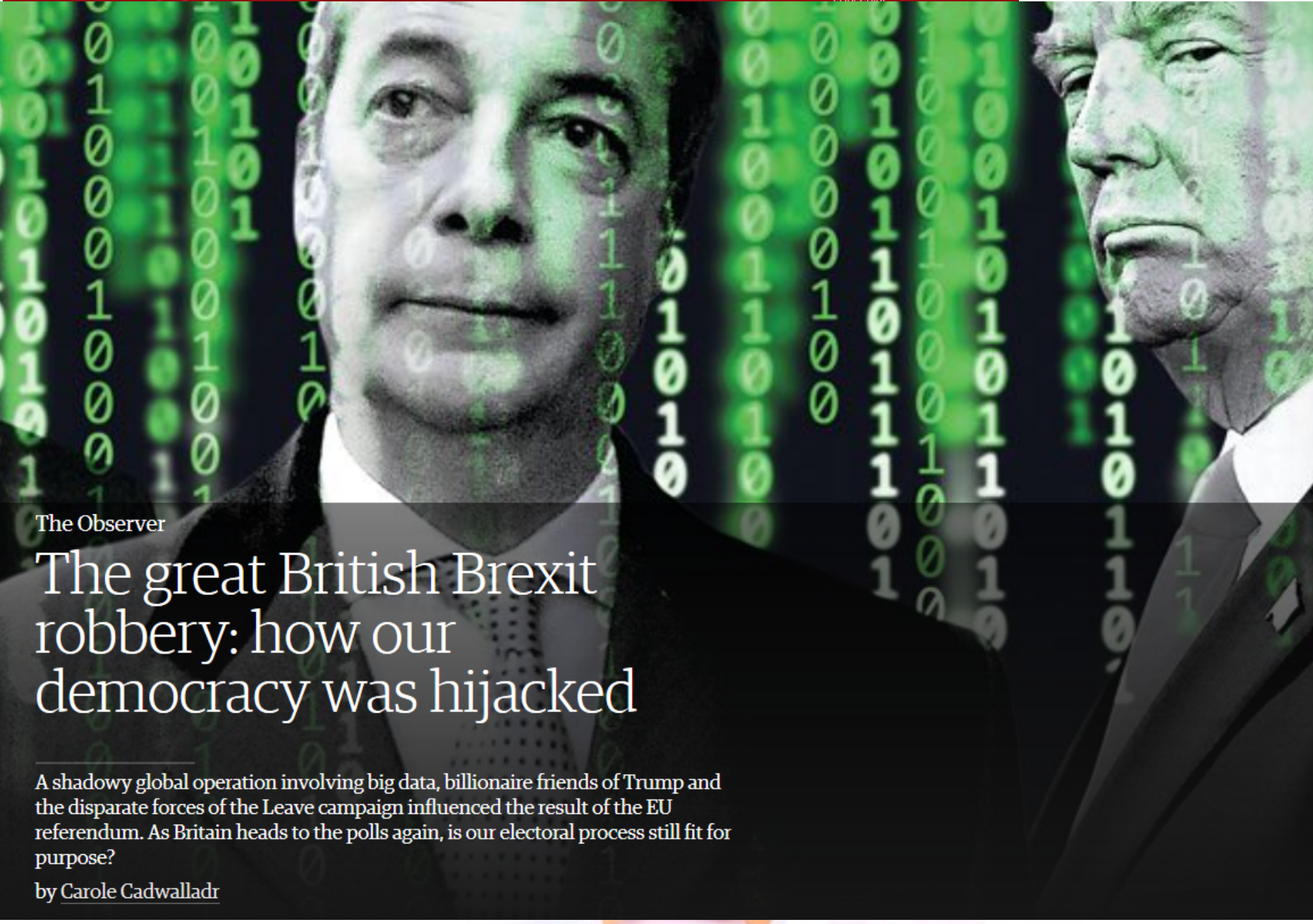
Ný persónuverndarlöggjöf 2018

Persónuvernd: lykilatriði í rekstri!

Vigdís Eva Líndal
skrifstofustjóri upplýsingaöryggis

Persónuvernd



The Observer

The great British Brexit robbery: how our democracy was hijacked

A shadowy global operation involving big data, billionaire friends of Trump and the disparate forces of the Leave campaign influenced the result of the EU referendum. As Britain heads to the polls again, is our electoral process still fit for purpose?

by Carole Cadwalladr

Persónuvernd

Tildrög / Nauðsyn

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“)

Til framkvæmda í **maí 2018**

Persónuvernd

Markmið nýrra reglna

Samræmd og öflug vernd

Frjálst flæði upplýsinga

Aukin réttarvissa – meiri fyrirsjáanleiki

Létta stjórnsýslulegar byrðar

Persónuvernd

Til hverra nær GDPR?

