

Mat á áhrifum á Persónuvernd (MÁP)

Tilgangur þessa skjals er að skjalfesta mat á áhrifum á persónuvernd samkvæmt 29. gr. laga nr. 90/2018, um persónuvernd og vinnslu persónuupplýsinga (PVL), sbr. 35. gr. reglugerðar 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 (almenna persónuverndarreglugerðin).

Skjal þetta skal fylla út vegna verkefna eða innleiðingu upplýsingakerfa sem krefjast vinnslu persónuupplýsinga og vegna umtalsverða breytinga á verkefnum eða upplýsingakerfum þar sem unnið er með persónuupplýsingar sem fela í sér mikla áhættu fyrir réttindi og frelsi hinna skráðu. Til að átta sig á því hvort þörf sé á því að framkvæma mat á áhrifum á persónuvernd er hægt að skoða lista Persónuverndar yfir vinnslur sem krefjast slíks mats:

<https://www.personuvernd.is/log-og-reglur/reglur-og-reglugerdir/auglysing-nr.-337-2019-um-skra-yfir-vinnsluadgerdir-thar-sem-krafist-er-mats-a-ahrifum-a-personuvernd>

Það er skylda þess sem ber ábyrgð á viðkomandi verkefni að tryggja að matið sé framkvæmt.

Öryggisstjóri og persónuverndarfulltrúi veita ráðgjöf við framkvæmd matsins og skylt er að veita persónuverndarfulltrúa tækifæri á að gera athugasemdir við matið. Ábyrgðaraðili verkefnisins ákveður byggt á niðurstöðu matsins, og að höfðu samráði við persónuverndarfulltrúa, hvort nauðsyn sé að leita fyrirframsamráðs við Persónuvernd skv. 30. gr. laga nr. 90/2018, sbr. 36. gr. almennu persónuverndarreglugerðarinnar.

Leiðbeiningar um framkvæmd matsins má finna hér:

<https://www.personuvernd.is/media/leidbeiningar-personuverndar/MAP-Mat-a-Ahrifum-a-Personuvernd.pdf> (íslenska)

<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/> (enska)

<https://www.datatilsynet.no/rettigheter-og-plikter/virksohmehenes-plikter/vurdere-personvernkonsekvenser/vurdering-av-personvernkonsekvenser/> (norska)

Upplýsingar um ábyrgðaraðila

Nafn	Embætti landlæknis
Efni	Bluetooth uppfærsla Rakning C-19
Tengiliðir ábyrgðaraðila	Ólafur Kristján Ragnarsson, verkefnisstjóri Arnaldur Axfjörð, öryggisstjóri Þórólfur Guðnason, sóttvarnalæknir

1: Er þörf á MÁPi?

Almenn lýsing á tilgangi verkefnisins og þeirri vinnslu persónuupplýsinga sem er nauðsynleg í tengslum við það.

Hér skal gerð grein fyrir því hvers vegna er þörf á mati á áhrifum á persónuvernd út frá þeim persónuupplýsingum sem þarf að vinna og þeirri áhættu sem sú vinnsla getur skapað. Hægt er að hafa lista Persónuverndar um MÁP skyldar vinnslur til hliðsjónar.

(Hér getur verið gagnlegt að vísa í önnur skjöl eins og verkefnislýsingu, ráðherrabréf, lagafrumvarp eða annað sem lýsir verkefninu nánar.)

Smitrakning hefur mikilvægur þáttur í sóttvarnarráðstöfunum í tengslum við yfirstandandi COVID-19 faraldur. Í apríl 2020 var gefið út smáforrit, Rakning C-19, sem aðstoðað hefur við smitakningu. Smáforritið safnar staðsetningargögnum á símtæki notandans sem getur valið að deila þeim niðurstöðum með rakningarteymi Almannaavarna greininst hann smitaður.

Nú hefur verið þróuð ný útgáfa af smáforritinu sem byggir á tækni sem þróuð var af ráðandi aðilum á sviði stýrikerfa fyrir snjallsíma, þ.e. Apple og Google. Tækni þessi er kölluð Google and Apple Exposure Notification, eða GAEN. Kerfið byggir á “random” lykllum sem notendur appsins deila með öðrum notendum í gegnum Bluetooth tækni og á sama tíma tekur viðkomandi notandi við lykllum frá öðrum notendum. Greinist viðkomandi notandi smitaður fær hann lykilorð frá starfsmanni rakningateymi sem gerir honum kleift að deila sínum lykllum. Út frá þeim upplýsingum eru þeir notendur sem uppfylla viss skilyrði og geyma lykla frá þeim smitaða á síma sínum viðvörun um þeir kunni að hafa verið útsettir fyrir smiti. Þeir sem fá slíka viðvörun fá ekki að vita frá hverjum viðvörunin stafar og yfirvöld geta heldur ekki rakið þá lykla sem miðlað er frá smituðum til þeirra sem fá viðvörun. Notkun smáforritsins er ætluð til stuðnings við þá rakningu smita sem fer þegar fram hjá rakningateymi almannaavarna.

Við uppfærslu verður slökkt á GPS skráningu sem fyrri útgáfa byggði á.

Þessi tækni er nú þegar notuð í smitakningarforritum í fjölmörgum Evrópulöndum, þ.m.t. Noregi, Danmörku, Þýskalandi, Írlandi og Austurríki.

Í tengslum við smitakningaforritið verður sett upp vefsíða þar sem þeir sem fá viðvörun í gegnum appið geta skráð sig í smitgát sem innifelur að viðkomandi berst boð í sýnatöku 7 dögum eftir útsetningu.

Þrátt fyrir að tækni Apple og Google, GAEN, byggir á ópersónugreinanlegum gögnum og að mikil vinna hafi farið í tryggja persónuvernd notenda, er ekki útilokað að í tengslum við appið kunni persónuupplýsingar um notendur þess að verða aðgengilegar beint, t.d. rakningateymi við skráningu í smitgát með sýnatöku, og óbeint t.d. notendum sem berast tilkynningar og hafa eingöngu umgengist

mjög fáa einstaklinga og geta þannig út frá dagsetningu útsetningar getið sér til um hvaða einstaklingur kann að hafa útsett þá fyrir smiti.

