Mat á áhrifum á Persónuvernd (MÁP)

Tilgangur þessa skjals er að skjalfesta mat á áhrifum á persónuvernd samkvæmt 29. gr. laga nr. 90/2018, um persónuvernd og vinnslu persónuupplýsinga (PVL), sbr. 35. gr. reglugerðar Evrópuþingsins og ráðsins (ESB)2016/679 frá 27. apríl 2016 um vernd einstaklinga í tengslum við vinnslu persónuupplýsinga og um frjálsa miðlun slíkra upplýsinga og niðurfellingu tilskipunar 95/46/EB (almenna persónuverndarreglugerðin).

Skjal þetta skal fylla út vegna verkefna eða innleiðingu upplýsingakerfa sem krefjast vinnslu persónuupplýsinga og vegna umtalsverða breytinga á verkefnum eða upplýsingakerfum þar sem unnið er með persónuupplýsingar sem fela í sér mikla áhættu fyrir réttindi og frelsi hinna skráðu. Til að átta sig á því hvort þörf sé á því að framkvæma mat á áhrifum á persónuvernd er hægt að skoða auglýsingu Persónuverndar um skrá yfir vinnsluaðgerðir sem krefjast slíks mats, auglýsing nr. 828/2019.

Það er skylda þess sem ber ábyrgð á viðkomandi verkefni að tryggja að matið sé framkvæmt.

Öryggisstjóri og persónuverndarfulltrúi veita ráðgjöf við framkvæmd matsins og skylt er að veita persónuverndarfulltrúa tækifæri á að gera athugasemdir við matið.
Ábyrgðaraðili verkefnisins ákveður byggt á niðurstöðu matsins, og að höfðu samráði við persónuverndarfulltrúa, hvort nauðsyn sé að leita fyrirframsamráðs við Persónuvernd skv. 30. gr. laga nr. 90/2018, sbr. 36. gr. almennu persónuverndarreglugerðarinnar.

Leiðbeiningar um framkvæmd matsins má m.a. finna hér:
https://www.personuvernd.is/media/leidbeiningar-personuverndar/MAP-Mat-a-Ahrifum-a-Personuvernd.pdf (íslenska)

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/ (enska)

https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/vurdere-personvernkonsekvenser/vurdering-av-personvernkonsekvenser/ (norska)

Upplýsingar um ábyrgðaraðila

Nafn	Sveitarfélag/stofnun og Samband íslenskra sveitarfélaga
Efni	Miðlun gagna vegna umboðs til kjarasamningsviðræðna

Tengiliðir ábyrgðaraðila	Inga Rún Ólafsdóttir, sviðsstjóri kjarasviðs, og Sigurður Ármann Snævarr, sviðsstjóri hag- og upplýsingasviðs

1.Er þörf á MÁPi?

Almenn lýsing á tilgangi verkefnisins og þeirri vinnslu persónuupplýsinga sem er nauðsynleg í tengslum við það.

Hér skal gerð grein fyrir því hvers vegna er þörf á mati á áhrifum á persónuvernd út frá þeim persónuupplýsingum sem þarf að vinna og þeirri áhættu sem sú vinnsla getur skapað. Hægt er að hafa lista Persónuverndar um MÁP skyldar vinnslur til hliðsjónar.

(Hér getur verið gagnlegt að vísa í önnur skjöl eins og verkefnislýsingu, lagafrumvarps eða annað sem lýsir verkefninu nánar.)

Samband íslenskra sveitarfélaga (sambandið) fer með fullnaðarumboð til kjarasamningsgerðar fyrir hönd þeirra sveitarfélaga og stofnana sem til þess veita umboð sitt. Til þess að sambandið geti sinnt því hlutverki sínu er nauðsynlegt að safna upplýsingum um laun og önnur starfskjör starfsmanna hlutaðeigandi sveitarfélaga/stofnana. Þetta fyrirkomulag hefur verið viðhaft um áratuga skeið og má því segja að ekki sé um að ræða nýja vinnslu persónuupplýsinga, en nýja aðferð við vinnslu þar sem að á vegum sambandsins hefur verið þróuð stafræn lausn til að auðvelda miðlun og úrvinnslu nauðsynlegra gagna. Um er að ræða upplýsingar um launakjör starfsmanna sveitarfélaga/stofnana sem veitt hafa sambandinu umboð auk lýðfræðilegra upplýsinga og upplýsinga um aðild að stéttarfélagi. Allar þessar upplýsingar teljast nauðsynlegar til að gefa rétta mynd af raunlaunatölum starfsmanna til undirbúnings kjaraviðræðna en einnig til að hægt sé að miðla nauðsynlegum ópersónugreinanlegum upplýsingum til stéttarfélaga um þeirra félagsmenn.

