SIÐASKIPTIN

SKÝRSLA:
Yfirferð á verkþáttum Dattaca Labs og innleiðingu Sveitarfélagsins Árborgar á lögum um persónuvernd og vinnslu persónuupplýsinga nr. 90/2018.

Unnið af:
DATTACA LABS ehf.

DATTACA LABS

Efnisyfirlit:

1. Aðdragandi

Þann 27. apríl 2016 var samþykkt reglugerð Evrópuþingsins og ráðsins frá 27. apríl 2016 um vernd einstaklinga í tengslum við vinnslu persónuupplýsinga og um frjálsa miðlun slíkra upplýsinga og niðurfellingu tilskipunar 95/46/EB („GDPR"). GDPR tók gildi í aðildarríkjum Evrópusambandsins 25. maí 2018. GDPR var svo innleidd í íslenskan rétt þann 15. júlí 2018 með lögum um persónuvernd og vinnslu persónuupplýsinga nr. 90/2018 („pvl."). Hér eftir eru GDPR og pvl. sameiginlega nefnd „persónuverndarlög".

Um var að ræða umfangsmestu breytingar sem höfðu orðið á persónuverndarlöggjöf í um tvo áratugi. Ljóst var að allir opinberir aðilar þyrftu að leggjast í mikla vinnu til að bregðast við breytingum á löggjöfinni. Í ljósi umfangs og flækjustigs gáfu ýmsir forstjórar persónuverndarstofnana það út að mestu máli skipti fyrir alla að byrja innleiðingarvinnuna. Þeir aðilar myndu, ef eitthvað kæmi upp á eftir gildistöku nýrra laga, sleppa betur en þeir sem ekki hefðu aðhafst neitt. Í dag má telja að mjög fámennur hluti opinberra aðila, ef einhver, uppfylli að fullu kröfur nýrra persónuverndarlaga.

2. Innleiðing á persónuverndarlögum í starfsemi

Almennt er viðurkennt að við innleiðingu á nýjum persónuverndarlögum þurfi að fara í gegnum þrjú skref. Þau eru sem hér segir:

1. Greiningarvinna eða svokölluð kortlagning. Hún felur í sér að kortleggja þarf alla ferla þar sem unnið er með persónuupplýsingar.
2. Könnuna á fylgni við löggjöfina. Það skref felur í sér að máta alla ferlana við viðeigandi ákvæði í löggjöfinni og taka ákvörðun um breytingar sem þurfa að eiga sér stað.
3. Innleiðing á breytingum í starfsemina. Það felur í sér að koma þarf þeim ákvörðunum sem teknar voru í skrefi 2 í framkvæmd.

Við innleiðingu á lögunum í starfsemi Sveitarfélagsins Árborgar (hér eftir „Árborg" eða „sveitarfélagið") hefur þessum þremur skrefum verið fylgt.

3. Greiningarvinnan hjá Árborg

Í greiningarvinnunni fékk Árborg aðstoð frá Dattaca Labs. Var grundvöllur vinnunnar að útfylla sniðmát sem lögfræðingar Dattaca Labs höfðu útbúið. Rétt er að taka fram að sniðmátið er grundvöllur að svokallaðri vinnsluskrá sem sveitarfélaginu ber að halda, sbr. 26. gr. pvl. og 30. gr. GDPR. Í sniðmátið voru skráðar ýmsar upplýsingar sem tengjast vinnslu persónuupplýsinga, svo sem:

- Hvaða vinnslu er um að ræða, til dæmis vinnsla á persónuupplýsingum vegna umsókna af ýmsu tagi eða launaútreikninga.
- Af hverju verið er að safna tilteknum persónuupplýsingum, til dæmis svo sveitarfélagið geti uppfyllt þá lagalegu skyldu sem að á því hvílir, beitt opinberu valdi eða efnt samningsskyldur sínar við starfsmenn.
- Hvaða persónuupplýsingum verið er að safna og hvar þær eru geymdar, til dæmis í læstri hirslu eða rafrænu kerfi.
- Hvort utanaðkomandi aðili meðhöndli upplýsingarnar, til dæmis OneSystems.
- Hve lengi verið er að varðveita þær.

Eftir að allar nauðsynlegar upplýsingar höfðu verið skráðar í sniðmátin gaf Dattaca Labs út stöðuskýrslu þar sem veittar voru leiðbeiningar um næstu skref í innleiðingarferlinu, þ.e. hvað þyrfti að gera til að ná ásættanlegri fylgni við löggjöfina.

