

# REGLUR

## um öryggi persónuupplýsinga við framkvæmd vísindarannsóknna á heilbrigðissviði.

### I. KAFLI

#### Efni, gildissvið o.fl.

##### 1. gr.

##### *Efni og markmið.*

Markmið reglna þessara er að tryggja öryggi við vinnslu persónuupplýsinga við framkvæmd vísindarannsóknna á heilbrigðissviði. Í því felst að tryggja leynd upplýsinganna gagnvart óviðkomandi, lögmætan aðgang að þeim, sem og gæði þeirra og áreiðanleika að því marki sem nauðsyn krefur í ljósi hagsmuna hinna skráðu af friðhelgi einkalífs.

Að öðru leyti en kemur fram í reglum þessum má til hliðsjónar og leiðbeiningar styðjast við staðalinn ÍST EN ISO/IEC 27001:2017 Upplýsingatækni – Öryggisaðferðir – Stjórnunarkerfi um upplýsingaöryggi – Kröfur.

##### 2. gr.

##### *Gildissvið.*

Reglur þessar gilda um vinnslu persónuupplýsinga í þágu vísindarannsóknna á heilbrigðissviði sem fellur undir lög nr. 90/2018 um persónuvernd og meðferð persónuupplýsinga og reglugerð (ESB) 2016/679.

##### 3. gr.

##### *Leyfi vísindasiðanefndar eða síðanefndar heilbrigðisrannsóknna.*

Öll meðferð heilbrigðisgagna í þágu vísindarannsóknna á heilbrigðissviði, þ. á m. samkeyrslur, öflun og notkun upplýsinga úr heilbrigðisskrám og öflun og notkun lífsýna, skal eiga stoð í og samrýmast leyfi frá vísindasiðanefnd eða síðanefnd heilbrigðisrannsóknna, veittu samkvæmt 12. gr. og, eftir atvikum, 27. gr. laga nr. 44/2014 um vísindarannsóknir á heilbrigðissviði. Þá er aðgangur að heilbrigðisgögnum háður leyfi ábyrgðaraðila þeirra, sbr. 2. mgr. síðarnefnda ákvæðisins.

##### 4. gr.

##### *Almennar kröfur.*

Til viðbótar því sem greinir í reglum þessum ber, við framkvæmd vísindarannsóknna á heilbrigðissviði, að fara að almennum kröfum til öryggis persónuupplýsinga samkvæmt 27. gr. laga nr. 90/2018 og 32.–34. gr. reglugerðar (ESB) 2016/679. Þá ber að fara að ákvæðum laganna og reglugerðarinnar að öðru leyti, sem og ákvæðum laga nr. 44/2014, reglna settra með stoð í þeim og öðrum lögum sem við eiga hverju sinni.

### II. KAFLI

#### Öryggisráðstafanir.

##### 5. gr.

##### *Trúnaður við öflun samþykkis.*

Þess skal gætt að trúnaður um persónuupplýsingar einstaklinga í rannsóknarúrtaki rofni ekki þegar til þeirra er leitað til að fá samþykki fyrir þátttöku í rannsókn, sbr. reglur vísindasiðanefndar nr. 230/2018 um hvernig velja má og nálgast fólk til þátttöku í vísindarannsóknnum á heilbrigðissviði og hvaða fræðslu skuli veita því áður en samþykkis þess er aflað.

##### 6. gr.

##### *Gagnasöfnun – auðkenning gagna.*

Við söfnun og skráningu heilbrigðisupplýsinga í þágu vísindarannsóknar á heilbrigðissviði, sem fram fer á grundvelli leyfis vísindasiðanefndar eða síðanefndar heilbrigðisrannsóknna, skal þess gætt

að í rannsóknargögnum liggja ekki fyrir auðkenning á því frá hvaða einstaklingum upplýsingarnar stafa.

Til að ná markmiði 1. mgr. skal þess gætt að í rannsóknargögnum komi ekki fyrir nein persónuauðkenni eða ígildi slíkra auðkenna, svo sem nöfn einstaklinga og kennitölur, heimilisföng, símanúmer eða annað sambærilegt. Persónuauðkenni skulu dulkóðuð eða þeim skipt út fyrir rannsóknarnúmer. Þá skulu breytur, sem gætu gert upplýsingar rekjanlegar til einstaklinga í ljósi samhengis, afmáðar eða gerðar grófari til að koma í veg fyrir slíkt. Getur það meðal annars falið í sér að aldursupplýsingar miðist, eftir atvikum, við tiltekin árabíl sem einstaklingar eru fæddir á, að ekki komi fram nákvæmar upplýsingar um þjóðerni heldur að einstaklingar séu til dæmis fæddir hérlendis eða erlendis, svo og að upplýsingar séu ekki auðkenndar með póstnúmerum þar sem fáir búa og slík póstnúmer því sameinuð til að mynda grófari auðkenni.

