Persónuvernd

LEIÐBEININGAR FYRIR VINNSLUAÐILA

1. Almennt

Í persónuverndarreglugerð ESB 2016/679 (pvrg.) eru gerðar sérstakar kröfur til vinnsluaðila sem þeir þurfa að vera meðvitaðir um og fylgja, enda gætu þeir orðið ábyrgir ef til öryggisbrots kemur.

Reglugerðinni er ætlað að auka persónuvernd einstaklinga og gerir hún ríkar kröfur til öryggis persónuupplýsinga hjá öllum ábyrgðar- og vinnsluaðilum, hvort sem þeir eru staðsettir innan EES-svæðisins eða utan þess.

Fjallað er um vinnsluaðila í 28. og 29. gr., 2. mgr. 30. gr., sbr. og 8. mgr. 4. gr. pvrg.

Efnisyfirlit

2. Hver er vinnsluaðili í skilningi persónuverndarreglugerðarinnar?

Vinnsluaðili er sá sem vinnur persónuupplýsingar fyrir, samkvæmt fyrirmælum og undir stjórn ábyrgðaraðila. Ábyrgðaraðili er hins vegar sá sem ákvarðar tilgang og aðferðir við vinnslu.

Margir þjónustuaðilar geta talist vinnsluaðilar í skilningi reglugerðarinnar. Hlutverk vinnsluaðila getur verið mjög misjafnt að umfangi, allt frá nánar tiltekinni vinnslu yfir í almenna og fjölbreytta vinnsluþjónustu fyrir stofnun/fyrirtæki. Þó skal hafa sérstaklega í huga að einstakir starfsmenn ábyrgðaraðila teljast ekki til vinnsluaðila, heldur falla þeir innan mengis ábyrgðaraðilans.

Vinnsluaðilar eru einkum:

- upplýsingatæknifyrirtæki sem veita tölvuþjónustu, s.s. hýsingu, umsjón, viðhald o.fl., netöryggisfyrirtæki eða fyrirtæki sem veita ráðgjöf á sviði upplýsingatækni og hafa aðgang að persónuupplýsingum,
- markaðs- eða samskiptafyrirtæki sem vinna persónuupplýsingar fyrir hönd viðskiptavina,
- hvers konar stofnanir/fyrirtæki sem sinna þjónustu er felur í sér vinnslu persónuupplýsinga fyrir hönd annarra stofnana/fyrirtækja,
- einstök stjórnvöld eða samtök gætu einnig fallið hér undir.

Þeir sem ekki vinna með eða hafa aðgang að persónuupplýsingum, t.a.m. útgefendur hugbúnaðar og framleiðendur tækja (t.d. lækningatækja), teljast almennt ekki til vinnsluaðila samkvæmt reglugerðinni.

Athuga skal þó að:

- stofnun/fyrirtæki sem er vinnsluaðili er hins vegar ábyrgðaraðili fyrir vinnslu þegar vinnslan er í þágu þeirrar tilteknu stofnunar/fyrirtækis en ekki fyrir viðskiptavini (stofnunin/fyrirtækið sér um sín verkefni sjálft).
- Þegar stofnun/fyrirtæki ákveður tilgang og aðferð við vinnslu er sá aðili ekki talinn vinnsluaðili heldur ábyrgðaraðili að því er varðar þá vinnslu, sbr. 10. mgr. 28. gr. pvrg.

Dæmi um mismunandi hlutverk vinnsluaðila og ábyrgðaraðila

Fyrirtæki A veitir fyrirtæki B þá þjónustu að senda bréf í markaðssetningartilgangi þar sem byggt er á upplýsingum um viðskiptavini B.

A er vinnsluaðili fyrir B svo framarlega sem vinnsla umræddra viðskiptamannaupplýsinga B er nauðsynleg til að senda bréfin fyrir hönd fyrirtækis B eða samkvæmt fyrirmælum þess.

Fyrirtæki B er ábyrgðaraðili vegna vinnslu persónuupplýsinga um viðskiptamannahópinn með tilliti til markaðssetningarbréfsins.

Hins vegar er fyrirtæki A ábyrgðaraðili að vinnslu persónuupplýsinga um eigin starfsmenn.

Til að meta hver er vinnsluaðili og hver er ábyrgðaraðili í hverju tilviki þarf að líta til eftirfarandi atriða:

- Hvaða áhrif hefur þjónustuaðilinn á þjónustuna?
- Hvernig er eftirliti viðskiptavinarins með umræddri þjónustu háttað?
- Hefur þjónustuaðilinn sérþekkingu á umræddu sviði?
- Þekkja skráðir einstaklingar, sem nýta þjónustu viðskiptavinarins, þjónustuaðilann?

Sjá nánar 4. gr. og 10. mgr. 28. gr. pvrg.

3. Nær persónuverndarreglugerðin til vinnsluaðila?

Persónuverndarreglugerðin gildir um vinnsluaðila í eftirfarandi tilvikum:

- ef þeir eru með staðfestu innan EES
- ef þeir eru með staðfestu utan EES og vinnslan felst í:
    - boði um vöru eða þjónustu innan EES, eða
    - eftirliti með einstaklingum innan EES.

Sjá nánar 3. gr. pvrg. um gildissvæði.

4. Hverjar eru meginbreytingarnar gagnvart vinnsluaðilum samkvæmt nýrri persónuverndarreglugerð?

Staðan í dag:

Í dag eru fyrst og fremst gerðar kröfur til ábyrgðaraðila við vinnslu persónuupplýsinga. Þar sem vinnsluaðilar koma að vinnslu starfa þeir fyrst og fremst á ábyrgð ábyrgðaraðila.

