

Ný persónuverndarlög – maí 2018

..og hvað svo?

Guðmundur Stefán Björnsson

Persónuupplýsingar

Hvers kyns upplýsingar um persónugreindan eða persónugreinan-legan einstakling, ef unnt að persónugreina hann beint eða óbeint

Dæmi: Nöfn, kennitölur, heimilisföng, IP-tala.....

Samhengi gagnanna sem leiðir af sér persónugreiningu

sensæ



Helstu breytingar

- Aukin ábyrgð á ábyrgðaraðila
 - Til að mæta auknum réttindum einstaklinga (samþykki, gagnsæi, stjórn)
- Strangari reglur varðandi vinnsluaðila
- Tilkynningar um brot á persónuverndarlögum
 - Til Persónuverndar innan 72 klst. / líka til hinna skráðu?
- Aukin réttindi hinna skráðu, svo sem:
 - Réttur til gagnaflutnings („Right to Data Portability“)
 - Milli þjónustuveitanda – með greiðum hætti
 - Rétturinn til að gleymast („Right to be forgotten“)
 - Réttur hins skráða til að óska eftir eyðingu upplýsinga um sig ef engin lögmætir hagsmunir fyrir varðveislu



Helstu breytingar (2)

- Mat á áhrifum á vinnslu („*Privacy Impact Assessment*“)
 - Áður en „áhættusöm“ vinnsla persónuupplýsinga hefst
 - Áhættumat fyrir einstaklingana – ekki starfsemina sjálfa
- Tilnefning persónuverndarfulltrúa („*Data Protection Officer*“)
 - Ef kjarnastarfsemi þess byggir á reglulegri og kerfisbundinni vöktun einstaklinga með umfangsmiklum hætti
- Innbyggð friðhelgi („*Data Protection by design*“)
 - Öryggisreglur og meginreglur innbyggðar í hugbúnað/upplýsingakerfi frá upphafi
 - Taka mið af áhættumati
- Sjálfgefin friðhelgi („*Data Protection by default*“)
 - Að takmarkað magn persónuupplýsinga sé safnað, notað og varðveitt (einungis nauðsynlegar upplýsingar unnar)



Helstu breytingar (3)

- Skrá yfir vinnsluaðgerðir/Vinnsluskrá
- Tryggja öryggi persónuupplýsinga
 - Áhættumat
 - Öryggisráðstafanir
 - Innra eftirlit
- Fylgja takmörkunum um flutning úr landi
- Vinnslusamningur
- Þung þvingunarúrræði



