

Hvernig innleiðum við persónuverndarlögin inn í skjala- og upplýsingastórn fyrirtækja og stofnana?
Hverju þarf að breyta í verklagi?

04.04.2018

Ásgerður Kjartansdóttir

Skjalastjóri Landsnets

Dagskrá

- Verklag sem er skylda
- Verklag sem er æskilegt
- Dæmi frá Landsneti

Vegferð Landsnets við innleiðingu

LANDSNET

Ágúst 2017	Vinnuhópur skipaður Undirbúningur úttektar
Sept.-okt.	Úttekt á vinnslu persónuupplýsinga Forgangsröðun úrbóta
Nóv.-des.	Kortlagning á UT kerfum sem hýsa persónuupplýsingar Persónuverndarreglur (3)
Janúar 2018	Fræðsla fyrir stjórnendur og þá sem sýsla með persónuupplýsingar Kortlagning á nauðsynlegum breytingum
Febrúar - mars	Fræðsla fyrir stjórnendur og þá sem sýsla með persónuupplýsingar Breytingar á verklagi Vinnsluskrá og vinnslusamningar
Apríl - maí	Innleiðing Fræðsla

Skylda

- Öryggisbrot - tilkynningar
- Innra eftirlit með vinnslu persónuupplýsinga
- Áhættumat

Æskilegt

- Beiðnir frá einstaklingum um leiðréttingu, aðgang, eyðingu eða takmörkun á vinnslu persónuupplýsinga
- Samþykki sem eintaklingar veita um vinnslu persónuupplýsinga
- Fyrirtæki með mörg UT kerfi – skilgreina eigendur kerfa, hlutverk eigenda og skyldur

Öryggisbrot

- Skylt er að tryggja viðunandi öryggi persónuupplýsinga m.t.t. nýjustu tækni, kostnaði við framkvæmd, eðli, umfangi, samhengi og tilgangi vinnslunnar og áhættu.
- Lögin krefjast þess að nýr hugbúnaður og UT-kerfi séu útfærð með sérstaka áherslu á friðhelgi einstaklinga og á þann hátt að hún sé innbyggð í viðkomandi lausn. Gengið verður út frá því að hámarksáhersla á persónuvernd sé sjálfgefin í öllum kerfum.
- Hvað er öryggisbrot?
brot á öryggi sem leiðir til óviljandi eða ólögsmætrar eyðingar persónuupplýsinga sem eru sendar, varðveittar eða unnar á annan hátt eða að þær glatist, breytist, verði birtar eða aðgangur veittur að þeim í leyfisleysi
- Á vef Persónuverndar eru góðar leiðbeiningar
Leiðbeiningar um tilkynningar um öryggisbrot

Tilkynning öryggisbrota

- Viðbrögð við öryggisbroti – tilkynningaskylda til Persónuverndar
 - Tilkynna innan 72 klst. frá því brots verður vart
 - Tilkynning til Persónuverndar er eingöngu nauðsynleg þegar líklegt er talið að öryggisbrotið leiði af sér **áhættu** fyrir réttindi og frelsi einstaklings.
 - Tilkynning til einstaklinga eru eingöngu nauðsynleg þegar líklegt er að öryggisbrot leiði af sér **mikla áhættu** fyrir réttindi og frelsi þeirra.
- Skylda að hafa verklag og viðbragðsáætlun
hvernig tilkynnt
hver ber ábyrgð á að tilkynna Persónuvernd um öryggisbrot
- Skylda að halda skal skrá yfir öryggisbrot

Skrá yfir öryggisbrot

Skylda að halda skal skrá yfir öryggisbrot

Dæmi frá Persónuvernd

Dæmi	Tilkynning til Persónuverndar?	Tilkynning til einstaklings?	Athuga
i. Ábyrgðaraðili varðveitti afrit af gögnum, sem innihéldu persónuupplýsingar, á geisladiski, en upplýsingarnar voru dulkóðaðar. Geisladisknum er stolið í innbroti.	Nei.	Nei.	Svo lengi sem gögnin eru dulkóðuð með aðferð sem byggir á nýjustu tækni, t.d. með algrími, og til eru önnur afrit af gögnunum, og afritunarlykillinn er ekki í hættu, kann þetta ekki að vera brot sem þarf að tilkynna um.
ii. Ábyrgðaraðili heldur úti þjónustu á netinu. Í kjölfar netárásar á þjónustuna eru persónuupplýsingar einstaklinga gerðar aðgengilegar, Viðskiptavinir ábyrgðaraðilans eru allir staðsettir í einu aðildarríki.	Já, þegar það er líklegt að brotið hafi einhverjar afleiðingar fyrir einstaklinganna í ljósi þess að hér er um að ræða öryggisbrot sem veldur því að persónuupplýsingar verða óaðgengilegar.	Já, en fer eftir eðli persónuupplýsinganna sem um er að ræða og alvarleika áhættunnar fyrir einstaklingana.	Ef áhættan er ekki mjög mikil, þá er mælt með því að upplýsa hina skráðu – en það fer þó eftir eðli aðstæðnanna. Til dæmis kann tilkynningar ekki að vera þörf þegar um er að ræða öryggisbrot varðandi fréttabréf um sjónvarpsþætti, en tilkynningar kann að vera þörf ef þetta fréttabréf getur leitt til þess að pólitísk skoðun hins skráða er gerð opinber.

