Persónuverndarskilmálar Háskóla Íslands (HÍ)

1 Gildissvið

Þessir skilmálar teljast ígildi vinnslusamnings samkvæmt 3. mgr. 25. gr. laga nr. 90/2018 um persónuvernd og vinnslu persónuupplýsinga (hér eftir persónuverndarlög) og varða vinnslu persónuupplýsinga HÍ í tengslum við þjónustu sem hann veitir stofnunum ríkisins sem felur í sér vinnslu persónuupplýsinga fyrir hönd viðkomandi stofnana. Með stofnunum er átt við menntastofnanir og aðrar ríkisstofnanir sem njóta þjónustu HÍ. Í slíkum tilvikum telst HÍ vinnsluaðili í skilningi persónuverndarlaga og viðkomandi stofnanir sem njóta þjónustunnar teljast ábyrgðaraðilar samkvæmt persónuverndarlögunum. Í ákveðnum tilvikum vinnur HÍ með persónuupplýsingar í því skyni að veita þjónustu sjálf og telst hann þá ábyrgðaraðili þeirrar vinnslu, svo sem vegna söfnun upplýsinga í aðgerðarskrár og söfnun greiningargagna. Gert er grein fyrir slíkri vinnslu í sérstakri fræðslu.

Skilmálarnir gilda um þá þjónustu sem stofnun hefur hjá HÍ á grundvelli þjónustusamnings/-a og felur í sér vinnslu persónuupplýsinga.

Í ákveðnum tilvikum hefur HÍ milligöngu um þjónustu þriðja aðila við stofnun og telst þá þriðji aðili vinnsluaðili gagnvart stofnuninni. Viðkomandi stofnanir sem njóta slíkrar þjónustu bera ábyrgð á að viðeigandi vinnslusamningar séu við slíka þriðju aðila.

2 Tilgangur og gildistími skilmála

Tilgangur þessara skilmála er að tilgreina skyldur HÍ sem vinnsluaðila gagnvart þeim stofnunum sem njóta þjónustu hennar sem fela í sér vinnslu persónuupplýsinga.

Merking hugtaka í þessum skilmálum fer samkvæmt skilgreiningum í ákvæðum persónuverndarlaga, sbr. einkum 3. gr. laganna.

Skilmálar þessir gilda á meðan stofnun nýtir sér þjónustu á vegum HÍ. Vinnsla HÍ á persónuupplýsingum mun fara fram á meðan þjónustusamningur er í gildi. Vinnslusamningar HÍ við stofnanir sem gerðir voru fyrir gildisstöku þessara skilmála falla úr gildi við útgáfu þeirra.

3 Lýsing á vinnslu

HÍ veitir margvíslega þjónustu sem felur í sér vinnslu persónuupplýsinga fyrir hönd stofnana en veitt þjónusta getur verið mismunandi. Veittri þjónustu er nánar lýst í þjónustusamningum.

4 Skyldur HÍ sem vinnsluaðili

1. HÍ skuldbindur sig til að vinna persónuupplýsingar einungis í samræmi við tilgang vinnslunnar, skilmála þessa, þjónustusamninga, viðauka við skilmálana og skrifleg fyrirmæli stofnunar.
2. Telji HÍ að fyrirmæli stofnunar samrýmist ekki persónuverndarlögum eða öðrum viðeigandi lagaákvæðum sem varða vinnslu persónuupplýsinga ber henni að tilkynna stofnun slíkt án tafar.

3. HÍ skal gera stofnun viðvart ef henni er skylt samkvæmt lögum að flytja persónuupplýsingar til þriðju landa eða alþjóðastofnana, nema lög banni að upplýst sé um slíkt.
4. Óski opinber eftirlitsaðili eftir aðgangi að gögnum og upplýsingum stofnunar skal HÍ tilkynna henni það svo fljótt sem verða má og áður en aðgangur er veittur ef það er mögulegt, nema HÍ sé það óheimilt samkvæmt lögum.
5. HÍ skal tryggja trúnað um vinnslu þeirra persónuupplýsinga sem skilmálar þessir taka til, þjónustusamningar og viðaukar.
6. HÍ skal tryggja að starfsfólk og verktakar sem hafa aðgang að persónuupplýsingum stofnunar í tengslum við framkvæmd þjónustu hafi undirritað trúnaðaryfirlýsingar eða séu bundnir þagnarskyldu samkvæmt lögum. Slík trúnaður og þagnarskylda helst þótt starfsmaður eða verktaki láti af störfum.
7. HÍ skal tryggja að starfsfólk sem hefur aðgang að persónuupplýsingum stofnunar í tengslum við framkvæmd þjónustu hafi fengið viðeigandi þjálfun og fræðslu um vernd persónuupplýsinga.
8. HÍ skal gæta þess að tæki og tól, vörur, forrit og þjónusta séu hönnuð með innbyggðu og sjálfgefna persónuvernd að leiðarljósi. Þetta tekur þó ekki til tækja og tóla, vöru og þjónustu sem keypt er af þriðja aðila með aðkomu, aðstoð eða milligöngu HÍ.