Vinnsla upplýsinga fer fram með þeim hætti að fyrirfram skilgreindum upplýsingum um starfsmenn sveitarfélaga/stofnana er miðlað úr launakerfum þeirra í svokallaða móttökugátt. Í móttökugáttinni eru persónuauðkenni starfsmanns fjarlægð og útbúið gerviauðkenni í staðinn. Þegar persónuauðkenni hafa verið fjarlægð er upplýsingum miðlað í svokallað gagnalón sem aðgengilegt er fáum starfsmönnum sambandsins. Starfsmenn sveitarfélaga munu geta fengið aðgang að gagnalóninu til að skoða upplýsingar sem varða þeirra sveitarfélag og jafnframt til að skoða ópersónugreinanlega tölfræði. Einnig er fyrirhugað að miðla ópersónugreinanlegum upplýsingum til stéttarfélaga um launakjör þeirra starfsmanna í tengslum við kjarasamningsviðræður. Ljóst er að upplýsingar geta ekki alltaf talist ópersónugreinanlegar þar sem aldur starfsmanna og vinnustaður þeirra eru nauðsynlegar breytur við kjarasamningsviðræður. Því kann að vera hægt að persónugreina einstakling út frá þeim breytum sem finnast í gagnalóninu. Nánari upplýsingar um vinnsluna og tæknilega högun er að finna í kafla 2.

Við vinnslu persónuupplýsinga teljast þau sveitarfélög sem veitt hafa sambandinu umboð til kjarasamningsviðræðna og sambandið sameiginlegir ábyrgðaraðilar, sbr. 26. gr. almennu persónuverndarreglugerðarinnar, þar sem báðir aðilar fara sameiginlega með ákvörðunarvald um tilgang og aðferð við vinnslu. Nánari grein er gerð fyrir hlutverkum og skyldum aðila í samkomulagi aðila um sameiginlega ábyrgð, sbr. fskj. 1.

Niðurstaða: Um er að ræða umfangsmikla vinnslu á persónuupplýsingum um alla starfsmenn sveitarfélaga í nánar tilgreindum stéttarfélögum, þar á meðal viðkvæmum persónuupplýsingum um stéttarfélagsaðild. Einnig er um að ræða einstaklinga sem standa höllum fæti gagnvart ábyrgðaraðila sem launþegar þeirra. Við vinnsluna verða samkeyrðar upplýsingar frá fleiri ábyrgðaraðilum, til að mynda heildstætt yfirlit yfir launakjör þeirra vegna kjarasamningsviðræðna.

Þá er um að ræða aðrar upplýsingar sem telja verður viðkvæms eðlis, þ.e. um laun einstaklinga. Við vinnsluna er beitt nýrri aðferð eða tækni, þó svo að vinnsla sé áþekk þeirri sem hér er til skoðunar teljist ekki ný á heimsvísu. Því er ljóst að nauðsynlegt er að framkvæma mat á áhrifum á persónuvernd, þar sem vinnslan fellur undir flokka 4, 5, 6, 7 og 8, í 2. gr. auglýsingar Persónuverndar nr. 828/2019.

2.Lýsing á vinnslu persónuupplýsinga

Hér á að lýsa vinnslu persónuupplýsinga: hvaða upplýsingar, hvernig verður þeim safnað, þeim miðlað, þær notaðar, þær geymdar og þeim eytt? Hvaðan koma upplýsingarnar? Verður þeim deilt með einhverjum? Hvaða vinnsluaðgerðir eru það sem teljast fela í sér mikla áhættu?

(Hér getur verið gagnlegt að vísa til flæðirits sem sýnir flæði persónuupplýsinga í tengslum við verkefnið eða annarra skjala sem geta varpað frekara ljósi .)

Þær persónuupplýsingar sem unnið er með eru eftifarandi:

Upplýsingar um vinnustað, vinnufyrirkomulag, launagreiðanda, hvenær laun voru greidd, vinnufyrirkomulag, flokkun starfs, kjarasamning og stéttarfélag:

Ár
Mánuður
Nafn sveitarfélags
Stéttarfélag
Kjarasamningur
Launatímabil
Svið
Tegund ráðningar
Vinnufyrirkomulag
Útborgunarlaunaþrep
Upplýsingar um launþega
Kyn
Kennitala (síðustu sex stafir)
Starfsaldur
Menntun (ISCED)
Starfsmaður auðkenni
Persónuálag vegna símenntunar (starfsreynslu)
Persónuálag vegna viðbótarmenntunar