Niðurstaða:

Smáforritið og tengd kerfi verða notuð af yfirvöldum til þess að aðstoða við smitrakningu.

Þá getur notkun þess falið í sér að í gegnum kerfin sem notuð eru fari upplýsingar sem staðfesta að viðkomandi notandi hafi greinst með COVID-19, þ.e. þegar viðkomandi einstaklingur samþykkir að deila lykklum úr símtæki sínu.

Vinnsla persónuupplýsinga fellur því undir tvo af þeim flokkum sem tilgreindir eru í 2. gr. auglýsingar Persónuverndar nr. 828/2019, um skrá yfir vinnsluaðgerðir sem krefjast ávallt mats á áhrifum á persónuvernd: V

- 3. tl. Umfangsmikil gagnavinnsla: þar sem vonir standa til að stór hluti þjóðarinnar, ásamt ferðamönnum hlaði niður forritinu
- 4. tl. Viðkvæmar persónuupplýsingar: þar sem upplýsingum um staðfest COVID-19 smit kanna vera miðlað um kerfið

Þá má einnig segja að verið sé að notast við nýja tækni eða eldri tækni á nýjan hátt, þó vissulega hafi önnur lönd innan EES þegar tekið í notkun smitrakningarforrit byggð á GAEN. Í þessum löndum hefur verið framkvæmt MÁP.

Við gerð þessa MÁPs hefur einkum verið litið til þess mats sem fram hefur farið í Bretlandi og í Noregi þau má nálgast hér:

Bretland: <https://www.gov.uk/government/publications/nhs-covid-19-app-privacy-information/nhs-covid-19-app-data-protection-impact-assessment>

Noregur: <https://www.fhi.no/contentassets/c5f8db72042c4112a1188cea0363abea/dpia-smittestopp-version-2-03.12.2020.pdf>

2: Lýsing á vinnslu persónuupplýsinga

Hér á að lýsa tilgangi vinnslu persónuupplýsinga og því hvernig þær verða unnar: hvernig verður þeim safnað, þær notaðar, þær geymdar og þeim eytt? Hvaðan koma upplýsingarnar? Verður þeim deilt með einhverjum? Hvaða vinnsluaðgerðir eru það sem teljast fela í sér mikla áhættu? Hversu lengi verða þær geymdar?

Tilgangur vinnslu

Tilgangur vinnslunnar er að auðvelda smitrakningu vegna yfirstandandi COVID-19 faraldurs. Smáforritinu er ætlað að vera til stuðnings þeirri rakningu sem þegar fer fram á vegum smitrakningateymis almannavarna. Slík smitrakning hefur reynst árangursrík en hefur vissar takmarkanir þegar kemur að aðstæðum þar sem smitaður einstaklingur hefur umgengist einstaklinga eða hópa sem hann veit ekki deili á eða sótt staði þar sem erfitt er að viðhafa skráningu viðstaddra. Í slíkum tilfellum hefur verið haft samband við þá einstaklinga eða hópa sem vitað er að hafa verið í samskiptum við smitaðan einstakling og þeim gert að sæta sóttkví sem lýkur við sýnatöku. Þessar ráðstafanir eru nauðsynlegar til þess að hefta útbreiðslu veirunnar og vernda þá einstaklinga sem þannig fá að vita af hugsanlegu smiti og þá sem þeir umgangast. Smitrakning, snemmgreining, sóttkví og einangrun hefur verið talin lykilinn að árangursríkri baráttu við COVID-19 heimsfaraldurinn.

Með smáforritinu verður mögulegt að ná til einstaklinga sem ekki hafa bein tengsl við hinn smitaða, t.d. tilheyra ekki skilgreindum hópi sem tengist smiti, hafa sótt viðburð þar sem smitaður einstaklingur hefur verið eða annað slíkt. Smáforritið og þau kerfi sem því tengjast er því ætlað að auka möguleika á að vara einstaklinga við því að þeir hafi hugsanlega verið útsettir fyrir smiti þannig að þeir geti gætt sérstaklega að einstaklingsbundnum sóttvörnum, takmarkaða samneyti við aðra einstaklinga og fengið boð í sýnatöku til að skera úr um hvort þeir hafi sýkst.

Hverjir eru hinir skráðu?

Hinir skráðu eru allir þeir sem taka smáforritið í notkun. Það er öllum frjálst að taka Rakning C-19 í notkun og verður appið aðgengilegt í gegnum App Store og Google Play. Það mun standa öllum til boða að sækja og nota smáforritið og því eru allir Íslendingar og aðrir sem heimsækja landið mögulegir framtíðarnotendur.

Við mat á því hvort líta ætti til þess að takmarka notkun við vissan aldur var litið til þess að ekki er um umfangsmikla vinnslu að ræða. Þá er einnig nánast útilokað að koma í veg fyrir að t.d. börn undir 13 ára aldri sæki forritið, sbr. 5. mgr. 10. gr. persónuverndarlaga. Hægt er að setja aldurstakmörk á niðurhal í App Store og Google play, en þeim er ekki hægt að framfylgja með öruggum hætti. Hins vegar er hægt að koma í veg fyrir að börn yngri en 13 ára deili lykllum vegna smits án samþykkis foreldra, þar sem slík deiling er aðeins möguleg með kóða frá sem starfsmaður rakningateymis gefur upp í samtali við smitaðan einstakling. Í þeim tilvikum er því hægt að óska eftir samþykki foreldra. Einnig er mögulegt að koma í veg fyrir að börn yngri en 13 ára skrái sig í smitgát með sýnatöku á þar til gerðri vefsíðu.

Hvaða persónuupplýsingar er verið að vinna?