5 Skyldur stofnunar sem ábyrgðaraðila

1. Stofnun skal skrá skriflega öll fyrirmæli varðandi vinnsluna sem beint er að HÍ.
2. Stofnun skal tryggja, fyrir og á meðan á vinnslu stendur, að hún starfi í samræmi við þær kröfur sem gerðar eru til hennar samkvæmt persónuverndarlögum.
3. Stofnun ber ábyrgð á og skal tryggja að vinnsla HÍ fyrir hennar hönd eigi sér lagastoð í 9. og eftir atvikum 11. gr. persónuverndarlaga og samræmist að öðru leyti meginreglum laganna í 8. gr. þeirra.
4. Stofnun skal hafa yfirumsjón með vinnslunni, þ.m.t. með því að framkvæma eða láta framkvæma úttektir og skoðanir hjá HÍ. Úttektir og skoðanir gerðar af sjálfstæðum þriðja aðila af frumkvæði HÍ eða annarra stofnanna uppfylla þessa skyldu.

6 Notkun undirvinnsluaðila

HÍ er heimilt að semja við annan aðila („undirvinnsluaðila“) um að framkvæma tilteknar vinnsluaðgerðir, í heild eða hluta, sem hann sinnir fyrir stofnun. 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 er að ræða viðbætur eða breytingu á gildandi fyrirkomulagi vinnsluaðgerða, skal HÍ upplýsa stofnun skriflega um breytingarnar. Þar skal sérstaklega taka fram hvaða vinnsluaðgerðir undirvinnsluaðilinn hyggst taka að sér, nafn og samskiptaupplýsingar undirvinnsluaðilans ásamt dagsetningu samnings. Ábyrgðaraðili hefur fjórtán (14) daga frá þeim degi sem hann móttekur upplýsingar um breytingu á notkun á undirvinnsluaðila til að andmæla því. Notkun á undirvinnsluaðila er heimil ef stofnun hefur ekki andmælt innan tímamarkanna.

HÍ tryggir að undirvinnsluaðilar hlíti sömu skyldum vegna vinnslu persónuupplýsinga og koma fram í þessum skilmálum og ber ábyrgð gagnvart stofnunum á að undirvinnsluaðilar efni skuldbindingar sínar.
HÍ nýtur þjónustu þriðju aðila við rekstur kerfa sinna þótt þeir komi sjaldnast að vinnslu

persónuupplýsinga. Vegna eðlis rekstursins og þeirrar sérfræðiþekkingar sem þörf er á hverju sinni getur farið eftir aðstæðum til hverra er leitað. HÍ viðheldur lista yfir undirvinnsluaðila á innraneti UTs.

7 Réttindi hinna skráðu

Stofnanir bera sjálfar ábyrgð á 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. HÍ aðstoðar stofnanir og veitir allar þær upplýsingar sem hann býr yfir til að stofnanir geti uppfyllt skyldur sínar samkvæmt þessu ákvæði.

Stofnanir bera jafnframt ábyrgð á að afgreiða beiðnir einstaklinga um að neyta réttinda sinna í tengslum við vinnslu persónuupplýsinga vegna þjónustu HÍ. Leggi einstaklingar fram beiðni um slíkt við HÍ skal hann áframsenda slíkar beiðnir án tafar til tengiliðs stofnunar við HÍ.

Þetta á þó ekki við um vinnslu HÍ á persónuupplýsingum vegna veitingu þjónustu sem HÍ telst ábyrgðaraðili að. HÍ ber þá að veita stofnun og starfsfólki hennar þessa fræðslu og afgreiða réttindabeiðnir. Þetta á svo sem við um aðgerðarskrár og greiningargögn.

