Nr. 920 4. október 2019

REGLUR

um öryggi við meðferð og varðveislu lífsýna í lífsýnasöfnum.

I. KAFLI
Efni, gildissvið o.fl.

1. gr.
Efni og gildissvið.

Reglur þessar lúta að því hvernig tryggja skuli öryggi við meðferð og varðveislu lífsýna í lífsýnasöfnum skv. lögum um lífsýnasöfn nr. 110/2000. Að öðru leyti en kemur fram í reglunum skal til leiðbeiningar hafa hliðsjón af eftirfarandi alþjóðlegum stöðlum:

1. ÍST EN ISO/IEC 27001:2017 – Upplýsingatækni – Öryggisaðferðir – Stjórnunarkerfi um upplýsingaöryggi – Kröfur.
2. ÍST EN ISO/IEC 27002:2017 – Upplýsingatækni – Öryggisaðferðir – Starfsvenjur fyrir upplýsingaöryggi.

Reglur þessar taka ekki til lífsýna sem varðveitt eru tímabundið vegna þjónusturannsókna, meðferðar, eða afmarkaðra vísindarannsókna, enda sé slíkum sýnum eytt þegar þjónustu, meðferð eða rannsókn lýkur.

2. gr.
Skilgreiningar.

Í öryggi við vinnslu lífsýna í lífsýnasöfnum felst að tryggja varðveislu, eðlilega leynd þeirra, lögmætan aðgang að þeim, gæði og áreiðanleika. Nánar tiltekið felst öryggið í að tryggja:

1. Að lífsýni séu ekki aðgengileg þeim sem ekki skulu hafa aðgang að þeim.
2. Að tryggja vandaða meðferð lífsýna og að þau hvorki glatist né skemmist.
3. Að tryggja þeim sem þurfa og mega hafa aðgang að lífsýnum og fylgigögnum, slíkan aðgang þegar lögmæt ástæða er til.

II. KAFLI
Öryggisreglur.

3. gr.
Öryggisstefna.

Stjórn lífsýnasafns skal marka stefnu um öryggi lífsýna og gefa út og viðhalda öryggisstefnu fyrir lífsýnasafnið. Við það má hafa hliðsjón af 5. kafla í staðlinum ÍST EN ISO/IEC 27002:2017 Upplýsingatækni – Öryggisaðferðir – Starfsvenjur fyrir upplýsingaöryggi.

4. gr.
Rekstur lífsýnasafns.

Rekstur lífsýnasafns felst í því að veita lífsýnum viðtöku, varðveita þau og veita lögmætan aðgang að þeim. Þeim einum er heimill slíkur rekstur sem hefur leyfi ráðherra skv. 4. gr. laga nr. 110/2000, í reglum þessum nefndur leyfishafi. Sé lífsýnasafn starfrækt í þágu vísindarannsókna á heilbrigðissviði er honum skylt að halda rekstri þess aðskildum frá annarri starfsemi sem hann hefur með höndum. Með aðskildum rekstri er m.a. átt við að tryggja skuli aðskilnað milli annars vegar þeirra er leyfa notkun á gögnum lífsýnasafns og hafa eftirlit með henni og hins vegar þeirra sem vilja fá að nota sýnin eða hafa þar hagsmuna að gæta. Mæla má fyrir um það í samningum safnstjórnar og þeirra sem leggja gögn í safnið á grundvelli 7. gr. b í lögum nr. 110/2000 hvernig þeir hagsmunir skuli tryggðir innan ramma laganna.

Halda verður meðferð heilsufarsupplýsinga um sýnagjafa og upplýsinga um niðurstöður sýnarannsókna aðskilinni frá rekstri lífsýnasafnsins. Skilgreina skal hvernig staðið verður að afgreiðslu beiðna vísindamanna og annarra um aðgang að lífsýnum. Í því felst að gera verður greinarmun á vinnslu lífsýna vegna daglegrar þjónustu við sjúklinga, afhendingu lífsýna vegna vísindarannsókna og afhendingu sýna í öðrum tilvikum að fengnu leyfi Persónuverndar, veittu að fullnægðum skilyrðum 5. mgr. 9. gr. laga nr. 110/2000.

