[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:

1. **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.

1. **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 vinnslunnar er [...]

Vinnsluaðila 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: [...]

1. **Gildistími samnings**

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

1. **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.

1. **Réttur hinna skráðu til upplýsinga.**

Hér er hægt að velja milli tveggja kosta:

1. 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.
2. 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.
3. **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 ákvarðanatöku, þ.m.t. notkun persónusniða. Hér er hægt að velja á milli tveggja kosta:

1. 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].
2. 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.
3. **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 áætlaðan 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.

1. **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).

1. **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.](https://www.stjornarradid.is/media/forsaetisraduneyti-media/media/utvefur/samningsvidauki-v-upploryggis.pdf)]

1. **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.

1. **Persónuverndarfulltrúi**

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

1. **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.

1. **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.

1. **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.