



## Persónuverndarstefna Heilsustofnunar

Heilsustofnun NLFÍ (Heilsustofnun) veitir sérhæfða heilbrigðisþjónustu, einkum á sviði endurhæfingar. Heilsustofnun starfar á grundvelli laga um heilbrigðisþjónustu nr. 40/2007 en hluti af aðstöðu hennar er einnig opin almenningi svo sem matsölustaður.

Heilsustofnun er nauðsynlegt, og í ákveðnum tilvikum skylt, að skrá og vinna með ýmsar persónuupplýsingar til að geta sinnt hlutverki sínu. Heilsustofnun leggur áherslu á að tryggja trúnað og öryggi persónuupplýsinga sem unnið er með innan stofnunarinnar.

Persónuverndarstefna þessi nær til allra persónuupplýsinga um dvalargesti og aðra einstaklinga sem eru í viðskiptum við okkur og/eða hafa samband við okkur, tengiliði sem koma fram fyrir hönd lögaðila í viðskiptum við okkur, sem og aðra tengiliði eða forráðamenn.

### 1. Lagaskylda

Heilsustofnun leggur sig fram við að uppfylla og virða virða reglur laga um persónuvernd og vinnslu persónuupplýsinga nr. 90/2018 og reglugerðar ESB um vernd einstaklinga í tengslum við vinnslu persónuupplýsinga (ESB 2016/679). Í því felst m.a. að lágmarka vinnslu persónuupplýsinga eins og kostur er og vinna aðeins með upplýsingarnar í lögmætum tilgangi.

Starfsfólk Heilsustofnunar er einnig bundið þagnarskyldu samkvæmt lögum um heilbrigðisstarfsmenn og lögum um réttindi sjúklinga. Þagnarskyldan nær til allra persónuupplýsinga sem starfsfólk í heilbrigðisþjónustu kemst að í starfi sínu og helst þótt sjúklingur látist eða starfsmaður láti af störfum. Heilsustofnun leggur ríka áherslu á að trúnaðar gagnvart persónuupplýsingum sé gætt.

### 2. Persónuupplýsingar

Samkvæmt lögum nr. 90/2018 um persónuvernd og vinnslu persónuupplýsinga teljast persónuupplýsingar hvers kyns upplýsingar um persónugreindan eða persónugreinanlegan einstakling. Með því er átt við upplýsingar sem hægt er að

rekja beint eða óbeint til ákveðins einstaklings, t.d. með nafni, kennitölu, netfangi eða öðrum þáttum sem einkenna einstakling. Persónuupplýsingar geta verið í rituðu máli eða á mynd, á pappír eða í starfrænu formi.

### 3. Vinnsla persónuupplýsinga

Til þess að geta sinnt þjónustunni þarf Heilsustofnun að skrá og vinna með ýmsar persónuupplýsingar. Ólíkum persónuupplýsingum er safnað eftir eðli viðskipta og/eða tengsla við Heilsustofnun.

Helstu flokkar persónuupplýsinga sem unnið er með innan Heilsustofnunar eru eftirfarandi:

- Persónuauðkenni, s.s. nafn og kennitala
- Tengiliðaupplýsingar, s.s. heimilisfang, símanúmer og netfang
- Samskipta- og viðskiptasaga
- Heilsufarsupplýsingar
- Upplýsingar um nánasta aðstandanda
- Upplýsingar um dvalargesti, s.s. dvalarstað, herbergisnúmer o.fl.

Upplýsingarnar eru fyrst og fremst unnar til að starfsfólk Heilsustofnunar geti sinnt þörfum dvalargesta og viðskiptavina og veitt þeim nauðsynlega meðferð og þjónustu í samræmi við 2. tl. 1. mgr. 9. gr. laga nr. 90/2018.

Heilsustofnun er skylt samkvæmt lögum nr. 55/2009 um sjúkraskrá að færa ákveðnar persónuupplýsingar í sjúkraskrá þeirra sem til okkar leita vegna heilbrigðisþjónustu. Samkvæmt lögnum skal færa öll þau atriði í sjúkraskrá sem nauðsynleg eru vegna meðferðar sjúklings. Lögin kveða á um ákveðnar lágmarksupplýsingar sem ber að skrá í sjúkraskrá, eftir því sem við á hverju sinni. Vinnsla upplýsinga í sjúkraskrá er nauðsynleg til að tryggja að heilbrigðisstarfsfólk sem kemur að meðferðinni hafi nákvæmar og réttar upplýsingar til að geta metið stöðuna og veitt viðeigandi meðferð. Lagagrundvöllur þessarar vinnslu er 8. tl. 1. mgr. 11. gr. laga nr. 90/2018.

