfsvenjur
6. Lögmæti vinnslu
  - Afmarka/skrásetja
7. Samþykki
  - Samþykkiseyðublöð og fræðsla
8. Öryggisbrestir
  - Útbúa verkferla
9. Innbyggð og sjálfgefin friðhelgi
10. Persónuverndarfulltrúi
  - Skipa og/eða þjálf
11. Alþjóðleg starfsemi
  - Útnefna tengilið innan EES/ESB

## Að lokum

- Persónuvernd meðal grundvallar mannréttinda
- Hugarfarsbreytingar er þörf!
- Ytri regluvarsla eða breytt framkvæmd innan frá?
- Tækifæri felast í öflugri og virkri vernd persónuupplýsinga:
  - Samkeppnislegt forskot
  - Auðveldari innganga á nýja markaði
  - Tækifæri til að nýta sér greiningu gagna till fulls

# Spurningar?

postur@personuvernd.is // alma@personuvernd.is  
www.personuvernd.is

 @Personuvernd