Samkvæmt gildandi persónuverndarlögum í dag, þ.e. lögum nr. 77/2000 um persónuvernd og meðferð persónuupplýsinga, er ábyrgðaraðila heimilt að semja við vinnsluaðila til að annast, í heild eða hluta, þá vinnslu persónuupplýsinga sem hann ber ábyrgð á. Það er þó háð því skilyrði að ábyrgðaraðili hafi áður *sannreynt* að umræddur vinnsluaðili geti framkvæmt viðeigandi öryggisráðstafanir og viðhaft innra eftirlit.

Þá gera lög nr. 77/2000 kröfu um að í gildi sé samningur milli vinnsluaðila og ábyrgðaraðila, þ.e. svokallaður vinnslusamningur. Í vinnslusamningi skuli m.a. koma fram að vinnsluaðila sé einungis heimilt að starfa í samræmi við fyrirmæli ábyrgðaraðila og að ákvæði laganna um skyldur ábyrgðaraðila gildi einnig um þá vinnslu sem vinnsluaðili annist.

Frá því að nýja löggjöfin kemur til framkvæmda 25. maí 2018:

Persónuverndarreglugerðin festir í sessi nýja meginreglu við vinnslu persónuupplýsinga, þ.e. *ábyrgðarskyldu*, en í henni felst að allir þeir sem koma að vinnslu persónuupplýsinga bera ábyrgð á að farið sé að reglunum og þurfa að geta sýnt fram á það bæði gagnvart Persónuvernd og hinum skráðu frá þeirri stundu er slík vinnsla varðar einstaklinga sem staðsettir eru innan EES.

Ábyrgðarskyldan felur enn fremur í sér að sérstakar skyldur eru lagðar á vinnsluaðila. Til að mynda eiga þeir að aðstoða ábyrgðaraðila sérstaklega í að tryggja að vinnsla þeirra uppfylli og sé í samræmi við reglugerðina.

Sjá nánar 28. gr., 2. mgr. 30. gr. og 37. gr. pvrg. um skyldur vinnsluaðila.

5. Hverjar eru skyldur vinnsluaðila frá 25. maí 2018?

Þegar vinnsluaðili tekur að sér verkefni sem felur í sér vinnslu persónuupplýsinga f.h. ábyrgðaraðila verður hann að veita ábyrgðaraðila/viðskiptavininum nægilegar tryggingar fyrir því að hann geri viðeigandi tæknilegar og skipulagslegar ráðstafanir til að vinnslan uppfylli kröfur reglugerðarinnar og að vernd hins skráða sé tryggð. (Sjá nánar 28. gr. pvrg.)

Vinnsluaðilinn getur þurft að aðstoða og ráðleggja viðskiptavinum/ábyrgðaraðilanum um hvernig uppfylla eigi tilteknar skyldur sem á honum hvíla (hér er t.d. átt við skyldur um mat á áhrifum á persónuvernd, tilkynningu um öryggisbrest, öryggi, eyðingu gagna og framlag til úttekta).

Í framkvæmd þýðir þetta eftirfandi:

5.1 Gagnsæi og rekjanleiki

Vinnsluaðili verður að:

- gera vinnslusamning við viðskiptavininn/ábyrgðaraðilann eða annað lögformlegt skjal þar sem skyldur og hlutverk hvors aðila fyrir sig koma fram, sbr. fyrirmæli í 28. gr. reglugerðarinnar.
- gera skriflegan lista yfir fyrirmæli viðskiptavinarins/ábyrgðaraðilans um vinnslu persónuupplýsinga til að sanna að unnið sé samkvæmt skriflegum fyrirmælum ábyrgðaraðilans.
- fá skriflegt leyfi viðskiptavinar/ábyrgðaraðila ef vinnsluaðilinn ræður annan vinnsluaðila/undirverktaka, t.d. erlendan hýsingaraðila (tölvuskýjaþjónustu).
- veita viðskiptavininum/ábyrgðaraðilanum allar nauðsynlegar upplýsingar til að sýna fram á reglufylgni og gefa honum kost á úttekt til eftirlits.
- halda vinnsluskrá skv. 2. mgr. 30. gr. reglugerðarinnar og tiltaka hvaða vinnslustarfsemi er framkvæmd fyrir hvern og einn ábyrgðaraðila.

5.2 Huga þarf að innbyggðri og sjálfgefinni persónuvernd

Vinnsluaðili skal gera viðeigandi tæknilegar og skipulagslegar ráðstafanir til að tryggja að vinnslan sem framkvæmd er fyrir hönd viðskiptavinarins/ábyrgðaraðilans uppfylli kröfur reglugerðarinnar og að vernd skráðra einstaklinga sé tryggð. Það þýðir:

- að persónuvernd þarf að vera innbyggð (e. data protection by design), þ.e að tækin, framleiðslan, hugbúnaður eða þjónusta sem vinnsluaðili veitir viðskiptavininum taki mið af meginreglum um persónuvernd með skilvirkum hætti og að nauðsynlegar verndarráðstafanir séu felldar inn í vinnsluna til að uppfylla kröfur reglugerðarinnar og tryggja réttindi einstaklinga, og
- að persónuvernd þarf að vera sjálfgefin (e. data protection by default), þ.e. að tæki, framleiðsla, hugbúnaður eða þjónusta vinnsluaðila tryggi að einungis þær persónuupplýsingar séu unnar sem nauðsynlegar eru vegna vinnslunnar, með tilliti til þess hversu miklum upplýsingum er safnað, að hvað marki er unnið með þær, hversu lengi þær eru varðveittar og fjölda þeirra sem hafa aðgang að þeim.

Þetta felur í sér:

- að viðskiptavinurinn hafi kost á því að stilla kerfi, a.m.k. hvað varðar söfnun upplýsinga, og að ekki sé gert að tæknilegu skilyrði að fyllt sé út í reiti sem eingöngu eru valkvæðir, t.d. við innslátt kennitölu í verslunarkerfi,
- að það sé sjálfgefið að einungis sé unnið með þær persónuupplýsingar sem eru nauðsynlegar vegna tilgangs vinnslunnar (lágmörkun gagna),
- að virkir gagnagrunnar séu með sjálfvirkum eða handunnum hætti hreinsaðir í lok tilgreinds tímabils,
- að hafa virka aðgangsstýringu ásamt því að persónuupplýsingar séu tiltækar þegar hinn skráði óskar eftir aðgangi að upplýsingum.