Innra eftirlit

- Innra eftirlit með vinnslu persónuupplýsinga framkvæmt árlega
skýrsla tekin saman um eftirlitið og hún varðveitt

Skylda

- Öryggisbrot - tilkynningar
- Innra eftirlit með vinnslu persónuupplýsinga
- Áhættumat

Æskilegt

- Beiðnir frá einstaklingum um leiðréttingu, aðgang, eyðingu eða takmörkun á vinnslu persónuupplýsinga
- Samþykki sem eintaklingar veita um vinnslu persónuupplýsinga
- Fyrirtæki með mörg UT kerfi – skilgreina eigendur kerfa, hlutverk eigenda og skyldur

Beiðnir frá einstaklingum

Réttur starfsfólks og ytri aðila

- fá aðgang að eigin persónuupplýsingum
- leiðréttu upplýsingar
- takmarka/andmæla/afturkalla vinnslu
- flytja eigin gögn
- eyða gögnum (ekki leyfilegt hjá afhendingarskyldum aðilum)

Verklag

- Hver tekur á móti beiðnum
- Hver vinnur úr beiðnunum
- Svarfestur 30 dagar, max 2 mánuðir

- Einkafyrirtæki setji verlagsreglur um eyðingu persónuupplýsinga (hverju eytt, hvenær, hver eyddi, hvernig eytt)

