

Leiðbeinandi reglur um meðferð persónuupplýsinga hjá lífeyrissjóðum.

1. gr.

Persónuupplýsingar

Persónuupplýsingar eru sérhverjar persónugreindar eða persónugreinanlegar upplýsingar um einstakling, látinn eða lifandi.

Viðkvæmar persónuupplýsingar sem kunna að liggja hjá lífeyrissjóðnum eru einkum upplýsingar um heilsuhagi.

2. gr.

Gæði gagna og vinnsla

Við meðferð persónuupplýsinga hjá lífeyrissjóðnum skal þess gætt að þær séu:

1. Unnar með sanngjörnum, málefnalegum og lögmætum hætti og að öll meðferð þeirra sé í samræmi við vandaða vinnsluhætti persónuupplýsinga.
2. Fengnar í yfirlýstum, skýrum, og málefnalegum tilgangi og ekki unnar frekar í öðrum og ósamrýmanlegum tilgangi.
3. Nægilegar, viðeigandi og ekki umfram það sem nauðsynlegt er miðað við tilgang vinnslunnar.
4. Áreiðanlegar og uppfærðar eftir þörfum. Persónuupplýsingar sem eru óáreiðanlegar eða ófullkomnar, miðað við tilgang með vinnslu þeirra, skal afmá eða leiðrétta.
5. Varðveittar í því formi að ekki sé unnt að bera kennsl á skráða aðila lengur en þörf krefur miðað við tilgang vinnslu. Varðveita skal gögn a.m.k. jafn lengi og viðkomandi gögn geta verið þáttur í úrskurði lífeyrissjóðsins til greiðslu lífeyris.

3. gr.

Heimild til vinnslu persónuupplýsinga

Vinnsla er sérhver aðgerð eða röð aðgerða þar sem unnið er með persónuupplýsingar, hvort heldur sem vinnslan er handvirk eða rafræn.

Til að vinnsla persónuupplýsinga sé heimil þurfa skilyrði sem tilgreind eru í 8. og 9. gr. laga um persónuvernd og meðferð persónuupplýsinga nr. 77/2000 að liggja fyrir. Varðandi heimildir lífeyrissjóða má einkum tilgreina að einhverjir eftirfarandi þátta þurfa að vera fyrir hendi:

- a) fyrir liggi samþykki hins skráða;
- b) vinnslan sé nauðsynleg til að efna samning sem hinn skráði er aðili að eða til að gera ráðstafanir að beiðni hins skráða áður en samningur er gerður;
- c) vinnslan sé nauðsynleg til að fullnægja lagaskyldu sem hvílir á lífeyrissjóðnum;
- d) vinnslan sé nauðsynleg til að vernda brýna hagsmuni hins skráða;
- e) vinnslan sé nauðsynleg vegna verks sem unnið er í þágu almannahagsmuna;
- f) vinnslan sé nauðsynleg við beitingu opinbers valds;

g) vinnslan sé nauðsynleg til að unnt sé að gæta lögmætra hagsmuna nema grundvallarréttindi og frelsi hins skráða sem vernda ber samkvæmt lögum vegi þyngra.

Til að vinnsla með viðkvæmar persónuupplýsinga sé heimil þarf eitthvert ofangreindra skilyrða að vera til staðar og enn fremur eitthvert af eftirfarandi skilyrðum:

- a) hinn skráði samþykki vinnsluna;
- b) sérstök lagaheimild standi til vinnslunnar;
- c) lífeyrissjóði beri skylda til vinnslunnar samkvæmt samningi aðila vinnumarkaðarins;
- d) vinnslan sé nauðsynleg til að verja verulega hagsmuni hins skráða eða annars aðila sem ekki er sjálfur fær um að gefa samþykki sitt skv. a. lið;
- e) vinnslan sé nauðsynleg til að krafa verði afmörkuð, sett fram eða varin vegna dómsmáls eða annarra slíkra laganauðsynja;
- f) vinnslan sé nauðsynleg vegna tölfræði- eða vísindarannsóknna, enda sé persónuvernd tryggð með tilteknum ráðstöfunum eftir því sem við á.

4. gr.

Aðgangur og varðveisla

Aðgangur að persónuupplýsingum skal aðgangsstýrður og takmarkaður við þá starfsmenn lífeyrissjóðsins sem vinna með viðkomandi gögn. Viðkvæmar persónuupplýsingar skulu ekki vera aðgengilegar öðrum en þeim starfsmönnum sem vinna innan viðkomandi einingar eða deildar og þurfa aðgang að þeim upplýsingum til að sinna starfi sínu.

Þess skal gætt við sendingar og geymslu persónurekjanlegra gagna að þau komist ekki í hendur annarra en þeirra sem þurfa starfs síns vegna að vinna með þau. Þannig skal hugað að aðgangsstýringum, meðhöndlun lykilorða og öryggis við sendingar gagna s.s. milli lækna og lífeyrissjóðsins og að pappírsgögn séu geymd í læstum hirslum að loknum vinnudegi.