5.3 Vinnsluaðili þarf að tryggja öryggi persónuupplýsinga

- Vinnsluaðili þarf að tryggja að starfsmenn sem koma að vinnslu persónuupplýsinga hjá honum hafi undirritað trúnaðaryfirlýsingu eða heyri undir lögboðna trúnaðarskyldu.
- Vinnsluaðli þarf að tilkynna viðskiptavininum/ábyrgðaraðilanum um öryggisbrot um leið og hann verður þeirra var.
- Vinnsluaðili þarf að tryggja að öryggi sé í samræmi við áhættu, t.a.m. með gerð áhættumats og ákvörðun öryggisráðstafana.
- Vinnsluaðili þarf, við lok þjónustunnar/efndir samningsins og í samræmi við fyrirmæli viðskiptavinarins/ábyrgðaraðilans:
    - að eyða persónuupplýsingum eða skila þeim til viðskiptavinarins, nema skylt sé að geyma upplýsingarnar lögum samkvæmt, og
    - að eyða afritum nema skylt sé að geyma þau lögum samkvæmt.

5.4 Skylt er að aðstoða, vekja athygli á og ráðleggja

- Telji vinnsluaðili að fyrirmæli viðskiptavinarins/ábyrgðaraðilans brjóti í bága við reglur um persónuvernd ber honum að upplýsa ábyrgðaraðilann um það án tafar.

- Þegar hinir skráðu óska eftir að neyta réttinda sinna samkvæmt reglugerðinni (t.d. með því að óska eftir aðgangi að persónuupplýsingum, leiðréttingu þeirra, eyðingu eða flutningi, eða með því að andmæla vinnslu, eða neyta réttinda sinna í tengslum við sjálfvirka ákvarðanatöku, þ.m.t. notkun persónusniða) á vinnsluaðili að aðstoða viðskiptavininn/ábyrgðaraðilann eins og hægt er.
- Með hliðsjón af þeim upplýsingum sem eru á forræði vinnsluaðila verður hann að aðstoða viðskiptavininn/ábyrgðaraðilann í að tryggja reglufylgni, t.d. með því að tryggja öryggi vinnslu, tilkynna um öryggisbrot og gera mat á áhrifum á persónuvernd.

6. Hvar eiga vinnsluaðilar að byrja?

6.1 Athuga hvort vinnsluaðili þurfi að tilnefna persónuverndarfulltrúa

Hlutverk persónuverndarfulltrúa er að hafa umsjón með að persónuverndarlöggjöfinni sé fylgt hjá viðkomandi stofnun/fyrirtæki. Vinnsluaðilar þurfa að tilnefna persónuverndarfulltrúa þegar:

- þeir eru stjórnvald
- meginstarfsemi vinnsluaðila lýtur að vinnsluaðgerðum f.h. viðskiptavinarins/ábyrgðaraðilans sem fela í sér umfangsmikið, reglubundið og kerfisbundið eftirlit með einstaklingum.
- meginstarfsemi vinnsluaðila er umfangsmikil vinnsla, f.h. viðskiptavinarins/ábyrgðaraðilans, á viðkvæmum persónuupplýsingum eða persónuupplýsingum er varða sakfellingar í refsimálum og refsiverð brot.

Í þeim tilvikum þar sem ekki er beinlínis skylt, skv. framangreindu, að tilnefna persónuverndarfulltrúa er engu að síður mælt með því að hann sé skipaður þannig að fyrirtækið hafi yfir að ráða sérfræðingi sem heldur utan um innleiðingu og eftirfylgni með að ákvæði reglugerðarinnar séu uppfyllt.

Dæmi 1

Lítið fjölskyldufyrirtæki selur heimilistæki í litlum bæ og notar þjónustu vinnsluaðila. Meginstarfsemi vinnsluaðilans er að veita þjónustu við greiningu á vefsíðu fjölskyldufyrirtækisins og aðstoð við að finna markhópa fyrir auglýsingar. Starfsemi fjölskyldufyrirtækisins felur ekki í sér umfangsmikla vinnslu persónuupplýsinga um viðskiptavini, í ljósi þess hve fáir viðskiptavinirnir eru og þess að fyrirtækið er með mjög afmarkaða starfsemi. Á hinn bóginn telst vinnsla persónuupplýsinga hjá vinnsluaðilanum, sem er með marga viðskiptavini eins og þetta litla fyrirtæki, vera umfangsmikil. Vinnsluaðilinn þarf því að tilnefna persónuverndarfulltrúa skv. b-lið 1. mgr. 37. gr. persónuverndarreglugerðarinnar. Hins vegar er litla fjölskyldufyrirtækinu ekki skylt að tilnefna persónuverndarfulltrúa.

Dæmi 2

Meðalstórt framleiðslufyrirtæki semur við utanaðkomandi vinnsluaðila um að sinna heilbrigðisþjónustu við starfsmenn. Vinnsluaðilinn er með marga sambærilega viðskiptavini. Vinnsluaðilinn þarf að tilnefna persónuverndarfulltrúa, skv. c-lið 1. mgr. 37. gr. pvrg., ef vinnslan er umfangsmikil. Framleiðslufyrirtækinu er það hins vegar ekki skylt.

Ef persónuverndarfulltrúi er tilnefndur hefur hann einnig eftirlit með annarri vinnslu vinnsluaðilans á persónuupplýsingum.

Sjá nánar 37. gr. pvrg. um skyldu vinnsluaðila til að tilnefna persónuverndarfulltrúa.