Smáforritið og þau kerfi sem því tengjast vinna með mismunandi tegundir persónuupplýsingar þeim er nánar lýst hér að neðan:

Rakning C-19

Þegar notandi hefur hlaðið niður forritinu og veitt samþykki fyrir því að virkja Bluetooth er útbúinn tilviljanakenndur lykill daglega, svokallaður TEK, eða Temporary Exposure Key. Þessir lykjar eru notaðir til að útbúa hlaupandi tilviljanakennd auðkenni á um 15 mínútna fresti. Þessi merki eru

svokölluð RPI, e. Rotating Proximity Identifiers, eða hlaupandi nálægðar auðkenni. Þessi merki nema aðra síma þar sem forritið er virkt og skrá á símtæki viðtakandans. Þessar upplýsingar eru eingöngu vistaðar á síma notenda og því engum öðrum aðgengilegar, þ.m.t. embætti landlæknis sem ábyrgðaraðila og útgefanda smáforritsins, eða Google eða Apple sem bjuggu til GAEN tæknina sem forritið byggir á. Þessar upplýsingar eru geymdar á símtækinu í 14 daga sem eyðast sjálfkrafa að þeim tíma liðnum. RPI gögn eru aðeins unnin á símtækjum, ekki beint aðgengileg í gegnum smáforritið og ekki er hægt að nota þau til að persónugreina einstakling og því teljast þau ekki persónuupplýsingar.

Greinist notandi með COVID-19 og samþykkir að deila upplýsingum úr appinu fær viðkomandi kóða frá starfsmanni rakningateymisins sem hann notar til þess að senda TEK lykla sína á miðlægan netþjón. Þá getur notandi einnig valið að tilgreina hvort hann finni til einkenna og þá hvenær þau byrjuðu og hvort hann hafi verið á ferðalegi s.l. 14 daga. Þeim upplýsingum er miðlað til miðlæga netþjónsins og þær notaðar til að ákvarða hverjir fá tilkynningu vegna viðkomandi smits. Þessar upplýsingar eru ekki vistaðar í forritinu.

Upplýsingum frá miðlæga netþjónum, það er um lykla sýktra aðila, er svo miðlað á u.þ.b. tveggja klukkustunda fresti til allra notenda Rakning C-19 og hlaðið niður á símtæki þeirra. Út frá TEK lyklinum eru RPI hins sýkta endursköpuð og kannað hvort þau séu skráð á símtæki annarra notenda. Sé svo fær viðkomandi notandi upplýsingar um að hann hafi útsettur fyrir smiti og á hvaða degi.

Tilkynning um úsetningu og dagsetningu hennar birtist í smáforritinu og er aðgengileg notanda í 14 daga.

Þessar upplýsingar eru í grunninn ópersónugreinanlegar. Hins vegar er það fræðilega mögulegt að tengja vissar upplýsingar við einstaklinga í þeim tilvikum þegar einstaklingur sem fær viðvörðun um mögulegt smit, ásamt dagsetningu, og hefur aðeins umgengist mjög fáa á þeim tíma. Þá væri einnig mögulegt fyrir aðila sem hefur aðgengi að miðlægum netþjónum sem tekur við TEK lyklum og veit hvenær einstaklingur hefur sent þá inn að gera sér grein fyrir hvaða upplýsingar tilheyra honum. Því er rétt að skilgreina þessar upplýsingar sem persónuupplýsingar.

Þá er notendum gert kleift að skrá símanúmer sitt í þeim tilgangi að móttaka neikvæða niðurstöðu úr landamæraskimun og mikilvægar tilkynningar sem kunna að vera sendar út t.d. um breytta stöðu faraldurs á tilteknum landsvæðum, tafir á niðurstöðum úr sýntatökum eða annað sem kann að teljast mikilvægt. Upplýsingar um símanúmer eru hins vegar aðeins aðgengilegar í síma viðkomandi notanda og á netþjónum sem hýsir símanúmerin. Ekki er hægt að tengja þessar upplýsingar við aðrar upplýsingar í smáforritinu.

Eftirfarandi persónuupplýsingar eru því unnar og þær vistaðar á síma notanda Rakning C-19:

- TEK lyklar
- Tilkynning um hugsanlega úsetningu fyrir smiti ásamt dagsetningu.
- Upplýsingar um að viðkomandi sé smitaður í þeim tilvikum sem notandi velur að tilkynna smit í gegnum forritið. Þær upplýsingar eru eingöngu aðgengilegar notanda sjálfum í smáforritinu.
- Símanúmer ef notandi velur að skrá það.

Skráningarsíða fyrir þá sem fá tilkynningu

Þegar notanda berst tilkynning um hugsanlega ústeningu fyrir smiti er honum ráðlagt að þrýsta á hnappinn Frekari upplýsingar. Notandinn flyst þá á örugga vefsíðu þar sem hann er upplýstur um það hvað tilkynningin þýðir. Þar eru ráðleggingar um smitgát og að bóka sýnatöku ef einhver einkenni gera vart við sig, ásamt tenglum t.d. á Heilsuveru þar sem hægt er að bóka sýnatöku og Covid.is þar sem má afla sér frekari upplýsinga.

Á vefsíðunni er einnig hægt að skrá sig í smitgát. Þeir sem velja að gera það fá sjálfkrafa boð í bólusetningu 7 dögum eftir útsetningu fyrir smiti.

Til skrá sig í smitgát þarf að gefa upp eftirfarandi persónuupplýsingar:

- Nafn
- Fæðingardag
- Netfang
- Símanúmer
- Hugsanleg tengsl við smit (hægt að velja veit ekki)

Þá er einnig valkvætt að gefa upp kennitölu.

Þessum upplýsingum er miðlað um örugga tengingu í sóttkvíargrunn sem er hluti smitsjúkdómaskrár. Upplýsingar sem berast með þessum hætti eru sérstaklega merktar sem upplýsingar vegna tilkynningar í Rakning C-19 og eyðast sjálfkrafa eftir 14 daga.

Starfsmenn rakningateymis hafa aðgang að þessum upplýsingum. Upplýsingarnar eru nýttar til þess að boða viðkomandi í sýnatöku og aðstoða rakningateymi við hefðbundna smitrakningu gerist þess þörf.