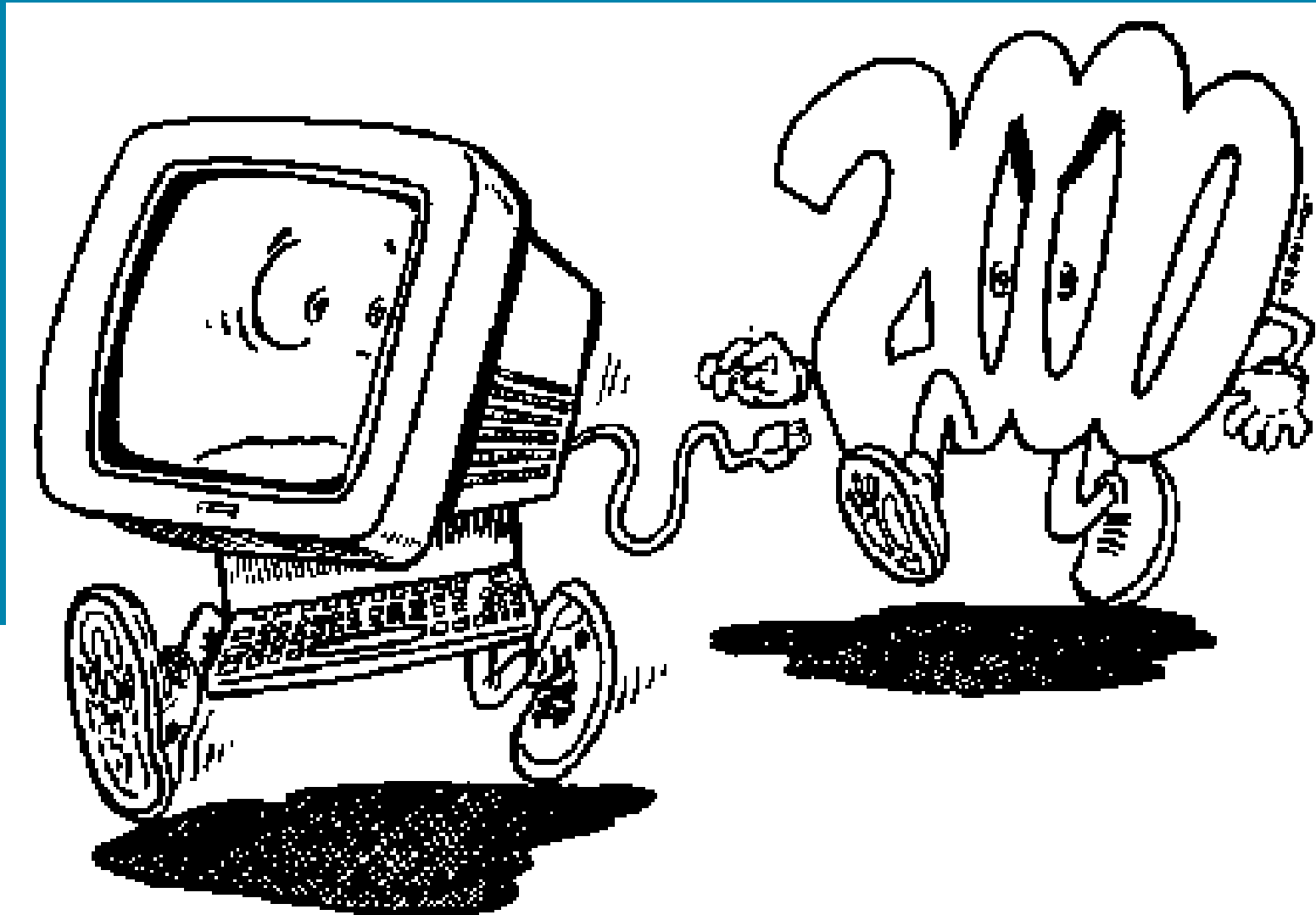
Sektarheimild

- Allt að 4% af ársveltu samsteypu
 - Hámark: 20 milljónir evra
- Nær líka til vinnsluaðila
- Persónuvernd gæti sektað ef t.d.:
 - ekki er uppfyllt fræðsluskylda,
 - meðhöndlaðar eru persónuupplýsingar án heimildar,
 - ekki er gætt að öryggi persónuupplýsinga með fullnægjandi hætti
 - ekki er tilkynnt um öryggisbrest til Persónuverndar eða hinna skráðu



GDPR minnir nokkuð á.....

- í gamni
- og alvöru



Ábyrgð og vinnsla?

ÁBYRGÐARAÐILI	VINNSLUAÐILI
• Ber ábyrgð á að vinnsla persónuupplýsinga (þ.m.t. geymsla) uppfylli skilyrði persónuverndarlaga • Ákveður tilgang vinnslu og ráðstöfun • Tryggir vernd, metur áhættu, gerir öryggisráðstafanir • <u>Leggur línur gagnvart vinnsluaðila með vinnslusamningi</u>	• Hlutverk ábyrgðaraðila að leggja línur með vinnslu sem hann felur vinnsluaðila • <u>Vinnsluaðili vinnur eftir fyrirmælum ábyrgðaraðila</u> • Ber þó ábyrgð á að tryggja öryggi umhverfis sem v.v. (ábyrgðaraðili) geymir og vinnur sín gögn