6.2 Greining og endurskoðun vinnslusamninga

Vinnslusamningur þarf að taka á eftirfarandi atriðum:

- viðfangsefni og tímalengd vinnslunnar,
- eðli og tilgangi vinnslunnar,
- tegund þeirra persónuupplýsinga sem unnar eru f.h. viðskiptavinarins,
- flokkum hinna skráðu,
- réttindum og skyldum viðskiptavinarins sem ábyrgðaraðila,
- skyldum vinnsluaðila skv. 28. gr. pvrg.

Í kafla 14 má finna fyrirmynd að ákvæðum sem eiga heima í vinnslusamningi, samkvæmt 8. mgr. 28. gr. pvrg. Hafa þarf í huga að vinnslusamningar verða engu að síður að vera sérsniðnir að þeirri vinnslu sem um ræðir.

Sjá nánar um efni vinnslusamninga í 28. gr. pvrg.

6.3 Skrá yfir vinnslustarfsemi

Vinnsluaðili þarf að halda skrá yfir vinnslustarfsemi sem fer fram hjá honum f.h. viðskiptavinarins/ábyrgðaraðilans.

Skráin þarf að vera skrifleg og innihalda:

- heiti og samskiptaupplýsingar hvers viðskiptavinar og eftir atvikum sameiginlegra ábyrgðaraðila,
- heiti og samskiptaupplýsingar undirvinnsluaðila, þar sem það á við,
- heiti og samskiptaupplýsingar persónuverndarfulltrúa,
- upplýsingar um flokka skráðra einstaklinga,
- upplýsingar um flutning persónuupplýsinga út fyrir EES-svæðið sem vinnsluaðila er falið að framkvæma, ef við á,
- lýsingu á tæknilegum og skipulagslegum öryggisráðstöfunum sem vinnsluaðili hefur framkvæmt, ef mögulegt er.

Það athugast að þar sem vinnsluaðili er jafnframt ábyrgðaraðili hvað varðar hans eigin starfsemi þarf hann einnig að halda skrá yfir þá vinnslustarfsemi sem hann er ábyrgðaraðili að, t.d. vegna vinnslu persónuupplýsinga um eigin starfsmenn eða viðskiptavini/ábyrgðaraðila. Hann getur því þurft að halda tvær vinnsluskrár. Sjá 2. (og 1. mgr.) 30. gr. pvrg. um skrá yfir vinnslustarfsemi.

Nánari upplýsingar um gerð skrár yfir vinnslustarfsemi má finna í væntanlegum leiðbeiningum Persónuverndar um það efni.

7. Hverjar eru skyldur vinnsluaðila ef hann ræður annan vinnsluaðila/undirvinnsluaðila?

Undirvinnsluaðilar eru gjarnan notaðir af vinnsluaðilum til að sinna tilteknum hluta vinnslustarfseminnar. Hér getur t.a.m. verið um að ræða tölvuskýjaþjónustu sem veitt er af þriðja aðila eða önnur mjög sérhæfð tölvuþjónusta sem upphaflegi vinnsluaðilinn býr ekki yfir.

Vinnsluaðili getur einungis ráðið annan vinnsluaðila/undirvinnsluaðila ef viðskiptavinurinn/ábyrgðaraðilinn samþykkir það skriflega. Samþykkið getur verið með tvennum hætti:

- Sérstakt samþykki: Vegna ráðningar/samningsgerðar við tiltekinn vinnsluaðila.
- Almennt samþykki: Getur tekið til hvers konar notkunar á undirvinnsluaðila. Ef notast er við almennt samþykki þarf vinnsluaðili að tilkynna viðskiptavininum/ábyrgðaraðilanum um allar fyrirhugaðar breytingar er fela í sér að bætt er við vinnsluaðila eða honum skipt út og gefa þannig viðskiptavininum/ábyrgðaraðilanum tækifæri á að andmæla breytingunum.

Undirvinnsluaðili sem er ráðinn af öðrum vinnsluaðila þarf að uppfylla sömu kröfur og gerðar eru til upphaflegs vinnsluaðila í samningi hans við viðskiptavininn/ábyrgðaraðilann. Hann þarf að veita nægilegar tryggingar fyrir því að hann geri tæknilegar og skipulagslegar ráðstafanir til að vinnsla persónuupplýsinga uppfylli kröfur reglugerðarinnar.

Athygli er vakin á því að ef undirvinnsluaðilinn uppfyllir ekki skyldur sínar er upphaflegi vinnsluaðilinn að fullu ábyrgur gagnvart viðskiptavininum/ábyrgðaraðilanum.

Sjá nánar um ráðningu undirvinnsluaðila í 2. og 4. mgr. 28. gr. pvrg.

8. Þarf vinnsluaðili að endurskoða gildandi samninga við viðskiptavini?

Já - þegar reglugerðin kemur til framkvæmda þurfa allir gildandi samningar, hvort sem þeir eru við ábyrgðaraðila eða undirvinnsluaðila, að uppfylla þær kröfur sem reglugerðin gerir til slíkra samninga.

Það er því mjög mikilvægt að vinnsluaðilar hefji strax vinnu við að endurskoða vinnslusamninga sína við ábyrgðaraðila þannig að tiltekin ákvæði gildi frá því að reglugerðin öðlast lagagildi hér á landi, en fyrirhugað er að það verði 25. maí 2018.

Frá þeim degi þegar löggjöfin kemur til framkvæmda þurfa vinnsluaðilar að viðhafa reglubundið eftirlit og endurskoðun til að tryggja reglufylgni í samræmi við ákvæði reglugerðarinnar um skyldur vinnsluaðila og gera nauðsynlegar lagfæringar ef þarf.

9. Hvert er hlutverk vinnsluaðila ef það verður öryggisbrot?

Öryggisbrot þýðir brot á öryggi sem leiðir til óviljandi eða ólögmætrar eyðingar persónuupplýsinga, sem eru sendar, varðveittar eða unnar á annan hátt, eða að þær glatist, breytist, séu birtar eða aðgangur veittur að þeim í leyfisleysi.