Upplýsingar skv. ráðningarsamningi

Vinnustaður
Starfsheiti á launaseðli
Starfsheiti samkvæmt starfsmati
Starfshlutfall
Grunnlaunaflokkur
Útborgunarlaunaflokkur
Fjöldi fastra yfirvinnutíma
Fjöldi breytilegra yfirvinnutíma

Launaupplýsingar:

TV einingar
Orlofsgreiðslur
Önnur laun
Heildarlaun
Aksturgreiðslur
Dagpeningagreiðslur
Launatengd gjöld
Dagvinnulaun
Yfirvinnulaun (fastir)
Yfirvinnulaun (breytilegir)
Vaktaálagslaun
Vaktaálagstímar
Vaktahvati (hlutfall)
Vaktahvati (laun)

Í þessu samhengi má taka fram að almenningi er tryggður aðgangur að hluta af þeim gögnum sem um ræðir samkvæmt 7. gr. upplýsingalaga nr. 140/2012. Rétturinn nær til fastra launakjara opinberra starfsmanna, ásamt aðgangs að ráðningarsamningum. Varðandi stjórnendur er rétturinn ríkari og nær til heildarlauna. Almennt getur almenningur þannig nálgast upplýsingar hjá sveitarfélögum um laun starfsmanna þeirra, ásamt afriti af ráðningarsamningi þó að fjarlægðum vissum upplýsingum s.s. um bankaupplýsingar og stéttarfélagsaðild.

Upplýsingar sem unnar verða vegna kjarasamningsumboðs og falla undir upplýsingarétt almennings eru þannig upplýsingar um: tegund ráðningar, starfsheiti, starfshlutfall, grunnlaunaflokk, fjölda fastra yfirvinnutíma að því marki sem slíkar upplýsingar er að finna í ráðningarsamningi. Þær upplýsingar sem ávallt ber að veita eru upplýsingar um dagvinnulaun, föst yfirvinnulaun, starfsheiti og vinnustað. Þessar upplýsingar er hægt að fá afhentar persónugreinanlegar og út frá þeim má greina fleiri upplýsingar með því að skoða kjarasamninga, s.s. um vaktaálag, yfirvinnutaxta o.fl. Því er ljóst að stór hluti þeirra upplýsinga sem um ræðir er aðgengilegur almenningi á persónugreinanlegu formi í dag, sé óskað eftir þeim.

Persónuupplýsingum verður miðlað úr launakerfum sveitarfélaganna, H3, Navision, Kjarni og SAP. Miðlun fer fram í gegnum forritaskil (e. API). Tvær aðferðir eru notaðar við gangasöfnunina eftir launakerfum.

Annars vegar eru það kerfi sem senda gögn í gagnalónið gegnum forritaskil og hinsvegar launakerfi sem hafa útfært eigin forritaskil þar sem gagnalónið hefur samskipti og sækir gögn í viðkomandi launakerfi . Auðkenning er mismunandi eftir kerfum, en nánar er fjallað um hana í 3. kafla.

Persónuupplýsingar eru auðkenndar með síðustu sex tölustöfum kennitölu, til að draga úr persónugreinanleika, í svokallaða móttökugátt þar sem útbúið er auðkennisnúmer sem nýtt er í Gagnalóninu og upplýsingar um viðkomandi launamann eru tengdar því ID-númeri. Eingöngu fæðingarári er miðlað í Gagnalónið af síðustu sex tölustöfum kennitölunnar þar sem aldur er mikilvæg breyta við kjarasamningsviðræður. Ástæða þess að ekki var gengið lengra í því að af persónugreina gögnin við miðlun er sú að gert er ráð fyrir því að vinnsla þeirra upplýsinga verði mjög takmörkuð, þ.e. þeim verði eytt um leið og búið er að útbúa gerviauðkenni, þ.e. í móttökugáttinni. Sú aðgerð að fara í frekari útfærslu á auðkenningu gagna við sendingu, s.s. með því að skipta út tölustaf fyrir bókstaf, hefði kallað á frekari þróun gagnvart öllum launkerfunum með tilheyrandi kostnaði. Með hliðsjón af eðli og umfangi vinnslunnar, og þeirri áhættu, misalvarlegri og mislíklegri, sem felst í tímabundinni miðlun á síðustu 6 stöfum í kennitölu, að teknu tilliti til kostnaðar, var talið ásættanlegt að fara þessa leið.

Úr móttökugáttinni verða þannig til svokölluð núllgögn. Að lokinni umbreytingu gagna er gögnum eytt úr móttökugáttinni og miðlað í Gagnalónið. Bæði móttökugáttin og gagnalónið eru hýst hjá Amazon Web Services (AWS) á grundvelli vinnslusamnings sambandsins og AWS.

