LEIÐIN TIL INNLEIÐINGAR

STUTT KYNNING:

Gátlisti sem ábyrgðaraðilar þurfa að fylgja til að hefja innleiðingu á nýju persónuverndarlöggjöfinni sem tók gildi í maí 2018 í Evrópu. Íslensku lögin tóku gildi 15. júlí 2018.

Unnið af:
DATTACA LABS ehf.

Leiðin til innleiðingar:

Leiðarvísir fyrir ábyrgðaraðila

1. Greining gagna (Analyzing data)

1.1. Er vitundarvakning farin að eiga sér stað?

- Er stjórnendum og starfsmönnum kunnugt um löggjöfina?
- Vita þeir hvaða þýðingu hún hefur?

1.2. Hver er starfsemin?

1.3. Að hvaða leyti er vinnsla persónuupplýsinga hluti af starfseminni?

- Til dæmis upplýsingar um starfsmenn, viðskiptavini, notendur og íbúa.

1.4. Hvernig er gögnunum safnað?

- Í gegnum hvaða kerfi?

1.5. Hvaða upplýsingar er þar að finna?

- Til dæmis nafn, kennitala, heimilisfang, heilsufarsupplýsingar, fjárhagsupplýsingar og allar aðrar upplýsingar sem hægt er að rekja til tiltekins einstaklings.

1.6. Í hvaða flokka skiptast þær?

- Almennar persónuupplýsingar.
- Viðkvæmar persónuupplýsingar.

1.7. Hvaðan koma þær?

- Viðskiptavinum?
- Utanaðkomandi þriðju aðilum?

1.8. Er utanaðkomandi þriðji aðili sem vinnur upplýsingarnar fyrir hönd ábyrgðaraðila?

- Tekur til dæmis sá aðili að sér að geyma eða að safna persónuupplýsingum?

1.9. Hverjum er upplýsingunum deilt með?

2. Fylgni við persónuverndarlöggjöfina (compliance part)

2.1. Er heimild til vinnslu persónuupplýsinga?

2.1.1. Almennar persónuupplýsingar; vinnsla er heimil í eftirfarandi tilvikum:

- Þegar skráður einstaklingur hefur samþykkt vinnsluna.
- Þegar vinnslan er *nauðsynleg* til að efna samning sem hinn skráði er aðili að.
- Þegar vinnslan er *nauðsynleg* til að uppfylla lagaskyldu.
- Þegar vinnslan er *nauðsynleg* til að vernda brýna hagsmuni hins skráða eða annars einstaklings.
- Þegar vinnslan er *nauðsynleg* vegna verks sem unnið er í þágu almannahagsmuna eða vegna opinbers valds sem ábyrgðaraðili fer með.
- Þegar vinnslan er *nauðsynleg* til að ábyrgðaraðili, eða þriðji maður geti gætt lögmætra hagsmuna sinna (réttindi hins skráða geta þó vegið þyngra, einkum þegar um barn er að ræða).

2.1.2. Viðkvæmar persónuupplýsingar; eitthvert af þeim skilyrðum sem talin eru upp í kafla 2.1.1. þurfa að eiga við, auk einhvers af eftirfarandi skilyrðum:

- Skýrt samþykki liggur fyrir frá skráðum aðila.
- Vinnslan er *nauðsynleg* vegna vinnu- eða almannatryggingaréttar.
- Vinnslan er *nauðsynleg* til að vernda brýna hagsmuni hins skráða, eða annars einstaklings, og hinn skráði er af líkamlegum ástæðum eða í lagalegum skilningi ófær um að veita samþykki sitt.
- Vinnslan er framkvæmd af samtökum sem ekki starfa í hagnaðarskyni og varðar eingöngu meðlimi, fyrrum meðlimi eða aðra sem hafa verið í reglubundnum samskiptum við þau.
- Vinnslan varðar persónuupplýsingar sem hinn skráði hefur sjálfur augljóslega gert opinberar.
- Vinnslan er nauðsynleg til að unnt sé að stofna, hafa uppi eða verja réttarkröfur.
- Vinnslan er nauðsynleg vegna verulegra almannahagsmuna.
- Vinnslan er nauðsynleg vegna heilsufarssjónarmiða.
- Vinnslan er nauðsynleg vegna heilsu almennings.
- Vinnslan er nauðsynleg vegna vísinda-, sögu eða tölfræðirannsókna.