8 Öryggisráðstafanir

Hjá HÍ er lögð rík áhersla á að gæta öryggis upplýsingakerfa og persónuupplýsinga. HÍ er með vottun frá British Standards Institution (BSI) um að skólinn hafi innleitt stjórnkerfi upplýsingaöryggis sem uppfyllir kröfur ÍST ISO/IEC 27001 – Stjórnunarkerfi um upplýsingaöryggi staðalsins. Hjá HÍ eru starfandi upplýsingaöryggisstjóri og persónuverndarfulltrúi.

HÍ ber ábyrgð á að taka ákvarðanir um og innleiða tæknilegar og skipulagslegar öryggisráðstafanir sem gera þarf til að tryggja öryggi persónuupplýsinga og annarra upplýsinga stofnana með hliðsjón af áhættu. HÍ skuldbindur sig til þess að hámarka öryggi gagna og upplýsinga stofnana með tilliti til leyndar, réttleika og tiltækileika. Til að tryggja það skal HÍ meðal annars:

- nota gerviauðkenni og dulkóðun á upplýsingum, þegar þörf er á,
- tryggja áframhaldandi trúnað, áreiðanleika, tiltækileika og álagsþol þeirra kerfa sem notuð eru og þeirrar þjónustu sem boðið er upp á,
- tryggja möguleika á að endurvekja tiltækileika og aðgang að persónuupplýsingum innan viðeigandi tímamarka í kjölfar fráviks, hvort sem það er raunlægs eða tæknilegs eðlis,
- hafa verkferla fyrir og gera reglubundnar prófanir og mat á virkni hinna tæknilegu og skipulagslegu ráðstafana sem gerðar hafa verið til að tryggja öryggi vinnslunnar,
- tryggja aðgangshindranir að upplýsingum,
- tryggja að upplýsingum sé veitt vernd í flutningi,
- tryggja að upplýsingum sé veitt vernd í geymslu.

Þá hafa verið innleiddar skipulagslegar og tæknilegar ráðstafanir, eins og:

- dulkóðun gagnagrunna, samskipta og gagna við flutning,
- aðgangsstýringar þannig að einungis þeir sem þurfa persónuupplýsingar starfa sinna vegna hafi aðgang að þeim,
- almennar tölvuvarnir, eins og vírusvarnir og eldveggir, sem eru uppfærðar reglulega,
- virkt öryggiseftirlit, svo sem með innri og ytri úttektum og áhættumati, og virkri skráningu
- öryggisbresta,
- virk fræðsla og þjálfun fyrir starfsfólk um öryggismál.

Þagnarskylda hvílir á öllu starfsfólki HÍ samkvæmt lögum um réttindi og skyldur starfsmanna ríkisins, nr. 70/1996, og verktakar eru látnir skrifa undir trúnaðarsamning áður en að þeir hefja störf.

Hafi stofnun þörf á frekari öryggisráðstöfunum, svo sem vegna eðli eða umfangs persónuupplýsinga í vinnslu hjá stofnuninni, er hægt að mæla fyrir um slíkt í sérstökum samningi milli aðila sem viðauka við þessa skilmála.

9 Öryggisbrestir og tilkynning þeirra

Verði vart við öryggisbrest í tengslum við þjónustu HÍ við stofnun skal HÍ tilkynna viðkomandi stofnun með sannanlegum hætti um hvers konar öryggisbrot eigi síðar en 48 klukkustundum eftir að vart verður við brotið innan HÍ. Með tilkynningunni skulu fylgja hver þau skjöl eða gögn sem nauðsynleg eru til þess að ábyrgðaraðili geti tilkynnt um brotið til viðeigandi eftirlitsstofnunar.

Stofnun ber ábyrgð á að tilkynna öryggisbrest við meðferð persónuupplýsinga til Persónuverndar og annarra viðeigandi eftirlitsstofnana nema ólíklegt þyki að bresturinn leiði til áhættu fyrir réttindi og frelsi einstaklinga í samræmi við 2. mgr. 27. gr. persónuverndarlaga.

Ef líklegt er að öryggisbrestur við meðferð persónuupplýsinga leiði af sér mikla áhættu fyrir réttindi og frelsi einstaklinga skal viðkomandi stofnun tilkynna skráðum einstaklingi um brestinn án ótilhlýðilegrar tafar, sbr. 3. mgr. 27. gr. persónuverndarlaga.