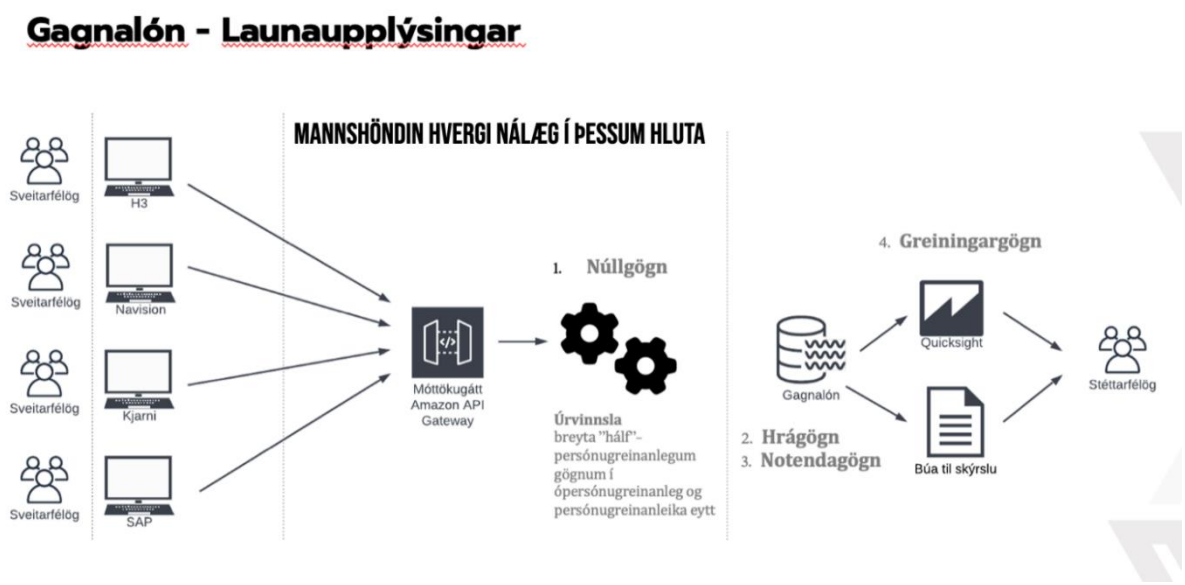
Allar tengingar milli kerfa eru dulkóðaðar með AES 256 dulkóðun.

Andes ehf. sérhæfður aðili í rekstri umsjón lausna í AWS umhverfi sér um utanumhald um dulkóðunarlykla og annast rekstur og þjónustu lausnarinnar á grundvelli vinnslusamnings við sambandið.

Eingöngu tilteknir starfsmenn sambandsins sem undirritað hafa trúnaðaryfirlýsingu hafa beinan aðgang að gögnum í Gagnalóninu. Einungis þeir starfsmenn sem sjá um samantektir og útreikninga munu hafa aðgang að kerfinu og er aðgangur háður samþykki sviðsstjóra. Aðrir starfsmenn sambandsins munu geta nýtt tölfræði og aðrar ópersónugreinanlegar samkeyrðar upplýsingar sem nauðsynlegar eru þeim vegna starfa þeirra á grundvelli umboðs sveitarfélaganna til kjarasamningsviðræðna.

Við miðlun til annarra aðila, s.s. stéttarfélaga verður þess gætt að miðla ekki upplýsingum um fámenna hópa sem kynnu að valda því að hægt væri að persónugreina einstaklinga. Sama á við um við vinnslu á upplýsingum innanhúss hjá sambandinu.

Á næstu síðu má sjá einfalda skýringarmynd af flæði gagna í lausninni.



3. Vinnsluheimild, meginreglur og réttindi hinna skráðu

Hér skal gera grein fyrir vinnsluheimild viðkomandi upplýsinga, hvernig skal tryggja að meginreglur persónuverndarlaga séu virtar og réttindi hinna skráðu tryggð: Á hvaða vinnsluheimild byggjum við, lagaskylda, almannahagsmunir, samningur, samþykki?

Hvernig tryggjum við að meginreglur PVL séu uppfylltar þ.e. að vinnslan sé lögmæt, sanngjörn og gagnsæ, aðeins framkvæmd í skýrum lögmætum og málefnalegum tilgangi, aðeins sé safnað nauðsynlegum upplýsingum til að ná þeim tilgangi, upplýsingar séu áreiðanlegar, þær aðeins varðveittar eins lengi og þörf krefur til að ná tilgangi vinnslunnar og að öryggi vinnslunnar sé tryggt?

Hvernig stuðlum við að réttindum hinna skráðu, þ.e. fræðslu um vinnsluna, aðgengis að eigin gögnum og rétti til að flytja, leiðréttingar og eyðingar, andmælarétti?