Vinnsluaðili skal tilkynna viðskiptavini/ábyrgðaraðila sínum um það án tafar þegar hann verður var við öryggisbrot sem varðar vernd persónuupplýsinga.

Á grundvelli þessarar tilkynningar skal viðskiptavinurinn, sem ábyrgðaraðili, tilkynna Persónuvernd (og ef við á, öðrum persónuverndaryfirvöldum innan EES) um öryggisbrotið skv. 33. gr. pvrg. og, ef við á, hinum skráðu einstaklingum skv. 34. gr. pvrg.

Viðskiptavinurinn/ábyrgðaraðilinn getur falið vinnsluaðila, í samningi þeirra á milli, að sjá um tilkynningar fyrir sína hönd.

Sjá nánar 12. mgr. 4. gr., 33. og 34. gr. pvrg.

10. Hvert er hlutverk vinnsluaðila við mat á áhrifum á persónuvernd (MÁP)?

Viðskiptavinur vinnsluaðila, sem ábyrgðaraðili, getur þurft að meta áhrif á persónuvernd vegna fyrirhugaðar vinnslu persónuupplýsinga skv. 35. gr. pvrg. Það er því ekki hlutverk vinnsluaðila að vinna slíkt mat. Vinnsluaðilinn hefur hins vegar það hlutverk að aðstoða viðskiptavininn/ábyrgðaraðilann við matið og útvega nauðsynlegar upplýsingar. Þetta hlutverk vinnsluaðila þarf að vera skilgreint í samningi á milli vinnsluaðilans og viðskiptavinarins/ábyrgðaraðilans.

Sjá nánar 3. mgr. 28. gr. pvrg.

11. Getur vinnsluaðili nýtt sér regluna um einn afgreiðslustað (e. one stop shop)?

Já, ef vinnsluaðili er með staðfestu í fleiri en einu ríki innan EES kemur reglan um einn afgreiðslustað að góðum notum.

Reglan um einn afgreiðslustað gefur fyrirtækjum, sem starfa í fleiri en einu ríki innan EES, möguleika á að leita til einnar persónuverndarstofnunar sem tekur ákvarðanir er varða allar vinnslustöðvarnar og gildir sú ákvörðun þá einnig í öðrum ríkjum. Þessi stofnun kallast forystueftirlitsyfirvald.

Forystueftirlitsyfirvaldið er persónuverndarstofnunin í því landi þar sem höfuðstöðvar fyrirtækisins eru staðsettar.

Ef fyrirtækið hefur engar höfuðstöðvar innan EES skal miða við þann stað þar sem meginvinnslustarfsemi þess fer fram.

Sjá nánar 16. mgr. 4. gr., 56. gr. og formálsorð 36 í reglugerðinni, svo og leiðbeiningar 29. gr. vinnuhópsins um hvaða stofnun er forystueftirlitsyfirvald vinnsluaðila eða ábyrgðaraðila og einnig væntanlegar leiðbeiningar Persónuverndar um það efni.

12. Hvaða kröfur eru gerðar til vinnsluaðila sem er staðsettur utan EES?

Vinnsluaðili sem er ekki með staðfestu innan EES getur fallið undir persónuverndarreglugerðina ef:

- vinnslan sem unnin er varðar skráða einstaklinga sem staðsettir eru innan EES

- vinnsluaðilinn f.h. ábyrgðaraðila, selur vörur veitir eða hefur eftirlit með skráðum einstaklingum innan EES.

Í þessum tilvikum þarf vinnsluaðilinn að tilnefna fulltrúa innan EES sem tengilið við skráða einstaklinga og persónuverndarstofnanir og til að svara fyrir vinnslu persónuupplýsinga hjá fyrirtækinu.

Sjá nánar 3. og 27. gr. pvrg.

13. Hver er áhættan ef vinnsluaðili uppfyllir ekki skyldur sínar skv. reglugerðinni?

Sá sem hefur orðið fyrir tjóni (efnislegu eða óefnislegu) vegna brots á ákvæðum reglugerðarinnar skal eiga rétt á skaðabótum frá ábyrgðaraðila eða vinnsluaðila fyrir það tjón sem hann hefur orðið fyrir.

Ef vinnsluaðili brýtur gegn ákvæðum reglugerðarinnar geta persónuverndarstofnanir lagt á viðkomandi sekt sem nemur allt að 2% eða 4% af árlegri heildarveltu fyrirtækis á heimsmarkaði eða allt að 10 eða 20 milljónum evra, hvort sem er hærra. Fjárhæð sekta fer eftir alvarleika brots. Stjórnvaldssektir kunna til dæmis að verða lagðar á fyrirtæki við eftirfarandi aðstæður:

- Ef vinnsluaðili fer út fyrir lögmæt fyrirmæli viðskiptavinarins/ábyrgðaraðilans eða aðhefst eitthvað í trássi við gefin fyrirmæli ábyrgðaraðila
- Ef vinnsluaðili aðstoðar ekki viðskiptavininn/ábyrgðaraðilann við að uppfylla skyldur sínar, t.d. vegna öryggisbrots eða við mat á áhættu á persónuvernd
- Ef vinnsluaðili veitir viðskiptavininum/ábyrgðaraðilanum ekki upplýsingar til að sýna fram á reglufylgni eða gerir ábyrgðaraðila ekki kleift að taka út starfsemina
- Ef vinnsluaðili upplýsir viðskiptavininn/ábyrgðaraðilann ekki um að fyrirmæli séu ekki í samræmi við ákvæði persónuverndarreglugerðarinnar
- Ef vinnsluaðili ræður undirvinnsluaðila án leyfis viðskiptavinarins/ábyrgðaraðilans
- Ef undirvinnsluaðili uppfyllir ekki kröfur um nægilegt öryggi
- Ef vinnsluaðili tilnefnir ekki persónuverndarfulltrúa þegar þess er krafist
- Ef vinnsluaðili heldur ekki skrá yfir vinnslustarfsemi sem fram fer á ábyrgð hans.