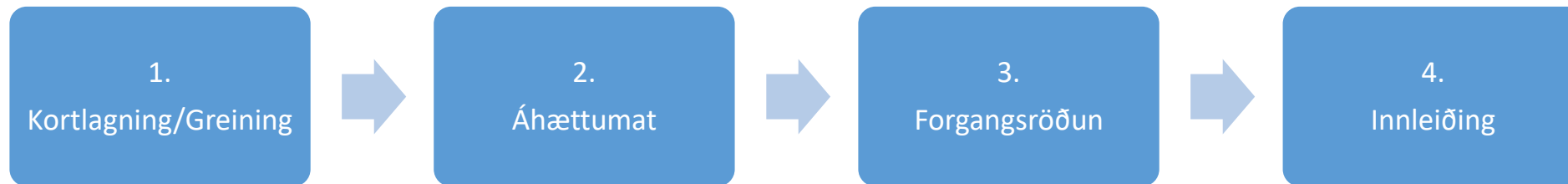
Ábyrgð er ekki hægt að úthýsa

Vinnsluaðili - hýsingarfyrirtæki

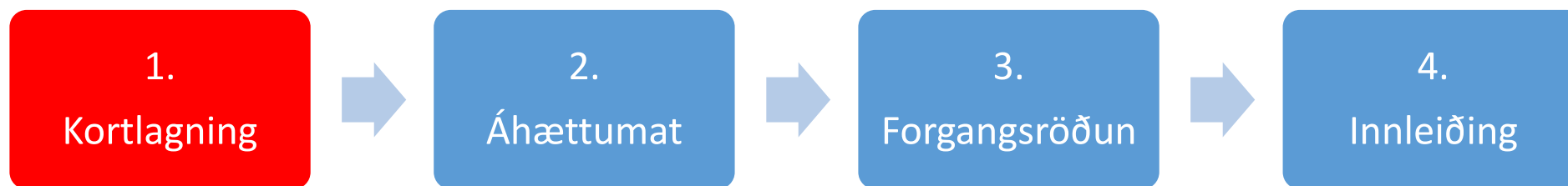
Þjónusta	Ábyrgð
Hýsing (Colocation)	<u>Ekki</u> vinnsluaðili - Búnaður í eigu ábyrgðaraðila og öll vinnsla hjá viðkomandi
Innviðaþjónusta (IAAS)	Vinnsluaðili - Net, vélar, diskastæður, afritunarkerfi innihalda gögn á ábyrgð eiganda
Grunnkerfisþjónusta (PAAS)	Vinnsluaðili - Grunnkerfi frá þriðja aðila, v.v geymir og vinnur gögn á hugbúnaði sem liggur á grunnkerfi
Hugbúnaðþjónusta (SAAS)	Vinnsluaðili - Hugbúnaður frá þriðja aðila, v.v geymir og vinnur gögn á hugbúnaði sem liggur á grunnkerfi
Hýsing og rekstur (Managed Services)	Vinnsluaðili - Umhverfi sem rekið er af Sensa. Sensa heldur utan um AD og tengir saman umhverfi