4. Könnun á fylgni Árborgar við persónuverndarlög og úrbætur

Lögfræðingar Dattaca Labs tóku að sér að máta niðurstöður úr greiningarvinnunni við viðeigandi ákvæði í löggjöfinni. Niðurstöður þeirrar vinnu voru að bæta þyrfti úr ákveðnum þáttum. Upplýsingar um hvaða þætti er um að ræða, hvernig reynt hefur verið að bæta úr þeim og hvað á eftir að gera má finna í eftirfarandi umfjöllun:

- ***Aukið gagnsæi***

Einn af hornsteinum nýrra persónuverndarlaga er að gangsæi verði aukið til mikilla muna. Það felur í sér að einstaklingum verður að vera kunnugt um hvað sveitarfélög eru að gera með þeirra persónuupplýsingar. Nánar tiltekið þarf einstaklingur meðal annars að vera upplýstur um eftirfarandi atriði samkvæmt 13. gr. GDPR:

- Af hverju verið er að safna upplýsingum um hann.
- Á hvaða lagagrundvelli verið er að safna persónuupplýsingum.
- Hverjir munu taka við þeim.
- Hve lengi á að geyma þær.

- Hvaða réttinda hann nýtur og fleira.

Fáir uppfylltu kröfuna um gagnsæi fyrir fram. Til að reyna mæta þessari kröfu laganna hjá Árborg var ákveðið að útbúa persónuverndaryfirlýsingu (sambærilegt því sem margir kalla persónuverndarstefnu) fyrir sveitarfélagið. Mikilvægt er að slík yfirlýsing sé aðgengileg einstaklingum, til dæmis á vefsíðu, enda geta þeir ekki nýtt réttindi sín ef þeim er ekki kunnugt um þau.

Rétt er að taka fram að útgáfa persónuverndaryfirlýsingu jafngildir því ekki að kröfunni um gagnsæi sé fullnægt. Í sumum tilfellum kann að vera réttlætanlegt að einstaklingur leiti eftir upplýsingum sjálfur, til dæmis persónuverndaryfirlýsingu á vefsíðu. Í öðrum verður fræðsla að vera til staðar um leið og upplýsingum er safnað frá honum, til dæmis þegar fyllt er út eyðublað af einhverju tagi þar sem safnað er viðkvæmum persónuupplýsingum. Í slíku tilfelli þarf að birtast kafli á eyðublaðinu um meðferð Árborgar á persónuupplýsingum vegna umsóknarinnar.

Lögfræðingar Dattaca Labs unnu persónuverndaryfirlýsingu fyrir Árborg og hafa jafnframt yfirfarið og bætt fræðslu á eyðublöð. Hér þarf að hafa í huga að persónuverndaryfirlýsingin er nokkuð almenn og hana þarf að uppfæra og bæta reglulega. Jafnframt væri heppilegt að hvert og eitt svið innan Árborgar myndi í framtíðinni gera sína eigin persónuverndaryfirlýsingu.

- ***Viðmiðunartími um geymslutíma persónuupplýsinga***

Ein af meginreglum persónuverndarlaga er að geyma ekki persónuupplýsingar lengur en nauðsynlegt er, sbr. 5. tl. 1. mgr. 8. gr. pvl. og e-liður 1. mgr. 5. gr. GDPR. Felur það í sér að annað hvort skal eyða gögnum eftir ákveðinn tíma eða gera þau ópersónugreinanleg.

Hjá Árborg er almenna reglan sú að afhendingarskyld skjöl (sem innihalda persónuupplýsingar) séu afhent skjalasafni þegar þau hafa náð 30 ára aldri, sbr. 1. mgr. 15. gr. laga um opinber skjalasöfn nr. 77/2014. Hér þarf að hafa í huga að ekki ber að skila öllum upplýsingum til skjalasafns, heldur þarf einungis að varðveita málsgögn sem varða mál sem er til meðferðar hjá sveitarfélaginu. Mynda þarf ramma um hvaða gögn er nauðsynlegt að afhenda skjalasafni og hvað gögnum má eyða eftir ákveðinn tíma.

Dattaca Labs mun undir formerkjum persónuverndarfulltrúa aðstoða Árborg við að mynda ramma um framangreint málefni.

- ***Vinnslusamningar við vinnsluaðila***

Í greiningarvinnunni kom í ljós að nokkrir aðilar vinna með persónuupplýsingar fyrir hönd Árborgar (vinnsluaðilar). Þegar þjónusta slíks aðila er nýtt verður fullnægjandi vinnslusamningur að vera til staðar, sbr. 3. mgr. 25. gr. pvl. og 3. mgr. 28. gr. GDPR. Ef vinnslusamningur er ekki til staðar er vinnsluaðila óheimilt að vinna með persónuupplýsingar fyrir hönd sveitarfélagsins. Þeir vinnsluaðilar sem um er að ræða eru eftirfarandi:

- OneSystems
- Wise
- InfoMentor.
- TRS
- Google
- Advania
- WordPress
- Kara Connect
- Advania (Vigor)
- Landskerfi bókasafna
- EFLA
- Origo
- LightSpeed
- Sensa
- Síminn

Samningar hafa borist frá eftirfarandi vinnsluaðilum:

- Landskerfi bókasafna
- Advania
- Wise

Mikilvægt er að kalla eftir og ganga frá vinnslusamningum við aðra vinnsluaðila. Áður en gengið er frá vinnslusamningum er mikilvægt að senda þá á Dattaca Labs til yfirferðar.