Miðlægur grunnur fyrir TEK lykla

Líkt og lýst er hér að ofan geta notendur Rakning C-19 valið að miðla TEK lykllum sínum greinist þeir með COVID-19. Slík miðlun fer fram á þann hátt að starfsmaður rakningateymis spyr notanda hvort hann noti forritið og vilji tilkynna um smit, þannig að aðrir notendur appsins fái tilkynningu um hugsanlega útsetningu fyrir COVID-19. Samþykki viðkomandi notandi það er útbúinn handahófskenndur kóði, af sérstöðum vefþjóni, sem starfsmaður rakningateymis tilkynnir notandanum. Notandinn þarf svo að slá þann kóða inn í forritinu til þess að deila lykklunum.

TEK lykklarnir eru geymdir í 14 daga á miðlægum netþjóni og eyðast að því loknu.

Samantekt:

Í allri þróun og hönnun GAEN lausnarinnar hefur persónuvernd og upplýsingaöryggi verið að leiðarljósi. Apple og Google þurfa sérstaklega að virkja möguleika í stýrikerfum símanna til þess að lausnin virki og er það gert eftir landsvæðum og aðeins mögulegt fyrir viðurkennd sóttvarnar- eða heilbrigðisfyrirvöld í viðkomandi löndum að koma smáforritum inni App Store og Google Play.

Við þróun á bakendakerfum og vefsíðu til að nýta þær upplýsingar sem safnast við notkun á Bluetooth tækninni hefur fyllsta öryggis og persónuverndar verið gætt. Sérstaklega hefur verið hugað að því að notkun smáforritsins er valkvæð og byggð á samþykki notenda. Þannig er það notandinn sem ákveður að hlaða niður forritinu, hann samþykkir svo þá vinnslu persónuupplýsinga sem fram fer í forritinu og veitir að auki sérstakstakt samþykki fyrir að kveikt sé Bluetooth virkninni. Smitaðir einstaklingar deila eingöngu upplýsingum af eigin vilja og enginn möguleiki er fyrir embætti landlæknis eða smitrakningarteymið að nálgast þær með öðrum hætti, þar sem þær eru eingöngu vistaðar á síma viðkomandi aðila.

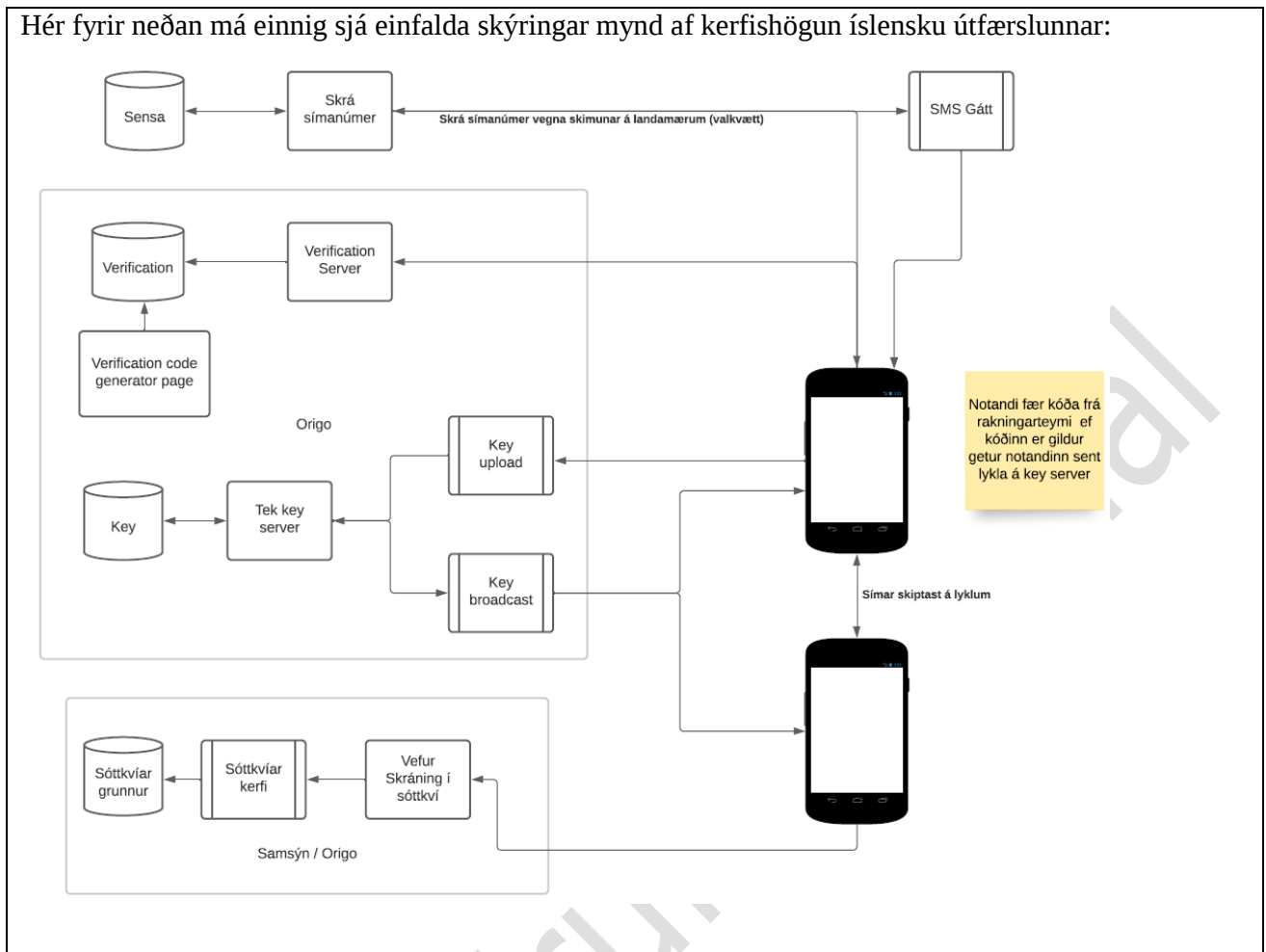
Þeir aðilar sem fá tilkynningu um hugsanlega úsetningu hafa einnig fullt val um hvort þeir skrái sig í svokallað smitgát með sýnatöku eður ei. Þeir munu engu að síður vita um hugsanlegt úsetningu og geta auðveldlega nálgast upplýsingar um hvernig rétt sé að bregðast við í gegnum smáforritið.