Auk framangreindra upplýsinga kann Heilsustofnun einnig að safna og vinna með aðrar upplýsingar sem viðskiptavinir eða forráðamenn/tengiliðir viðskiptavinar láta okkur sjálfir í té sem og upplýsingar sem eru stofnuninni nauðsynlegar vegna starfseminnar, t.d. í eftirlits- eða öryggisskyni, og/eða vegna rekstrarhagsmuna, t.d. tölfræðiupplýsingar vegna áætlana- og skýrslugerðar. Lagagrundvöllur slíkrar vinnslu er 6. tl. 1. mgr. 9. gr. laga nr. 90/2018. Þá þarf Heilsustofnun að vinna með persónuupplýsingar til þess að geta uppfyllt margvíslegar skyldur sem á stofnunni hvíla, t.d. í tengslum við lög og reglur um bókhald og á grundvelli

samningssambanda. Heilsustofnun skráir því einnig upplýsingar um viðskiptavinum í rekstrar- og bókhaldslegum tilgangi. Í þeim tilvikum er lagagrundvöllur vinnslunnar 3. tl. 1. mgr. 9. gr. laga nr. 90/2018.

Að meginstefnu til aflar Heilsustofnun persónuupplýsinga beint frá viðskiptavinum eða tengiliðum þeirra. Í sumum tilvikum fær stofnunin upplýsingar frá þriðja aðila, t.d. aðstandendum, öðru heilbrigðisstarfsfólki og/eða opinberum stofnunum. Þá getur stofnunin þurft að nálgast persónuupplýsingar á netinu, t.d. símanúmer, kennitölu eða heimilisfang. Sé persónuupplýsinga aflað frá þriðja aðila mun Heilsustofnun leitast við að upplýsa um slíkt sé það unnt, nema um sé að ræða upplýsingar sem falla undir trúnaðarskyldu.

Ef þú ert að sækja um starf á Heilsustofnun verða innsend gögn frá þér einungis notuð við vinnslu starfsumsóknarinnar eða til að uppfylla skyldu stofnunarinnar samkvæmt lögum ef þörf krefur. Heilsustofnun er ábyrgðaraðili allra gagna sem þú kannt að láta af hendi í tengslum við ráðningarferlið nema annað sé tekið fram. Upplýsingar um þig eru notaðar til þess að við getum haft samband við þig og unnið frekar með þína umsókn og metið hæfi þitt í auglýst starf. Við söfnum ekki meiri upplýsingum en þörf er á til þess að uppfylla fram kominn tilgang okkar með auglýstu starfi. Við söfnum einnig upplýsingum um alla nema í starfsnámi og/eða þjálfun til þess að halda utan um og skipuleggja nám á stofnuninni. Lagagrundvöllur þessarar vinnslu er 2. tl. 1. mgr. 9. gr. laga nr. 90/2018 eða 6. tl. sama lagaákvæðis eftir atvikum.

#### **4. Varðveisla**

Þau persónugreinanlegu gögn sem Heilsustofnun hefur undir höndum eru ýmist vistuð í læstum skjalahirslum eða rýmum og/eða í viðeigandi tölvukerfum, svo sem í sjúkraskrárkerfi, bókhaldskerfi o.fl. Hýsing umræddra tölvukerfa er á Íslandi. Gerðir eru sérstakir vinnslusamningar við hýsingaraðila allra tölvukerfa og Heilsustofnun leggur áherslu á að farið sé með persónuupplýsingar í samræmi við ákvæði laga um persónuvernd og vinnslu persónuupplýsinga.

Heilsustofnun geymir upplýsingar um viðskiptavinum og forsvarsmenn/tengiliði viðskiptavina almennt í sjö ár frá lokum viðskipta/viðskiptasambands. Sé um að ræða upplýsingar sem falla undir bókhaldslög er skylt að varðveita þær í sjö ár frá lokum viðkomandi reikningsárs. Hvað varðar færslu persónuupplýsinga í sjúkraskrár þá er Heilsustofnun ávallt skylt að varðveita sjúkraskrár í samræmi við lög þar að lútandi. Þá er Heilsustofnun skylt að varðveita ákveðin gögn sem verða til í starfseminni í allt að 30 ár, þar til þau eru afhent viðeigandi skjalasafni, í samræmi við ákvæði laga um opinber skjalasöfn.