Dæmi:

Telur til dæmis ábyrgðaraðili vinnsluna heimila á grundvelli samþykkis? Eru skilyrði fyrir samþykki til staðar? Er samþykki:

- Upplýst? Fékk hinn skráði fullnægjandi fræðslu?
- Sértækt? Nær samþykki til fyrirsjáanlegrar vinnslu?
- Óþvingað? Er aðstöðumunur á milli aðila? Vinnuveitandi vs. starfsmaður?
- Ótvírætt viljayfirlýsing? Þögn eða athafnaleysi getur ekki orðið grundvöllur samþykkis.
- Getur ábyrgðaraðili sýnt fram á að samþykki hafi verið veitt?
- Er jafn auðvelt að afturkalla samþykki eins og það var að veita það?
- Á að afla samþykkis frá barni? Ekki er mögulegt að fá samþykki frá barni þegar því er boðin þjónusta á Internetinu nema foreldri eða forráðamaður þess samþykki.

Telur ábyrgðaraðili vinnslu viðkvæmra persónuupplýsinga heimila á grundvelli samþykkis?

- Sömu kröfur og að framan.
- Ekki er þó hægt að veita samþykki í verki.
- Skrifleg eða munnleg yfirlýsing frá hinum skráða verður að liggja fyrir.

Telur ábyrgðaraðili vinnsluna nauðsynlega til að efna samning sem hinn skráði er aðili að?

- Af hverju er ekki hægt að efna samning við hann nema vinna tilteknar persónuupplýsingar?

Telur ábyrgðaraðili vinnsluna nauðsynlega vegna lagaskyldu?

- Hvaða lagaheimild styðst ábyrgðaraðili við?

Telur ábyrgðaraðili vinnsluna nauðsynlega vegna lögmætra hagsmuna?

- Hverjir eru hinir lögmætu hagsmunir?

2.2. Samrýmist vinnsla persónuupplýsinga meginreglum löggjafarinnar?

2.2.1. *Sanngirnisreglan* – er vinnslan gagnsæ? Hefur hinn skráði fengið fullnægjandi fræðslu?

2.2.2. *Tilgangsreglan* – er tilgangurinn með vinnslunni nógu skýr og afmarkaður?

2.2.3. *Magnreglan* – er safnað meiri persónuupplýsingum en nauðsynlegt er?

2.2.4. *Áreiðanleikareglan* – eru upplýsingarnar réttar?

2.2.5. *Varðveislureglan* – eru upplýsingar geymdar lengur en nauðsyn krefur?

2.2.6. *Öryggisreglan* – er öryggi persónuupplýsinga tryggt? Hefur ábyrgðaraðili gert:

- *Skriflega öryggisstefnu?*
- *Skriflegt áhættumat?*
- *Gripið til öryggisráðstafana á grundvelli áhættumatsins?*
  - *Til dæmis aðgangsstýringar, tryggja rekjanleika uppflettinga, fá þagnayfirlýsingar frá starfsmönnum o. fl.*
- *Meiri kröfur eru gerðar þegar um viðkvæmar persónuupplýsingar er að ræða, til dæmis heilsufarsupplýsingar.*
- *Að fylgja reglum 299/2001 uppfyllir þessa kröfu.*
- *Að fylgja að öðru leyti ISO 27001 er líka gagnlegt.*

2.3. Innbyggð og sjálfgefin persónuvernd.

2.3.1. Innbyggð persónuvernd.

- Er hugbúnaður hannaður með meginreglur persónuupplýsinga í huga?
- Hversu miklar kröfur eru gerðar í þessum efnum veltur á þörf ábyrgðaraðila fyrir vernd.

2.3.2. Sjálfgefin persónuvernd.

- Persónuvernd verður að vera sjálfgefin. Hinn skráði á ekki að þurfa að bregðast við, til dæmis á vefsíðu með því að merkja úr reit, til að koma í veg fyrir að unnið verði með persónuupplýsingar um hann.

2.3.3. Mat á áhrifum á persónuvernd.

2.3.3.1. Löggjöfin gerir kröfu um að áhættumat fari fram þegar tiltekin vinnsla er til þess fallin að skapa mikla áhættu fyrir réttindi einstaklinga. Til dæmis þegar:

- Ný tækni er innleidd.
- Umfangsmikið mat fer fram á persónulegum þáttum einstaklinga.
- Um umfangsmikla vinnslu viðkvæmra persónuupplýsinga er að ræða.
- Um er að ræða umfangsmikið eftirlit á almenningssvæði.