Ítarlegri upplýsingar um GAEN kerfi Apple og Google má nálgast hér:

<https://www.google.com/covid19/exposurenotifications/>

Þá má sjá frekari upplýsingar um íslensku útfærsluna í BluetoothAPP-kynning, sem er fylgiskjal með MÁPi þessu.

Hér fyrir neðan má einnig sjá einfalda skýringar mynd af kerfishögun íslensku útfærslunnar:



3: Vinnsluheimild, meginreglur og réttindi hinna skráðu

Hér skal gera grein fyrir vinnsluheimild viðkomandi upplýsinga, hvernig skal tryggja að meginreglur persónuverndarlaga séu virtar og réttindi hinna skráðu tryggð: Á hvaða vinnsluheimild byggjum við, lagaskylda, almannahagsmunir, samningur, samþykki?

Vinnsluheimild:

Samþykki hins skráða, sbr. 1. tl. 1. mgr. 9. gr. laga nr. 90/2018 um persónuvernd og vinnslu persónuupplýsinga.

Samþykki sbr. 1. tl. 1. mgr. 11. gr., laga nr. 90/2018, hvað varðar vinnslu viðkvæmra persónuupplýsinga.

Lögbundið hlutverk sóttvarnalæknis, sbr. 3. tl. 9. gr. og 9. tl. 11. gr. laga nr. 90/2018.

Samkvæmt sóttvarnalögum, nr. 19/1997, svo sem þeim var breytt með lögum nr. 2/2021, skal sóttvarnalæknir skv. nýjum 8. tl. 5. gr. gera faraldsfræðilega rannsókn á uppruna smits, og eftir atvikum hefja smitrakningu. Smitrakning er skilgreind á eftirfarnadi í nýjum 10. tl. 3. gr. laganna sem: *Þegar rakin eru smit á milli einstaklinga með nákvæmu samtali við þá sem eru smitaðir til að komast að því hvar viðkomandi smitaðist og hverja hann gæti hafa smitað, og önnur upplýsingaöflun í því skyni að finna þá sem kunna að hafa verið útsettir fyrir smiti.*

Samkvæmt breyttri 3. mgr. 12. gr. sóttvarnalaga skal sóttvarnalæknir rekja uppruna smits og eftir atvikum hefja smitrakningu ef farsótt ef farsótt brýst út. Skv. nýjum 4. til 7. mgr. er sóttvarnalækni heimil vinnsla persónuupplýsinga í þessum tilgangi. Þar er einnig kveðið á um að heimilt sé að safna gögnum beint frá smituðum einstaklingi, t.d. með aðstoð hugbúnaðar. Þá er þar einnig kveðið á um tiltekna ráðstafanir til að draga úr áhrifum persónuvernd viðkomandi einstaklingi, s.s. því að upplýsingar sem safnað er sérstaklega við smitrakningu sé ekki skilt að varðveita skv. lögum um opinber skjalasöfn. Þá er einnig kveðið á um heimild sóttvarnalæknis til að halda sérstaka skrá yfir einstaklinga sem sæta sóttkví.

Heimild til vinnslu persónuupplýsinga í smáforritinu, og tengdum kerfum, byggir á því fyrst og fremst á upplýstu og óþvinguðu samþykki notanda og að öðru leyti á heimildum sóttvarnalæknis skv. sóttvarnalögum. Líkt og lýst er hér að ofan þarf notandi að sjálfviljugur að hlaða niður forritinu, samþykkja að persónuupplýsingum sé safnað og að kveikt sé á Bluetooth virkninni. Þá er það einnig byggt á samþykki smitaðs einstaklings hvort hann velji að deila lykklum sínum svo hægt sé að tilkynna öðrum notendum um hugsanlega útsetningu. Þeim sem berst slík tilkynning er svo í sjálfsveld sett hvort þeir skrá sig í smitgát og sýnatöku. Um aðra vinnslu, s.s. vinnslu á þeim upplýsingum sem skráðar eru um aðila sem fengið hafa tilkynningu vísast til heimilda og lagaskyldu sóttvarnalæknis varðandi smitrakningu og aðrar sóttvarnaráðstafanir.

Varðandi ferli við boðun í sýntaöku, miðlun strikamerkja sem aðilar taka með sér í sýnatöku, greiningu sýna og miðlunar niðurstöðu vísast til lýsingar í fyrri samskiptum embættis landlæknis og Persónuverndar, m.a. vegna sóttvarnaráðstafana á landamærum. Sýnataka fer fram með sama hætti og í öðrum tilvikum og neikvæðum niðurstöðum er miðlað í gegnum Heilsuveru. Reynist sýni jákvætt er haft samband við viðkomandi af rakningateymi og göngudeild Covid hjá Landspítala. Skráning á niðurstöðum fer fram í smitsjúkdómaskrá sóttvarnalæknis, skv. sóttvarnalögum.

Hlíting við meginreglur:

Hér verður gerð grein fyrir því hvernig gætt verður að meginreglum persónuverndarlaga við vinnslu persónuupplýsinga í tengslum við nýja útgáfu af Rakning C-19.

Sanngirnireglan:

Smitrakningarforritinu, kerfi því tengd og sú vinnsla persónuupplýsinga sem fylgir notkun þeirra er ætlað að styðja baráttu við yfirstandandi farsótt. Er þar um að ræða mikla almannahagsmuni sem varða líf og heilsu.