Þrátt fyrir 1. mgr. er heimilt að notast við persónuauðkenni tímabundið við söfnun upplýsinga liggja fyrir að slíkt sé nauðsynlegt til að tryggja áreiðanleika rannsóknargagna. Á það einkum við ef afla þarf heilbrigðisupplýsinga um einstaklinga í rannsóknarúrtaki úr fleiri en einni skrá og ekki reynist unnt, án notkunar persónuauðkenna, að tengja upplýsingar í rannsóknargögnum við rétta einstaklinga. Þegar heilbrigðisupplýsingar hafa verið skráðar í rannsóknargögn, og eftir atvikum staðreynt að þær séu réttar, og gögnin að öðru leyti fullgerð, skulu persónuauðkenni afmáð og þess gætt að öðru leyti að ekki verði unnt að rekja upplýsingar til einstaklinga út frá því sem fram kemur í gögnunum.

#### 7. gr.

##### *Greiningar- og dulkóðunarlyklar.*

Heimilt er að útbúa greiningarlykil sem tengir saman persónuauðkenni og rannsóknarnúmer, enda sé slíkt nauðsynlegt í ljósi rannsóknarmarkmiða. Þá er með sama skilyrði heimilt að útbúa dulkóðunarlykil til að afkóða dulkóðunarnúmer sem umbreytast þá í persónuauðkenni. Greiningar- og dulkóðunarlyklar skulu ávallt varðveittir aðskildir frá öðrum rannsóknargögnum á öruggan hátt.

#### 8. gr.

##### *Meðferð lífsýna.*

Lífsýni, sem tekin eru úr rannsóknarþátttakendum eða aflað úr lífsýnasafni í samræmi við ákvæði laga nr. 110/2000 um lífsýnasöfn og söfn heilbrigðisupplýsinga, skulu varðveitt á tryggum stað þar sem þau njóta verndar fyrir skemmdum. Um auðkenningu þeirra fer eftir 6. gr. reglna þessara, þó að undanskilinni 3. mgr. þeirrar greinar. Að lokinni notkun lífsýna skal þeim eytt, þeim skilað til þess lífsýnasafns sem þeirra var aflað úr eða þau send til frambúðarvarðveislu í lífsýnasafni vísindasýna. Skal varðveisla í slíku safni samrýmast samþykki hlutaðeigandi einstaklinga.

#### 9. gr.

##### *Samkeyrslur.*

Samkeyrslur skulu fara fram undir dulkóðuðum persónuauðkennum. Sé utanaðkomandi aðili fenginn til að annast samkeyrslu skal gerður vinnslusamningur við þann aðila í samræmi við 25. gr. laga nr. 90/2018 og 28. gr. reglugerðar (ESB) 2016/679.

Persónuvernd getur veitt undanþágu frá kröfu 1. mgr. um dulkóðun persónuauðkenna við samkeyrslur, enda verði aðrar ráðstafanir, metnar í heild sinni, taldar geta veitt persónuupplýsingum nægilega vernd. Skulu þá persónuauðkenni fjarlægð þegar að samkeyrslu lokinni og rannsóknarnúmer sett í staðinn. Undanþágur samkvæmt þessari málsgrein geta ekki verið veittar aðilum sem hafa með höndum reglulegar, kerfisbundnar samkeyrslur.

#### 10. gr.

##### *Öryggi í gagnaflutningi.*

Þess skal gætt við flutning gagna, þ. á m. lífsýna, sem unnið er með vegna vísindarannsókna á heilbrigðissviði, að þau komist ekki í hendur óviðkomandi, né heldur glatist eða skemmist þannig að einkalífshagsmunir sjúklings skaðist eða, eftir atvikum, hagsmunir hans af öruggri meðferð. Einkum ber að líta til síðarnefndu hagsmunanna þegar um ræðir annars vegar lyfjarannsóknir og hins vegar

lífsýni sem tekin hafa verið í þágu meðferðar sjúklings og aflað hefur verið úr safni þjónustusýna í samræmi við lögbundnar heimildir þar að lútandi.

Til að ná markmiði 1. mgr. skulu heilbrigðisgögn, sem send eru rafrænt, varin með tæknilegum aðferðum, svo sem dulkóðun. Einnig skulu minnislyklar og aðrir færirlegir geymslumiðlar, sem notaðir eru til flutnings heilbrigðisgagna, vera í innsigliðum umbúðum og boðsendir, auk þess sem beitt skal tæknilegum aðferðum, svo sem dulkóðun, til að verja gögn. Þá skulu lífsýni boðsend í innsigliðum umbúðum. Að öðru leyti ber að gera þær ráðstafanir sem við eiga hverju sinni til að tryggja öryggi í gagnaflutningi.