I. Efnislegt gildissvið

Vinnsla um alla einstaklinga innan EES svæðisins – óháð ríkisfangi

II. Landfræðilegt gildissvið

A. Öll fyrirtæki með staðfestu innan EES óháð því hvar vinnslan fer fram
B. Öll fyrirtæki utan EES ef:
   → Vörur/þjónusta eða eftirlit með hegðun
   → Allur heimurinn undir!

III. *Sjálfstæð ábyrgð vinnsluaðila!*

Persónuvernd

Hvað breytist ekki?

- Hvað eru persónuupplýsingar?
  - Almennar og viðkvæmar
- Hvaða heimild stendur til vinnslunnar?
  - Samþykki
    - Ath. auknar kröfur
  - Lagaheimild/skylda - almannahagsmunir
  - Lögmætir hagsmunir
    - Ath. auknar kröfur
- Er vinnslan lögmæt, gagnsæ, hófleg, áreiðanleg?
- Hver er tilgangur vinnslunnar?
- Veit einstaklingurinn af vinnslunni?
- Er búið að tryggja öryggi upplýsingana?
- Hvar eru upplýsingarnar vistaðar og hvar má vista þær? Innan eða utan EES?

Persónuvernd

Helstu skyldur ábyrgðaraðila

Ábyrgðarskylda og gagnsæi

Skrá yfir vinnslustarfsemi

Mat á áhrifum á persónuvernd

Innbyggð og sjálfgefin persónuvernd

Persónuverndarfulltrúi

Sjálfvirk ákvarðanataka - persónusnið

Réttindi einstaklinga

Persónuvernd

Ábyrgðarskylda

2. mgr. 5. gr. og 24. gr. GDPR

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

- ✓ Hvernig?
  - Skjalfesta verklagsreglur
  - Ráðstafanir sem tryggja persónuvernd
  - Persónuverndarfulltrúi
- ✓ Gagnvart hverjum?
  - Persónuvernd og einstaklingum
- ✓ Sönnun
  - Frumkvæðisskylda á ábyrgðaraðila

Skrá yfir vinnslustarfsemi

30. gr. GDPR

Persónuvernd

Ábyrgðaraðili og vinnsluaðili
- Ítarlegri skrá hjá ábyrgðaraðilum

Efni og form

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?

Öryggi
- Ef mögulegt er – almenn lýsing á tæknilegum og skipulagslegum öryggisráðstöfunum

Persónuvernd

Mat á áhrifum á persónuvernd(DPIA)

35.-36. gr. GDPR

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

Hvað ef vinnsla er áfram mjög áhættusöm þrátt fyrir að öryggisráðstafanir hafi verið gerðar?

