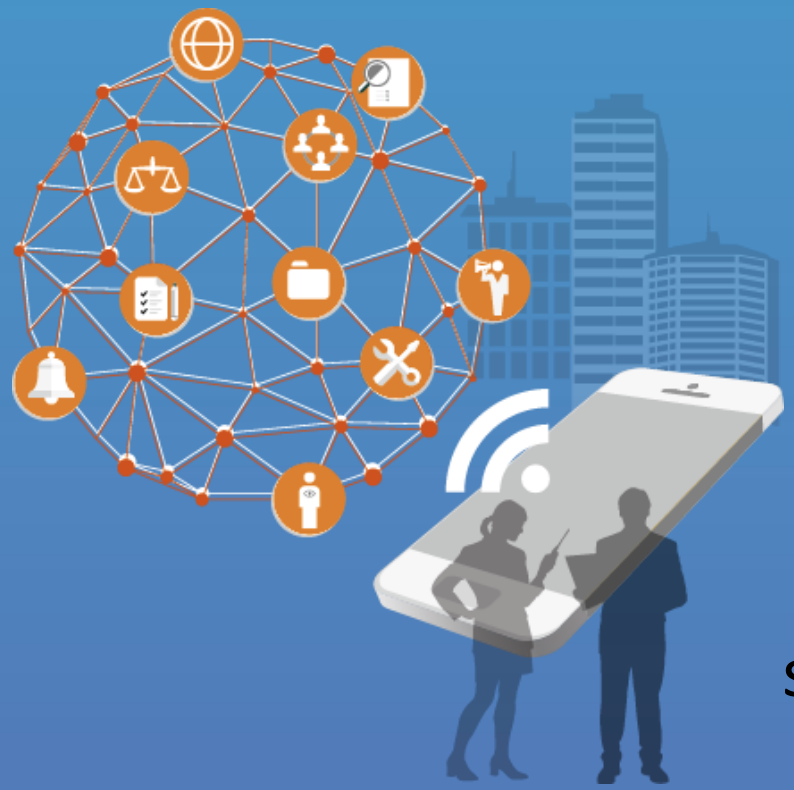
Skyldur fyrirtækja og stofnana

Landsfundaröð Persónuverndar

Akureyri, 31. október 2018



Vigdís Eva Líndal
skrifstofustjóri upplýsingaöryggis

PERSÓNU VERND

Ný persónuverndarlöggjöf 2018

Reglugerð 2016/679 (ESB) um vernd persónuupplýsinga kom til framkvæmda 25. maí 2018 í Evrópu

- 99 lagagreinar, 173 formálsorð, 81 bls.
- **Helstu markmið**
  - Auka réttindi einstaklinga
  - Þróun á hinum innri stafræna markaði

Lög nr. 90/2018 um persónuvernd og vinnslu persónuupplýsinga tóku gildi 15. júlí 2018

PERSÓNU VERND

Hvað breytist ekki?

Þarf áfram að fylgja ákveðnum kröfum:

- Hvaða heimild stendur til vinnslunnar?
- Er vinnslan lögmæt, gagnsæ, hófleg, áreiðanleg?
- Hver er tilgangur vinnslunnar?
- Veit einstaklingurinn af vinnslunni?
- Er búið að tryggja öryggi upplýsinganna?
- Hvar eru upplýsingarnar vistaðar og hvar má vista þær? Innan eða utan EES?

PERSÓNU VERND

Skilgreiningar

Persónuupplýsingar

- Allar upplýsingar sem hægt er að tengja beint eða óbeint við einstakling, t.d. kennitala, IP-tala, lífkenni, ljósmynd o.fl.
- Viðkvæmar persónuupplýsingar sérstaklega skilgreindar
  - Heilsufar, stjórnmálaskoðanir, kynhneigð, lífsskoðanir o.fl.

Vinnsla

- Skráning, leit, miðlun, varðveisla, eyðing o.fl.

Ábyrgðaraðili

- Fyrirtæki, stofnanir, skólar, heilbrigðisstofnanir o.fl.

Vinnsluaðili

- Til dæmis hýsingaraðilar, tæknifyrirtæki, auglýsingastofur, verktakar/ráðgjafar o.fl.

