REGLUR

um öryggi persónuupplýsinga.

I. KAFLI
Markmið og gildissvið.

1. gr.
Markmið.

Markmið reglna þessara er að tryggja öryggi við vinnslu persónuupplýsinga. Í því felst að tryggja eðlilega leynd upplýsinganna, lögmætan aðgang að þeim, gæði þeirra og áreiðanleika.

Að öðru leyti en kemur fram í reglum þessum má til hliðsjónar og leiðbeiningar styðjast við staðalinn ÍST BS 7799 Stjórnun upplýsingaverndar.

2. gr.
Gildissvið.

Reglur þessar gilda um vinnslu persónuupplýsinga sem lög nr. 77/2000, um persónuvernd og meðferð persónuupplýsinga, taka til.

Persónuvernd getur veitt undanþágu frá fyrirmælum reglna þessara ef um er að ræða vinnslu persónuupplýsinga sem ekki telst hafa í för með sér hættu fyrir friðhelgi einkalífs, t.d. þegar litið er til umfangs vinnslunnar, áhættu af vinnslunni og eðlis þeirra gagna sem verja á.

II. KAFLI
Öryggiskerfi.

3. gr.

Ábyrgðaraðila ber að útbúa öryggiskerfi til að tryggja vernd persónuupplýsinga. Undirbúningur öryggiskerfis fer fram í þessum áföngum:

1. Ábyrgðaraðili setur sér skriflega *öryggisstefnu*. Í henni skal m.a. koma fram almenn lýsing á afstöðu æðsta stjórnanda ábyrgðaraðila til öryggismála. Við mótun öryggisstefnu skal taka mið af því hvaða persónuupplýsingar skuli vernda, hvernig skuli vernda þær og þeirri aðferð sem viðhöfð verður við vinnslu þeirra.
2. Ábyrgðaraðili gerir skriflegt *áhættumat*. Áhættumat er mat á hættunni á því að óviðkomandi fái aðgang að persónuupplýsingum, geti breytt upplýsingunum eða skert öryggi þeirra að öðru leyti. Áhættumat tekur einnig til athugunar á umfangi og afleiðingum hættunnar m.t.t. eðlis þeirra persónuupplýsinga sem unnið er með. Markmið áhættumats er að skapa forsendur fyrir vali á öryggisráðstöfunum, sbr. III. kafla reglna þessara. Þá skal tilgreina hvað geti farið úrskeiðis, hvaða áhrif slíkt geti haft á öryggi upplýsinganna og hvaða líkur séu á slíku. Áhættumat skal endurskoðað reglulega.
3. Ábyrgðaraðili velur hvaða *öryggisráðstafanir* skulu viðhafðar í samræmi við III. kafla reglna þessara og setja fram skriflega lýsingu á þeim. Í lýsingunni skal m.a. koma fram afstaða ábyrgðaraðilans til þess hvað sé ásættanleg áhætta við vinnsluna. Þá skal rakið hvaða öryggisráðstöfunum verði beitt og hvernig þær verði útfærðar, þ.á m. við hönnun, þróun, rekstur, prófun og viðhald þess kerfis, þ.m.t. hugbúnaðar, sem notað verður við vinnslu upplýsinganna. Þar skal og tekið fram hvernig brugðist verði við áföllum í rekstri vinnslukerfisins, hvernig flutningi persónuupplýsinga milli vinnslukerfa verði hagað, þ. á m. mögulegum flutningi gagna milli ábyrgðar- og vinnsluaðila. Öryggisráðstafanir skal endurskoða reglulega.

Persónuvernd skal hvenær sem hún óskar hafa aðgang að öryggisstefnu ábyrgðaraðila, áhættumati og lýsingu á viðkomandi öryggisráðstöfunum.

III. KAFLI
Öryggisráðstafanir.

4. gr.
Almennt.

