Innri persónuverndarstefna
Læknafélag Íslands

DATTACA LABS

Efnisyfirlit

Samþykkt: 4. apríl 2022

Tók gildi: 5. apríl 2022

Endurskoðun: Næst 2023

Almennt

Í starfsemi Læknafélag Íslands[1] er nauðsynlegt að safna og vinna með persónuupplýsingar um einstaklinga. Með persónuupplýsingum er átt við allar upplýsingar sem hægt er að rekja beint eða óbeint til tiltekins einstaklings, svo sem upplýsingar um nafn, kennitölu, heimilisfang, netfang, símanúmer, fjárhag, heilsufar, IP tölu og fleira.

Þær persónuupplýsingar sem LÍ hefur undir höndum geta verið um starfsmenn þess, félagsmenn, starfsmenn birgja og aðra þriðju aðila sem nauðsynlegt er að eiga samskipti við.

Með þessari persónuverndarstefnu er kveðið á um hvernig Læknafélag Íslands skuli safna, geyma og að öðru leyti meðhöndla persónuupplýsingar í samræmi við lög um persónuvernd og vinnslu persónuupplýsinga nr. 90/2018 (hér eftir „persónuverndarlög“).

Þessari persónuverndarstefnu er einkum ætlað að tryggja:

- að LÍ vinni persónuupplýsingar í samræmi við persónuverndarlög og fylgi viðurkenndum starfsreglum til að tryggja öryggi þeirra;
- að LÍ standi vörð um þau réttindi sem einstaklingar njóta samkvæmt persónuverndarlögum;
- að gagnsæi ríki um hvernig LÍ meðhöndlar persónuupplýsingar;
- að lágmarka þá áhættu sem brot á persónuverndarlögum getur haft í för með sér.

Persónuverndarlög

Í persónuverndarlögum er kveðið á um hvernig sé heimilt að safna, geyma og meðhöndla persónuupplýsingar að öðru leyti. Þær reglur gilda óháð því á hvaða formi upplýsingar eru geymdar, svo sem hvort það er á rafrænu formi eða pappírsformi.

Óheimilt er að safna og vinna með persónuupplýsingar nema heimild standi til þess samkvæmt persónuverndarlögum. Þá verður slík söfnun og vinnsla einnig að fara fram með sanngjörnum hætti. Auk þess má einungis geyma persónuupplýsingar á öruggum stað og óheimilt er að veita óviðkomandi aðila aðgang að þeim.

Læknafélag Íslands mun grípa til nauðsynlegra ráðstafana til að tryggja að ávallt sé heimild í persónuverndarlögum til þess að vinna með persónuupplýsingar. Auk þess mun LÍ grípa til

[1] Hér eftir „Læknafélag Íslands“ eða „LÍ“.

nauðsynlegra ráðstafana til að tryggja að ávallt sé farið eftir þeim sex meginreglum sem löggjöfin kveður á um. Þær meginreglur sem átt er við eru í stuttu máli eftirfarandi:

1) Persónuupplýsingar séu unnar með sanngjörnum og lögmætum hætti.
2) Persónuupplýsingum sé einungis safnað í skýrum og lögmætum tilgangi.
3) Ekki sé safnað og unnið meira með persónuupplýsingar en nauðsynlegt er.
4) Persónuupplýsingar séu nákvæmar og uppfærðar þegar þörf krefur.
5) Persónuupplýsingar séu ekki geymdar lengur en þörf er á.
6) Gætt sé að öryggi persónuupplýsinga með viðeigandi varúðarráðstöfunum.