Gildissvið

- Öll vinnsla persónuupplýsinga, sjálfvirk að hluta eða í heild og handvirk (ef hluti af skrá)
  - Ekki vinnsla einstaklinga um einkahagi sína
  - Látnir einstaklingar: fimm ár frá andláti

- Allir aðilar sem hafa staðfestu innan EES eða ef vinnslustarfsemi lýtur að:
  - Boði um vörur eða þjónustu
  - Eftirliti með hegðun einstaklinga innan EES
- Allur heimurinn undir!

PERSÓNU VERND

Lögmæti vinnslu

- Óheimilt er að vinna persónuupplýsingar nema hafa til þess sérstaka heimild
- Heimildir til vinnslu persónuupplýsinga:
  - *Almennar* persónuupplýsingar, sbr. 9. gr. pvl., sbr. 6. gr. pvrg.
  - *Viðkvæmar* persónuupplýsingar, sbr. 9. og 11. gr. pvl., sbr. 6. og 9. gr. pvrg.
  - Vinnsla upplýsinga um *refsiverða háttsemi*, sbr. 12. gr. pvl., sbr. 10. gr. pvrg.

PERSÓNU VERND

Hvenær má vinna með persónuupplýsingar?

- **Samþykki**
- Til að **efna samning** sem hinn skráði er aðili að
- **Lagaskylda** sem hvílir á ábyrgðaraðila
- Til að **vernda brýna hagsmuni hins skráða eða annars einstaklings**
- Verk sem unnið er í þágu **almannahagsmuna** eða við **beitingu opinbers valds**
- **Lögmætir hagsmunir** sem ábyrgðaraðili eða einhver annar gætir, **nema hagsmunir eða grundvallarréttindi og frelsi hins skráða**, sem krefjast verndar persónuupplýsinga, **vegi þyngra**, einkum ef hinn skráði er barn.
  - Stjórnvöld geta almennt ekki byggt á þessari heimild

Hvenær má vinna með viðkvæmar persónupplýsingar

- **Afdráttarlaust samþykki**
- Til þess að ábyrgðaraðili/hinn skráði geti staðið við **skuldbindingar** sínar og **nýtt sér tiltekin réttindi samkvæmt vinnulöggjöf** eða **löggjöf um almannatryggingar** eða **félagslega vernd**.
- Verulegir hagsmunir einstaklings eða annars einstaklings sem er ófær um að gefa samþykki.
- Vinnsla hjá góðgerðastofnunum og sambærilegum aðilum.
- Ef einstaklingur hefur sjálfur augljóslega **gert upplýsingar opinberar**.
- Til að stofna, hafa uppi eða verja réttarkröfu eða **þegar dómstólar fara með dómsvald sitt**
- Verulegir **almannahagsmunir,** á grundvelli laga
- Til að fyrirbyggja sjúkdóma eða vegna **atvinnusjúkdómalækninga**
- Almannahagsmunir á sviði **lýðheilsu**
- **Skjalavistun** í þágu almannahagsmuna, **rannsóknir** á sviði vísinda eða sagnfræði eða í **tölfræðilegum** tilgangi

Sakfellingar í refsimálum og refsiverð brot

Strangari skilyrði en gilda um almennar persónuupplýsingar

Stjórnvöld

- Vinnsla nauðsynleg vegna lögbundinna verkefna

Einkaaðilar

- Samþykki eða lögmætir hagsmunir

PERSÓNU VERND

Hvernig á að vinna með persónuupplýsingar?

1. Lögmætisreglan
   - Unnar með lögmætum, sanngjörnum og gagnsæjum hætti
2. Tilgangsreglan
   - Unnar í skýrum og lögmætum tilgangi, ekki unnar í öðrum og ósamrýmanlegum tilgangi
3. Meðalhófsreglan
   - Nægilegar, viðeigandi og takmarkast við það sem er nauðsynlegt
4. Áreiðanleikareglan
   - Upplýsingar séu áreiðanlegar og uppfærðar eftir þörfum
5. Varðveislureglan
   - Varðveittar á því formi að ekki sé unnt að persónugreina einstakling lengur en þörf er á

Hvernig á að vinna með persónuupplýsingar? Frh.