5. gr.

Lýsing á stjórnun öryggismála.

Leyfishafi skal setja fram skriflega lýsingu á stjórnun öryggismála lífsýnasafnsins. Þar skulu a.m.k. öll eftirtalin atriði koma fram eftir því sem við á:

1. Með hvaða hætti rekstri lífsýnasafns sé haldið aðskildum frá annarri starfsemi leyfishafa, sbr. 4. gr.
2. Með hvaða hætti þess sé gætt í lífsýnasafni vísindasýna að slík lífsýni séu án persónuauðkenna, sbr. 1. mgr. 8. gr. laga nr. 110/2000, og hvernig persónuauðkenni séu varðveitt. Einnig hvaða starfsmaður beri ábyrgð á vörslu persónuauðkenna og öryggi gagna sem gera kleift að tengja þau við lífsýni. Að auki skal tilgreint hver það er sem ber ábyrgð á dulkóðun auðkenna í samræmi við 6. málsl. 4. mgr. 7. gr. sömu laga.
3. Hvernig staðið hafi verið að mati á áhrifum á persónuvernd í samræmi við 35. gr. reglugerðar (ESB) 2016/679, sbr. 29. gr. laga nr. 90/2018.
4. Hvernig innbyggð og sjálfgefin persónuvernd sé tryggð, sbr. 25. gr. reglugerðar (ESB) 2016/679, sbr. 24. gr. laga nr. 90/2018.
5. Hvernig staðið hafi verið að mati á áhættu í samræmi við 2. mgr. 32. gr. reglugerðar (ESB) 2016/679, sbr. 1. mgr. 17. gr. laga nr. 90/2018.
6. Hvaða öryggisráðstafanir séu viðhafðar í samræmi við 1. mgr. 32. gr. reglugerðar (ESB) 2016/679, sbr. fyrrgreint ákvæði laga nr. 90/2018.
7. Hvar lífsýni séu varðveitt og hver beri daglega ábyrgð á öryggi þeirra.
8. Hvaða leiðbeiningar starfsmenn hafi fengið um viðbrögð við öryggisógnum og öryggisbrestum.
9. Hvernig öryggisráðstafanir einstakra deilda safnsins hafi verið samræmdar, ef safnið er deildaskipt.
10. Hvernig staðið sé að aðgangsstjórnun.

Leyfishafi skal tilkynna Persónuvernd með sannanlegum hætti hver fari með fyrirsvar gagnvart Persónuvernd um alla þætti er varða meðferð lífsýna og persónuupplýsinga á vegum safnsins, þ. á m. á því að uppfyllt séu skilyrði 3. mgr. 9. gr. laga nr. 110/2000.

Leyfishafi skal að öðru leyti uppfylla þau skilyrði sem Persónuvernd ákveður á hverjum tíma.

Persónuvernd skal hafa aðgang að skjölum samkvæmt reglum þessum hvenær sem eftir er leitað í samræmi við þá upplýsingaskyldu gagnvart stofnuninni, auk landlæknis og vísindasiðanefndar, sem mælt er fyrir um í 6. gr. laga nr. 110/2000.

6. gr.

Ytra öryggi og aðrar öryggisráðstafanir.

Viðhafa skal ráðstafanir til að hindra og takmarka tjón af völdum óheimils aðgangs að lífsýnasafni. Í því skyni skal þess gætt að hýsa sýni og persónuauðkenni á fyrirfram skilgreindum svæðum er lúta skýrri aðgangsstjórnun. Þá skal haga ytra umhverfi safnins þannig að það hindri óheimilan aðgang, skemmdir og truflanir. Þegar vinnudegi lýkur, eða þegar ekki er verið að vinna með sýni, skal varðveita þau eftir því sem við verður komið í læstum hirslum eða með öðrum sambærilega tryggum hætti.