Læknafélag Íslands skal tryggja að í þeim tilvikum að um viðkvæmar persónuupplýsingar er að ræða eða upplýsingar viðkvæms eðlis að notkun, meðferð og vinnsla samrýmist þeim kröfum sem gerðar eru í persónuverndarlögum og aðeins þeir starfsmenn sem starfs síns vegna þurfa, hafi aðgang að slíkum upplýsingum. Með viðkvæmum persónuupplýsingum er átt við:

- Upplýsingar um kynþátt, þjóðernislegan uppruna, stjórnmálaskoðanir, trúarbrögð, lífskoðun og aðild að stéttarfélagi.
- Heilsufarsupplýsingar, þ.e. persónuupplýsingar sem varða líkamlegt eða andlegt heilbrigði einstaklings.
- Upplýsingar um kynlíf manna og kynhneigð.
- Erfðafræðilegar upplýsingar, þ.e. persónuupplýsingar sem varða arfgenga eða áunna erfðaeiginleika einstaklings sem gefa einkvæmar upplýsingar um lífeðlisfræði eða heilbrigði einstaklingsins og fást einkum með greiningu á líffræðilegu sýni frá viðkomandi einstaklingi.
- Líkennaupplýsingar, það er perónuupplýsingar sem fást með sérstakri tæknivinnslu og tengjast líkamlegum, lífeðlisfræðilegum eða atferðisfræðilegum eiginleikum einstaklings og gera það mögulegt að hægt sé að greina eða staðfesta deili á einstaklingi með ótvíræðum hætti, svo sem gögn um fingraför.

Áhættur og ábyrgðir

Lágmörkun áhættu

Lágmarka verður þá áhættu sem felst í því að meðhöndla persónuupplýsingar og koma þarf í veg fyrir

- að brotið verði gegn þeirri trúnaðarskyldu sem hvílir á fyrirtækinu, til dæmis að persónuupplýsingum verði ekki miðlað til óviðkomandi aðila,
- að einstaklingar hafi ekki val um hvort unnið verði með persónuupplýsingar um þá,
- að orðspor fyrirtækisins verði fyrir skaða, en gjarnan má hafa í huga þær afleiðingar sem LÍ yrði fyrir ef brotið er gegn persónuverndarlögum og
- að þeir einstaklingar sem upplýsingarnar eru um verði ekki fyrir tjóni. Hér má hafa í huga þær afleiðingar sem þeir kynnu að verða fyrir ef persónuupplýsingar þeirra kæmust í hendur óviðkomandi aðila.

Ábyrgðir og hlutverk

Allir stjórnendur og starfsmenn Læknafélag Íslands bera ábyrgð á því hvernig persónuupplýsingar eru meðhöndlaðar. Sérstaklega ríkar skyldur hvíla á þeim aðilum sem vinna með persónuupplýsingar sem teljast viðkvæmar eða viðkvæms eðlis. Framkvæmdastjóri Læknafélag Íslands ber ábyrgð á því að LÍ framfylgi persónuverndarlögum.

Hlutverk framkvæmdastjóra er:

- að tryggja að öll kerfi, þjónusta og búnaður fullnægi þeim öryggiskröfum sem gerðar eru samkvæmt persónuverndarlögum,
- að láta framkvæma reglulega úttektir sem eiga að tryggja að hug- og vélbúnaður virki með öruggum hætti og
- að meta þá þjónustu sem LÍ hyggst nýta sér frá utanaðkomandi þriðja aðila, til dæmis þar sem til stendur að geyma gögn.

Hlutverk persónuverndarfulltrúa er:

- að LÍ fái reglulega fræðslu um þær skyldur sem á þeim hvíla samkvæmt persónuverndarlögum
- að fara reglulega yfir ferla og stefnur sem tengjast meðferð persónuupplýsinga
- að veita fræðslu og þjálfa starfsmenn sem meðhöndla persónuupplýsingar
- að taka á móti og svara spurningum frá þeim einstaklingum sem upplýsingarnar varða

- að taka á móti beiðnum frá skráðum einstaklingum, svo sem vegna réttar þeirra til aðgangs að gögnum, til að mótmæla vinnslu eða til að gleymast
- að yfirfara og samþykkja alla samninga við utanaðkomandi þriðja aðila sem ætlað er að vinna persónuupplýsingar fyrir hönd fyrirtækisins
- að vega og meta hvort tilkynna þurfi öryggisbrest til viðeigandi aðila og
- að annast samskipti við Persónuvernd

Almennar verklagsreglur um meðferð persónuupplýsinga

Eftirfarandi verklagsreglur um meðferð persónuupplýsinga gilda hjá Læknafélag Íslands:

- Einungis þeir starfsmenn, sem starfs síns vegna þurfa, eiga að hafa aðgang að persónuupplýsingum.
- Starfsmönnum er óheimilt að deila persónuupplýsingum sín á milli óformlega.
- Starfsmenn skulu ávallt gæta fyllsta öryggis þegar þeir meðhöndla persónuupplýsingar og fylgja þeim leiðbeiningum sem hér koma fram.
- Þegar unnið er með persónuupplýsingar skulu starfsmenn ávallt gæta þess að tölvuskjáir séu læstir þegar farið er frá borðum.
- Starfsmenn skulu aldrei deila persónuupplýsingum með óviðkomandi aðila og gildir þar einu hvort um sé að ræða annan starfsmann fyrirtækisins eða utanaðkomandi aðila.
- Persónuupplýsingar skal aldrei senda út fyrir Evrópska efnahagssvæðið nema fyrir því sé sérstök lagaheimild.
- Starfsmenn skulu ráðfæra sig við persónuverndarfulltrúa ef þeir eru í vafa um hvernig skuli meðhöndla persónuupplýsingar.

Verklagsreglur um meðferð pappírsgagna

Geymsla persónuupplýsinga á pappír

Persónuupplýsingar sem geymdar eru á pappír skulu vera á öruggum stað þar sem óviðkomandi aðili getur ekki nálgast þær.

- Persónuupplýsingar sem geymdar eru á pappír skulu vera í læstum skjalaskáp eða í læstri skjalageymslu.
- Starfsmönnum ber að tryggja að pappírsgögn, þar sem persónuupplýsingar má finna, séu ekki skilin eftir þar sem óviðkomandi aðilar geta séð þær.
- Pappírsgögnum skal eytt með fullnægjandi hætti þegar þeirra er ekki lengur þörf.

Notkun pappírs sem inniheldur persónuupplýsingar

Þegar unnið er með persónuupplýsingar á pappír skal gæta að eftirfarandi verklagsreglum:

- Ekki skal skilja við pappírsgögn þannig að óviðkomandi aðili geti komist yfir upplýsingarnar. Ganga skal frá skjölum á tryggan hátt.
- Ekki skal senda viðkvæmar persónuupplýsingar eða upplýsingar viðkvæms eðlis með almennum bréfpósti heldur skal senda slíkar upplýsingar í ábyrgðapósti.

Meðhöndlun pappírsgagna utan fyrirtækisins

Starfsmenn eiga eftir fremsta megni og eftir því sem framkvæmanlegt er að meðhöndla pappírsgögn sem innihalda persónuupplýsingar innan veggja fyrirtækisins. Þegar starfsmenn taka pappírsgögn sem innihalda persónuupplýsingar út fyrir veggi fyrirtækisins þarf að fylgja eftirfarandi verklagsreglum:

- Óheimilt er að taka viðkvæmar persónuupplýsingar eða upplýsingar viðkvæms eðlis út fyrir veggi fyrirtækisins nema fyllsta öryggis sé gætt.
- Starfsmaður skal gæta að umhverfi sínu þegar hann vinnur með gögnin og þegar vinnu er lokið skal hann tryggja að óviðkomandi aðili komist ekki í gögnin.
- Starfsmanni er óheimilt að geyma pappírsgögn utan fyrirtækisins svo sem á heimili starfsmanns.

Verklagsreglur varðandi meðferð rafrænna gagna

Persónuupplýsingar sem geymdar eru með rafrænum hætti skulu njóta verndar gegn óleyfilegum aðgangi og þess skal gætt að þeim verði ekki eytt fyrir mistök.