2.4. Er vinnsluaðili til staðar?

2.4.1. Hvernig var hann valinn?

2.4.2. Tryggir hann nægjanlega vernd?

2.4.3. Hvar er hann staðsettur? Innan eða utan EES?

2.4.4. Ef utan EES. Er heimild til þess að flytja persónuupplýsingar út fyrir EES?

2.4.5. Er fullnægjandi vinnslusamningur til staðar?

2.4.6. Er undirvinnsluaðili til staðar?

- Hefur ábyrgðaraðili samþykkt hann?

2.5. Eru réttindi einstaklinga tryggð?

2.5.1. Réttur til vitneskju.

2.5.2. Réttur til aðgangs.

2.5.3. Réttur til leiðréttingar.

2.5.4. Réttur til að gleymast.

2.5.5. Hreyfanleiki gagna.

2.5.6. Rétturinn til að takmarka vinnslu o.fl.

2.6. Fá hinir skráðu fullnægjandi fræðslu?

2.6.1. Er fræðsla á aðgengilegu formi?

2.6.2. Er hún á skýru og einföldu máli?

- Er um barn að ræða? Þá skal fræðsla taka mið af skilningi þess og þroska.

2.6.3. Heimilt er að notast við sjónræna fræðslu.

2.6.4. Fræðsla verður m.a. að innihalda upplýsingar um eftirfarandi atriði:

- Heiti og samskiptaupplýsingar ábyrgðaraðila.
- Upplýsingar um persónuverndarfulltrúa (ef það á við).
- Tilgang vinnslunnar og lagagrundvöll hennar.
- Hverjir viðtakendur upplýsinganna eru.
- Hvort upplýsingum verði miðlað út fyrir EES.
- Hve lengi upplýsingarnar verða geymdar.

- Hver réttindi hins skráða eru.
- Ath. Mismunandi kröfur eru gerðar eftir því hvort gagna er aflað frá hinum skráða eða þriðja aðila.

2.7. Hvernig verður brugðist við öryggisbrotum?

2.7.1. Hvernig verður tryggt að öryggisbrot séu tilkynnt innan 72 klukkustunda til Persónuverndar?

- Tilkynna verður um brot sem fela í sér hættu fyrir frelsi og réttindi einstaklinga.
- Hvar innan fyrirtækis er líklegt að öryggisbrot feli í sér slíka hættu?

2.7.2. Hvernig verður tryggt að tilkynnt sé um öryggisbrot til hinna skráðu?

- Tilkynna verður hinum skráðu um slík brot ef það felur í sér mikla áhættu fyrir frelsi og réttindi þeirra.
- Hvar innan fyrirtækis er líklegt að brot leiði til slíkrar áhættu?

2.8. Mun ábyrgðaraðili viðhafa innra eftirlit?

2.8.1. Til dæmis ganga úr skugga um:

- Að vinnslan sé heimil.
- Að meginreglum sé fylgt.
- Að réttindi hins skráða séu virt.
- Að öryggisráðstöfunum sé fylgt.

2.9. Getur ábyrgðaraðili sýnt fram á að löggjöfinni sé framfylgt?

2.9.1. Fylgir hann til dæmis viðurkenndri persónuverndarstefnu?

2.10 . Þarf að skipa persónuverndarfulltrúa?

2.10.1 Stjórnvöld og allar opinberar stofnanir.
2.10.2 Þar sem meginstarfsemin er umfangsmikið, reglulegt og kerfisbundið eftirlit með hinum skráðu.
2.10.3 Þar sem unnið er með viðkvæmar persónuupplýsingar í umfangsmiklu mæli.

2.11 . Þarf ábyrgðaraðili að halda skrár yfir vinnslustarfsemi?

2.11.1 Nær öllum sem vinna með persónuupplýsingar er skylt að halda skrá yfir vinnslustarfsemi, þ.e. vinnsluskrá.

- Fyrirtæki og stofnanir sem hafa færri en 250 starfsmenn eru undanþegin skyldunni til að halda vinnsluskrár að því er varðar ákveðnar vinnslur. Undanþágan er mjög þröng og því er sjaldgæft að hún eigi við að öllu leyti um fyrirtæki eða stofnun.

3. Afhending gagna til viðskiptavina (giving data back)

3.1. Á hvaða formi þurfa gögnin að vera?

- Skilyrði að þau séu á svokölluðu API formi.

3.2. Hvaða leiðir eru færar?

- Notast við Digi.me forrit sem Dattaca Labs getur látið útfæra til að afhenda gögn til viðskiptavina.
- Útbúa eigið snjallsímaforrit fyrir viðskiptavini.