Viðhafa skal sérstakar ráðstafanir til að draga úr hættu á truflunum, að rekstur rofni eða lífsýni og persónuvernd skaðist. Í því skyni skal viðhafa vinnuferli er tryggi órofinn rekstur lífsýnasafns og dragi úr hættu á truflunum vegna óhappa eða annarra atvika sem ógna öryggi þess, t.d. af völdum náttúruhamfara, slysa, bilunar í búnaði eða skemmdarverka. Skal annars vegar viðhafa fyrirbyggjandi ráðstafanir og hins vegar ráðstafanir er geri kleift að endurræsa hrunin kerfi og eftir atvikum að endurheimta upplýsingar sem kunna að hafa glatast eða skemmst.

7. gr.

Öryggisráðstafanir varðandi starfsmannamál.

Beita skal öryggisráðstöfunum varðandi starfsmannamál í því skyni að draga úr hættu á tjóni af völdum mannlegra mistaka, þjófnaðar, svika eða annarrar misnotkunar.

Taka skal afstöðu til ábyrgðar á öryggismálum við gerð ráðningarsaminga og í annars konar samningum sem varða starfsemina og/eða starfsmanninn. Skal ábyrgð skipt eftir því sem við á til að draga úr hættu á vanrækslu eða vísvitandi misnotkun upplýsinga eða upplýsingakerfa. Fylgjast skal

reglulega með því að unnið sé í samræmi við umsamda ábyrgð viðkomandi starfsmanns. Taka skal afstöðu til þess að hvaða marki kanna skuli hvort tiltekin atriði í ferli umsækjanda um starf gefi tilefni til að óttast að ráðning hans raski öryggi safnsins. Allir starfsmenn, og aðrir sem aðgang hafa að lífsýnum og persónuupplýsingum, skulu bundnir trúnaði og undirrita sérstakar trúnaðaryfirlýsingar því til staðfestingar.

Veita skal starfsmönnum leiðbeiningar um viðbrögð við öryggisógnum og öryggisbrotum.

8. gr.

Aðgangsstjórnun.

Viðhafa skal aðgangsstjórnun í því skyni að stjórna aðgangi að upplýsingum til að tryggja öryggi þeirra, sbr. 2. gr. reglna þessara. Skal þar höfð hliðsjón af öryggiskröfum og þeim ákvörðunum sem leyfishafi, stjórn lífsýnasafns eða annar þar til bær aðili hefur tekið um miðlun upplýsinga og aðgang að þeim.

9. gr.

Ákvarðanir um öryggismál.

Skilgreina skal, rökstyðja og skjalfesta allar þær ákvarðanir sem teknar eru um öryggismál, þ. á m. um viðbrögð ef öryggisráðstafanir bregðast. Leyfishafi skal staðfesta ákvarðanirnar með formlegum hætti.

III. KAFLI

Önnur atriði.

10. gr.

Endurskoðun og innra eftirlit.

Endurskoða skal reglulega, og eigi sjaldnar en árlega, þær aðgerðir sem gripið er til á grundvelli reglna þessara. Slík endurskoðun skal fara fram með reglulegu millibili og hvenær sem þurfa þykir, s.s. við verulegar breytingar á rekstraraðstæðum og umhverfi.

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, gildandi lög og reglugerð um lífsýnasöfn og önnur lög sem kunna að eiga við um rekstur lífsýnasafna.

11. gr.

Gildistími o.fl.

Reglur þessar eru settar samkvæmt 9. tölul. 1. mgr. 5. gr. laga nr. 110/2000 um lífsýnasöfn og söfn heilbrigðisupplýsinga og öðlast þegar gildi. Samhliða birtingu þeirra falla úr gildi fyrri reglur um sama efni nr. 918/2001.

Persónuvernd, 4. október 2019.

Björg Thorarensen formaður stjórnar.

Helga Þórisdóttir forstjóri.

B-deild – Útgáfud.: 23. október 2019