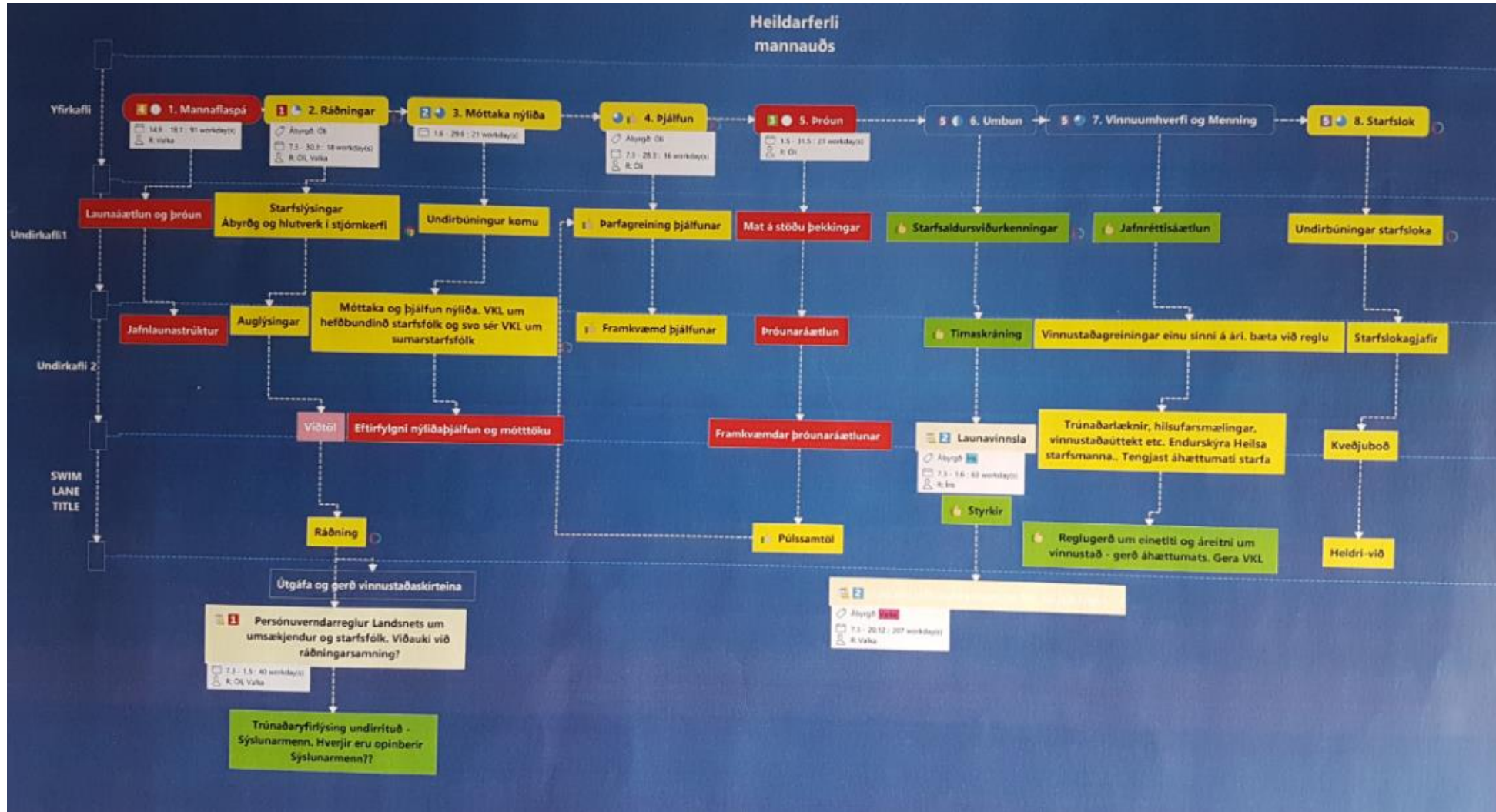
Samþykki

- Ef vinnsla byggir á samþykki þarf samþykki að vera óþvinguð, sértæk, upplýst og ótvíræð viljayfirlýsing hins skráða um að hann samþykki
 - a) með yfirlýsingu eða
 - b) ótvíræðri staðfestingu
- Fyrirtæki þurfa að geta sýnt fram á að skráður einstaklingur hafi samþykkt vinnslu persónuupplýsinga um sig
 - halda vel utan um allt sem einstaklingar samþykkja

Mörg UT kerfi með persónuupplýsingum

- Skilgreina eigendur kerfa
- Skilgreina hlutverk eigenda og skyldur
- Rík fræðsluskylda gagnvart starfsfólki sem telst vera eigendur UT-kerfa