Þeir sem velja að hlaða forritinu niður og veita þau leyfi sem þarf, þ.e. samþykki skv. persónuverndarlögum og að kveikt sé á Bluetoothtæknni í símtæki þeirra, eru vel upplýstir um tilgang þess og þá miklu almannahagsmuni sem leiða til þess að því er dreift og almenningur hvattur til að virkja það. Gerð er góð grein fyrir virkni þess í innskráningarferli og jafnframt verður sérstök vefsíða um smáforritið með frekari upplýsingum.

Fjallað hefur verið um notkun á tækni sem þessari af Evrópska persónuverndarráðinu og eru hönnun byggð á leiðbeiningum þess. Þannig er gert ráð fyrir þeim möguleika að tengjast samevrópskum gagnagrunni fyrir TEK lykila, til að gæta að samkvæmni forritisins við smittrakningaforrit annarra landa sem notast við sömu tækni, þ.e. GAEN. Ekki hefur verið ákvörðun um slíkt ennþá, en af verður verður miðlun gagna í þann gagnagrunn byggð á samþykki notenda.

Þá hefur Sóttvarnarstofnun Evrópu einnig fjallað um gagnsemi slíkra smáforrita til stuðning hefðbundinni smittrakningu.

<https://www.ecdc.europa.eu/sites/default/files/documents/covid-19-mobile-applications-contact-tracing.pdf>

Tilgangsreglan:

Tilgangur forritisins og þeirra kerfa sem því tengjast er skýrt afmarkaður, þ.e. að stuðla að árangursríkri og hraðri smittrakningu COVID-19, með því að vara þá við sem kunna að hafa verið útsettir fyrir smiti, veita þeim upplýsingar um hvernig þeir skuli bera sig að og bjóða þeim að skrá sig og fá þannig boð í sýnatöku.

Gögn verða ekki notuð í öðrum tilgangi en til smittrakningar, enda er kveðið skýrt á um það í nýrri 7. mgr. 12. gr. sóttvarnalaga að óheimilt sé að nota gögn sem aflað er við smittrakningu í öðrum tilgangi. Þá eru gögn aðeins geymd í 14 daga og eytt að þeim tíma loknum. Gögn verða því ekki nýtt öðrum tilgangi en þeim sem notendur hafa samþykkt.

Meðalhófsreglan:

Aðeins er safnað nauðsynlegum gögnum í tengslum við notkun smáforritisins, þ.e. er þeim lyklum sem sími notanda sendir frá sér og nemur frá öðrum sísum. Þá er notendum gert kleift að skrá símanúmer í appið til að móttaka tilkynningar. Þessar upplýsingar eru í grunninn ópersónugreinanlegar, geymdar dulkóðaðar á sísum notenda og aðeins miðlað ef viðkomandi greinist smitaður. Sé upplýsingum miðlað er það gert á öruggan hátt og upplýsingarnar aðeins geymdar í 14 daga.

Við skráningu í smitgát og sýnatöku er aðeins aflað nauðsynlegra upplýsinga svo hægt sé að koma upplýsingum til notandans, ásamt boði í sýnatöku með strikamerki sem nýtt er til að auðkenna sýni viðkomandi.

Haldin verður tölfraði yfir þá sem smitrakningarteymi hefur samband við og hafa þegar fengið tilkynningu í Rakning C-19 og þá hversu löngu áður þeim barst sú tilkynning. Leiði tölfraðigreining til þeirrar niðurstöðu að smitrakning með aðstoð forritsins bæti engu við þá hefðbundnu smitrakningu sem stuðst er við verður ráðlagt að hætta notkun þess, þar sem hún væri óþarfi og uppfyllti þannig ekki skilyrði um meðalhóf.

Áreiðanleikareglan:

Stillingar í smáforritinu gera það að verkum að eingöngu þeir sem hafa verið í minna en 2 metra frá öðrum einstaklingi í 15 mínútur eða meira fá viðvörðun um hugsanlega útsetningu. Er þar miðað við sömu reglu og notuð er við hefðbundna smitrakningu. Bluetooth tæknin er hins vegar ekki óbrigðul hvað þetta varðar, þar sem mögulegt er að hún gefi vissar falskar tilkynningar. Það er hins vegar metið svo að þar sem að afleiðingar þess að fá tilkynningu er ekki aðrar en þær að viðkomandi fær viðvörðun og getur skráð sig í smitgát og sýnatöku séu upplýsingar nægilega áreiðanlegar til að uppfylla tilgang vinnslunnar. Hægt er að breyta þeim viðmiðunum sem virkja tilkynningar, t.d. stytta fjarlægð eða tíma, og kann að vera að slíkt verði gert bendi rannsóknir á smiti til þess að það sé nauðsynlegt.

Varðandi upplýsingar um smitaða einstaklinga koma þær frá smitrakningarteymi, sem fær nöfn og kennitölur allra smitaðra einstaklinga til þess að hægt sé að rekja smit þeirra. Starfsmaður smitrakningarteymis sér svo að upplýsa notanda smáforritsins um kóða sem þarf til að senda inn TEK lykila, kjósi notandinn að gera svo. Því ættu þær upplýsingar að teljast áreiðanlegar.

Varðandi upplýsingar um þá sem skrá sig í smitgát og sýnatöku byggja þær á þeim upplýsingum sem viðkomandi aðili gefur upp. Þar þarf að gefa upp bæði símanúmer og tölvupóstfang og berst viðkomandi SMS til staðfestingar á skráningu og kennitölu. Við boðun í sýnatöku er notast við sömu tengiliðaupplýsingar. Þær upplýsingar verða því aldrei réttari en viðkomandi aðili gefur upp. Þessi sami háttur hefur verið hafður á við landamæraskimun og ekki hefur borið á misnotkun. Því eru þessar upplýsingar taldar áreiðanlegar.

Varðveislureglan:

Varðveislutími upplýsinga er takmarkaður. Þær upplýsingar sem safnast á símtæki viðkomandi eru geymdar í 14 daga og eyðast sjálfkrafa að þeim tíma liðnum, að frátöldu símanúmeri þeirra sem velja að skrá það. Símanúmerið er geymt á meðan smáforritið er í notkun, en notandi getur hvenær sem er valið að eyða því.