Ábyrgðaraðili skal gera viðeigandi öryggisráðstafanir og ber ábyrgð á því að vinnsla persónuupplýsinga séu í samræmi við lög, reglur og fyrirmæli Persónuverndar um hvernig tryggja skuli öryggi upplýsinga, þ.m.t. þá staðla sem hún ákveður. Markmið skipulags- og tæknilegra öryggisráðstafana er til að tryggja nægilegt öryggi og vernda persónuupplýsingar gegn ólöglegri eyðileggingu, gegn því að þær glatist eða breytist fyrir slysni, gegn óleyfilegum aðgangi og gegn allri annarri ólögmætri vinnslu.

Við val öryggisráðstafana skal taka mið af áhættu af vinnslunni og eðli þeirra gagna sem verja á. Skulu þær tryggja nægilegt öryggi með hliðsjón af nýjustu tækni og kostnaði við framkvæmd þeirra. Sé persónuupplýsingum miðlað um netið skal taka mið af þeirri auknu áhættu sem sú aðferð hefur í för með sér.

5. gr.
Öryggisráðstafanir varðandi starfsmannamál.

Í þeim tilgangi að fyrirbyggja og takmarka tjón af völdum mannlegra mistaka, þjófnaðar, svika og annarrar misnotkunar, skal ábyrgðaraðili grípa til þeirra öryggisráðstafana sem við eiga hverju sinni, t.d.:

1. Kanna feril umsækjenda um störf.
2. Fá skjalfestar þagnaryfirlýsingar starfsmanna.
3. Skilgreina með skýrum hætti hlutverk og skyldur hvers starfsmanns sem hefur aðgang að persónuupplýsingum, þ.á m. hverjir beri ábyrgð á einstökum skráasöfnum.
4. Gera nauðsynlegar ráðstafanir til þess að starfsmönnum sé með reglubundnum hætti gerð grein fyrir starfsskyldum sínum og þeim afleiðingum sem það getur haft í för með sér að brjóta þær.

6. gr.
Ytra öryggi.

Í þeim tilgangi að fyrirbyggja og takmarka tjón af völdum óheimils aðgangs, skal ábyrgðaraðili grípa til þeirra öryggisráðstafana sem við eiga hverju sinni, t.d.:

1. Stýra aðgangi að húsnæði með úthlutun lykla, aðgangskorta o.þ.h.
2. Viðhafa öryggisvörslu, t.d. með öryggisvörðum, viðvörunarkerfum eða rafrænni vöktun.

7. gr.
Skipulagslegar og tæknilegar öryggisráðstafanir.

Í þeim tilgangi að fyrirbyggja og takmarka tjón af völdum bilana og óheimils aðgangs að vinnslubúnaði, skal ábyrgðaraðili grípa til þeirra öryggisráðstafana sem við eiga hverju sinni, t.d.:

1. Stýra aðgangi að búnaði með úthlutun aðgangs- og lykilorða.
2. Dulkóða eða eyða persónuauðkennum, eða að setja númer í stað persónuauðkenna og varðveita greiningarlykil með tryggum hætti.
3. Tryggja rekjanleika uppflettinga og vinnsluaðgerða.

4. Varðveita persónuupplýsingar á ónettengdri tölvu.
5. Takmarka aðgang að persónuupplýsingum við lesaðgang (uppflettiaðgang), svo sem í þeim tilgangi að hindra óheimila eyðingu, afritun eða samkeyrslu.
6. Viðhafa sívirkar veiruvarnir.

IV. KAFLI
Innra eftirlit.

8. gr.

Ábyrgðaraðili skal viðhafa innra eftirlit með vinnslu persónuupplýsinga til að ganga úr skugga um að unnið sé í samræmi við gildandi lög og reglur, þ. á m. þá skilmála sem Persónuvernd hefur sett um viðkomandi vinnslu.