Eftirlitsaðilum skal heimilaður aðgangur að persónuupplýsingum að því marki sem nauðsynlegt getur talist til að unnt sé að sinna lögbundnu eftirlitshlutverki.

5. gr.

Þagnarskylda

Aðilar skv. 4. og 6. gr. eru bundnir þagnarskyldu um þau atriði sem þeir fá vitneskju um og leynt skulu fara samkvæmt lögum, fyrirmælum eða eðli máls. Þagnarskyldan helst þó látið sé af viðkomandi starfi.

6. gr.

Útvistun og innra eftirlit

Innan lífeyrissjóðsins skal viðhafa kerfi sem felur í sér eftirlit með því að meðferð persónuupplýsinga sé í samræmi við gildandi reglur og þær öryggisráðstafanir sem ákveðnar hafa verið. Semji lífeyrissjóðurinn við vinnsluaðila um að annast ákveðin verkefni skal sannreynt að hann uppfylli viðeigandi öryggisráðstafanir og innra eftirlit. Samningur við vinnsluaðila skal vera skriflegur og þar tilgreint að aðeins sé heimilt að vinna með persónuupplýsingar í samræmi við

fyrirmæli lífeyrissjóðsins og að sömu skyldur hvíli á vinnsluaðila og lífeyrissjóðnum um meðferð persónuupplýsinga.

7. gr.

Öryggisstefna, áhættumat og ráðstafanir

Lífeyrissjóðurinn skal gera viðeigandi tæknilegar og skipulagslegar öryggisráðstafanir til að vernda persónuupplýsingar gegn ólöglegri eyðileggingu, gegn því að þær glatist eða breytist fyrir slysi og gegn óleyfilegum aðgangi.

Beita skal ráðstöfunum sem tryggja nægilegt öryggi miðað við áhættu af vinnslunni og eðli þeirra gagna sem verja á, með hliðsjón af nýjustu tækni og kostnaði við framkvæmd þeirra.

Lífeyrissjóðurinn setur sér skriflega öryggisstefnu og reglulega skal framkvæma áhættumat og öryggisráðstafanir ákvarðaðar fyrir vinnslu persónuupplýsinga. Við þá vinnu skal tekið mið af reglum um öryggi persónuupplýsinga og leiðbeinandi tilmælum Fjármálaeftirlitsins um upplýsingakerfi eftirlitsskyldra aðila.

8. gr.

Aðgangur sjóðfélaga og annarra að upplýsingum

Sjóðfélagi eða umboðsmaður hans á rétt á aðgangi að upplýsingum er hann varðar og skulu afrit gagna afhent sé eftir því óskað. Þess skal sérstaklega gætt að umboðsmaður hafi sannanlegt umboð frá sjóðfélaga til að fá aðgang að upplýsingum.

Þrátt fyrir ákvæði 1. mgr. skal það metið hvort réttur sjóðfélaga til að fá gögn þykir eiga að víkja að nokkru eða öllu leyti fyrir hagsmunum annarra eða hans eigin. Við slíkt mat kann að þurfa að taka tillit til heilsu sjóðfélaga og hagsmuna venslamanna hans. Í slíkum tilvikum má samkvæmt beiðni veita umboðsmanni sjóðfélaga vitneskjuna, enda mæli engar sérstakar ástæður gegn því. Sé talið að það þjóni ekki hagsmunum sjóðfélaga að fá upplýsingar s.s. aðgang að læknisvottorðum kann að vera rétt að beina því til sjóðfélaga að snúa sér beint til viðkomandi læknis.

Almennt skal ekki veita öðrum en sjóðfélaga eða umboðsmanni hans aðgang að viðkvæmum persónuupplýsingum. Ríkar ástæður þarf til að svo verði en slíkt kann þó að vera réttlætlegt við ákveðnar aðstæður s.s. við mat á hagsmunum eftirlifandi maka eða afkomanda látins sjóðfélaga.

9. gr.

Fræðsluskyllda

Lífeyrissjóðurinn skal veita sjóðfélaga upplýsingar um tilgang öflunar, varðveislu og skráningu á upplýsingum og sjóðfélagi skal sérstaklega upplýstur um afleiðingar þess séu umbeðnar upplýsingar ekki veittar.

10. gr.

Varðveislutími gagna

Þess skal gætt að gögn séu varðveitt á aðgengilegan hátt þann tíma sem sjóðfélagi eða aðrir kunna að byggja réttindi sín á upplýsingunum. Þegar ekki þykir lengur málefnalegar ástæður til að varðveita upplýsingar skal það metið hvort þeim skuli eytt eða eftir atvikum hvort afhenda beri þau Þjóðskjalasafni til varðveislu.

Staður og dagsetning

Reglur þessar voru unnar af vinnuhópi á vegum LL. Þær voru sendar Persónuvernd til umsagnar og hefur verið tekið tillit til gagnlegra ábendinga sem bárust þaðan. Sendar í ofangreindu formi á sjóðina í ágúst 2014.