#### 11. gr.

##### *Varðveisla persónuupplýsinga.*

Þegar varðveisla skráðra persónuupplýsinga og lífsýna er ekki lengur nauðsynleg í þágu rannsóknar skal þeim eytt nema því aðeins að þeim hafi verið komið fyrir í safni heilbrigðisupplýsinga eða lífsýnasafni í samræmi við 7. gr. laga nr. 44/2014, sbr. lög nr. 110/2000 um lífsýnasöfn og söfn heilbrigðisupplýsinga, sbr. lög nr. 45/2014. Skal flutningur gagna í safn heilbrigðisupplýsinga eða lífsýnasafn samrýmast kröfum 9. gr. reglna þessara. Að flutningnum loknum fer um öryggi gagnanna samkvæmt reglum nr. 660/2019 um öryggi við vinnslu persónuupplýsinga í söfnum heilbrigðisupplýsinga og reglum nr. 920/2019 um öryggi við meðferð og varðveislu lífsýna í lífsýnasöfnum.

#### 12. gr.

##### *Fyrirmæli Persónuverndar.*

Persónuvernd getur sett fyrirmæli um öryggisráðstafanir vegna vísindarannsókna á heilbrigðisviði, sbr. 3. másl. 2. mgr. 13. gr. laga nr. 44/2014. Geta slík fyrirmæli tekið til einstakra vinnsluáðgerða í þágu rannsóknar, svo sem samkeyrslna, en einnig vinnslu vegna tiltekinnar rannsóknar í heild sinni, sem og fleiri en einnar og, eftir atvikum, allra rannsókna á vegum sama rannsakanda.

### III. KAFLI

#### **Önnur atriði.**

#### 13. gr.

##### *Mat á áhrifum á persónuvernd.*

Um skyldu til að gera mat á áhrifum á persónuvernd fer samkvæmt 29. gr. laga nr. 90/2018 og 4. mgr. 35. gr. reglugerðar (ESB) 2016/679, sbr. einnig auglýsingu nr. 828/2019 um skrá yfir vinnsluáðgerðir sem krefjast ávallt mats á áhrifum á persónuvernd, sbr. einkum 4.-8. tölul. 2. gr. og 6., 8., 10. og 13. tölul. 3. gr. þeirrar auglýsingar.

Gerð umsóknar til vísindasiðanefndar eða siðanefndar heilbrigðisrannsókna, sbr. 9.-12. gr. laga nr. 44/2014, telst fela í sér mat á áhrifum á persónuvernd í samræmi við framangreint, enda hafi þau atriði sem talin eru upp í 7. mgr. 35. gr. reglugerðar (ESB) 2016/679 verið tekin til fullnægjandi skoðunar og þau skrásett í umsókn eða, eftir atvikum, fylgigögn með henni. Teljist þess þörf í ljósi eðlis vinnslunnar getur Persónuvernd, við málsmeðferð samkvæmt 13. gr. laga nr. 44/2014 og í fyrirmælum samkvæmt 12. gr. reglna þessara, krafist ítarlegra mats, enda sé þess talin þörf í ljósi eðlis eða umfangs vinnslu.

#### 14. gr.

##### *Flutningur heilbrigðisgagna úr landi.*

Séu heilbrigðisgögn, sem aflað hefur verið í þágu rannsókna, þ. á m. lífsýni, flutt úr landi, skal þess gætt að þau séu ekki merkt með persónuauðkennum. Sé um að ræða land, sem ekki veitir fullnægjandi persónuupplýsingavernd, skal þess ávallt gætt að gögnum verði eytt strax að úrvinnslu í landinu lokinni, eða þau að öðrum kosti send rannsakanda hér á landi, nema samþykki hins skráða standi til annars. Að öðru leyti fer um flutning heilbrigðisgagna úr landi vegna vísindarannsókna samkvæmt V. kafla reglugerðar (ESB) 2016/679.

15. gr.

*Innra eftirlit.*

Viðhafa skal stöðugt innra eftirlit í því skyni að tryggja að þær aðgerðir sem gripið er til á grundvelli reglna þessara séu örugglega viðhafðar. Einnig skal innra eftirlit lúta að því að sannreyna að unnið sé í samræmi við reglur þessar, lög nr. 90/2018, reglugerð (ESB) 2016/679, lög nr. 44/2014 og önnur lög sem kunna að eiga við um vinnslu persónuupplýsinga í þágu vísindarannsókna á heilbrigðissviði.

16. gr.

*Gildistaka.*

Reglur þessar, sem settar eru samkvæmt heimild í 3. mgr. 13. gr. laga nr. 44/2014 um vísindarannsóknir á heilbrigðissviði, öðlast þegar gildi.

*Persónuvernd, 8. júní 2020.*

**Björg Thorarensen** formaður.

Helga Þórisdóttir.