Innra eftirlit skal m.a. beinast að:

1. Athugun á því hvort vinnslan sé heimil skv. lögum nr. 77/2000.
2. Hvort fullnægt hafi verið tilkynningar- eða leyfisskyldu þeirri sem kveðið er á um í lögunum.
3. Hvort uppfylltar séu reglur 7. gr. laganna um lögmæti vinnslu, þ. á m. ákvæði 5. tl. um eyðingu persónuupplýsinga sem ekki þarf að varðveita lengur, miðað við upphaflegan tilgang með söfnun þeirra.
4. Hvort virt séu í framkvæmd ákvæði um rétt hins skráða samkvæmt lögunum.
5. Hvort fylgt sé þeim öryggisráðstöfunum sem valdar hafa verið skv. c-lið 1. mgr. 3. gr. og III. kafla reglna þessara.
6. Innra eftirlit skal viðhaft með reglubundnum hætti. Tíðni eftirlitsins og umfang þess skal ákveðið með hliðsjón af áhættunni sem er samfara vinnslunni, eðli þeirra gagna sem unnið er með, þeirri tækni sem notuð er til að tryggja öryggi upplýsinganna og kostnaði af eftirlitinu. Það skal þó eigi fara fram sjaldnar en árlega.

Að jafnaði skal viðhafa innra eftirlit samkvæmt fyrirfram skilgreindu kerfi.

Ábyrgðaraðili skal sjá til þess að gerð sé skýrsla um hverja aðgerð sem er liður í innra eftirliti. Í slíkri skýrslu skal lýsa niðurstöðu hvers þáttar eftirlitsins. Skýrslur um innra eftirlit skal varðveita tryggilega og hefur Persónuvernd rétt til aðgangs að þeim hvenær sem þess er óskað.

V. KAFLI
Vinnsluaðili.

9. gr.

Ábyrgðaraðila er heimilt að semja við tiltekinn aðila um að annast, í heild eða að hluta til, þá vinnslu persónuupplýsinga sem hann ber ábyrgð á. Slíkt er þó háð því skilyrði að ábyrgðaraðili hafi áður sannreynt að umræddur vinnsluaðili geti viðhaft þær öryggisráðstafanir sem um vinnsluna gilda og framkvæmt innra eftirlit með vinnslunni.

Samningur skv. 1. mgr. skal vera skriflegur og í að minnsta kosti tveimur eintökum. Þar skal m.a. koma fram að vinnsluaðili skuli starfa í samræmi við fyrirmæli ábyrgðaraðila og að ákvæði reglna þessara um skyldur ábyrgðaraðila gildi einnig um þá vinnslu sem vinnsluaðili framkvæmir. Ábyrgðaraðili og vinnsluaðili skulu hvor varðveita sitt eintak af samningnum.

Hafi vinnsluaðili staðfestu í öðru EES ríki en ábyrgðaraðili, sbr. 1. mgr. 6. gr. laga nr. 77/2000, þá skal jafnframt geta þess í samningi að lög og reglur þess ríkis þar sem vinnsluaðili hefur staðfestu, gildi um öryggisráðstafanir við vinnslu persónuupplýsinga.

Hverjum þeim er starfar í umboði ábyrgðaraðila eða vinnsluaðila er aðeins heimilt að vinna með persónuupplýsingar í samræmi við fyrirmæli ábyrgðaraðila, nema lög mæli fyrir á annan veg.

VI. KAFLI
Gildistaka o.fl.

10. gr.
Tilkynning til Persónuverndar um öryggisráðstafanir.

Í tilkynningu til Persónuverndar skv. 31. gr. laga nr. 77/2000 skal koma fram með hvaða hætti ábyrgðaraðili fullnægir ákvæðum reglna þessara.

11. gr.
Gildistaka.

Reglur þessar, sem settar eru samkvæmt heimild í 11. og 12. gr. laga nr. 77/2000, um persónuvernd og meðferð persónuupplýsinga, öðlast þegar gildi.

Persónuvernd, 20. mars 2001.

Páll Hreinsson.

Sigrún Jóhannesdóttir.