|  |  |
| --- | --- |
| **Mat á áhrifum á persónuvernd – sniðmát** | |
| Sniðmát þetta er hugsað fyrir mat á áhrifum á persónuvernd (MÁP). Í ákveðnum tilvikum er ábyrgðaraðila að vinnslu [persónuupplýsinga](https://www.personuvernd.is/fyrirtaeki-og-stjornsysla/spurt-og-svarad/allar-spurningar-og-svor/hvad-eru-personuupplysingar-1) skylt að gera mat á áhrifum á persónuvernd, sbr. ákvæði [auglýsingar nr. 828/2019](https://www.personuvernd.is/log-og-reglur/reglur-og-reglugerdir/auglysing-nr.-337-2019-um-skra-yfir-vinnsluadgerdir-thar-sem-krafist-er-mats-a-ahrifum-a-personuvernd). Það á þó ekki við ef slíkt mat fór fram sem hluti af almennu áhrifamati í tengslum við samþykkt laga, nema löggjafinn telji það engu síður nauðsynlegt áður en vinnsla fer fram, sbr. 10. mgr. 36. gr. reglugerðar (ESB) 2016/679.  Mat á áhrifum á persónuvernd er ferli þar sem kennsl eru borin á ógnir sem verkefni eða kerfi hefur í för með sér fyrir einstaklinga; þannig að hægt sé að grípa til viðeigandi ráðstafana til að draga úr líkum eða afleiðingum ógnanna. Með því er mögulegt að greina vandamál áður enn þau koma fram og þar með auka traust og tiltrú þeirra sem verkefnið nær til. Það getur leitt til sparnaðar þar sem kostnaðarsamt getur verið að koma ráðstöfunum á eftir á. Matið gefur jafnframt góða yfirsýn yfir verkefnið og helstu þætti þess, svo sem hvaða persónuupplýsingar þörf er að vinna og í hvaða tilgangi.  Leita skal ráðgjafar persónuverndarfulltrúa við gerð matsins. Varði regluverk umfangsmikla vinnslu persónuupplýsinga, t.d. miðlæga gagnagrunna, og vinnslu viðkvæmra persónuupplýsinga ætti einnig að hafa samráð við Persónuvernd.  Hægt er að nálgast nánari leiðbeiningar um gerð MÁP-s á vef [Persónuverndar](https://www.personuvernd.is/fyrirtaeki-og-stjornsysla/spurt-og-svarad/allar-spurningar-og-svor/mat-a-ahrifum-a-personuvernd-og-fyrirframsamrad-vid-personuvernd). Leiðbeiningar fyrir mat á áhrifum á persónuvernd vegna Office 365 má nálgast á vef [Microsoft](https://docs.microsoft.com/en-us/compliance/regulatory/gdpr-dpia-office365) og sniðmát frá Microsoft [hér](https://www.microsoft.com/en-us/download/details.aspx?id=102398). | |
| **Stofnun** | Smelltu hér til að færa inn texta. |
| **Vinnsluaðili** | Umbra – þjónustumiðstöð Stjórnarráðsins  Microsoft |
| **Persónuverndarfulltrúar** | Smelltu hér til að færa inn texta.  Daði Heiðar Kristinsson, persónuverndarfulltrúi Stjórnarráðsins/vinnsluaðila |
| **Tengiliður ábyrgðaraðila** | Smelltu hér til að færa inn texta. |
| **Tengiliður vinnsluaðila** | Sigurður Helgi Sturlaugsson hugbúnaðarstjóri hjá Umbru |

|  |  |
| --- | --- |
| **1. Samhengi vinnslu og þörf fyrir MÁP** | |