- ***Stjórnkerfi upplýsingaöryggis***

Samkvæmt 27. gr. pvl. og 32. gr. GDPR þarf sérhver ábyrgðaraðili og vinnsluaðili að grípa til tæknilegra og skipulagslegra öryggisráðstafana til að tryggja öryggi

persónuupplýsinga. Í einföldu máli má segja að tæknilegar og skipulagslegar öryggisráðstafanir feli í sér að koma þurfi á svokölluðu öryggiskerfi („stjórnkerfi upplýsingaöryggis"), sbr. einnig reglur nr. 299/2001 um öryggi persónuupplýsinga. Öryggiskerfi felur í sér að:

- Útbúa skriflega öryggisstefnu, en þar kemur fram afstaða viðkomandi aðila til öryggismála og að ráðstafanir verði viðhafðar til að tryggja öryggi upplýsinga.
- Framkvæma reglulega skriflegt áhættumat. Það felur í sér annars vegar að meta þær afleiðingar sem ófullnægjandi meðferð á persónuupplýsingum getur haft á einstaklinga og hins vegar að meta líkur á því að eitthvað fari úrskeiðis.
- Grípa til öryggisráðstafana á grundvelli áhættumatsins til að koma í veg fyrir að tilteknir hlutir fari úrskeiðis.
- Skrá niður frávik, þ.e. ef tiltekinn atburður gerist sem stofnar öryggi upplýsinga í hættu þá verður að leita uppi ástæður þess og koma í veg fyrir að sambærilegt atvik endurtaki sig.

Stjórnkerfi upplýsingaöryggis var ekki til staðar hjá Árborg og hefur Dattaca Labs aðstoðað sveitarfélagið við að koma því á laggirnar. Upphaflega var fræðsla fyrir starfsmenn haldin og fyrstu skrefin í áhættumati hafa verið tekin. Mikilvægt er að bæta úr þeim veikleikum sem áhættumat á eftir að leiða í ljós með viðeigandi öryggisráðstöfunum.

- ***Mat á áhrifum á persónuvernd***

Í ákveðnum tilfellum þarf að fara fram svokallað mat á áhrifum á persónuvernd. Á það einkum við þegar líklegt er að tiltekin tegund vinnslu geti haft í för með sér mikla áhættu fyrir frelsi og réttindi einstaklinga, sbr. 29. gr. pvl. og 35. gr. GDPR. Dattaca Labs hefur greint út frá vinnsluskránni hvar slíkt mat þarf að fara fram (sjá athugasemdir í vinnsluskrá). Mjög mikilvægt er að framkvæma matið og ganga úr skugga um að öryggisráðstafanir séu til staðar til að lágmarka áhættu fyrir frelsi og réttindi einstaklinga.

- ***Ferlar vegna öryggisbrests***

Þegar persónuupplýsingar glatast, er breytt, eða aðgangur veittur að þeim í leyfisleysi er um öryggisbrest að ræða, sbr. 11. tl. 1. mgr. 3. gr. pvl. og 12. tl. 1. mgr. 4. gr. pvl. Í ákveðnum tilfellum getur verið nauðsynlegt að tilkynna um slíkan brest til Persónuverndar, sérstaklega ef hann felur í sér áhættu fyrir frelsi og réttindi einstaklinga, sbr. 2. mgr. 27. gr. pvl. og 1. mgr. 33. gr. GDPR. Einnig getur eftir atvikum verið nauðsynlegt að tilkynna öryggisbrest til þeirra einstaklinga sem málið varðar, sbr. 3. mgr. 27. gr. pvl. og 1. mgr. 34. gr. pvl.

Til að Árborg geti uppfyllt þessa skyldu verða skilvirkir ferlar að vera til staðar, einkum vegna þess skamma tíma sem sveitarfélagið hefur til að tilkynna öryggisbrest. Öllum starfsmönnum þarf að vera kunnugt um hvað öryggisbrestur er og hvert eigi að tilkynna hann. Dattaca Labs hélt fræðslu fyrir forstöðumenn þar sem ítarlega var farið yfir öryggisbrest og verklag sem þarf að vera til staðar. Sú fræðsla verður endurtekin á næstunni fyrir stjórnendur. Einnig verður haldin sambærileg fræðsla fyrir almenna starfsmenn.