- **Fyrirframsamráð** við Persónuvernd

⇒ Sjá nánar álit 29. gr. hópsins

Persónuvernd

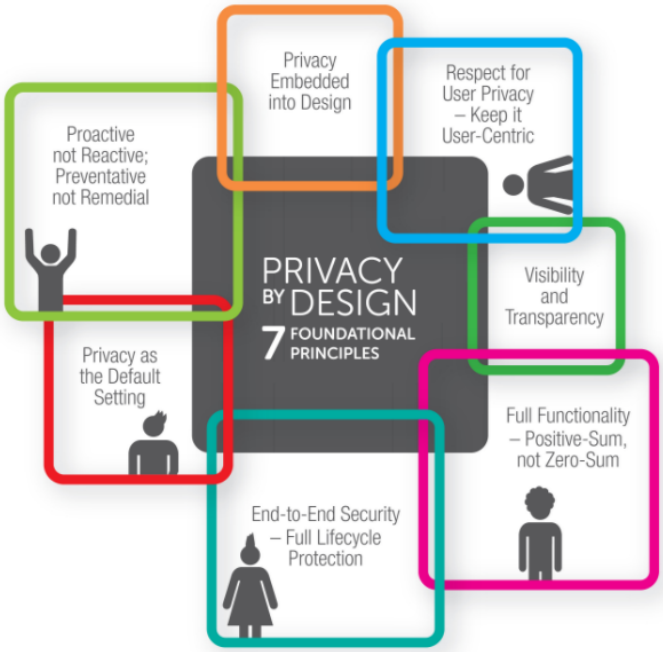
Innbyggð og sjálfgefin persónuvernd

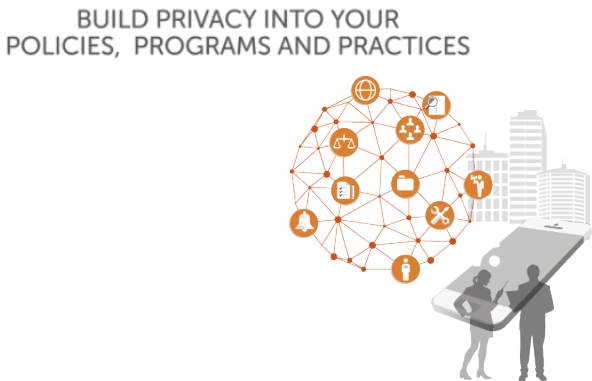
25. gr. GDPR

Verndarráðstafanir innbyggðar í vinnslu frá upphafi

Einungis nauðsynlegar upplýsingar séu unnar

Persónuverndarvottun eða -innsigli





Persónuvernd

Persónuverndarfulltrúi

37.-39. gr. GDPR

Öll **stjórnvöld**

—Samnýting möguleg

Fyrirtæki ef aðalstarfsemi er:

– Umfangsmikil, reglubundin og kerfisbundin vöktun á einstaklingum
– Umfangsmikil vinnsla viðkvæmra persónupplýsinga

Sjálfstæður og óháður í störfum

Reglufylgni, fræðsla, ráðgjöf, tengiliður

Hæfisskilyrði – sérþekking á pvlöggjöf

Leiðbeiningar 29. gr. hópsins

Persónuvernd

Breytt tilkynningarskylda

33.-34. gr. GDPR

Tilkynna öryggisbrot til *Persónuverndar*

- Innan 72 klst.
- Efniskröfur

Tilkynna um öryggisbrot til *einstaklinga*

- Án tafar ef mikil áhætta
- Á skýru og einföldu máli
- Undantekningar

Drög að áliti 29. gr. hópsins um öryggisbrot

Persónuvernd

Notkun vinnsluaðila

28. gr. GDPR

Eingöngu heimilt ef:

- *Nægilegar tryggingar* fyrir öryggi og réttindum einstaklinga

- *Vinnslusamningur* hefur verið gerður um m.a.:
  - Viðfangsefni og tímalengd vinnslu
  - Eðli og tilgang
  - Tegundir persónuupplýsinga
  - Flokkar skráðra einstaklinga
  - Réttindi ábyrgðaraðila
  - Sértæk ákvæði, m.a. um þagnarheit, öryggi, úttektir, fyrirmæli ábyrgðaraðila o.fl.

Persónuvernd

Sjálfstæð skylda á vinnsluaðila

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

Persónuvernd

Réttindi einstaklinga

Réttindi	Aukin réttindi	Ný réttindi	Ákvæði
Upplýsingaréttur	X		13. og 14. gr.
Aðgangsréttur	X		15. gr.
Leiðrétting og eyðing	X		16./17./19. gr.
Takmörkun vinnslu		X	18./19. gr.
Flutningsréttur		X	20. gr.
Andmælaréttur	X		1. mgr. 21. gr.
Andmælaréttur vegna beinnar markaðssetningar	X		2. mgr. 21. gr.
Sjálfvirk ákvarðanataka		X	22. gr.

Persónuvernd

Sjálfvirk ákvarðanataka – persónusnið

22. gr. GDPR

- Einstaklingar þurfa ekki að undirgangast sjálfvirka ákvörðun sem hefur áhrif á réttindi og skyldur *nema*
  - vegna *samningsgerðar*
    - ≠ Viðkvæmar persónuupplýsingar
  - *lagaheimild*
  - yfirlýst *samþykki*
    - ≠ Lögmætir hagsmunir

- Réttur til mannlegrar íhlutunar og til að láta skoðun sína í ljós

⇒ Sjá nánar álit 29. gr. hópsins

Persónuvernd

Breytt eftirlit – sektir

VI. kafli

Nýjar og stórauknar sektarheimildir

- Allt að 4% af árlegri heildarveltu eða 20 milljón evrum
- Allt að 2% af árlegri heildarveltu eða 10 milljón evrum

Einn afgreiðslustaður (e. One stop shop)

„Samræmingarkerfi“ (e. Consistency mechanism)