Vinnsluheimild: Sveitarfélögum ber að semja um launakjör starfsmanna sinna við viðkomandi stéttarfélög skv. lögum. Sveitarfélaginu sem vinnuveitanda ber að gera kjarasamninga við starfsmenn sína skv. lögum nr. 94/1986, um kjarasamninga opinberra starfsmanna og skv. lögum nr. 80/1938 um stéttarfélög og vinnudeilur. Ljóst að sú skylda felur eðli síns vegna í sér vinnslu viðkvæmra persónuupplýsinga um stéttarfélagsaðild starfsmanna.

Samband íslenskra sveitarfélaga er sameiginlegur málsvari þeirra sveitarfélaga sem aðild eiga að sambandinu, og fer með sameiginlega hagsmunamál þeirra svo sem þau ákveða sbr. 1. mgr. 98. gr. sveitarstjórnarlaga nr. 138/2011. Sveitarfélögum er heimilt að hafa með sér samvinnu um gerð og samþykkt kjarasamninga og önnur atriði tengd framkvæmd og stefnumótun í launamálum, skv. 99. gr. sveitarastjórnarlaga. Þá er einnig kveðið á um heimild sveitarstjórna til að skipa sameiginlega samninganefnd til að annast kjarasamninga í 4. og 5. mgr. 3. gr. laga nr. 94/1986.

Þær sveitastjórnir sem veitt hafa sambandinu umboð til að annast kjarasamninga undirrita einnig samkomulag um sameiginlega ábyrgð á vinnslu persónuupplýsinga í þeim tilgangi.

Heimild til vinnslu persónupplýsinga leiðir því af skyldu sveitarfélaga til að gera kjarasamninga við stéttarfélög starfsmanna sinna og heimild þeirra skv. sveitarstjórnarlögum til að fela sambandinu umboð til þeirra viðræðna.

Vinnsluheimild almennra persónuupplýsinga er því lagaskylda, sbr. 3. tl. 9. gr. laga nr. 90/2018 og fyrir vinnslu viðkvæmra persónuupplýsinga um stéttarfélagsaðild byggir á 2. tl. 11. gr. laganna þar er vinnslan nauðsynleg til að ábyrgðaraðili geti staðið við skyldur sínar samkvæmt vinnulöggjöf.

Rétt er að geta þess að sambandið leitaði ráðgjafar frá Persónuvernd um viðeigandi vinnsluheimild árið 2018, í tengslum við endurnýjun kjarasamningsumboða og tilheyrandi vinnslu persónuupplýsinga. Persónuvernd taldi í svari sínu að vinnsluheimildum væri rétt lýst með þeim hætti sem gert er hér að ofan. Persónuvernd áréttaði einnig að rétt væri að kanna, út frá raunverulegri aðkomu aðila við að ákveða tilgang og aðferð við vinnslu, hvort um væri að ræða sameiginlega ábyrgðaraðila. Í ljósi þess að sambandið fer með kjarasamningsgerðarumboð fyrir hönd sveitarfélaga og hefur þannig komið að mati á því hvaða gögn um starfsmenn eru nauðsynleg og jafnframt staðið að þróun á aðferð við vinnslu, upplýsinganna teljast aðilar sameiginlegir ábyrgðaraðilar.

Hlíting við meginreglur:

Lögmætisreglan: Vinnslan byggir á vinnsluheimildum þeim sem tilgreindar eru hér að ofan sem tryggja lögmæti hennar. Vinnslan telst sanngjörn gagnvart hinum skráðu þar sem starfsmenn geta reiknað með því að unnið sé með launaupplýsingar þeirra við gerð nýrra kjarasamninga og til meta kjaraþróun. Vinnslan verður kynnt starfsmönnum þegar miðlun upplýsinga hefst, þar sem útskýrður verður tilgangur vinnslu, umfang og nauðsyn og þannig er gagnsæi tryggt.

Tilgangsreglan: Tilgangur vinnslunnar er skýrt skilgreindur samkvæmt umboði og samkomulagi um sameiginlega ábyrgð. Tilgangur vinnslunnar er að gera sveitarfélögunum kleift að fela sambandinu að fara með kjarasamningsumboð og sameiginlega framkvæmd kjarasamninga við þau stéttarfélög sem starfsmenn sveitarfélaganna tilheyra.