## 5. Aðgangur og miðlun persónuupplýsinga

Heilsustofnun takmarkar aðgang að persónuupplýsingum eins og kostur er og hefur einungis það starfsfólk sem það þarf aðgang að þeim. Hvað varðar sjúkraskrárupplýsingar þá er það einungis heilbrigðisfagfólk í samræmi við lög þar að lútandi og þeir starfsmenn sem þess þurfa af rekstrarlegum ástæðum stofnunarinnar.

Einnig er persónuupplýsingum miðlað til þriðju aðila sem veita Heilsustofnun upplýsingatækniþjónustu og aðra þjónustu sem tengist vinnslu og er hluti af rekstri stofnunarinnar. Heilsustofnun er skylt að gera samninga um slíka vinnslu við þriðja aðila og sjá til þess að gætt sé að lögum og reglum um persónuvernd.

Heilsustofnun miðlar ekki persónuupplýsingum til þriðja aðila nema það sé heimilt á grundvelli lagaskyldu, samnings eða samþykkis. Heilsustofnun er t.d. skylt samkvæmt lögum að skila tilteknum upplýsingum til ríkisstofnana, svo sem embættis landlæknis, Sjúkratrygginga Íslands, skattayfirvalda o.fl. Þá getur einnig verið þörf á því að deila heilsufarsupplýsingum með öðru heilbrigðisstarfsfólki eða -stofnunum.

Persónuupplýsingar kunna jafnframt að vera afhentar þriðja aðila að því marki sem heimilað er eða krafist er á grundvelli umboðs eða viðeigandi laga eða reglna, s.s. til opinberra stofnana, dómstóla og/eða lögmanna.

Heilsustofnun mun ekki miðla persónuupplýsingum utan evrópska efnahagssvæðisins nema það sé heimilt á grundvelli persónuverndarlöggjafarinnar.

## 6. Vefsíða og vafrakökur

Þegar vefsíða Heilsustofnunar er heimsótt þá safnar síðan upplýsingum um notendur með sk. vafrakökum. Vafrakökur eru smáar textaskrár sem eru geymdar á tölvum eða snjalltækjum. Við heimsókn á vefsíðu Heilsustofnunar eru skráðar upplýsingar um tíma, dagsetningu, leitarorð, frá hvaða vef er komið, gerð vafra, gerð stýrikerfis o.fl. Upplýsingarnar eru notaðar til að betrubæta vefsíðuna sem og upplifun notenda hennar. Athygli nýrra notenda er vakin á því þegar heimasíðan er heimsótt og er notendum í sjálfsvald sett hvort þeir heimili vinnsluna. Upplýsingarnar eru ekki seldar þriðja aðila.

Að öðru leyti en hvað varðar vefsíðu byggir vinnsla persónuupplýsinga hjá Heilsustofnun ekki á sjálfvirkri ákvarðanatöku.

## 7. Öryggisráðstafanir

Heilsustofnun leitast við að grípa til viðeigandi tæknilegra og skipulegra ráðstafana til að vernda persónuupplýsingar með sérstöku tilliti til eðlis þeirra. Þessum ráðstöfunum er ætlað að vernda persónuupplýsingar gegn því að þær glatist eða breytist fyrir slysi og gegn óleyfilegum aðgangi, afritun, notkun eða miðlun.

Dæmi um öryggisráðstafanir sem Heilsustofnun grípur til eru:

- Aðgangsstýring að öllum kerfum.
- Upplýsingar á pappírformi eru geymdar í læstum hirslum eða læstum rýmum.
- Öryggi sjúkraskrárupplýsinga er gætt í samræmi við ákvæði laga og reglugerða þar um.
- Fræðsla til starfsfólks.

Hvað varðar öryggi sjúkraskráa sérstaklega, þá gilda bæði lög, reglur og fyrirmæli frá landlæknisembættinu þar um sem Heilsustofnun leggur ríka áherslu á að fara eftir.

## 8. Breytingar og leiðréttingar á persónuupplýsingum

Það er mikilvægt að þær persónuupplýsingar sem Heilsustofnun vinnur með séu réttar. Því er mikilvægt að Heilsustofnun sé tilkynnt um breytingar sem kunna að verða á persónuupplýsingum.

Einstaklingar geta átt rétt á því að fá óáreiðanlegar persónuupplýsingar um sig leiðréttar. Að teknu tilliti til tilgangs vinnslu persónuupplýsinga geta einstaklingar jafnframt átt rétt á að láta fullgera ófullkomnar persónuupplýsingar um sig, þ.m.t. með því að leggja fram frekari upplýsingar.

