



GDPR

engar holur?

Tannlæknafélagið

—

7. júní 2018



Dagskrá

- 1 | **Ný Evrópureglugerð um persónuvernd (GDPR)**
- 2 | **Áherslur**
- 3 | **Verkefnið og vinnugögn**
- 4 | **Umræður**

Ný persónuverndarlöggjöf – hvers vegna?



**Tímabil stafrænnar
væðingar**



**Samræming reglna
milli allra ríkja ESB og
EES**



**Réttur einstaklinga
styrktur**

Áherslur



Fræðsluskylda

Aukinn réttur einstaklinga til fræðslu um þá vinnslu persónuupplýsinga sem fer fram á stofunum, meðhöndlun þeirra og aðgengi í gögn.



Gagnameðhöndlun og öryggisráðstafanir

Aukin meðvitund um meðhöndlun gagna, hverjir hafa aðgang, hvaða gögnum er verið að að safna og í hvaða tilgangi.



Gagnavarðveisla

Hvar eru gögn varðveitt, hve lengi og hvernig.



Vinnsluskrá/vinnslusamningur

Ferlar innan eininga. Byggir á samantekt á m.a. framangreindum þáttum.



Persónuverndarfulltrúi

Nýtt hlutverk í lögum. Skal vinna að innleiðingu nýrrar löggjafar, veita fræðslu til starfsmanna og annarra. Leita úrlausn álitaefna og vera tengiliður við Persónuvernd. Matskennt.

Persónuupplýsingar / viðkvæmar persónuupplýsingar

Persónuupplýsingar

Sérhverjar persónugreindar eða persónugreinanlegar upplýsingar, þ.e. upplýsingar sem rekja má beint eða óbeint til tiltekins einstaklings. Upplýsingarnar verða að vera nógu nákvæmar til að hægt sé að sjá hvaða einstaklingi þær tilheyra. Hér getur t.d. verið um að ræða nöfn, kennitölur, heimilisföng, símanúmer, bílnúmer eða önnur einkenni tiltekins einstaklings. Einnig tölvupóstföng, notendanafn á netinu, IP tölur o.fl.

Viðkvæmar persónuupplýsingar

Upplýsingar um kynþátt, stjórnámálaskoðanir, trúarviðhorf, sakarferil, heilsufar, kynlíf og stéttarfélagsaðild. Felur þó ekki í sér fjárhagsupplýsingar eða t.d. einkunnir

Ábyrgðaraðili – Vinnsluaðili

Ábyrgðaraðili

Sá sem ákvarðar, einn eða í samstarfi við aðra, tilgang og aðferðir vinnslu.

Vinnsluaðili

Sá sem vinnur persónuupplýsingar fyrir, samkvæmt fyrirmælum og undir stjórn ábyrgðaraðila.



Fræðsluskylda

Veittar upplýsingar um vinnslu þurfa að vera:

- ☐ nákvæmar, gagnsæjar, á vel skiljanlegu máli og aðgengi að þeim gott.
- ☐ skrifaðar á réttu tungumáli og á þann hátt að þær séu auðskiljanlegar, sérstaklega ef börn eiga í hlut.
- ☐ án endurgjalds fyrir viðskiptavin.
- ☐ Persónuverndarstefna

Hvernig gæti þetta verið uppfyllt af hálfu tannlækna?