Meðalhófsreglan: Eingöngu eru unnar þær upplýsingar sem nauðsynlegt er að byggja á við kjarasamningsgerð. Þá eru persónuauðkenni fjarlægð og gengið eins langt í að gera persónuupplýsingar ópersónurekjanlegar og hægt er, miðað við tilgang vinnslunnar, þ.m.t. að nota síðustu sex tölustafi í kennitölu einstaklinga. Þó er, líkt og áður er getið, ekki hægt að útiloka að hægt sé að persónugreina einstaka einstaklinga þar sem fáir starfsmenn eru á ákveðnum aldri, eða störfum í fámennum sveitarfélögum.

Áreiðanleikareglan: Prófanir hafa verið gerðar til að tryggja að upplýsingar úr launakerfum skili sér með réttum hætti. Þá verða reglulega gerðar athuganir á gæðum gagna með því að bera saman tölfræðiupplýsingar sem vinna má úr Gagnalóni við raunupplýsingar í viðkomandi launakerfum, út frá starfsheiti, aldri, starfsaldri, stéttarfélagi og fleira, til að tryggja viðvarandi áreiðanleika gagna.

Varðveislureglan: Upplýsingar verða varðveittar með þeim hætti að mögulegt er að persónugreina einstaka starfsmenn í fámennari sveitarfélögum á meðan þess gerist nauðsyn vegna kjarasamnings viðræðna. Þar sem um er að ræða ítarlegar upplýsingar sem safnað er, er ekki hægt að koma algerlega í veg fyrir að hægt sé að tengja upplýsingar tilgreindum einstaklingi vegna fjölda breyta. Þær upplýsingar sem slíkt á við um verða fjarlægða þegar þeirra er ekki lengur þörf og eingöngu varðveittar tölfræðilegar upplýsingar á ópersónugreinanlegu formi.

Öryggisreglan: Við hönnun á lausninni hefur verið gætt að innbyggðri persónuvernd og öryggisráðstafanir miðaðar að eðli og umfangi vinnslunnar og þeirri áhættu sem henni kann að fylgja fyrir réttindi og frelsi hinna skráðu einstaklinga.

Samskipti við launakerfi eru í meginatriðum tvennskonar. Annars vegar eru launakerfi sem senda gögnin til kerfisins. Í þeim tilvikum er auðkenningarþjónusta AWS notuð til auðkenningar en hver og einn þjónustuaðili hefur API lykil sem er auðkenndur af AWS API Gateway sem sér um að auðkenna og veita aðgang að forritaskilum kerfisins.

Hins vegar eru það launakerfi þar sem kerfi sambandsins hefur samskipti og sækir gögn í viðkomandi launakerfi (SAP og Kjarni). Í tilfelli SAP er notast við notandanafn og lykilorð sem kerfi sambandsins hefur verið úthlutað en aðgangur er einnig skilyrtur við IP-tölur kerfisins. Í tilfelli Kjarna er fyrst kallað í auðkenningarþjónustu Kjarna með notandanafni og lykilorði. Þjónustan úthlutar tokeni sem notað er til að tengjast viðkomandi þjónustu. Í öllum tilfellum er um dulkóðuð samskipti að ræða.

Upplýsingar sem miðlað er, eru eingöngu tengdar síðustu 6 stöfum í kennitölu og í móttökugáttinni eru þær upplýsingar fjarlægðar og notast við handahófskennt auðkenni í staðinn, til að lágmarka beina persónugreiningu hinna skráðu. Upplýsingum er eytt úr móttökugátt strax að lokinni þessari aðgerð, þ.e. um leið og umbreytingu á síðustu 6 stöfum og miðlun þeirra upplýsinga í Gagnlónið er lokið. Tilgangur þess að geyma upplýsingar ekki á fleiri stöðum en nauðsynlegt er og á sem minnst persónugreinanlegu formi.

Eftir að kennitölur eru afmáðar eru gögnin vistuð í skráastafni AWS (S3). Hver eining (bucket) er dulkóðuð með SSE-KMS dulkóðun (encryption) og er sérstakur lykill fyrir hverja einingu. Til að hægt sé að skoða gögnin þarf því a.m.k. lesréttindi á viðkomandi einingu ásamt leyfi til að nota viðkomandi KMS lykil til að afkóða (decrypt).

Allar kerfiseiningar eru hýstar í öruggu umhverfi AWS og hafa þær ráðstafanir sem þar eru viðhafðar verið rýndar í vinnslusamningi, upplýsingum sem AWS veitir á heimasíðu sinni og af Andes ehf. sem er sérhæfður aðili í rekstri lausna í AWS og með yfirgripsmikla þekkingu á öryggisráðstöfunum sem þar eru viðhafðar. Árásarvarnir, vöktun á netumferð, vírusvarnir og eldveggir eru til staðar og uppfærðar eftir því sem breytingar verða á árásarmynstri og tæknilegri getu illviljaðra aðila.

