Persónuvernd – helstu atriði við aðlögun fyrirtækja að nýjum reglum

Hafliði K. Lárusson

Fundur Samtaka iðnaðarins, 7. apríl 2017

Yfirlit

- Yfirlit yfir núgildandi meginreglur og helstu breytingar í nýrri reglugerð ESB
- Helstu þættir í aðlögun fyrirtækja að nýjum reglum

Núgildandi reglur um persónuvernd (1)

- Lög nr. 77/2000 um persónuvernd og meðferð persónuupplýsinga
  - Byggð á tilskipun ESB frá árinu 1995
- Persónuupplýsingar
  - Nánast allar upplýsingar, sem tengjast einstaklingi og eru persónugreinanlegar, t.d. heimilisfang, starf, launakjör, fjárhagsupplýsingar, viðskiptahegðun, áhugamál, ljósmyndir, pólitískar skoðanir, trúarskoðanir, kynhneigð, refsimálefni...
- Vinnsla persónuupplýsinga
  - Í raun öll meðferð persónuupplýsinga, hvaða nafni sem hún nefnist: söfnun, vistun, aðgangur, birting, flutningur, afritun, fjölfjöldun, breyting, framsal, eyðing...

Núgildandi reglur um persónuvernd (2)

- Ábyrgðaraðili
  - Sá, sem ber ábyrgð á vinnslu persónuupplýsinga
  - Flestar núgildandi reglur beinast að ábyrgðaraðila
- Vinnsluaðili
  - Sá, sem vinnur persónuupplýsingar fyrir hönd ábyrgðaraðila
  - Til þessa að mestu „í skjóli“ ábyrgðaraðila
  - Þarf einnig að virða meginreglur um vinnslu persónuupplýsinga

Núgildandi reglur um persónuvernd (3)

- Heimild til vinnslu persónuupplýsinga
  - Samþykki er lykilhugtak og almennt skilyrði til vinnslu persónuupplýsinga
    - Þarf að vera veitt með virkum og skýrum hætti
    - Afmarkar heimila vinnslu
    - Veitt með mismunandi hætti: skriflega með undirritun; á netinu með því að haka við samþykki...
  - Stundum er beint samþykki ekki nauðsynlegt
    - Í tilviki fyrirtækja einkum ef vinnsla er nauðsynleg til að efna samning við einstaklinginn
    - Æskilegt að byggja á samþykki eins og unnt er

Núgildandi reglur um persónuvernd (4)

- Meginreglur um vinnslu persónuupplýsinga
  - Unnar með sanngjörnum, málefnalegum og lögmætum hætti og í samræmi við vandaða vinnsluhætti
  - Fengnar í yfirlýstum, skýrum og málefnalegum tilgangi
  - Nægilegar, viðeigandi og ekki umfram nauðsyn
  - Ekki persónugreinanlegar lengur en þörf krefur
  - Sérstakar reglur um flutning á milli landa (innan EES; út fyrir EES...). - Aðgengi erlendis frá telst vera „flutningur“

Helstu breytingar í nýrri reglugerð ESB

- Aukin réttarvernd einstaklinga
- Auknar skyldur um skjölun, ferla, verklagsreglur og samninga. – Þáttur í skipulagi, rekstri, öryggisstefnu, tæknimálum, upplýsingamálum og „persónuverndarmenningu“ fyrirtækja
- Nýjar og sjálfstæðar skyldur vinnsluaðila
- Stórauknar sekarheimildir með því yfirlýsta markmiði auka persónuvernd, tryggja að skert flæði raski ekki samkeppni og að persónuverndaryfirvöld geti tryggt að markmið reglnanna náist

Meginreglur (gamlar og nýjar)

- Lögmæt, sanngjörn og gegnsæ vinnsla
- Einungis vinnsla sem samrýmist yfirlýstum/umsömdum tilgangi
- Ekki meiri persónuupplýsingar en þörf krefur
- Réttar og uppfærðar persónuupplýsingar
- Ekki geyma persónuupplýsingar lengur en þörf krefur
- Heilindi og trúnaður við vinnslu
- Ábyrg vinnsla

Samþykki

- „Hjartað“ í lögmætri vinnslu fyrirtækja á persónuupplýsingum
- Veitt með skýrum og virkum hætti og á auðskildu máli
- Má ekki vera „falið“ í lengri texta eða samningi
- Má ekki vera „þvingað“ með þeim hætti að þjónusta sé eingöngu möguleg ef samþykki er veitt fyrir vinnslu, sem ekki er nauðsynleg vegna þjónustunnar
- Auðvelt að afturkalla og með sama hætti og samþykkið var veitt
- Aðlögun:
  - Kanna núverandi samþykki og vinnslu í því ljósi
  - Kanna hvort breyta þurfi samningum og orðalagi samþykkis
  - Kanna hvort vinnsla er umfram það nauðsynlega

Viðkvæmar persónuupplýsingar

- Ríkari skyldur um sérstakan skýrleika samþykkis
- Nýir flokkar: Genaupplýsingar og stafræn lífkenni (fingraför, lithimna)
- Aðlögun:
  - Nýir flokkar sem hluti persónuupplýsinga?
  - Samþykki og vinnsla til samræmis?