Sjá nánar 82. og 83. gr. pvrg., leiðbeiningar 29. gr. hópsins um stjórnvaldssektir og væntanlegar leiðbeiningar Persónuverndar um sama efni.

14. Fordæmi fyrir föstum samningsákvæðum í vinnslusamningum

Vinsamlegast athugið að hér er eingöngu um að ræða framsetningu í dæmaskyni. Vinnsluaðili þarf ávallt að gæta að því að ákvæðin endurspegli þá vinnslu persónuupplýsinga sem honum er falin. Af hálfu Persónuverndar er fyrirhugað að taka upp föst samningsákvæði í vinnslusamningum í samræmi við 8. mgr. 28. gr. pvrg. og eru ábyrgðaraðilar og vinnsluaðilar því hvattir til að fylgjast með á vefsíðu Persónuverndar hvað það varðar.

Fordæmi:

[Heiti fyrirtækis], með staðfestu á/í [land], hér eftir nefndur „ábyrgðaraðili“

OG

[Heiti fyrirtækis], með staðfestu á/í [land], hér eftir nefndur „vinnsluaðili“

gera með sér svofelldan vinnslusamning, í samræmi við 28. gr. reglugerðar Evrópuþingsins og ráðsins (ESB) 2016/679 frá 27. apríl 2016:

I. Tilgangur samnings

Tilgangur þessara samningsákvæða er að tilgreina þær skyldur sem vinnsluaðili sinnir f.h. ábyrgðaraðila, í tengslum við þá vinnslustarfsemi sem samningurinn tekur til, sjá nánar í kafla [...]

Samningsaðilar skulu bundnir af öllum viðeigandi lagaákvæðum sem varða vinnslu persónuupplýsinga hjá þeim og þá sérstaklega reglugerð Evrópuþingsins og ráðsins (ESB) 2016/679, frá 27. apríl 2016, um vernd einstaklinga í tengslum við vinnslu persónuupplýsinga og um frjálsa miðlun slíkra upplýsinga og niðurfellingu tilskipunar 95/46/EB (almennu persónuverndarreglugerðinni) sem kemur/kom til framkvæmda 25. maí 2018.

II. Lýsing á þeirri vinnslu sem samið er um að vinnsluaðili sinni (undirvinnsluaðili, ef það á við)

Vinnsluaðila er heimilt að vinna, f.h. ábyrgðaraðila, þær persónuupplýsingar sem eru honum nauðsynlegar til að veita eftirfarandi þjónustu [hér skal lista upp þá þjónustu sem vinnsluaðili skal veita]

Eðli þeirrar vinnslustarfsemi sem hér um ræðir er [...]

Tilgangur vinnslunar er [...]

Vinnsluðaðila er heimilt að vinna með eftirfarandi tegundir persónuupplýsinga: [...]

Vinnsluaðila er heimilt að vinna með eftirfarandi flokka af skráðum einstaklingum: [...]

Til að vinnsluaðili geti veitt umbeðna þjónustu, skal ábyrgðaraðili veita vinnsluaðila eftirfarandi upplýsingar: [...]

III. Gildistími samnings

Samningur þessi gildir frá [dags.] til [dags].

IV. Skyldur vinnsluaðila gagnvart ábyrgðaraðila

Vinnsluaðili skal:

1. eingöngu vinna persónuupplýsingar í samræmi við tilgang vinnslunnar, skv. samningi þessum
2. eingöngu vinna persónuupplýsingar samkvæmt skriflegum fyrimælum ábyrgðaraðila, sem fylgja samningi þessum. Í þeim tilvikum þegar vinnsluaðili telur að fyrirmæli ábyrgðaraðila samrýmist ekki almennu persónuverndarreglugerðinni eða öðrum

viðeigandi lagaákvæðum sem varða vinnslu persónuupplýsinga ber honum að tilkynna ábyrgðaraðilanum slíkt án tafar. Þá skal vinnsluaðili gera ábyrgðaraðila viðvart ef vinnsluaðila er skylt samkvæmt lögum að flytja persónupplýsingar til þriðju landa eða alþjóðastofnana, nema lög banni að upplýst sé um slíkt.

3. tryggja trúnað um vinnslu þeirra persónuupplýsinga sem þessi samningur tekur til, og
4. tryggja að þeir starfsmenn sem hafi aðgang að persónuupplýsingum í tengslum við framkvæmd samningsins hafi undirritað trúnaðaryfirlýsingu eða séu bundnir þagnarskyldu samkvæmt lögum og að þeir fái viðeigandi þjálfun í vernd persónuupplýsinga.
5. gæta þess að tæki og tól, vörur, forrit og þjónusta séu hönnuð með innbyggða og sjálfgefna persónuvernd að leiðarljósi.

6. Notkun á undirvinnsluaðila

Leið A (almennt samþykki): Vinnsluaðila er heimilt að semja við annan aðila („undirvinnsluaðila“) um að framkvæma tilteknar vinnsluaðgerðir. Áður en ætlaðar breytingar taka gildi, bæði þegar bætt er við undirvinnsluaðila og þegar gerðar eru breytingar á þeim undirvinnsluaðilum sem þegar eru notaðir, eða þegar um að ræða viðbætur eða breytingu á gildandi fyrirkomulagi vinnsluaðgerða, skal vinnsluaðili upplýsa ábyrgðaraðila skriflega um breytingarnar. Þar skal sérstaklega taka fram hvaða vinnsluaðgerðir undirvinnsluaðilinn hyggst taka að sér, nafn og samskiptaupplýsingar undirvinnsluaðilans ásamt dagsetningu samnings. Ábyrgðaraðili hefur [x daga/mánuði] frá þeim degi sem hann móttekur upplýsingar um breytingu á notkun á undirvinnsluaðila til að andmæla því. Notkun á undirvinnsluaðila er eingöngu heimil þegar ábyrgðaraðili hefur ekki andmælt því innan tímamarkanna.