6. Öryggisreglan
   - Viðeigandi öryggi og trúnaður persónuupplýsinga sé tryggður

7. Ábyrgðarskyldan
   - Ábyrgðaraðili ber ábyrgð á því að farið sé að reglunum og þarf að geta **sýnt fram á** það

PERSÓNU VERND

Ábyrgðarskylda

Ábyrgðaraðili er ábyrgur fyrir því að farið sé að meginreglum og **þarf að geta sýnt fram á það**

Ábyrgðaraðili þarf að gera viðeigandi **tæknilegar og skipulagslegar ráðstafanir** til að sýna fram á reglufylgni

- Skjalfesta verklagsreglur – skrá yfir öryggisbresti
- Vinnsluskrá
- Áhættumat – öryggisráðstafanir
- Mat á áhrifum á persónuvernd
- Skráning niðurstöðu hagsmunamats

Fræðsluskylda - persónuverndarstefna

Persónuverndarstefna Persónuverndar

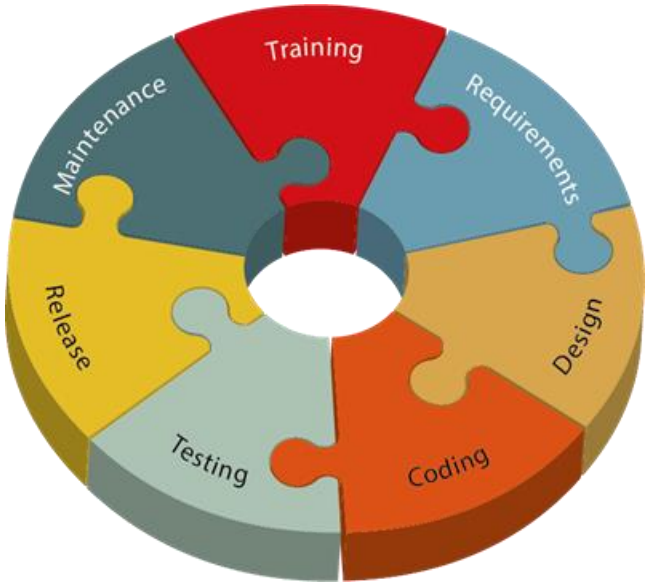
1. Persónuvernd er ábyrgðaraðili að vinnslu persónuupplýsinga
2. Persónuverndarfulltrúi Persónuverndar
3. Hvenær vinnur Persónuvernd með persónuupplýsingar?
4. Þín réttindi samkvæmt persónuverndarlöggjöfinni
5. Hvað er skráð um þig þegar þú notar vefsíðu Persónuverndar?
6. Hvað er skráð þegar þú hefur samband við Persónuvernd?
7. Vinnsla persónuupplýsinga þegar þú hefur samband við Persónuvernd
8. Starfsmenn ábyrgðaraðila eða vinnsluaðila
9. Upplýsingar um starfsmenn og umsækjendur um störf
10. Upplýsingaöryggi og vinnsluaðilar hjá Persónuvernd

PERSÓNU VERND

Innbyggð og sjálfgefin persónuvernd

Ráðstafanir sem hannaðar eru til að fylgja meginreglum séu innbyggðar í hugbúnað, upplýsingakerfi og vinnslu **frá upphafi**

- Sjálfvirk eyðing, gerviauðkenni, uppfærslur, o.s.frv.



Að **sjálfgefið** sé að eingöngu nauðsynlegar upplýsingar séu unnar

Matskennt

- Nýjasta tækni, eðli, umfang, samhengi og tilgangur

PERSÓNU VERND

Útvistun til vinnsluaðila

Eingöngu heimilt ef:

- *Nægilegar tryggingar* fyrir öryggi og réttindum einstaklinga
- *Vinnslusamningur* hefur verið gerður í samræmi við 25. gr. pvl., sbr. 28. gr. pvrg.

Sjálfstæðar skyldur á vinnsluaðila

- Tryggja **öryggi** upplýsinga
- Halda **skrá yfir vinnslustarfsemi**
- Tilkynna ábyrgðaraðila um **öryggisbrest**
- Útnefna **persónuverndarfulltrúa**
- Notkun **undirvinnsluaðila** (t.d. skýjaþjónustu) óheimil nema með samþykki ábyrgðaraðila
- **Sektir**

Skrá yfir vinnslustarfsemi

Ábyrgðaraðili og vinnsluaðili
- Ítarlegri skrá hjá ábyrgðaraðilum

Efni og form – 6H

Aðgengileg Persónuvernd

Undantekning <250 starfsmenn, nema:
- Líkleg til að leiða af sér áhættu, er ekki tilfallandi eða viðkvæmar persónuupplýsingar