Heilsustofnun vekur þó athygli á því að stofnuninni er skylt samkvæmt lögum um sjúkraskrá að vinna ákveðnar persónuupplýsingar með því að færa þær í sjúkraskrá, sbr. 3. kafla hér að ofan, og er Heilsustofnun ekki heimilt að breyta eða leiðrétta þær upplýsingar nema í ákveðnum tilvikum. Óheimilt er að eyða upplýsingum úr sjúkraskrá nema með samþykki landlæknis.

Vinsamlega beinið öllum uppfærslum eða beiðnum hvað þetta varðar til persónuverndarfulltrúa Heilsustofnunar, sbr. 12. kafla stefnu þessarar.

## 9. Réttindi einstaklinga vegna vinnslu

Einstaklingar njóta ýmissa réttinda samkvæmt lögum um persónuvernd og vinnslu persónuupplýsinga, og geta t.d. óskað eftir aðgangi að persónuupplýsingum,

eyðingu, takmörkun vinnslu og/eða flutningi þeirra. Þá eiga einstaklingar í ákveðnum tilvikum andmælarétt auk þess sem þeir njóta sérstakra réttinda í þeim tilvikum þar sem um öryggisbrot er að ræða við meðferð persónuupplýsinga.

Einstaklingar sem hyggjast leggja fram beiðni í tengslum við ofangreind réttindi eru beðnir um að hafa samband við persónuverndarfulltrúa Heilsustofnunar, sbr. 12. kafla stefnu þessarar.

Framangreind réttindi eru ekki fortakslaus. Þannig kunna lög t.d. að skylda Heilsustofnun til að hafna ósk um eyðingu eða aðgang að gögnum, sbr. einnig umfjöllun um sjúkraskrár í 8. kafla.

Ef upp koma aðstæður þar sem Heilsustofnun getur ekki orðið við beiðni vegna ofangreinds mun stofnunin leitast við að útskýra hvers vegna beiðninni hefur verið hafnað, þó með tilliti til takmarkana á grundvelli lagaskyldu.

## **10. Samþykki**

Í þeim tilvikum þar sem vinnsla persónuupplýsinga byggir á samþykki, á skráður einstaklingur hvenær sem er rétt á því að draga samþykki sitt til baka. Afturköllun samþykkis hefur ekki áhrif á lögmæti vinnslu á grundvelli samþykkisins fram að afturkölluninni.

Rétt er að geta þess að vinnsla persónuupplýsinga hjá Heilsustofnun byggir sjaldnast á samþykki. Færsla upplýsinga í sjúkraskrá byggir t.d. á lagaskyldu, sbr. 3. kafla.

## **11. Fyrirspurnir og kvörtun til Persónuverndar**

Ef þú vilt nýta þér þau réttindi sem lýst er í 8. og 9. kafla í stefnu þessari, eða ef þú hefur einhverjar spurningar varðandi persónuverndarstefnu þessa eða það hvernig Heilsustofnun vinnur með persónuupplýsingar, vinsamlegast hafðu samband við persónuverndarfulltrúa Heilsustofnunar sbr. 12. kafla hér á eftir.

Ef þú ert ósátt/ur við vinnslu Heilsustofnunar á persónuupplýsingum getur þú sent erindi til Persónuverndar (sjá frekari upplýsingar á [www.personuvernd.is](http://www.personuvernd.is)).

## 12. Upplýsingar um Heilsustofnun og persónuverndarfulltrúa

Þú getur náð í Heilsustofnun með að hafa samband í síma eða með tölvupósti:

Heilsustofnun NLFÍ  
Grænumörk 10  
810 Hveragerði  
S: 483-0300

Forstjóri Heilsustofnunar er Þórir Haraldsson; [thorir\[hjá\]heilsustofnun.is](mailto:thorir[hjá]heilsustofnun.is).

Við höfum skipað persónuverndarfulltrúa, sem hefur eftirlit með málum er varða persónuvernd, þ.m.t. stefnu þessari:

Tinna Björk Gunnarsdóttir, lögmaður  
Lögmannsstofunni Fortis ehf.  
[tinna\[hjá\]fortislogmenn.is](mailto:tinna[hjá]fortislogmenn.is) / 520-5800

## 13. Gildistími og endurskoðun

Heilsustofnun kann að þurfa að breyta persónuverndarstefnu þessari, t.d. í samræmi við breytingar á viðeigandi lögum eða reglugerðum eða vegna breytinga á því hvernig unnið er með persónuupplýsingar innan stofnunarinnar.

Þessi persónuverndarstefna var síðast uppfærð 10. maí 2022