Leið B (sérstakt samþykki): Vinnsluaðila er heimilt að nota þjónustu [heiti fyrirtækis], hér eftir „undirvinnsluaðila“, til að framkvæma eftirfarandi vinnsluaðgerðir: [...]

Þegar vinnsluaðili ætlar að nýta sér þjónustu undirvinnsluaðila, þá er honum skylt að afla sérstaks, skriflegs samþykkis frá ábyrgðaraðila, áður en gengið er til samninga við undirvinnsluaðilann.

7. Réttur hinna skráðu til upplýsinga.

Hér er hægt að velja milli tveggja kosta:

A) Ábyrgðaraðili ber ábyrgð á því að veita hinum skráðu upplýsingar (fræðslu) um vinnslustarfsemina fyrir eða um leið og vinnsla hefst, í samræmi við ákvæði almennu persónuverndarreglugerðarinnar um upplýsingar sem ber að veita hinum skráða, sbr. m.a. 13. og 14. gr. hennar.

B) Vinnsluaðili veiti hinum skráðu upplýsingar um vinnslustarfsemina þegar persónuupplýsinga er aflað, til samræmis við ákvæði almennu persónuverndarreglugerðarinnar um upplýsingar sem ber að veita hinum skráða, sbr. m.a. 13. og 14. gr. hennar. Ábyrgðaraðili þarf að samþykkja þá fræðslu sem veitt er og form hennar áður en vinnsla persónuupplýsinga hefst.

8. Veiting réttinda til handa hinum skráðu

Að því marki sem hægt er ber vinnsluaðila að aðstoða ábyrgðaraðila við að sinna þeirri skyldu sinni að bregðast við erindum skráðra einstaklinga vegna réttinda þeirra, svo

sem vegna aðgangsréttar, réttar til leiðréttingar og eyðingar upplýsinga og til að andmæla vinnslu eða takmarka hana, flutningsréttar og réttar til að þurfa ekki að sæta sjálfvirkri ákvarðanataöku, þ.m.t. notkun persónusniða. Hér er hægt að velja á milli tveggja kosta:

A) Þegar hinn skráði leggur fram beiðni um að neyta réttinda sinna hjá vinnsluaðila skal vinnsluaðilinn áframsenda slíka beiðni án tafar til [nafn/staða starfsmanns hjá ábyrgðaraðila].

B) Vinnsluaðili skuldbindur sig til að svara beiðnum hinna skráðu um að neyta réttinda sinna hvað varðar þær persónuupplýsingar sem samningur þessi lýtur að. Vinnsluaðili skal svara umræddum beiðnum í nafni og f.h. ábyrgðaraðila og innan þeirra tímamarka sem almenna persónuverndarreglugerðin gerir kröfu um.

9. Tilkynning vegna öryggisbrots

Vinnsluaðili skal tilkynna ábyrgðaraðila [með símtali, tölvupósti eða öðrum leiðum] um hvers konar öryggisbrot eigi síðar en [...] klukkustundum eftir að hann verður var við brotið. Með tilkynningunni skulu fylgja hver þau skjöl eða gögn sem nauðsynleg eru til þess að ábyrgðaraðili geti tilkynnt um brotið til viðeigandi eftirlitsstofnunar (Persónuverndar).

[VALKVÆTT:

Ábyrgðaraðili getur falið vinnsluaðila að tilkynna fyrir hans hönd um öryggisbrot til viðeigandi eftirlitsyfirvalds, sbr. 33. gr. almennu persónuverndarreglugerðarinnar, án ótilhlýðilegrar tafar, og, ef mögulegt er, eigi síðar en 72 klst. eftir að hann verður brotsins var, nema ólíklegt þyki að brotið leiði til áhættu fyrir réttindi og frelsi einstaklinga. Sé eftirlitsvaldinu ekki tilkynnt um brotið innan 72 klst. skulu ástæður fyrir töfinni fylgja tilkynningunni. Tilkynningin skal í það minnsta innihalda upplýsingar um:

- eðli öryggisbrotsins, þ.m.t., þegar það á við, um flokka og gróflega áætluðan fjölda þeirra einstaklinga sem verða fyrir áhrifum af brotinu, og flokka og magn þeirra gagna (e. records) sem um ræðir,
- nafn og samskiptaupplýsingar persónuverndarfulltrúa eða annars tengiliðar þar sem hægt er að nálgast frekari upplýsingar,
- hverjar séu líklegar afleiðingar öryggisbrotsins,
- til hvaða aðgerða hafi verið gripið eða lagt til að gripið verði til til að bregðast við brotinu, þ.m.t., þar sem það á við, aðgerða til að draga úr áhrifum brotsins á einstaklinga.

Þegar ekki er hægt að veita allar upplýsingar strax er hægt að miðla þeim áfram í nokkrum skrefum. Skal það gert án tafar.

Ábyrgðaraðili getur einnig samþykkt að vinnsluaðili upplýsi, f.h. ábyrgðaraðilans, hina skráðu um öryggisbrotið án tafar þegar brotið er líklegt til að hafa áhrif á réttindi og frelsi einstaklinga.]

Upplýsingar sem sendar eru hinum skráðu skulu vera á skýru og einföldu máli og lýsa í það minnsta:

- eðli öryggisbrotsins, þ.m.t., þegar það á við, flokkum og gróflega áætluðum fjölda þeirra einstaklinga sem verða fyrir áhrifum af brotinu og flokkum og magni þeirra gagna (e. records) sem um ræðir,
- nafni og samskiptaupplýsingum persónuverndarfulltrúa eða annars tengiliðar þar sem hægt er að nálgast frekari upplýsingar,
- hverjar séu líklegar afleiðingar öryggisbrotsins,
- til hvaða aðgerða hafi verið gripið eða lagt til að gripið verði til til að bregðast við brotinu, þ.m.t., þar sem það á við, aðgerða til að draga úr áhrifum brotsins á einstaklinga,
- til hvaða aðgerða einstaklingarnir geti gripið til að lágmarka tjón sitt, t.a.m. að skipta um lykilorð.