- Persónuupplýsingar skal vernda með illrekjanlegum lykilorðum og þeim má aldrei deila með öðrum óviðkomandi. Lykilorð þarf að vera að lágmarki 12 stafir að lengd og innihalda hástaf, lágstaf, tölustaf og tákn. Ekki skal nota lykilorð sem vitnar í persónuupplýsingar. Skipta skal um lykilorð á 12 mánaða fresti.
- Ef persónuupplýsingar eru geymdar á tilteknu formi, til dæmis á USB lykli, þá skal geyma þau á læstum stað þegar ekki er verið að nota þau.
- Persónuupplýsingar skal einungis geyma á tilgreindum drifum og netþjónum. Einungis skal notast við tölvuskýjaþjónustu sem uppfyllir þau skilyrði sem persónuverndarlög kveða á um.

- Netþjónar sem innihalda persónuupplýsingar skulu staðsettir á öruggum stað og fjarri almennu skrifstofurými.
- Taka skal afrit af gögnum með reglubundnum hætti og jafnframt skal kanna reglulega hvort afritun tekst.
- Vernda skal alla netþjóna og tölvur sem innihalda persónuupplýsingar með viðeigandi öryggisbúnaði og eldveggjum.
- Starfsmenn skulu ekki vista afrit af viðkvæmum persónuupplýsingum á tölvu, síma eða annan búnað í einkaeigu.
- Gera skal skýran greinarmun á almennum persónuupplýsingum og persónuupplýsingum sem eru viðkvæmar eða viðkvæms eðlis. Ef mögulegt er skal ekki geyma upplýsingarnar á sama stað, svo sem í sömu möppu.

Meðhöndlun rafrænna gagna utan fyrirtækisins

Starfsmenn eiga eftir fremsta megni og eftir því sem framkvæmanlegt er að meðhöndla rafræn gögn sem innihalda persónuupplýsingar innan veggja fyrirtækisins. Þegar starfsmenn vinna rafræn gögn utan fyrirtækisins þarf að fylgja eftirfarandi verklagsreglum:

- Óheimilt er að vinna með rafræn gögn utan fyrirtækisins nema fyllsta öryggis sé gætt.
- Starfsmaður skal gæta að umhverfi sínu þegar hann vinnur með gögnin og þegar vinnu er lokið skal hann tryggja að óviðkomandi aðili komist ekki í gögnin.

Verklagsreglur um tölvupóstnotkun

Notkun á tölvupósti

Þegar senda á tölvupóst með persónuupplýsingum er það aðeins heimilt ef öryggi upplýsinganna er tryggt og eftirfarandi verklagsreglum er fylgt:

- Ekki skal senda persónuuppplýsingar með tölvupósti nema unnt sé að tryggja fullnægjandi öryggi þeirra.
- Ef senda á viðkvæmar persónuupplýsingar eða persónuupplýsingar viðkvæms eðlis með tölvupósti skal grípa til viðeigandi öryggisráðstafana. Með viðeigandi öryggisráðstöfunum er átt við að senda skal upplýsingarnar í skjali sem sett er í viðhengi og skal læsa því skjali með lykilorði.
- Þegar skjali hefur verið læst með lykilorði skal ekki senda lykilorðið í sama tölvupósti. Ef mögulegt er skal hringja í viðtakanda til að gefa upp lykilorðið. Sé sá möguleiki ekki

fyrir hendi skal senda aðskilinn tölvupóst þar sem ekkert viðfangsefni er tiltekið og ekkert innihald í tölvupóstinum að undanskildu lykilorðinu.

- Áður en tölvupóstur er sendur skal ávallt tryggja að viðtakandi sé réttur, að innihald tölvupóstsins sé rétt og ef við á, að viðhengi sem á að fylgja tölvupóstinum sé hið rétta.

Notkun á tölvupósti í tækjum í einkaeigu starfsmanns

Þegar starfsmaður notar tölvu, síma eða annan búnað í einkaeigu til að opna tölvupóst fyrirtækisins er það aðeins heimilt ef eftirfarandi verklagsreglum er fylgt:

- Einungis skal vinna í gegnum örugga nettengingu. Til að mynda telst WIFI á opinberum stöðum svo sem flugvöllum, hótelum og kaffihúsum ekki örugg nettenging og er því óheimilt að opna eða senda tölvupóst ef starfsmaður er tengdur slíkri tengingu.
- Tölva, sími og annar búnaður í einkaeigu starfsmanns skal innihalda örugga læsingu.