Hvers vegna	• Tilgangur: • *Af hverju* eru persónuupplýsingar unnar?
Hverjir	• Flokkar einstaklinga: • *Um hverja* eru persónuupplýsingar unnar?
Hvaða	• Tegundir persónuupplýsinga: • *Hvaða* persónuupplýsingar eru unnar?
Hvenær	• *Hvenær* eru persónuupplýsingar unnar, *af hverjum* og *hversu* lengi?
Hvar	• *Hvar* eru persónuupplýsingar varðveittar?
Heilindi	• Ef mögulegt er – almenn lýsing á tæknilegum og skipulagslegum öryggisráðstöfunum

Öryggi - Tilkynningar um öryggisbrest

Ábyrgðaraðilar og vinnsluaðilar þurfa að gera viðeigandi **tæknilegar og skipulagslegar ráðstafanir** til að tryggja öryggi

- Dulkóðun, notkun gerviauðkenna, tryggja tiltækileika, álagsþol o.s.frv.
- Skipulagðir ferlar nauðsynlegir
- Innbyggð og sjálfgefin persónuvernd

Skylda til að tilkynna öryggisbrest

- Til Persónuverndar innan **72 klst.** nema ef *ólíklegt* er að áhætta sé til staðar
- Til hins skráða ef **mikil** áhætta
- Vinnsluaðilar þurfa að tilkynna til ábyrgðaraðila

Mat á áhrifum á persónuvernd

Þegar líklegt er að **tegund vinnslu geti verið sérstaklega áhættusöm** fyrir frelsi og réttindi einstaklinga

- Ný tækni tekin í notkun
- Eðli, umfang, samhengi og tilgangur vinnslunnar

Hvenær?

- Kerfisbundið og umfangsmikið mat á persónulegum þáttum eða eftirlit
- Umfangsmikil vinnsla viðkvæmra persónuupplýsinga

Hvenær þarf ekki?

- Lög mæla fyrir um vinnslu *og* mat á áhrifum farið fram við undirbúning
- Listi yfir þá vinnslu sem þarf ekki að fara í mat á áhrifum

Fyrirframsamráð við Persónuvernd ef vinnsla ennþá mjög áhættusöm

Persónuverndarfulltrúi

Öll **stjórnvöld** og **fyrirtæki** ef aðalstarfsemi er umfangsmikil, reglubundin og kerfisbundin vöktun eða umfangsmikil vinnsla viðkvæmra persónuupplýsinga

- Starfsmaður eða verktaki
- Tilkynna til PV og samskiptaupplýsingar aðgengilegar öllum

Sjálfstæður og óháður í störfum

- Heyrir undir æðsta stjórnanda
- Má sinna öðrum störfum, en mega ekki vera hagsmunaárekstrar

Reglufylgni, fræðsla, ráðgjöf, tengiliður við hina skráðu og Persónuvernd

Hæfisskilyrði

- Sérþekking á persónuverndarlöggjöf

PERSÓNU VERND

Breytt eftirlit

Einn afgreiðslustaður (One Stop Shop)

Einstaklingar
- Föst búseta
- Atvinna
- Brot á sér stað

Fyrirtæki = meginstarfsemi

Samræmingarkerfi (Consistency mechanism)

Forystustjórnvald

Sameiginleg niðurstaða í ágreiningsmálum

Evrópska persónuverndarráðið (EDPB)

Taka ákvörðun ef persónuverndarstofnanir eru ósammála

Samræma túlkun og beitingu pvrg.

Viðurlög

- Nýjar og þungar stjórnvaldssektir
  - ‼ Allt að 4% af árlegri heildarveltu eða 2,4 milljörðum kr.
  - ‼ Allt að 2% af árlegri heildarveltu eða 1,2 milljörðum kr.
- Önnur viðurlög, s.s. fyrirmæli um stöðvun vinnslu, t.d. við flutning úr landi, eyðingu upplýsinga o.s.frv.
- Réttarúrræði
  - Kvörtun til Persónuverndar
  - Málshöfðun, þ.m.t. hópmálshöfðun
  - Skaðabætur eftir almennum reglum