Gegnsæi og upplýsingar um vinnslu

- Ríkari skyldur um að fyrirtæki upplýsi einstaklinga um vinnslu, t.d. umfang, tilgang og hvort flutningur yfir landamæri þegar samþykkis er leitað
- Einnig upplýsingar um hvernig hægt sé að fá upplýsingar leiðréttar, um afturköllun samþykkis o.fl.
- <u>Aðlögun</u>:
  - Kanna og þá uppfæra slíkar upplýsingar

Aðgangur og flutningshæfi

- Aukinn réttur til aðgangs að eigin persónuupplýsingum
- Flutningshæfi (*portability*) – réttur til að fá allar upplýsingar afhentar í aðgengilegu og flutningshæfu formi (bankar, tryggingafélög, samfélagsmiðlar...)
- <u>Aðlögun</u>:
  - Tryggja ferla til að halda saman öllum upplýsingum um einstakling og veita afrit með aðgengilegum hætti

Réttur til eyðingar persónuupplýsinga

- „Rétturinn til að gleymast“
- Ef upplýsingar eru ekki lengur nauðsynlegar vegna vinnslunnar eða ef einstaklingur afturkallar samþykki
- Fyrirtæki þarf að bregðast við tafarlaust og innan mánaðar
- Einnig að tilkynna öðrum, sem hafa fengið upplýsingarnar, að þeim skuli eytt
- Aðlögun:
  - Tryggja rétta innri ferla, verklagsreglur og persónuverndarstefnu

Réttur barna

- Hafa útskýringar á samþykki og vinnslu auðskilin fyrir börn
- Samþykki foreldra nauðsynlegt ef netþjónustu er sérstaklega beint að börnum
- „Barn“ yngra en 16 ára (eða yngra en 14 ára)
- Aðlögun:
  - Tryggja rétta innri ferla, verklagsreglur og persónuverndarstefnu

Skipulag og innra eftirlit með vinnslu

- Viðamiklar breytingar
- Tryggja tæknilega þætti og innra skipulag þannig að reglurnar séu virtar
- Fyrirtæki skulu hafa sérstaka, skriflega persónuverndarstefnu
  - Um alla þætti persónuverndar, vinnslu og skyldur í því sambandi
- Fyrirtæki kunna að þurfa að skipa sérstakan persónuverndarstjóra
  - T.d. ef þau stunda reglubundið og skipulagt „eftirlit“ með einstaklingum í stórum stíl eða vinna viðkvæmar persónuupplýsingar í stórum stíl
  - Þarf að vera sjálfstæður og má ekki fá nein fyrirmæli. Má sinna öðrum störfum einnig
- <u>Aðlögun</u>:
  - Tryggja allt ofangreint

Sérstakar og auknar skyldur vinnsluaðila

- Nýjar skyldur:
  - Halda skriflega skrá um alla þá vinnslu persónuupplýsinga, sem á sér stað
  - Tilkynna um brot til ábyrgðaraðila (sbr. fyrri umfjöllun)
  - Gera skriflega samninga við ábyrgðaraðila (athuga leiðbeiningar og stöðluð ákvæði)
  - Eingöngu vinna persónuupplýsingar skv. skriflegum fyrirmælum ábyrgðaraðila
  - Skipa persónuverndarstjóra með sama hætti og ábyrgðaraðilar, þegar þess er þörf
- Aðlögun:
  - Tryggja innri ferla, skráningu, skjölun og persónuverndarstefnu

Aðlögun fyrirtækja að nýjum reglum (1)

- Heildstætt verkefni sem tengist ýmsum þáttum í starfsemi fyrirtækja:
  - Tækni- og hugbúnaðarmál (kröfur um rétta vinnslu, kröfur um öryggi...)
  - Innri ferlar (rannsókn og tilkynning á brotum; samþætting...)
  - Starfsmannamál (uppfræðsla og þjálfun...)
  - Stjórnun (persónuverndarstefna, áhættustjórnun...)
- Helstu þættir:
  - Endurskoða/móta persónuverndarstefnu
  - Endurskoða/móta innri ferla
  - Nánari skjölun vinnslu
  - Lögmæti vinnslu; samþykki eða framfylgd samnings
  - Endurskoða samninga og samningsákvæði, sem varða persónuupplýsingar

Aðlögun fyrirtækja að nýjum reglum (2)

1. Heildstætt mat á eftirfarandi þáttum (2. ársfjórðungur 2017):
    1) Meta að hvaða leyti þarf að bæta vitund og þekkingu á persónuverndarreglum
    2) „Kortleggja“ persónuupplýsingar og hvaða vinnsla á sér stað
    3) Kanna lagalegan grundvöll vinnslu, hvernig samþykkis er aflað og hvernig það er orðað
    4) Meta hvort að núverandi vinnsla og ferlar eru í samræmi við nýjar reglur, t.d. varðandi flutningshæfi , eyðingu gagna...
    5) Skipuleggja ferla ef brot eiga sér stað
    6) Móta og „sérsníða“ persónuverndarstefnu
    7) Gera öryggis- og reglufylgnipróf til að meta áhættu og þörf á umbótum
    8) Meta hvort skipa þurfi persónuverndarstjóra (ekki að fullu ljóst)

Aðlögun fyrirtækja að nýjum reglum (3)

2. Móta almenna stefnu og aðgerðaáætlun (3. ársfjórðungur 2017)
   - Fer eftir niðurstöðum úr persónuverndarúttekt
3. Koma aðgerðaáætlun í framkvæmd (seinni hluti 2017)
4. Gera nýtt persónuverndarmat til að tryggja að allir helstu þættir séu til staðar (1. ársfjórðungur 2018)
5. Aðlögun að nýjum reglum lokið fyrir maí 2018
6. Aðlögun er í raun þegar hafin!

Spurningar?