Ábyrgðaraðili
– Gögn og loggar úr kerfum

Undirbúningur

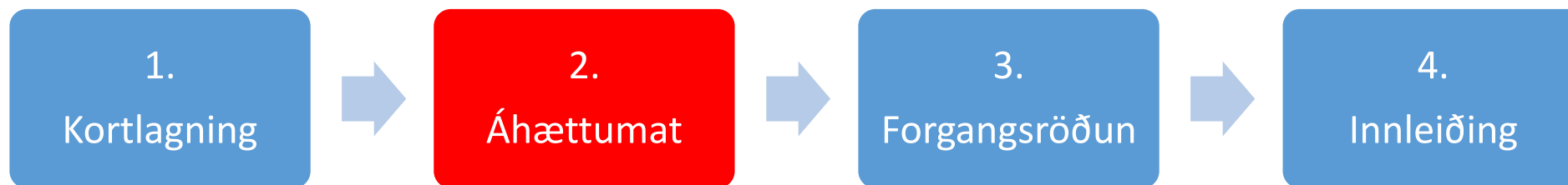


Undirbúningur - kortlagning



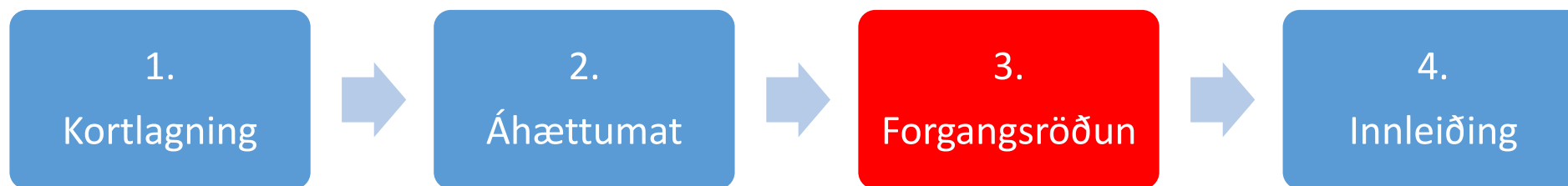
- Hvaða persónuupplýsingar er verið að vinna með?
- Hvaðan koma upplýsingarnar? (Er vinnslusamningur?)
- Hvernig er öryggi upplýsinganna tryggt?
- Tæknilegar ráðstafanir (t.d. aðgangsstýringar, tengingar við önnur kerfi?)
- Skipulagslegar ráðstafanir (t.d. ytra öryggi húsnæðis og aðgangur að búnaði)
- Er verið að flytja gögn/upplýsingar úr landi?
- Hvenær á að eyða upplýsingunum?

Undirbúningur - áhættumat



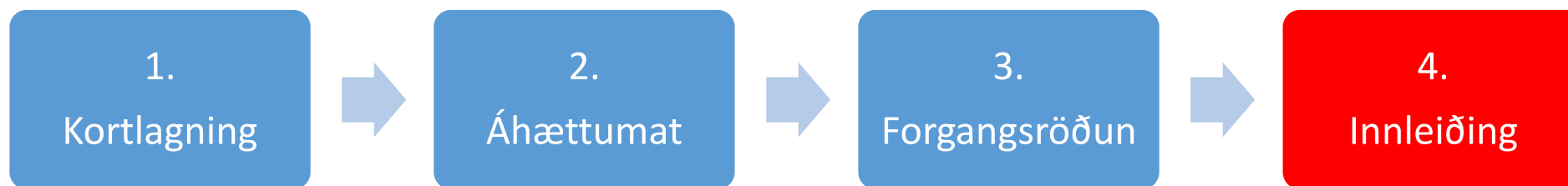
- Hvar er mesta áhættan á broti gegn friðhelgi einkalífs einstaklinga?
- Áhættumeta þá ferla sem fyrir eru og hvort það þurfi að skerpa á þáttum

Undirbúningur - forgangsröðun



- Með hliðsjón af niðurstöðum áhættumats
- Breytingar á upplýsingakerfum til að uppfylla skilyrði reglugerðarinnar
 - Ef hinn skráði vill flytja upplýsingar til annars aðila
 - Ef hinn skráði óskar eftir eyðingu upplýsinga um sig
 - Vinnsluaðili þarf að aðstoða ábyrgðaraðila við að uppfylla þessar skyldur!