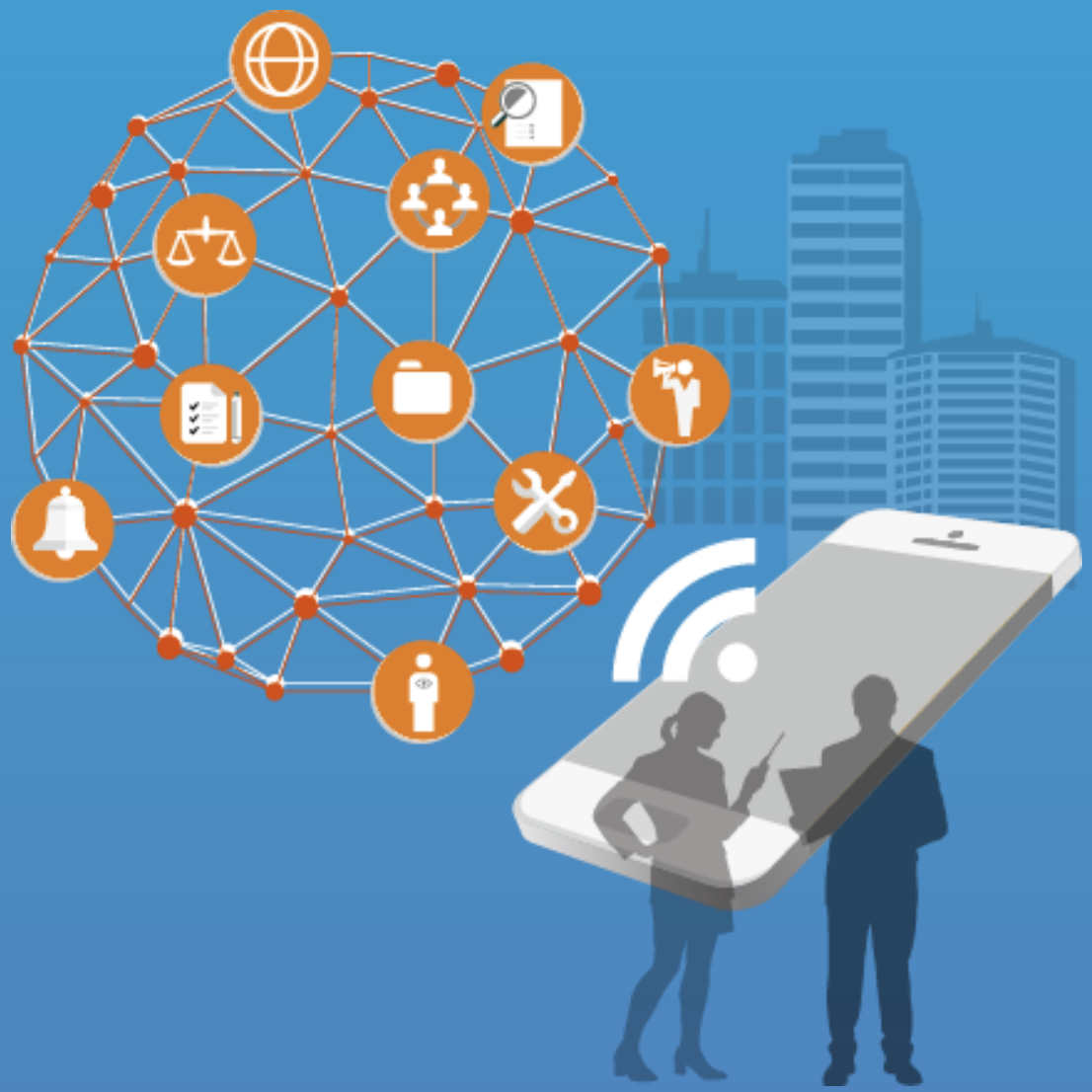
Hvar eigum við að byrja?

1. Kynnið ykkur reglurnar vandlega
2. Gerið vinnsluskrá
3. Verkferlar uppfylli kröfur laganna
4. Uppfyllið fræðsluskyldu – gerið persónuverndarstefnu
5. Hugið að öryggi upplýsinga
6. Fylgið reglum um eyðingu gagna
7. Tilkynnið öryggisbresti til Persónuverndar
8. Athugið hvar persónuupplýsingar eru geymdar
9. Innbyggð og sjálfgefin persónuvernd
10. **Nýtið tækifærin!**

PERSÓNU VERND

Landsfundaröð Persónuverndar er styrkt af Evrópusambandinu - The European Union's Rights, Equality and Citizenship Programme (2014-2020).

Efni kynningarfundarins er unnið af Persónuvernd sem ber fulla ábyrgð á því. Framkvæmdastjórn Evrópusambandsins ber enga ábyrgð á notkun þeirra upplýsinga sem veittar eru á fundinum.



postur@personuvernd.is
www.personuvernd.is
Leiðbeiningar Persónuverndar

@Personuvernd
#Persónuvernd #PV2018

STOFNUN ÁRSINS 2018

PERSÓNU VERND