10. **Aðstoð gagnvart ábyrgðaraðila við að uppfylla skilyrði almennu persónuverndarreglugerðarinnar**
    Vinnsluaðili skal aðstoða ábyrgðaraðila við að framkvæma mat á áhrifum á persónuvernd.
    Vinnsluaðili skal aðstoða ábyrgðaraðila við að uppfylla ákvæði reglugerðarinnar um fyrirframsamráð við eftirlitsyfirvaldið (Persónuvernd).
11. **Öryggisráðstafanir**
    Vinnsluaðili skal innleiða eftirfarandi öryggisráðstafanir:
    [Hér þarf að koma fram lýsing á þeim viðeigandi tæknilegu og skipulagslegu öryggisráðstöfunum sem gera þarf til að tryggja öryggi upplýsinga með hliðsjón af áhættu, þ.m.t.:
    - notkun gerviauðkenna og dulkóðun á upplýsingum
    - möguleikum á að tryggja áframhaldandi trúnað, áreiðanleika, tiltækileika og álagsþol þeirra kerfa sem notuð eru og þeirrar þjónustu sem boðið er upp á,
    - möguleikum á að endurvekja tiltækileika og aðgang að persónuupplýsingum innan viðeigandi tímamarka í kjölfar fráviks, hvort sem það er raunlægs eða tæknilegs eðlis.
    - verkferli fyrir reglubundnar prófanir og mat á virkni hinna tæknilegu og skipulagslegu ráðstafana sem gerðar hafa verið til að tryggja öryggi vinnslunnar.]

    Vinnsluaðili undirgengst að innleiða öryggisráðstafanir í samræmi við [hátternisreglur, vottun, ISO-staðal.]

    [Til að tryggja sem besta reglufylgni er mælt með því að í samningnum sé nákvæmlega mælt fyrir um á hverju hver samningsaðili fyrir sig beri ábyrgð þegar kemur að innleiðingu öryggisráðstafana.]

    [Sjá dæmi um fyrirmæli í tengslum við öryggi í drögum að samningsviðauka frá Netöryggisráði.]

12. **Hvað verður um persónuupplýsingar við lok vinnslu**

Þegar þjónustu lýkur samkvæmt samningi þessum samþykkir vinnsluaðili að [hér þarf ábyrgðaraðili að velja hvað verður um upplýsingarnar]:

- eyða öllum persónugreinanlegum upplýsingum, eða
- skila öllum persónugreinanlegum upplýsingum til ábyrgðaraðila, eða
- skila öllum persónugreinanlegum upplýsingum til annars vinnsluaðila, tilnefnds af ábyrgðaraðila.

Þegar upplýsingum er skilað þarf einnig að eyða öllum afritum af persónugreinanlegum upplýsingum sem finna má í kerfum vinnsluaðila. Þegar upplýsingum hefur verið eytt skal vinnsluaðili sýna fram á það skriflega.

13. Persónuverndarfulltrúi

Vinnsluaðili skal senda ábyrgðaraðila upplýsingar um nafn og samskiptaupplýsingar persónuverndarfulltrúa síns, ef hann hefur verið tilnefndur, sbr. 37. gr. reglugerðarinnar.

14. Skrá yfir vinnslustarfsemi

Vinnsluaðili skal halda skrá yfir alla vinnslustarfsemi sem fram fer fyrir ábyrgðaraðila. Í henni skal koma fram eftirfarandi:

- heiti og samskiptaupplýsingar vinnsluaðila, eins eða fleiri, og sérhvers ábyrgðaraðila sem vinnsluaðilinn starfar í umboði fyrir og, eftir atvikum, fulltrúa ábyrgðaraðila eða vinnsluaðila og persónuverndarfulltrúa,
- flokkar vinnslu sem fram fer fyrir hönd hvers ábyrgðaraðila,
- ef við á, miðlun persónuupplýsinga til þriðja lands eða alþjóðastofnunar, þ.m.t. um hvaða þriðja land eða alþjóðastofnun er að ræða, og, ef um er að ræða miðlun sem um getur í annarri undirgrein 1. mgr. 49. gr., gögn um viðeigandi verndarráðstafanir,
- ef mögulegt er, almenn lýsing á þeim tæknilegu og skipulagslegu öryggisráðstöfunum sem um getur í 1. mgr. 32. gr.

15. Skjölun vegna sönnunar á reglufylgni

Vinnsluaðili skal útvega ábyrgðaraðila öll nauðsynleg skjöl til að hann geti sýnt fram á reglufylgni og til að ábyrgðaraðili eða úttektaraðili geti framkvæmt úttektir, þ.m.t. skoðanir, og veita aðstoð við slíkar úttektir.

V. Skyldur ábyrgðaraðila gagnvart vinnsluaðila

Ábyrgðaraðili skal:

1. afhenda vinnsluaðila þau gögn sem nefnd eru í kafla II.
2. skrá skriflega öll fyrirmæli varðandi vinnsluna sem beint er að vinnsluaðila.
3. tryggja, fyrir og á meðan á vinnslu stendur, að hann starfi í samræmi við þær kröfur sem gerðar eru til hans samkvæmt almennu persónuverndarreglugerðinni, og
4. hafa yfirumsjón með vinnslunni, þ.m.t. með því að framkvæma úttektir og skoðanir hjá vinnsluaðilanum.

Unnið í janúar 2018 upp úr samantekt frönsku persónuverndarstofnunarinnar, CNIL (Commission Nationale Informatique & Libertés), útg. í september 2017.