Undirbúningur - innleiðing



- Fylgja forgangsröðun
 - Klára strax sem er auðvelt að innleiða
- Eftirlit með framfylgni
 - Endurtaka áhættumat eða uppfæra vinnsluskrá eftir því sem framvindur
- **Vitundarvakning, þjálfun, þjálfun, þjálfun.....!**

Nálgun Sensa

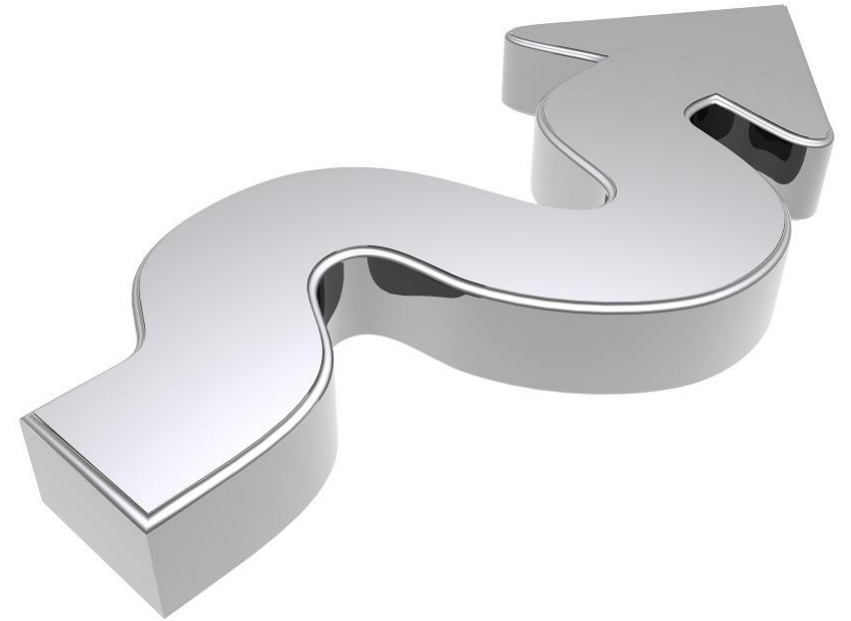
- undir umsjón lögfræðisviðs Símans

sensa

15 ára

Hvernig nálgast Sensa GDPR?

- Lá ekki ljóst fyrir í upphafi hvernig ætti að nálgast
- Nálgast út frá verðmætum
 - Hvernig vinnsla (hýsing, öryggi, umsýsla, flutningur)
 - Ábyrgð (ábyrgðaraðili, vinnsluaðili)
 - Er um að ræða flutning utan Evrópu
 - Er um að ræða persónugreinanleg gögn
 - ...og þá hvernig gögn (nafn, símaumferð, IP tölur....)



Hvernig nálgast Sensa GDPR? (2)

Þar sem um er að ræða persónugreinanleg gögn

- Kortlagning upplýsinga um starfsmenn, verktaka og viðskiptavini
 1. Tegund, hvern varðar, uppruni
 2. Varðveislutími- og aðferð
 3. Tilgangur og heimild
 4. Viðkvæmar?
 5. Ábyrgðaraðili, vinnsluaðili
 6. Aðgangur
 7. Fræðsla
- Áhættumat – yfirfara sérstaklega m.t.t. GDPR



Vinnslusamningar við viðskiptavini

- Sett saman form fyrir vinnslusamning
- Gera vinnslusamninga
 - Tímalína yfir framkvæmd



Leitum eftir aðstoð

- Þarf að taka alvarlega
- Oft gerum við okkur ekki grein fyrir því að það sem við erum að gera varðar persónuvernd
 - Söfnun gagna
 - Samfélagsmiðlar
 - Slúður