Varðveislutími ganga í öðrum kerfum tengdum smáforritinu, það er netþjóns fyrir TEK lykila og sóttkvíargrunni þar sem upplýsingar um þá sem skrá sig í smitgát er einnig takmarkaður við 14 daga og eyðast upplýsingar sjálfkrafa að þeim tíma liðnum.

Öryggisreglan:

Öryggi gagna á símtækjum notenda er tryggt með þeim hætti að upplýsingar eru dulkóðaðar í tækinu. RPI lykilar eru þar engum aðgengilegir. Að öðru leyti er öryggi tækja eingöngu jafn öruggt og notandi velur. Komist einhver yfir tæki viðkomandi og opni forritið gæti viðkomandi mögulega nálgast upplýsingar um tilkynningu um hugsanlega útsetningu og upplýsingar um að viðkomandi sé smitaður og hafi tilkynnt smit í gegnum appið. Því verður brýnt fyrir notendum í upplýsingum um appið að læsa símtækjum sínum með t.d. fingrafari, andlitsmynd eða öruggu lykilorði.

Öryggi gagna í flutning milli símtækis og netþjóna er tryggt með dulkóðun samskipta, það á einnig við um vefsíðu til skráningar í smitgát og sýnatöku.

Upplýsingar sem aflagð er í gegnum skráningarsíðu og miðlað í sóttkvíargrunn eru eingöngu aðgengilegar starfsfólki smitrakningarteymis. Aðgangi að þeim grunni er stýrt með rafrænum skilríkjum og allt aðgengi er skráð (loggað).

Framkvæmt hefur verið áhættumat á helstu eignum og er það fylgiskjal með þessu MÁPi. Þá hefur einnig farið fram öryggisúttekt af hálfu óháðra sérfræðinga í upplýsingaöryggi og eru niðurstöður hennar einnig að finna í fylgiskjali.

Réttindi hinna skráðu:

Þar sem vinnsla persónuupplýsinga byggir á samþykki hinna skráðu er mikil áhersla lögð á að tryggja að þeim sé veitt nægileg fræðsla. Þannig koma upplýsingar um vinnslu persónuupplýsinga fram á samþykkisskjá í appinu, sjá fylgiskjal BluetoothAPP-kynning og fylgiskjal Samþykki og Persónuvernd. Í þeim texta er einnig hlekkur á persónuverndarstefnu fyrir Rakning C-19. Hana er að finna á sérstakri síðu fyrir forritið undir Covid.is þar sem einnig verða aðgengilegar ýmsar upplýsingar um smáforritið.

Þá getur hinn skráði hvenær sem er valið að eyða forritinu og við það fellur samþykki fyrir vinnslu úr gildi.

Varðandi möguleika hinna skráðu til að nýta sér önnur réttindi svo sem rétt til aðgangs að eigin gögnum, eyða eða leiðrétta gögn, takmarka vinnslu, óska eftir að gögn séu flutt til annars ábyrgðaraðila bera fram kvörtun til Persónuverndar er upplýst um þau réttindi í persónuverndarstefnu.

Persónuverndarstefnuna má finna í fylgiskjali.

Það er mismunandi eftir því hvaða upplýsingar um ræðir hver réttindanna er hægt að nýta. Varðandi þær upplýsingar sem vistast á símtæki notanda eru þær eingöngu aðgengilegar honum sjálfum. Honum er hins vegar frjálst að eyða forritinu og við það er upplýsingum eytt. Þá er einnig mögulegt að eyða einstökum TEK lykllum með því að fara í gegnum stýrikerfi símans. Leiðbeiningar um þann möguleika verður að finna á vefsíðu með upplýsingum um forritið.

TEK lykllum sem miðlað hefur veirð á vefþjón er ekki hægt að eyða þar sem þeir eru ópersónugreinanlegir og ekki hægt að finna út hvaða lykklar tilheyra hvaða notanda. Þar er því ekki heldur hægt að leiðrétta þá, veita aðgengi að þeim eða takmarka vinnslu þeirra.

Varðandi upplýsingar í sóttkvíargrunni sem miðlað er í gegnum vefsíðu fyrir skráningu í smitgát og sýnatöku þá geta hinir skráðu óskað eftir því að nýta þau réttindi sem þeim eru tryggð samkvæmt persónuverndarlögum, þ.e. til aðgangs að eigin gögnum, leiðréttingar, eyðingar, flutnings gagna og takmörkunar vinnslu.

4: Samráð við hlutaðeigandi aðila

Hvernig var samráði háttað: lýsing á því hvernig samráð var haft við hina skráðu, t.d. með því að kynna fyrirhugaða vinnslu opinberlega og kalla eftir sjónarmiðum skráðra einstaklinga. Þetta gæti t.d. verið sjúklingahópur eða hópur heilbrigðisstarfsfólks sem halda á sérstaka skrá um eða almenningur ef um er að ræða skrá sem nær yfir alla sjúklinga sem koma á heilsugæslu. Ef ekki var haft samráð við slíka hópa skal útskýra hvers vegna. Þá skal gerð grein fyrir samráði við aðila innan embættis landlæknis sem tengjast fyrirhugaðri vinnslu. Einnig getur verið nauðsynlegt að hafa samráð við vinnsluaðila og fá hans sjónarmið eða utanaðkomandi öryggissérfræðinga eða aðra sérfræðinga sem gætu haft mikil sjónarmið fram að færa.

Samráð var haft við starfsmenn þeirra sviða embættis landlæknis sem málið varðar.

Starfsfólk sóttvarnalæknis var leiðandi í þessari vinnu og þeirra sjónarmið þau mikilvægustu vegna tilgangs vinnslunnar. Reglulegir fundir voru haldnir með þeim málið varðaði.

Starfsfólk miðstöðvar rafrænna heilbrigðislausna stýrði vinnu varðandi upplýsingatækni mál og samskiptum við vinnsluaðila og þróunaraðila þeirra lausna sem nýttar eru við vinnsluna. Þá var einnig haft samráð við öryggisstjóra embættisins og persónuverndarfulltrúa.