10 Persónuupplýsingar við lok vinnslu

Þegar þjónustu lýkur samkvæmt þjónustusamningi skal HÍ aðstoða stofnun við flutning gagna og upplýsinga til nýs þjónustuveitanda eða skila stofnun þeim á algengu tölvulesanlegu formi, sé óskað eftir því.

Þar sem HÍ er afhendingarskyldur aðili samkvæmt 14. gr. laga nr. 77/2014 um opinber skjalasöfn er henni óheimilt að eyða gögnum og upplýsingum nema með samþykki þjóðskjalavarðar, reglna eða á grundvelli sérstaks lagaákvæðis, sbr. 1. mgr. 24. gr. sömu laga.

HÍ er heimilt að taka gjald fyrir aðstoð við flutning og skil gagna samkvæmt samkomulagi.

11 Úttektir

Óski stofnun eftir því skal HÍ veita henni, eða þriðja aðila sem stofnun tilnefnir fyrir sína hönd, aðgang að gögnum og upplýsingakerfum til að framkvæma úttektir og öryggisprófanir til að ganga úr skugga um að HÍ uppylli skyldur sínar samkvæmt þessum skilmálum, þjónustusamningi, viðaukum og samkvæmt lögum. Þetta á t.d. við um innri og ytri endurskoðendur viðskiptavinar sem og öryggisstjóra og/eða öryggisteymi.

HÍ samþykkir einnig að veita eftirlitsaðilum s.s. ríkisendurskoðanda, lögreglu, fjármálaeftirlitinu og örðum eftirlitsaðilum aðgang að gögnum og upplýsingakerfum sínum ef þau óska eftir því í tengslum við rannsókn á/hjá stofnun að fengnu samþykki stofnunar.

Úttektir og prófanir á grundvelli þessa ákvæðis skulu gerðar í samráði og með vitund HÍ. Aðilar skulu koma sér saman um dagsetningu og ráðstafanir til að tryggja öryggi og trúnað við úttekt eða prófun. HÍ áskilur sér rétt til að hafna úttektar-/prófunaraðila en skal færa málefnaleg rök fyrir slíkri höfnun. HÍ kann að krefjast gjalds vegna úttektar eða prófunar feli hún í sér kostnað fyrir HÍ. HÍ áskilur sér rétt til að fá aðgang og afrit af öllum úttektum, öryggisprófunum, áhættumati og öðru slíku sem gert er á kerfum hennar og þjónustu, og birta fyrir þjónustuþegum sínum að eigin frumkvæði eða ósk þeirra.

12 Flutningur gagna til þriðju ríkja

Gögn og persónuupplýsingar í vörslum HÍ í tengslum við þjónustu hennar við stofnanir verða hvorki fluttar né varðveittar utan Evrópska efnahagssvæðisins nema á grundvelli fyrirmæla stofnunar. Geri stofnun kröfu um að gögn séu varðveitt innanlands skal kveðið á um það í sérstökum samningi milli HÍ og stofnunar sem viðauka við þessa skilmála.

13 Ábyrgð

Um ábyrgð, takmarkanir á ábyrgð og skaðleysi fer samkvæmt því sem segir í þjónustusamningi. Ábyrgð aðila á brotum gegn persónuverndarlögum fer samkvæmt 51. gr. persónuverndarlaga og 82. gr. Almennu persónuverndarreglugerðarinnar.

14 Samningsskil

Þessir skilmálar gilda framar öðrum samningum sem aðilar hafa gert með sér hvað varðar vinnslu HÍ á persónuupplýsingum fyrir hönd stofnana. Hafi aðilar gert með sér viðauka við þessa skilmála um vinnslu persónuupplýsinga ganga þeir þó framar ákvæðum þessara skilmála.

15 Endurskoðun

Skilmálar þessir geta tekið breytingum í samræmi við breytingar á lögum og stjórnvaldsfyrirmælum, vegna úrskurða og álita Persónuverndar og vegna breytinga á þjónustu HÍ. Stofnanir verða upplýstar um breytingar og hafa 30 daga til að andmæla þeim. Hafi andmæli ekki borist innan frestsins teljast breytingarnar samþykktar.

Breytingar taka gildi við birtingu nýrrar útgáfu skilmálanna.