| **Stutt almenn lýsing á forsögu og tilurð verkefnis**  Íslenska ríkið undirritaði í júní 2018 heildstæðan samning við Microsoft. Samningurinn tryggði Íslandi meiri afslátt en býðst í mörgum nágrannaríkjum og er liður í stærra átaki ríkisins sem felst í að auka og bæta opinbera þjónustu. Samningurinn er í tveimur hlutum, annars vegar fyrir almennar stofnanir og hins vegar fyrir menntastofnanir. Upphaflega var gerður samningur um Microsoft M365 E3 hugbúnaðarpakkann en þann 1. júní 2021 var samningurinn við Microsoft endurnýjaður þar sem E5 leyfi voru keypt fyrir alla A-hluta ríkisaðila sem stuðlar að öruggara og sveigjanlegra vinnuumhverfi. Sjá nánar [hér](https://stafraentisland.atlassian.net/wiki/spaces/PLSTJARNAN/pages/1413283841/Microsoft+365+E5+-+Fer+alagi+heldur+fram).  Markmiðin sem lögð voru til grundvallar af hálfu ríkisins við gerð samningana voru eftirtalin:   * Að ná fram hagstæðari heildarkjörum en þeim sem byðist einstökum stofnunum og lækka þar með heildarkostnað ríkisins vegna Microsoft-hugbúnaðar. * Að koma öllum stofnunum ríkisins á nýjan og samræmdan tæknigrunn sem gæfi kost á sveigjanlegri og öruggari samskiptamáta milli stofnana ríkisins. * Að allar stofnanir ríkisins væru með rétt og gild leyfi og lækka þar með rekstraráhættu ríkisins vegna hugbúnaðarmála. * Að stórauka öryggi gagna og bæta rekstur kerfa.   Í september 2019 hófst vinna við að innleiða stofnanir inn í skýjageira ríkisins. Hluti af þeirri vinnu felst í því að stofnun sem ábyrgðaraðili að meðferð gagna ber að gera mat á áhrifum á persónuvernd og áhættumat á vinnslu persónuupplýsinga í þeim Microsoft þjónustum og vörum sem þeim stendur til boða hverju sinni samkvæmt samningum ríkisins við Microsoft. Þetta sniðmát var útbúið til að auðvelda stofnunum þá vinnu. Í sniðmátinu er búið að taka saman helstu svör frá rekstraraðila skýjageira sem og atriði er varða vinnslu persónuupplýsinga hjá Microsoft. Stofnun færir síðan nánari umfjöllun um vinnsluna í textareiti. Í umfjöllun um vinnslu persónuupplýsinga, öryggi og annars hjá Microsoft er oft látið nægja að vísa til upplýsinga á vef fyrirtækisins til að tryggja að vísað sé til nýjustu upplýsinga hverju sinni. Þess vegna er mikilvægt að stofnun kynni sér vel upplýsingar á vef Microsoft og hafi þær til hliðsjónar við gerð matsins.  Smelltu hér til að færa inn texta. | |
| **Aðilar sem koma að vinnslu og samband þeirra** *[Hér skal tilgreina hlutverk aðila, svo sem* [*ábyrgðaraðilar, vinnsluaðilar eða undirvinnsluaðila*](https://www.personuvernd.is/fyrirtaeki-og-stjornsysla/spurt-og-svarad/abyrgdaradilar-vinnsluadilar-og-vinnslusamningar/abyrgdaradilar-vinnsluadilar-og-vinnslusamningar-1)*r, og hvernig sambandi þeirra er háttað, t.d. hvort til staðar séu (eða fyrirhugað sé að ganga frá) vinnslusamningar eða samkomulag um ábyrgð.]*  Smelltu hér til að færa inn texta.  **Almennt um hlutverk og aðkomu aðila**  *Stofnun – þjónustukaupandi*  Stofnun er A-hluta ríkisaðili sem tilheyrir tilgreindum skýjageira ríkisins og er þjónustukaupandi. Stofnun er skuldbundin til að fylgja tæknilegri útfærslu á eigin upplýsingatækniumhverfi í samræmi við skjalfestingu Arktitektaráðs, þ.m.t. kröfum til notendaumsjónar (e. Active Directory). Þjónustukaupandi annast fræðslu til eigin starfsfólks á sviði almennrar öryggisvitundar og setur sér verklagsreglur um notkun þjónustunnar. Notendastýringar eru alfarið á ábyrgð þjónustukaupanda, t.d. nöfn, réttindi og viðhald lykilorða. Það er á ábyrgð stofnana að ákveða hvaða gögn þau vinna með og hvernig í þeim þjónustum og vörum sem eru í boði innan leyfa Microsoft hverju sinni.  *Rekstraraðili skýjageira*  Rekstraraðili skýjageira er stofnun sem rekur skýjageira fyrir hönd fjármála- og efnahagsráðuneytið. Rekstraraðili ber ábyrgð á rekstri geirans, svo sem að þjónustukaupandi fái aðgang að þeim Microsoft 365 þjónustum og vörum sem í boði eru og þjónustukaupandi hefur leyfi fyrir. Rekstraraðili hefur umsjón með réttindum og stýringum að skýjageira auk lausnaframboðs fyrir þann hóp stofnana sem er innan þess skýjageira sem hann rekur.  Rekstraraðili ber ábyrgð á öryggi skýjageira og öryggi gagna í skýjageiranum samkvæmt tækniforskrift Arkitektaráðs. Rekstraraðili ber ábyrgð á því að uppsetning á skýjageira og að tengingum við þá sé samkvæmt bestu stöðlum samkvæmt ákvörðunum Þjónustueigandaráðs og Arkitektúrráðs auk leiðbeininga sem framleiðendur gefa út hverju sinni.  *Fjármála- og efnahagsráðuneytið*  Fjármála- og efnahagsráðuneytið annaðist samningagerð og hefur yfirumsjón með umsýslu hugbúnaðarleyfa fyrir Microsoft hugbúnaðarlausnir fyrir skrifstofuumhverfi. Mennta- og menningarmálaráðuneytið var formlegur samningsaðili vegna hugbúnaðarkaupa fyrir menntastofnanir og fjármála- og efnahagsráðuneytið fyrir stofnanir utan menntageirans. Fjársýslu ríkisins var falið að annast umsýslu samningana.  *Arkitektaráð*  Arkitektaráð starfar í umboði fjármála- og efnahagsráðuneytisins og er skipað fulltrúum rekstraraðila allra skýjageira sem falla undir samning ríkisins við Microsoft og fulltrúa ráðuneytisins sem fer með forstöðu ráðsins. Arkitektaráð hefur það hlutverk að útfæra, hanna og skjalfesta ákvarðanir sem Þjónustueigandaráð ákveður er varðar vörur og þjónustur, svo sem um uppsetningu, öryggisstillingar og aðgangsstýringar milli stofnana. Arkitektaráð skilgreinir lágmarkskröfur sem framfylgja skal á milli rekstraraðila og þjónustukaupanda, t.d. um meðferð gagna hjá stofnun.  Arkitektaráð tekur fyrir beiðnir rekstraraðila, og stofnana eftir atvikum, um undanþágu frá útgefnum stöðlum og metur þær beiðnir, tilkynnir rekstraraðila um niðurstöðu, skjalfestir undanþáguna og gefur út.  *Þjónustueigendaráð*  Þjónustueigendaráð starfar í umboði fjármála- og efnahagsráðuneytisins og er skipað fulltrúum stofnana úr öllum skýjageirum sem falla undir samning ríkisins við Microsoft og fulltrúa ráðuneytisins sem fer með forstöðu ráðsins. Þjónustueigendaráð fjallar um og forgangsraðar þeim þjónustum og vörum sem eru í boði innan leyfa Microsoft hverju sinni, ásamt því að fjalla um framtíðarþjónustuþörf og eftir atvikum breytingu á leyfum á samningi fjármála- og efnahagsráðuneytisins við Microsoft fyrir hönd ríkisins. Þjónustueigendaráð mótar stefnu fyrir þá þjónustuþætti sem eru innifaldir í áskriftaleiðum ríkisins á hverjum tíma í samningi við Microsoft. Ráðið ákvarðar hvaða þjónustuþætti skuli taka í notkun, í hvaða skrefum og í hvaða tilgangi. Þjónustueigendaráð felur Arkitektaráði að útfæra tæknilega gangsetningu og virkjun þeirra þjónustuþátta sem ákveðið er að taka í notkun.  *Fjársýsla ríkisins*  Fjársýsla ríkisins fer með umsjón yfir miðlægum leyfagrunni, aðstoðar stofnanir við pantanir, breytingar og afpöntun leyfa gagnvart Microsoft og flutning leyfa milli stofnana. Fjársýslan sér jafnframt um innheimtu leyfisgjalda og þjónustukostnaðar gagnvart stofnunum. Fjársýslan starfrækir þjónustuborð fyrir leyfamál og veitir innheimtuþjónustu gagnvart stofnunum og rekstraraðilum. Fjársýslan hefur heimild til afla upplýsinga um fjölda og tegundir leyfa allra rekstraraðila og þjónustukaupanda er varða samninga ríkisins við Microsoft / leyfabirgja ríkisins á Íslandi.  **Um skiptingu ábyrgðar og hlutverk aðila**  *Stofnun* telst ábyrgðaraðili samkvæmt lögum nr. 90/2018 að eigin vinnslu persónuupplýsinga með þeim þjónustum og vörum sem eru í boði innan leyfa Microsoft hverju sinni, þar á meðal hvaða gögn og upplýsingar verða varðveittar og unnið með. Stofnun ber ábyrgð á að gera áhættumat á sínum gögnum og hvort vinnsla þeirra í þjónustunum samræmist kröfum um öryggi og persónuvernd. Stofnun ber ábyrgð á að setja sér verklagsreglur um notkun lausnanna sem taka mið af niðurstöðum áhættumats.  *Þjónustueigendaráð* og *Arkitektaráð* taka ákvarðanir f.h. fjármála- og efnahagsráðuneytisins um hvaða þjónustu og vörur standa til boða innan leyfa Microsoft hverju sinni og hvernig öryggi og meðhöndlun gagna skuli háttað. Ráðin auk fjármála- og efnahagsráðuneytisins teljast því ábyrgðaraðili að rekstri Microsoft skýjageirans og þeirrar vinnslu persónuupplýsinga sem í rekstrinum felst, þar á meðal er ábyrgð á ákvörðunum um öryggi gagna í lausninni og tæknilegum útfærslum.  *Rekstraraðili* ber ábyrgð á daglegum rekstri skýjageirans samkvæmt ákvörðunum Þjónustueigendaráðs og Arkitektaráðs og þjónustusamningi við fjármála- og efnahagsráðuneytið annars vegar og stofnun hins vegar. Rekstraraðili telst því vinnsluaðili samkvæmt lögum nr. 90/2018. Í samræmi við það hafa einhverjir rekstraraðilar sett sér vinnsluskilmála að ígildi vinnslusamnings sem nær yfir vinnslu persónuupplýsinga í tengslum við rekstur skýjageirans. Hjá þeim stendur stofnunum auk þess til boða að gera viðauka við vinnsluskilmálana þar sem þær geta gefið nánari fyrirmæli um vinnsluna. Hjá öðrum er gerður sérstakur vinnslusamningur um vinnsluna.  *Microsoft* er þjónustuveitandi og vinnsluaðili að gögnum og upplýsingum stofnunar sem það vinnur með fyrir hennar hönd við veitingu þeirra þjónustna og vara sem eru í boði innan leyfa Microsoft hverju sinni samkvæmt ákvörðun Þjónustueigendaráðs. Microsoft hefur sett sér vinnsluskilmála sem gilda um vinnsluna. Frekari fyrirmæli af hálfu stofnunar um vinnsluna krefst samþykkis samningsaðila. Microsoft vinnur einungis með gögn stofnana í samræmi við vinnsluskilmálana, nánari fyrirmæli stofnunar og til að veita þjónustuna. Stofnun heldur öllum réttindum að þeim gögnum sem Microsoft vinnur fyrir hönd stofnunar við veitingu þjónustunnar og telst eigandi þeirra.  