# Mikilvægi starfsmannaþjálfunar við innleiðingu GDPR

NÝHERJI

12.12.2017

*Arna Hrönn Ágústsdóttir, lögfræðingur og CIPP/E*

# Hvar skal byrja?

Persónuverndarstefna

Innbyggð og sjálfgefin persónuvernd

Lagagrundvöllur fyrir vinnslu

Flutningur gagna utan EES

Tilkynning öryggisbrots

Vinnslusamningar

Lágmörkun gagna

Tæknilegar og skipulagslegar ráðstafanir

Áreiðanleiki gagna

Skipun persónuverndarfulltrúa

Starfsmannamál

Aðgangsbeiðni skráðs einstaklings

Áhættumat um áhrif á persónuvernd

Gagnsæi vinnslu

Varðveislutími gagna

Skrá yfir vinnslustarfsemi

Réttur einstaklings til að flytja gögn

Rétturinn til að GLEYMAST

# Forgangsröðun og áhættugreining

NÝHERJI

**How Risky Is Non-Compliance With the Following GDPR Obligations**
**(Scale Of 1-5, With 1 Being "No Risk" And 5 Being "High Risk")**

| Overall | | U.S. | | EU | |
|---|---|---|---|---|---|
| Prep. for breach | 3.66 | Int'l data transfers | 3.76 | Prep. for breach | 3.68 |
| Data inventory/mapping | 3.57 | Obtaining consent | 3.61 | Data inventory/mapping | 3.57 |
| Obtaining consent | 3.54 | Prep. for breach | 3.6 | Maintain. Art. 30 records | 3.51 |
| Int'l data transfers | 3.54 | Data inventory/mapping | 3.6 | Obtaining consent | 3.44 |
| Maintain Art. 30 records | 3.48 | Maintain Art. 30 records | 3.42 | Conducting DPIAs | 3.35 |
| Conducting DPIAs | 3.36 | Data subject requests | 3.37 | Int'l data transfers | 3.31 |
| Operationalizing RTBF | 3.34 | Conducting DPIAs | 3.33 | Data subject requests | 3.3 |
| Data subject requests | 3.34 | Operationalizing RTBF | 3.26 | Operationalizing RTBF | 3.21 |
| Establish legit interest | 3.14 | Establish legit interest | 3.18 | Establish legit interest | 3.08 |
| Data portability | 2.88 | Data portability | 2.92 | Appoint DPO | 2.85 |
| Appoint DPO | 2.87 | Appoint DPO | 2.9 | Data portability | 2.79 |

iapp

- Könnun IAPP frá okt 2017

# Forgangsröðun og áhættugreining

## » Forgangsröðun eftir áhættu

- ✓ Undirbúningur öryggisbrots
- ✓ Kortlagning gagna
- ✓ Viðhalda skrá yfir vinnslustarfsemi

## » Hvernig má draga úr áhættu?

- ✓ Starfsmannaþjálfun
- ✓ Fjárfesting í viðeigandi tækni

iapp

***Training employees on data protection and privacy tops the list for 10 of 11 GDPR compliance risks.***

- Könnun IAPP frá okt 2017

# Innleiðingarferlið

- **ISO 27001 stjórnkerfi upplýsingaöryggis Nýherja**

- **Kortlagning vinnslu**
  - Hvaða kerfi vinna persónuupplýsingar, í hvaða tilgangi, flutningur þeirra, öryggisráðstafanir ofl.

- **Skráning verðmæta í eignaskrá (IT assets)**
  - Mikill fjöldi rekstrarkerfa
  - Veitir yfirsýn yfir vinnslu
  - Hjálpar við að halda skrá yfir vinnslustarfsemi

- **Skönnun gagnagrunna og skráa með hjálp Guardium frá IBM**
  - Hvar eru persónugreinanleg gögn?
  - Flokkun gagna – sérstakir flokkar persónuupplýsinga
  - Nær bæði til mótaðra gagna (structured data) og ómótaðra gagna (unstructured data)

- **Þjálfun starfsfólks**

# Fjárfesting í þekkingu starfsmanna

NÝHERJI

- **CIPP/E og CIPM fagvottun á vegum IAPP**



- **Námskeið hjá Endurmenntun HÍ**
- **Skyldunámskeið fyrir alla starfsmenn samstæðunnar**
  - Bæði á íslensku og ensku
  - Yfir 300 starfsmenn hafa setið námskeiðið
- **Fræðsla á Workplace**
- **Hvað er framundan?**
  - Sérhæfðari námskeið sem taka mið af starfshlutverki
  - Vinnustofur og fundir til að kynna nýjar verklagsreglur

# Fyrirstaða í innleiðingarferlinu

» **Verkefnið tímafrekt og krefst mikillar sérfræðiþekkingar**

» **Flækjustig og óvissa nýrrar persónuverndarlöggjafar**

**Biggest Barriers to GDPR Compliance**

| Overall | | U.S. | | EU | |
|---|---|---|---|---|---|
| Complexity of law | 32% | Complexity of law | 38% | Inadequate budget | 25% |
| Inadequate budget | 22% | Lack of qualified staff | 20% | Complexity of law | 24% |
| Too little time | 20% | Too little time | 18% | Too little time | 22% |
| Lack of qualified staff | 19% | Inadequate budget | 17% | Lack of qualified staff | 18% |
| Shortage of tech tools | 9% | Shortage of tech tools | 7% | Shortage of tech tools | 10% |

- Könnun IAPP frá okt 2017


# Takk fyrir mig!