Heildarferli mannaúðs



Dæmi tengt beiðnum

LANDSNET

Skjal: VIN-33

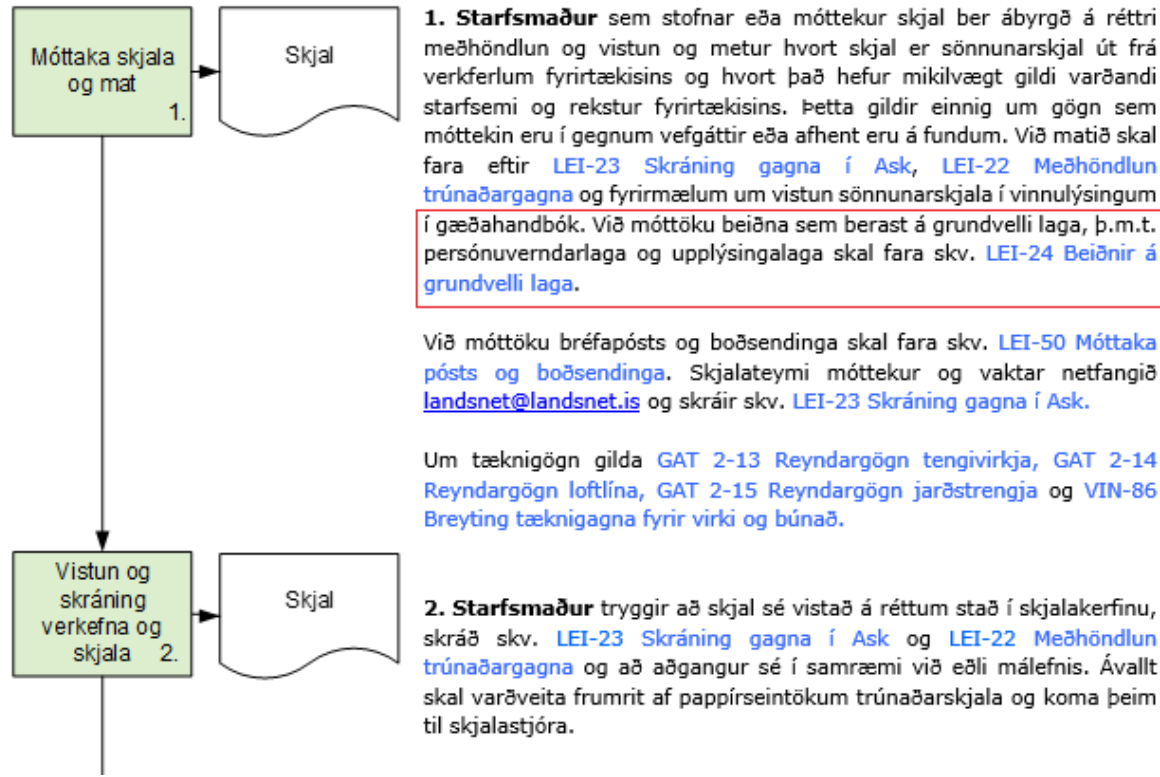
Útgáfa: 4.0

Útgáfudagur: 28.03.2018

Samþykkt af: Framkvæmdastjóra ST

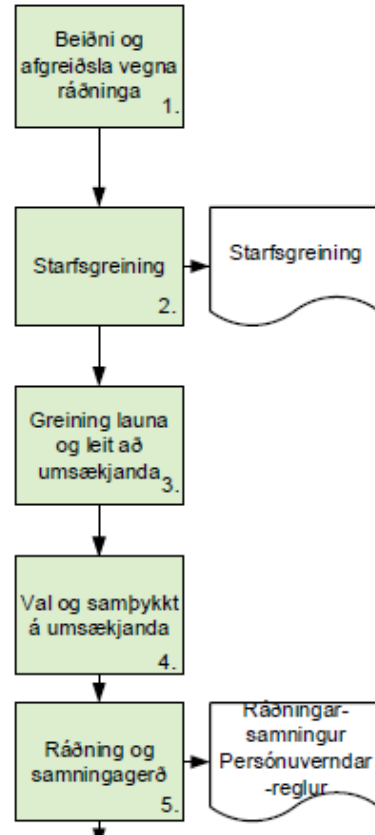
LANDSNET

Ferli verkefna og gagna



Dæmi tengt persónuverndarreglum

Framkvæmd ráðningar



1. Forstjóri samþykkir mannaflaspá ár hvert og er haft til hliðstjórar við heimild til ráðninga. Yfirmaður sendir beiðni um nýráðningu til Mannauðs.

2. Yfirmaður fullgerir starfsgreiningu í samvinnu við Mannauð eftir þörfum. Í starfsgreiningu eru skilgreindar kröfur til menntunar, reynslu og hæfni starfa. Starfsgreining starfa er vistuð í starfsmannakerfi.

3. Mannauður leggur fram tillögu til yfirmanns að starfskjörum út frá launauppbyggingu fyrirtækisins. Stjórnandi ákvarðar laun með hliðsjón af tillögu. Mannauður sér um öflun umsækjenda, situr viðtöl og er til ráðgjafar um val á væntanlegum starfsmanni.

4. Yfirmaður velur umsækjanda í samráði við Mannauð.

5. Yfirmaður sér um að semja við viðkomandi starfsmann um starfskjör og gengur frá undirritun ráðningargagna (ráðningarsamningur, starfskjör, trúnaðaryfirlýsing, starfslýsing og persónuverndarreglur LEI-10 Persónuverndarreglur Landsnets – starfsfólk. Mannauður undirbýr ráðningargögn.

6. Mannauður sér um vistun allra ráðningargagna og tryggir innfærslu starfsmanns í launa- og starfsmannakerfi. Allir undirritaðir samningar, eru skráðir og vistaðir í starfsmannakerfi. Frumrit eru vistuð á pappírform í læstum skjalaskáp.

Grunnupplýsingar

Samskiptaupplýsingar - nafn, kt., heimilisfang, símanr., netfang

Starfsumsókn, meðmæli og upplýsingar úr starfsviðtölum

Upplýsingar um menntun, þjálfun og starfsreynslu

Ráðningarsamningur

Upplýsingar um nánasta aðstandanda

Upplýsingar um innihald sakaskráa

Laun og starfskjör og aðrar tengdar upplýsingar

Bankareikningar

Stéttarfélagsaðild

Lífeyrissjóður

Ýmis gjaldheimta

Tímaskráningar og upplýsingar um fjarveru

Upplýsingar í starfi

Aðgangur að húsnæði og UT-kerfum

Innskráningar í UT-kerfi

Notkun á Workplace og Wiki

Netnotkun

Tölvupóstar sem starfsfólk sendir og móttækur á viðkomandi netfang sem LN á

Upplýsingar úr ökuritum

Upptökur úr öryggismyndavélum

Vinnutengd slys

Aðild og þátttaka í viðburðum á vegum starfsmannafélags LN