Einnig var fundað með fulltrúum Apple og Google og veittu þeir m.a. ráðgjöf um uppsetningu á netþjónum í tengslum við verkefnið. Þá var rætt við fulltrúa heilbrigðisyfirvalda í öðrum löndum þar sem sambærileg smáforrit hafa verið þróuð og tekin í notkun.

Öryggissérfræðingar á vegum Syndis gerðu úttekt á skipulagslegum og tæknilegum öryggisráðstöfunum, ásamt því sem náði samráð var haft við vinnsluaðila og þróunaraðila lausna, Stokk, Origo og Sensa.

Ekki var leitað samráðs við skráða einstaklinga þar sem það þótti ekki gerlegt vegna fjölbreytileika þess hóps sem kann að nota appið. Þá var ekki talið að gerlegt væri að bregðast við slíkum ábendingum þar sem svigrúm til breytinga er mjög takmarkað af þeim kröfum sem Apple og Google gera til þeirra lausna sem styðjast við GAEN lausnina.

5: Áhætta fyrir réttindi og frelsi hinna skráðu og ráðstafanir til að draga úr áhættu

Í fylgiskjalinu Áhættumat – MÁP – Rakning C-19 er gerð grein fyrir helstu áhættu fyrir réttindi og frelsi hinna skráðu ásamt þeim ráðstöfunum sem gripið hefur verið til. Þar er einnig að finna skilgreiningar á bak við áhættustig og líkur ásamt því að þar er að finna áhættumatrísu.

Við gerð þessa MÁPs hefur verið miðað við að áhætta eftir ráðstafanir verði ekki meiri en miðlungs, skv. skilgreiningum í fylgiskjalinu. Er það vegna eðlis þeirra upplýsinga sem um ræðir, þ.e. upplýsingar tengdum heilsufari að erfitt er að lágmarka áhættu meira en það.

6: Undirskriftir, samantekt á ráðleggingum persónuverndarfulltrúa og áætlun um eftirfylgni

Item	Name/position/date	Notes
Ráðstafanir samþykktar af:	Ólafur Kristján Ragnarsson, verkefnisstjóri embættis landlæknis, 25. Mars.	Tryggja að þær ráðstafanir sem grípa skal til séu að fullu komnar til framkvæmdar áður en vinnsla hefst.
Áhætta eftir ráðstafanir samþykkt af:	Arnaldur Axfjörð, öryggisstjóri, embættis landlæknis, 25. Mars.	Ef áhætta eftir ráðstafanir telst miðlungs eða hærri skal að höfðu samráði við persónuverndarfulltrúa leitað fyrirframsamráðs við Persónuvernd.
Ráðleggingar persónuverndarfulltrúa:	Hólmur Örn Finnsson, persónuverndarfulltrúi embættis landlæknis, 25. Mars.	Persónuverndarfulltrúi skal eiga kost á því að veita ráðleggingar við val á ráðstöfunum og vinnslu persónuupplýsinga almennt í verkefninu.

Samantekt af ráðleggingum persónuverndarfulltrúa:

Persónuverndarfulltrúi telur að vinnsla persónuupplýsinga í tengslum við notkun á Rakning C-19 teljist fela í sér ásættanlega áhættu fyrir Persónuvernd sé tekið mið af þeim tilgangi sem lagt er upp með. Svo virðist sem gætt hafi verið meðalhófs í vinnslu persónuupplýsinga til að vinna að þeim miklu almannahagsmunum sem undir eru.

Persónuverndarfulltrúi telur að vel hafi verið staðið að þróun og öryggisráðstöfunum, miðað við þær upplýsingar sem liggja fyrir.

Persónuverndarfulltrúi lagði til vissar breytingar, s.s. varðandi skýrara samþykki notenda fyrir vinnslu persónuupplýsinga með nægilegum upplýsingum um þá vinnslu sem fram fer. Einnig var lagt til að kannað yrði hvort það gera einstaklingum eingöngu kleift að skrá sig í sóttkví vegna tilkynninga eða

skrá ekki neitt væri rétta leiðin, eða hvort hægt væri að bjóða uppá mildara úrræði sem jafnframt gæfi notendum aukið öryggi varðandi stöðuna hvað varða útsetningu fyrir Covid-19. Endanleg útfærsla sú sem lýst er í þessu MÁPi virðist hafa tekið tillit til þessara athugasemda.		
Ráðleggingum persónuverndarfulltrúa fylgt eða þeim hafnað. Ábyrgðaraðili verkefnis staðfestir:	Ráðleggingum persónuverndarfulltrá var fylgt. Staðfest af: Ólafur Kristján Ragnarsson	Ef ráðleggingum persónuverndarfulltrúa er ekki fylgt skal gerð grein fyrir því hvers vegna.
Athugasemdir:		
Álit þeirra aðila sem leitað var samráðs við. Samþykkt eða ekki. Ábyrgðaraðili verkefnis staðfestir:	Sjá öryggisúttekt Syndis Tekið var tillit til þarfa smitrakningateymis og starfsmanna sóttvarnalæknis. Staðfest af: Ólafur Kristján Ragnarsson	Ef ekki er tekið tillit til athugasemd sem berast við samráð skal gerð grein fyrir því hvers vegna.
Athugasemdir:		
Áhættumatið verður uppfært og því fylgt eftir af:	Ólafur Kristján Ragnarsson	Ef breytingar verða á vinnslu sem hefur áhrif á matið skal persónuverndarfulltrúi upplýstur og veitt tækifæri til að gera athugasemdir.
7. Fylgiskjöl		
Áhættumar-MÁP-Rakning C19, excel skjal Áhættumat Rakning C-19-Eignir, excel BluetoothApp-kynning, pdf Samþykki og Persónvernd – skjár rakning C19, pdf. Öryggisúttekt Syndis-Bluetooth-RakningC19, pdf Uppfærð persónuverndarstefna Rakning-C19, word skjal		