- ***Réttindi einstaklinga***

Einstaklingar njóta mikilla réttinda samkvæmt persónuverndarlögum. Má þarf nefna rétt til upplýsinga, aðgangs, leiðréttingar, eyðingar, takmörkunar, að flytja gögn og að andmæla, sbr. 12. – 21. gr. GDPR. Rétt er að taka fram að réttindi þeirra eru takmörkunum háð og gilda ekki fortakslaust. Ferlar verða þó að vera til staðar ef beiðni kemur frá einstaklingi um að nýta réttindi sín, til dæmis ef beiðni kemur um að hann óski eftir aðgangi að eigin gögnum. Dattaca Labs hélt fræðslu fyrir forstöðumenn þar sem ítarlega var farið yfir réttindi einstaklinga og verklag sem þarf að vera til staðar. Stefnt er að því að endurtaka fræðsluna.

5. Samantekt um það sem á eftir að gera í innleiðingarferlinu

- Samþykkja upplýsingaöryggisstefnu (má birta á heimasíðu í kjölfarið).
- Samþykkja innri persónuverndarstefnu (þarf ekki endilega að birta á heimasíðu).
- Láta starfsmenn undirrita fræðsluskjal, þ.e. um meðferð sveitarfélagsins á þeirra persónuupplýsingum.
- Kalla eftir þeim vinnslusamningum sem ekki hafa borist nú þegar.
- Yfirfara og samþykkja vinnslusamninga.
- Koma á viðeigandi ferlum í tengslum við stjórnkerfi upplýsingaöryggis og öryggisbrest (förum vel í þetta í fræðslunni sem haldin verður fyrir forstöðumenn og starfsmenn).
- Koma á viðeigandi ferlum vegna réttinda einstaklinga (förum vel í þetta í fræðslunni sem verður haldin).
- Setja viðmið um geymslutíma gagna.
- Klára áhættumat.
- Bregðast við niðurstöðum úr áhættumati.
- Framkvæma „mat á áhrifum á persónuvernd“, þar sem við á.

6. Verkþættir Dattaca Labs

- Almennir verkþættir:
  - Persónuverndaryfirlýsing – Lokið
  - Innri persónuverndarstefna – Lokið
  - Fræðsla til forstöðumanna/stjórnenda. *Innbyggð og sjálfgefin persónuvernd* - Lokið
  - Fræðsla til forstöðumanna/stjórnenda. *Áhættumat og öryggisbrestur* - Lokið
  - Fræðsla til forstöðumanna/stjórnenda. *Réttindi einstaklinga* - Lokið
  - Fræðsla til forstöðumanna/stjórnenda. *Persónuverndarfulltrúi* - Lokið
  - Fræðsluskjal til starfsmanna - Lokið
  - Lokaskýrsla - Lokið
- Sértækir verkþættir – Fjármálasvið:
  - Könnun á fylgni – Lokið
  - Listi þar sem úrbóta er þörf – Lokið
  - Fræðsla á eyðublöð – Lokið
  - Yfirferð á vinnslusamningum – Ólokið
  - Niðurstöður kynntar forstöðumönnum/stjórnendum – Lokið
- Sértækir verkþættir – Framkvæmda- og veitusvið:
  - Könnun á fylgni – Lokið
  - Listi þar sem úrbóta er þörf – Lokið
  - Fræðsla á eyðublöð – Lokið
  - Yfirferð á vinnslusamningum – Ólokið
  - Niðurstöður kynntar forstöðumönnum/stjórnendum – Lokið
- Sértækir verkþættir – Félagsþjónusta:
  - Könnun á fylgni – Lokið
  - Listi þar sem úrbóta er þörf – Lokið
  - Fræðsla á eyðublöð – Lokið
  - Yfirferð á vinnslusamningum – Ólokið
  - Niðurstöður kynntar forstöðumönnum/stjórnendum – Lokið
- Sértækir verkþættir – Fræðslusvið:
  - Könnun á fylgni – Lokið
  - Listi þar sem úrbóta er þörf – Lokið
  - Fræðsla á eyðublöð – Lokið
  - Yfirferð á vinnslusamningum – Ólokið
  - Niðurstöður kynntar forstöðumönnum/stjórnendum – Lokið
- Sértækir verkþættir – Menningar- og frístundasvið

  - Könnun á fylgni – Lokið
  - Listi þar sem úrbóta er þörf – Lokið
  - Fræðsla á eyðublöð – Lokið
  - Yfirferð á vinnslusamningum – Ólokið
  - Niðurstöður kynntar forstöðumönnum/stjórnendum – Lokið
- Sértækir verkþættir - Skipulags- og byggingardeild:
  - Könnun á fylgni – Lokið
  - Listi þar sem úrbóta er þörf – Lokið
  - Fræðsla á eyðublöð – Lokið
  - Yfirferð á vinnslusamningum – Ólokið
  - Niðurstöður kynntar forstöðumönnum/stjórnendum – Lokið