⇒ Álit 29. gr. hópsins um stjórnvaldssektir

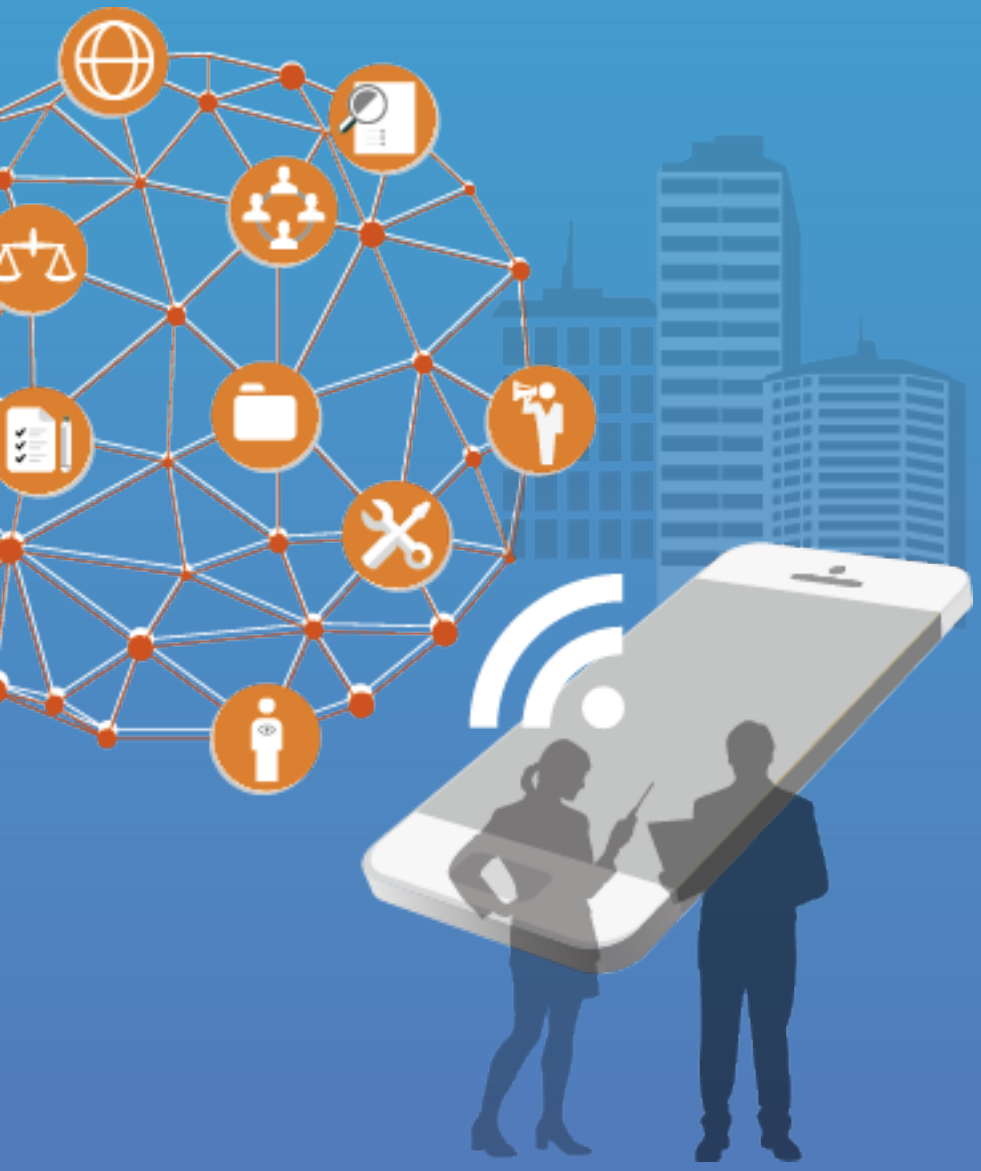
⇒ Álit 29. gr. hópsins um forystueftirlitsyfirvald

Persónuvernd

Næstu skref?

1. Vitundarvakning og þekkingaröflun
2. Kortleggja og greina

   →Gerð vinnsluskráar
3. Forgangsraða verkefnum / aðgerðum í aðlögunarferlinu
4. Uppfæra og innleiða verklagsreglur o.fl. skv. forgangslista
5. Yfirfara og endurskoða



postur@personuvernd.is

www.personuvernd.is

@Personuvernd

#Persónuvernd #PV2018

Persónuvernd