Viðbrögð við öryggisbresti

Samkvæmt persónuverndarlögum telst það vera öryggisbrestur þegar óviðkomandi aðili fær aðgang að persónuupplýsingum, þær glatast eða er breytt í leyfisleysi. Eftirfarandi reglur skulu gilda um öryggisbresti og viðbrögð því:

- Ef upp kemur öryggisbrestur eða grunur um öryggisbrest ber að láta framkvæmdastjóra vita án tafar. Ef forstjóri er vant við látinn skal hafa samband við persónuverndarfulltrúa Læknafélag Íslands án tafar með því að senda tölvupóst á **dpo@dattacalabs.com** eða tengilið innan Læknafélags Íslands á netfang lis@lis.is eða hringja í síma **517 3444**.
- Halda skal skrá um frávik í upplýsingaöryggi, til dæmis ef starfsfólk fylgir ekki verklagsreglum um geymslu á persónuupplýsingum.
- Tilkynna skal persónuverndarfulltrúa um hvert það frávik sem verður í upplýsingaöryggi, til dæmis ef óviðkomandi aðili kemst yfir persónuupplýsingar.
- Bregðast skal við öryggisbresti í samræmi við persónuverndarlög, þ.e. með tilkynningu til Persónuverndar og einstaklinga þegar við á.
- Öryggisbrest ber að rannsaka og grípa skal til skynsamlegra ráðstafana til að tryggja að sambærilegt atvik endurtaki sig ekki.

Nákvæmni persónuupplýsinga

Persónuverndarlög gera kröfu um að gripið sé til viðeigandi ráðstafana sem eiga að tryggja að persónuupplýsingar séu nákvæmar og réttar. Hversu mikilla ráðstafana þarf að grípa til veltur

á því hve mikil áhrif ónákvæmar upplýsingar geta haft á þann einstakling sem upplýsingarnar eru um.

Allir starfsmenn Læknafélag Íslands skulu grípa til hæfilegra og skynsamlegra ráðstafana til að tryggja að persónuupplýsingar séu nákvæmar og réttar. Eftirfarandi verklagsreglum skal fylgja:

- Persónuupplýsingar skal geyma á eins fáum stöðum og mögulegt er.
- LÍ skal auðvelda einstaklingum að fá ónákvæmar persónuupplýsingar leiðréttar.
- Persónuupplýsingar skulu uppfærðar um leið og í ljós kemur að þær séu ekki réttar. Sem dæmi skal fjarlægja gamalt netfang starfsmanns úr gagnagrunnum um leið og það uppgötvast.

Aðgangur einstaklinga

Allir einstaklingar sem Læknafélag Íslands á upplýsingar um eiga rétt á eftirfarandi:

- Að vera upplýstir um það hvernig LÍ mætir skyldum sínum samkvæmt persónuverndarlögum.
- Að fá vitneskju um hvaða upplýsingar það eru sem LÍ á um þá.
- Að vera upplýstir um af hverju LÍ hefur þær undir höndum.
- Að krefja LÍ um aðgang að sínum persónuupplýsingum.

Þegar beiðni um aðgang berst mun LÍ grípa til allra nauðsynlegra ráðstafana til að tryggja að um sé að ræða réttan aðila. Upplýsingar skulu almennt veittar einstaklingum án endurgjalds og mun LÍ veita framangreindar upplýsingar innan þeirra tímamarka sem persónuverndarlög kveða á um.

Upplýsingagjöf til einstaklinga

Markmið Læknafélag Íslands er að einstaklingar séu meðvitaðir um að LÍ vinni persónuupplýsingar um þá og að þeir skilji

- af hverju persónuupplýsingum er safnað um þá
- hvernig LÍ notar upplýsingar um þá og
- hvernig þeir geti leitað réttar síns.

Læknafélag Íslands hefur gefið út persónuverndaryfirlýsingu um hvernig unnið er með persónuupplýsingar um einstaklinga. Þeir aðilar og aðrir geta nálgast það skjal á heimasíðu fyrirtækisins www.lis.is