Aðgengi að hrágögnum í Gagnalóninu er takmarkað við mjög fáa einstaklinga hjá sambandinu. Aðrir fá aðgang að notenda gögnum þar sem gengið er úr skugga um að ekki sé hægt að persónugreina einstaklinga þar sem það á við.

4. Samráð við hlutaðeigandi aðila

Hvernig var samráði háttað: lýsing á því hvernig samráð var haft við hina skráðu, t.d. með því að kynna fyrirhugaða vinnslu opinberlega og kalla eftir sjónarmiðum skráðra einstaklinga. Ef ekki var haft samráð við slíka hópa skal útskýra hvers vegna. Þá skal gerð grein fyrir samráði við aðila hjá ábyrgðaraðila sem tengjast fyrirhugaðri vinnslu. Einnig getur verið nauðsynlegt að hafa samráð við vinnsluaðila og fá hans sjónarmið eða utanaðkomandi öryggissérfræðinga eða aðra sérfræðinga sem gætu haft mikilvæg sjónarmið fram að færa.

Samráð var haft við starfsfólk sveitarfélaga sem vinna að launa- og mannauðsmálum við þróun lausnarinnar. Einnig var sent kynningarbréf til allra sveitarfélaga í tengslum við öflun umboðs til handa sambandinu vegna kjarasamningsviðræðna. Voru hlutaðeigandi þar hvattir til að leita ráðgjafar persónuverndarfulltrú/ráðgjafa. Persónuverndarfulltrúa sendu athugasemdir sem tekið hefur verið tillit til og gerð er grein fyrir í lið 6 í MÁPi þessu. Einnig var haldinn kynningarfundur þar sem sátu framkvæmdastjórar og launafulltrúar sveitarfélaga og stofnana, sem sambandið fer með umboð fyrir, ásamt mannauðsstjórum og persónuverndarfulltrúum.

Andes ehf., vinnsluaðili, veitti sérfræðiráðgjöf á sviði öruggrar högunar í AWS umhverfi og við forritaskil milli Gagnalóns og launakerfa sveitarfélaganna. Einnig varðandi aðgangsstýringar að kerfum og við móttöku gagna í þeim tilgangi að fjarlægja bein persónuauðkenni og umbreyta þeim í handahófskennt auðkenni.

5. Áhætta fyrir réttindi og frelsi hinna skráðu og ráðstafanir

Í fylgiskjalinu Áhættumat – MÁP – er gerð grein fyrir helstu áhættum fyrir réttindi og frelsi hinna skráðu ásamt þeim ráðstöfunum sem gripið hefur verið til. Þar er einnig að finna skilgreiningar á bak við áhættustig og líkur ásamt því að þar er að finna áhættumatríxu.

Við gerð þessa MÁPs hefur verið miðað við að áhætta eftir ráðstafanir verði ekki meiri en miðlungs skv. skilgreiningum í fylgiskjalinu. Ástæða þess að miðlungs áhætta er talin ásættanleg er sú að þar sem um viðkvæmar persónuupplýsingar er að ræða, þ.e. varðandi stéttarfélagsaðild, og aðrar upplýsingar viðkvæms eðlis sem tengjast fjármálum einstaklinga, er erfitt að ná afleiðingum þess að gögn lendi í höndum óviðkomandi aðila niður fyrir „Alvarlegar“. Áhersla er hins vegar lögð á að draga úr persónugreiningu þeirra eins og hægt er við alla vinnslu, en megin áherslan er á öryggisráðstafanir til að draga úr líkum og þannig ná áhættunni á ásættanlegt stig. Þá var einnig brugðist við ábendingum persónuverndarfulltrúa sveitarfélaga varðandi söfnun upplýsinga um veikindadaga og fallið frá því að safna slíkum upplýsingum þar sem nauðsyn þess var ekki nægjanleg skýr og einnig voru efasemdir um áreiðanleika þeirra ef þeim yrði safnað með sama hætti og öðrum upplýsingum.

Helstu niðurstöður áhættumatsins eru þær að með þeim ráðstöfunum sem gripið verður til er engin áhætta útistandandi sem metin er hærra en miðlungs.
Gripið var til sérstakra ráðstafana vegna notkunar á AWS þar sem Amazon er fyrirtæki í Ameríkskri eigu. Hýsingarstaður var valinn í vestur-Evrópu til að tryggja að gögn fari ekki út fyrir EES-svæðið.

Þá eru gögn einnig dulkóðuð í gagnagrunni og þannig væri ekki hægt að verða við beiðni um afhendingu til ameríska yfirvalda ef svo ólíklega vildi til að slík beiðni bærist. Þær ráðstafanir koma því til viðbótar því að persónuauðkenni eru færð yfir í gerviauðkenni áður en gögnum er miðlað í gagnalón til varðveislu.