Áskorunin / viðskiptavinir

..ekki tæknilegs eðlis
– just do it



..heldur umgengni og
umsýsla með gögnin
- þjálfun starfsmanna

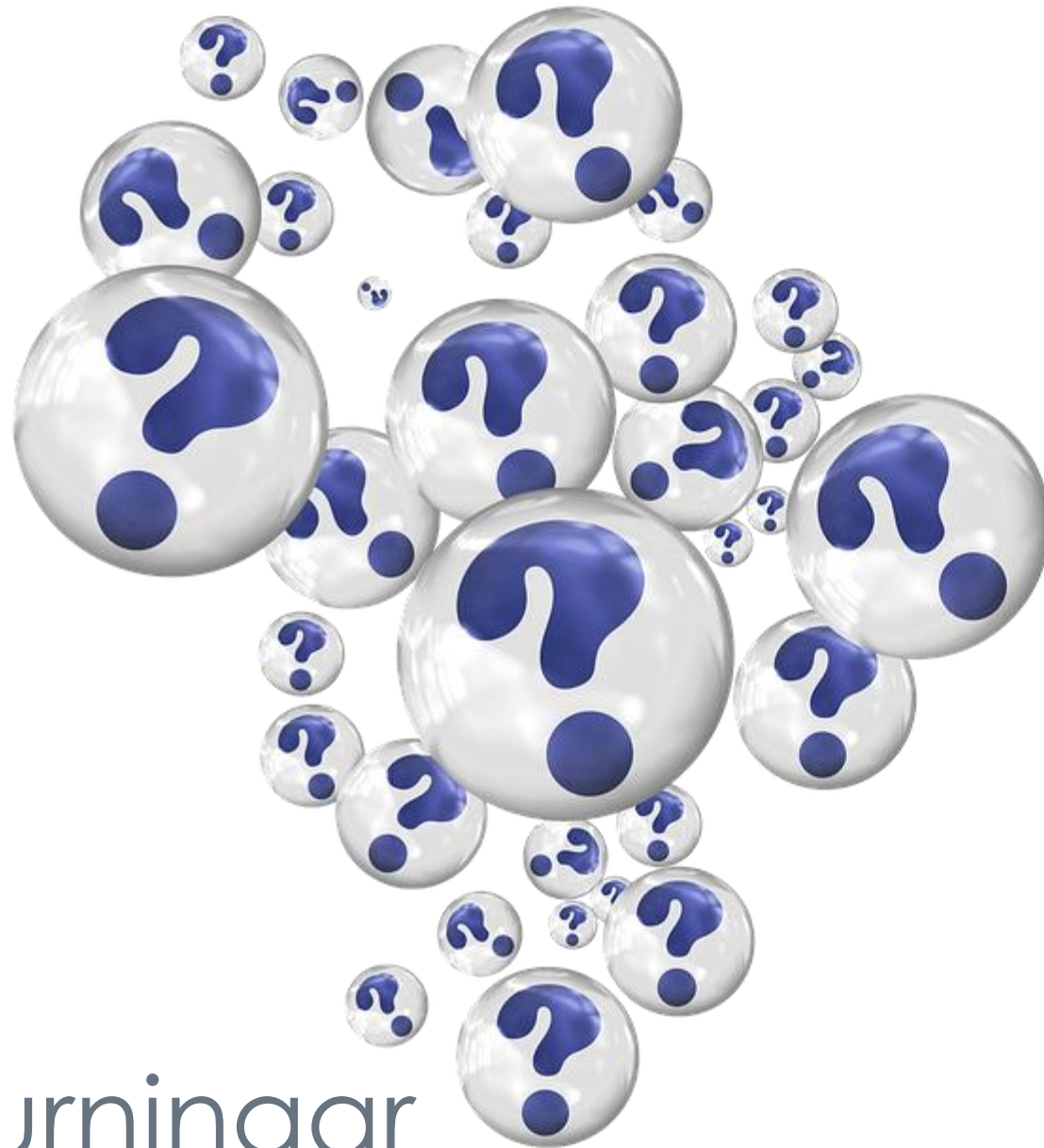
Tækifæri að færa upp á yfirborðið – með starfsfólkinu
Fá aðstoð

Þjálfun starfsmanna

- Nálgast verkefnið saman sem hópur
- Regluleg vitundarvakning (innri eða ytri)
- Leiðbeiningar – kvitta fyrir lestur
- Mæla árangurinn – saman



Takk fyrir



Spurningar

sensæ

15 ára