- Heimasíða
- Útprentað á stofunni

Gagnameðhöndlun og öryggisráðstafanir

- ☐ Hvaða gögnum er verið að safna?
- ☐ Í hvaða tilgangi?
- ☐ Hverjir hafa aðgengi í upplýsingarnar, hvert fara þær og hver notar þær?
- ☐ Er gagnasöfnun í lágmarki?
- ☐ Aðgangur starfsmanna í gögn sjúklinga
- ☐ Er til staðar aðgangsstýring á kerfi?
- ☐ Notkun upplýsinga, er hún skráð og rekjanleg?
- ☐ Miðlun upplýsinga til þriðja aðila
- ☐ Dulkóðun á tölvupósti ef senda þarf gögn til þriðja aðila – önnur aðferð við afhendingu gagna (minnislykill)
- ☐ Þegar ekki er greitt við afhendingu þjónustu
 - ☐ Frestun greiðslu
 - ☐ Stærri verk – sérstakur samningur

Öryggisráðstafanir

Breytingarstjórnun

Uppfærslur stýri- og netkerfa

- Úreld kerfi = áhætta

Einkvæm auðkenni

Aðgangsheimildir

- Byggt á starfshlutverki

- Stofnun, lokun og rýni

Lykilorðastýringar

- Sterk lykilorð

Vírusvarnir

Dulkóðun gagna

- Best til að takmarka óheimilan aðgang

Líftími gagna



Öryggisráðstafanir, frh

Ábyrgð

Afhending persónuupplýsinga

Hugbúnaðarnotkun

Aðgangur að upplýsingum

- Lykilorð

- Uppbygging heimilda

- Aðgerðaskráning

Tilkynning öryggis frávika

Rafræn samskipti og internetnotkun

- Varasamar vefsíður

- Póstar frá óþekktum aðilum

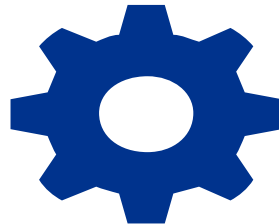


Dæmi um öruggari samskipti

Persónuupplýsingar



Örugg gátt



Íslykill

Kennitala:

Sláðu inn kennitölu

Íslykill:

Sláðu inn Íslykil

Rafræn skilríki

Skilríki í síma:

7 stafa símanúmer, síminn ólæstur

Innskrá

Skilríki á korti:

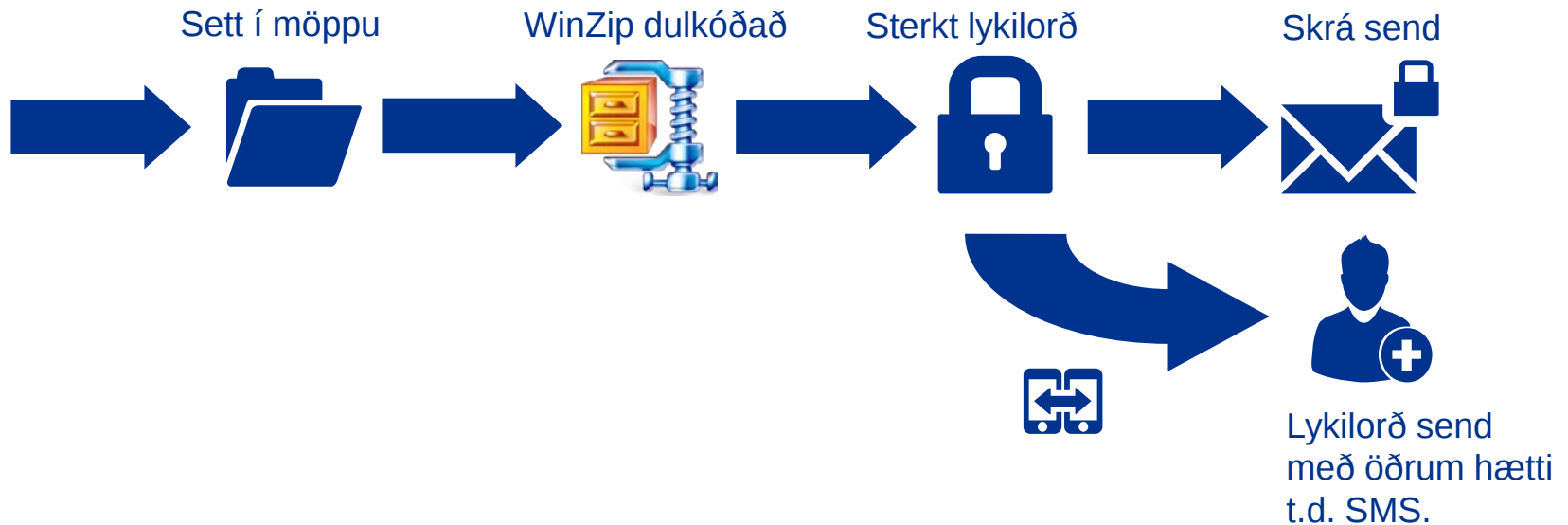
Staðfesta

Staðfesta

island.is

Dæmi um öruggari samskipti, frh

Persónuupplýsingar



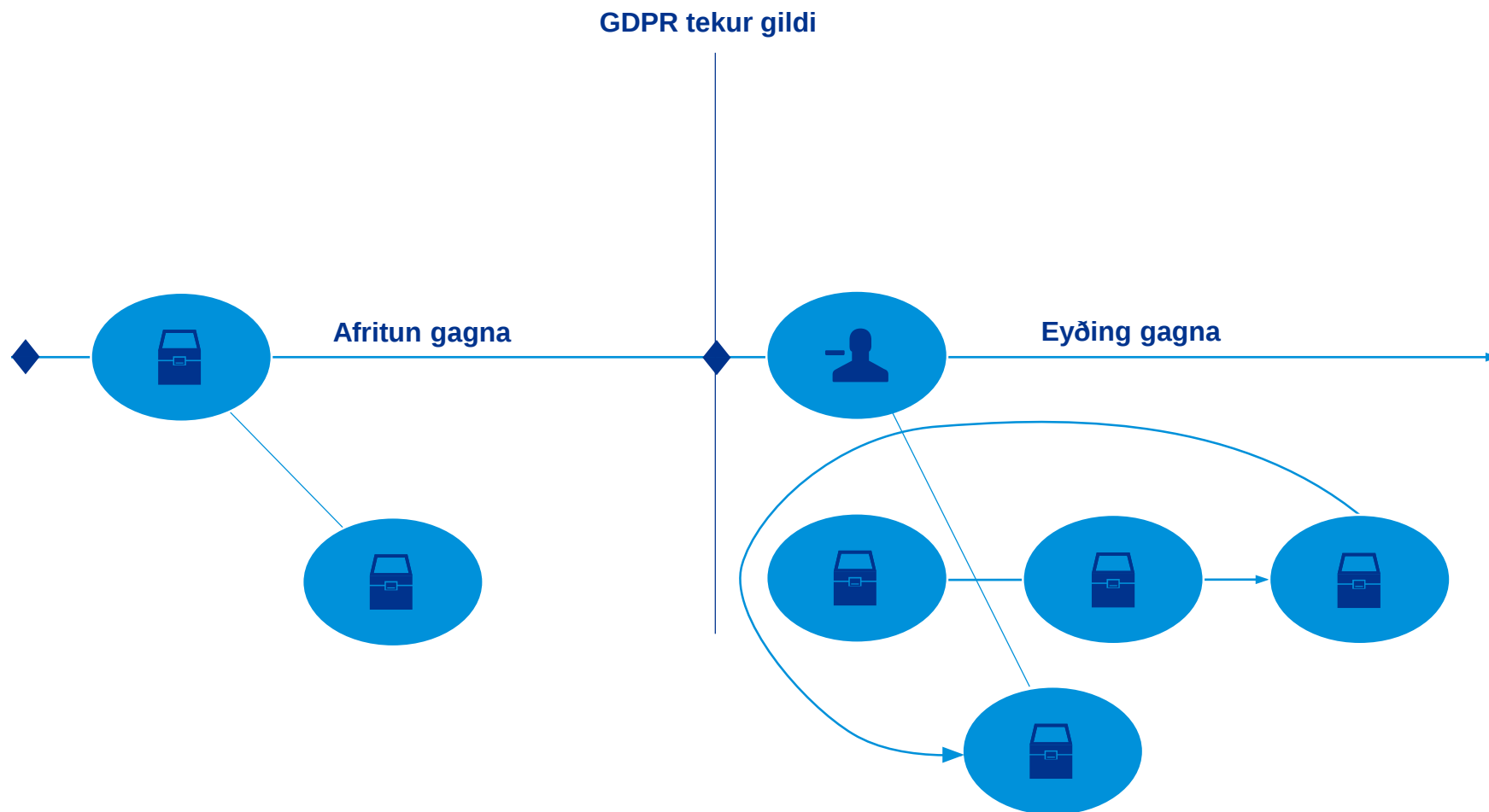
Gagnavarðveisla

- ☐ Hvar eru gögn varðveitt?
- ☐ Hvernig eru gögnin varðveitt?
- ☐ Hvað verður um pappírsgögn?
- ☐ Aðgangur í eldri gögn?
- ☐ Grisjun gagna?
- ☐ Afhending gagna ?

Lög um sjúkraskrár nr. 55/2009

Lög um opinber skjalasöfn nr. 77/2014

Afritun



Vinnsla / Vinnslusamningar

- ☐ Fara yfir alla ferla og verklag innandyr.
- ☐ Hefur vinnsluskrá verið aðlöguð að starfsemi stofunnar, byggt á verkferlum?
- ☐ Er til staðar ráðningarsamningur við alla starfsmenn þar sem tekið er á trúnaðarskyldu starfsmanns?
- ☐ Ef sameiginlegur rekstur nokkurra aðila; er til þjónustusamningur ?
- ☐ Er til staðar samningur við þjónustuaðila tölvukerfis?
- ☐ Aðrir þriðju aðilar?
- ☐ Ef sjúklingur óskar eftir eigin gögnum, til afhendingar til þriðja aðila. Hvernig var samþykkis aflað?

Vinnslusamningur

Tilgangur vinnslusamnings

Að tryggð sé samningssamband á milli ábyrgðaraðila og vinnsluaðila í ljósi ólíkra hlutverka. Þarf að vera til skriflegt og hægt að vísa í ef þarf.

Meginatriði:

- Tilgangur og eðli vinnslu
- Tímalengd vinnslu
- Tegund gagna
- Útlistun á skyldum aðila
- Heimild til að nota þriðja aðila, ef þarf.
- Meðhöndlun öryggisfrávika - tilkynningar
- Lok vinnslu

Persónuverndarfulltrúi / Tengiliður sjúklinga

- ☐ Hver mun svara spurningum og erindum vegna persónuverndar og sinna fræðsluskyldu þegar það á við.
- ☐ Tölvupóstfang fyrir fyrirspurnir og mál tengd persónuupplýsingum og meðferð þeirra.
- ☐ Er til áætlun um viðbrögð ef upp kemur frávik s.s. gagnaleki eða rangar upplýsingar berast til sjúklings?