6. Undirskriftir, samantekt á ráðleggingum persónuverndarfulltrúa og áætlun um eftirfylgni

	Nafn og staða	**Athugasemdir**
Ráðstafanir samþykktar af:		Tryggja að þær ráðstafanir sem grípa skal til séu að fullu komnar til framkvæmdar áður en vinnsla hefst.
Áhætta eftir ráðstafanir samþykkt af:		Ef áhætta eftir ráðstafanir telst hærri en miðlungs skal að höfðu samráði við persónuverndarfulltrúa leitað fyrirfram samráðs við Persónuvernd.
Ráðleggingar persónuverndarfulltrúa:	Hér fyrir neðan er gerð grein fyrir ráðleggingum og athugasemdum PVF.	Persónuverndarfulltrúi skal eiga kost á því að veita ráðleggingar við val á ráðstöfunum og vinnslu persónu-upplýsinga almennt í verkefninu.

Fram komu athugasemdir frá persónuverndarfulltrúum sveitarfélaga og verður hér gerð grein fyrir þeim.

Athugasemdir bárust um að óskað væri nánari tilgreiningar á vinnsluheimild ábyrgðaraðilanna. Var brugðist við því að gera ítarlegri grein fyrir vinnsluheimildum í MÁP-inu og auk þess var bætt við tilvísun í samskipti við Persónuvernd vegna sambærilegra vinnslu, með annarri aðferð þó, frá árinu 2018. Þar lagði Persónuvernd áherslu á að kannað yrði hvort ekki væri réttast að aðilar teldust sameiginlegir ábyrgðaraðilar að vinnslunni.

Gerð var athugasemd við að unnar væru upplýsingar um veikindadaga og fjarvistardaga frá vinnu, enda væri þar um að ræða viðkvæmar upplýsingar sem ekki var sýnt fram á að væru nægjanlega áreiðanlegar eða nauðsynlegar í því formi sem þær eru aðgengilegar í launakerfum. Var því vikið frá því að vinna þær upplýsingar í tengslum við kjarasamningsumboð.

Fram komu athugasemdir um mögulega persónugreiningu einstaklinga í gagnalóninu þrátt fyrir þá ráðstöfun að unnið sé með persónuupplýsingar á gerviauðkenni. Vegna fjölda breyta um hvern einstakling munu vera einstaklingar sem hægt verður að persónugreina þar sem einungis einn eða mjög fáir einstaklingar falla í hóp. Verður brugðist við með því að gæta sérstaklega að því við miðlun gagna úr gagnalóni að ekki verði miðlað upplýsingum þegar um er að ræða færri en 5 einstaklinga sem kunna að falla í hóp, t.d. með því að fjarlægja þá breytur eða halda upplýsingum eftir við miðlun t.d. til stéttarfélaga.

Persónuverndarfulltrúar bentu á nauðsyn þess að takmarka varðveislutíma gagna. Verður tekið á því sérstaklega í verklagsreglum um meðferð gagna í gagnalóni. Verður lagt upp með að gera gögn ópersónugreinanleg eins fljótt og þeirra er ekki nauðsyn lengur á persónugreinanlegu formi, t.d. með því að fjarlægja tilteknar breytur.		
Ráðleggingum persónuverndarfulltrúa fylgt eða þeim hafnað. Ábyrgðar-aðili verkefnis staðfestir:		Ef ráðleggingum persónuverndarfulltrúa er ekki fylgt skal gerð grein fyrir því hvers vegna.
Athugasemdir: Ráðleggingum verður fylgt.		
Álit þeirra aðila sem leitað var samráðs við. Samþykkt eða ekki. Ábyrgðaraðili verkefnis staðfestir:		Ef ekki er tekið tillit til athugasemd sem berast við samráð skal gerð grein fyrir því hvers vegna.
Athugasemdir: Álit þeirra sem leitað var álits hjá voru fyrst og fremst frá starfsmönnum launadeilda sveitarfélaga, persónuverndarfulltrúum þeirra og frá starfsmönnum Sambandsins sem sinna kjaraviðræðum og munu koma að vinnslu gagna. Einnig var stuðst við álit og ábendingar vinnsluaðilans Andes varðandi öryggisráðstafanir og Tekið var tillit til athugasemda		
Áhættumatið verður uppfært og því fylgt eftir af:	Kristín Ólafsdóttir, lögfr. Björgvin Sigurðsson	Ef breytingar verða á vinnslu sem hefur áhrif á matið skal persónuverndarfulltrúi upplýstur og veitt tækifæri til að gera athugasemdir.