Háttarnisreglur

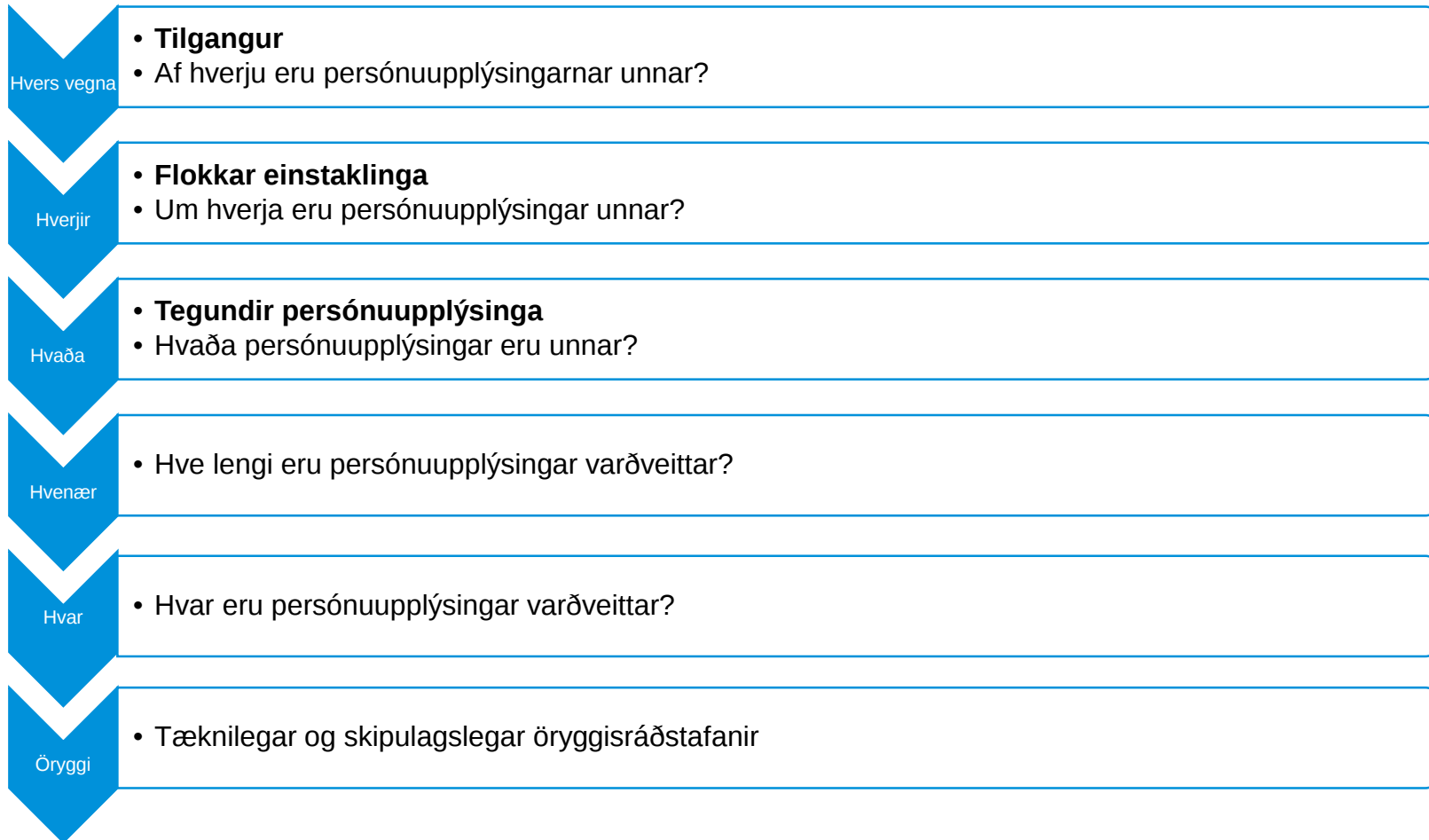
Háttarnisreglur, 40.- 41. gr. GDPR

Reglurnar hvetja til setningar siða- og háttarnisreglna af hálfu einstakra starfs- eða faggreina

Gert er ráð fyrir samráðsferli við samningu slíkra reglna

Afla verður staðfestingar persónuverndaryfirvalda á slíkum reglum

Samantekt





kpmg.com/socialmedia



kpmg.com/app

© 2018 KPMG ehf. á Íslandi er aðili að alþjóðlegu neti KPMG, samtökum sjálfstæðra fyrirtækja sem aðild eiga að KPMG International Cooperative, svissnesku samvinnufélagi. Allur réttur áskilinn.

Nafn og vörumerki KPMG eru skráð vörumerki KPMG International.