Microsoft telst sjálfstæður ábyrgðaraðili í þeim tilfellum sem það vinnur persónuupplýsingar í tengslum við greiningargögn vegna veitingu þjónustunnar, svo sem í atburðaskrám.  Hægt er að nálgast nánari upplýsingar um persónuvernd hjá Microsoft hér:   * Traustsíða Microsoft, <https://www.microsoft.com/en/trust-center/> * Vinnsluskilmálar Microsoft: <https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA> * Deiling ábyrgðar: <https://docs.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility> * Undirvinnsluaðilar Microsoft: <https://aka.ms/Online_Serv_Subcontractor_List> | |
| **Hvers vegna þarf að gera MÁP?** *[Merkja skal við atriði í eftirfarandi lista. Ef merkt er við tvö eða fleiri atriði þarf að gera MÁP.]*  Mat eða einkunnagjöf/stigagjöf  Sjálfvirk ákvarðanataka sem hefur áhrif á réttindi hins skráða, t.d. með notkun gervigreindar  Kerfisbundið eftirlit  Viðkvæmar persónuupplýsingar eða aðrar persónuupplýsingar viðkvæms eðlis  Umfangsmikil gagnavinnsla  Samkeyrsla og sameining gagnasafna  Upplýsingar um aðila sem standa höllum fæti  Vinnsla þar sem beitt er nýrri tækni eða skipulagslausnum eða eldri tækni er beitt á nýjan hátt  Vinnsla persónuupplýsinga sem kemur í veg fyrir að hinn skráði geti notið réttinda, fái fyrirgreiðslu, þjónustu eða samning  Nánari skýring: Smelltu hér til að færa inn texta. | |
| **2. Lýsing á vinnslu** | |
| **Almenn lýsing á vinnslunni og vinnsluaðgerðum** *[Hér skal lýsa vinnslunni og vinnsluaðgerðum, svo sem hvernig verður upplýsingunum safnað, þær notaðar, með hverjum verðum þeim deilt með, í hvaða kerfum verður unnið með þær, hversu lengi mun vinnslan standa yfir? Í stað þess að lýsa ferlinu hér er hægt lýsa ferlinu í viðauka við MÁP-ið. Flæðirit með myndum er góð leið til að lýsa ferlinu.]*  Smelltu hér til að færa inn nánari lýsingu á ferlinu.  *Aðrar stofnanir í skýjageira*  Starfsfólk stofnana innan sama skýjageira getur skoðað upplýsingar í notendaumsjón (e. Active Directory) hjá öðrum stofnunum. Starfsfólk stofnana getur flett upp og skoðað tengiliðaupplýsingar innan umhverfisins. Aðilar utan umhverfisins geta ekki skoðað þessar upplýsingar. Starfsfólk getur valið að gera skrár opnar fyrir öllum innan sama skýjageira og getur þá starfsfólk allra stofnan innan geirans séð skrárnar og innihald þeirra. Almenna stillingin er að skrár eru lokaðar öðrum en þeim sem starfsmaður hefur veitt aðgang eða hópum sem hafa aðgang að þeim, svo sem þegar skrá búin til inn á Teams-svæði. Þegar starfsfólk notar samfélagsmiðla eiginleika í þjónustum og vörum Microsoft, svo sem að líka við færslur, getur annað starfsfólk innan sama skýjageira séð það.  *Umbra*  Meginvinnsla persónuupplýsinga liggur hjá Microsoft í tengslum við hýsingu gagna og upplýsinga í þeim skýjaþjónustum sem stofnun stendur til boða hverju sinni, söfnun upplýsinga í atburðaskrár og annað. Vinnsla Umbru á persónuupplýsingum fyrir hönd stofnunar afmarkast við eftirfarandi:   * Afritun gagna: Afrit eru tekin af gögnum stofnunar í skýjageira og þau varðveitt, svo sem Office skjöl og önnur gögn sem Microsoft gefur möguleika á að afrita. Notast er við afritunarlausn frá Veeam ([Veeam Backup for Microsoft Office 365](https://www.veeam.com/backup-microsoft-office-365.html?ad=menu-products)) en þau eru geymd á netþjóni hjá Umbru. Afritun nær þannig til allra gagna stofnunar sem hún ákveður að vinna með innan þeirra Office 365 þjónustna og vara sem henni stendur til boða. Þar á meðal geta verið allar tegundir persónuupplýsinga, almennra og viðkvæmra. * Aðgangur að gögnum og atburðaskrám: Skilgreint starfsfólk Umbru getur gefið sér aðgang að gögnum stofnunar, þar á meðal aðgerðir notenda, greiningargögn, samskiptagögn og skrár í Microsoft lausnum. Verklagsregla eru í gildi um slíkan aðgang. Samkvæmt henni eiga kerfisstjórar að skrá skriflega beiðni frá stofnun um aðgang áður en þeir veita sér aðgang. Þá fá allir aðrir kerfisstjórar og upplýsingaöryggisstjóri Umbru tilkynning um veitingu slíks aðgangs og það er skráð í aðgerðarskrá umhverfisins. * Notendaumsjón þegar það á við: Almennt sér stofnun sjálf um notendaumsjón en ef óskað er eftir því þá getur Umbra stofnað og eytt notendum og endurstillt lykilorð fyrir stofnanir sem ekki hafa eigin notendaumsjón (e. Active Directory) samstillta við notendaumsjón hjá Microsoft (Azure Active Directory). Upplýsingum um starfsfólk sem fara í notendaumsjón Microsoft (e. Azure Active Directory) er safnað frá stofnun sem sendir lista yfir notendur sem á að stofna í excel skrá til rekstraraðila. Sjá nánar um notendaumsjón Microsoft [hér](https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-whatis). * Símaþjónusta þegar það á við: Umbra býður upp á þá þjónustu að virkja landlínunúmer í Teams sem leysir af hólmi hefðbundinn borðsíma. Umbra vinnur þá með upplýsingar um símanúmer notenda og getur gefið sér aðgang að símtalaskrám með sama hætti og á við um aðgang að atburðaskrám. * Verkbeiðnir: Umbra notar verkbeiðnakerfið Freshdesk til að taka við verkbeiðnum frá stofnunum vegna rekstur skýjageirans. Kerfið er hýst í skýi innan EES svæðisins á vegum Freshdesk. Sjá nánar um persónuvernd hjá Freshdesk [hér](https://freshdesk.com/gdpr) og öryggi [hér](https://www.freshworks.com/security/). Í því er unnið með eftirfarandi upplýsingar í þeim tilgangi að móttaka og afgreiða verkbeiðnir:   + Samskiptaupplýsingar eins og nafn, netfang, póstfang, heimilisfang, símanúmer.   + Efni þjónustubeiðni.   + Notendanafn og lykilorð.   *Microsoft*  Vinnsla Microsoft felst fyrst og fremst í hýsingu þeirra gagna og upplýsinga sem það vinnur með fyrir hennar stofnunar við veitingu þeirra þjónustna og vara sem eru í boði innan leyfa Microsoft hverju sinni. Samkvæmt samningum við Microsoft skulu gögn í tengslum við þjónustur og vörur einungis varðveitt innan EES-svæðisins, nánar tiltekið á Írlandi. Þá vinnur Microsoft ýmsar upplýsingar í greiningargögnum í tengslum við veitingu þjónustunnar sjálfrar. Sjá nánar hér:  Persónuverndarstefna Microsoft: <https://privacy.microsoft.com/en-US/privacystatement>  Nánar um upplýsingar sem Microsoft vinnur: <https://privacy.microsoft.com/en-US/#whatinformationwecollectmodule>   * Tilkynningar um persónuverndarmál: <https://privacy.microsoft.com/en-US/privacy-report>   *Þjóðskjalasafn*  Stofnun skilar öllum afhendingarskyldum gögnum til Þjóðskjalasafns Íslands úr eigin kerfum í samræmi við afhendingar- og varðveisluskyldu samkvæmt lögum nr. 77/2014 um opinber skjalasöfn. | |
| **Upplýsingaeignir sem notaðar eru við vinnsluna** *[Svo sem vélbúnaður, hugbúnaður, net, fólk, pappír.]*  Smelltu hér til að færa inn texta.  Upplýsingar um hvaða þjónustur og vörur stofnunum innan skýjageira ríkisins stendur til boða hverju sinni má nálgast [hér](https://stafraentisland.atlassian.net/wiki/spaces/PLSTJARNAN/pages/1413677059/Microsoft+365+E5+-+Hva+er+pakkanum). | |
| **Hvaða tegundir persónuupplýsingar verður unnið með?** | |
| Nöfn, fæðingardaga, heimilisföng  Kennitölur  Tengiliðaupplýsingar  Auðkennisupplýsingar  Fjárhagsupplýsingar  Opinberar upplýsingar  Staðsetningarupplýsingar  Launaupplýsingar | Heilsufarsupplýsingar  Erfðafræðilegar upplýsingar  Lífkenni  Stjórnmálaskoðanir  Trúarbrögð eða lífsskoðanir  Upplýsingar um kynhneigð og kynlíf  Refsiverður verknaður / viðurlög |
| Annað / Nánar:  Smelltu hér til að færa inn texta. | |
| **Um hvaða flokka einstaklinga eru upplýsingarnar?** | |
| Ríkisborgarar  Málsaðilar  Starfsfólk  Umsækjendur | Viðskiptavinir  Sjúklingar  Ólögráða einstaklingar  Viðkvæmir hópar einstaklinga |
| Annað / Nánar:  Smelltu hér til að færa inn texta.  Vinnslu Microsoft á upplýsingum / gögnum má skipta í fimm flokka:   1. Öll gögn sem stofnun vinnur með innan þjónusta og vara Microsoft, svo sem í Teams, OneDrive, Sharepoint og Outlook Exchange. Þar af leiðandi getur vinnslan falið í sér allar tegundir viðkvæmra persónuupplýsinga. 2. Gögn sem verða sjálfkrafa til við notkun þjónustu og lausna og varða notkun og afköst. Slíkum gögnum eru gefin dulkóðuð auðkenni. 3. Greiningargögn í atburðaskrám sem eru auðkennt með eigindum í þjónustunni eða vélbúnaðinum sem þjónustan er keyrð á. 4. Gögn sem er safnað frá notanda þegar leitað er tæknilegrar aðstoðar Microsoft. 5. Upplýsingar um þá sem hafa kerfisstjórnaraðgang, svo sem tengiupplýsingar, og upplýsingar vegna innheimtu leyfisgjalda. | |
| **Hversu lengi eru persónuupplýsingarnar varðveittar og hvar?** *[Hér skal lýsa hversu lengi persónuupplýsingar skulu varðveittar og hvar þær eru varðveittar (land). Sé unnið með marga flokka persónuupplýsinga í fleiri en einu kerfi, skal greina frá varðveislutíma fyrir hvern flokk og kerfi - sé varðveislutími mismunandi.]*  Smelltu hér til að færa inn texta.  Gögnum í skýjageiranum er ekki eytt. Gögn notanda eru varðveitt í 30 daga frá því að notanda var eytt. Eftir það færast gögn í óvirka stöðu og eru varðveitt áfram í samræmi við ákvæði laga nr. 77/2014.  Afrit eru geymd samkvæmt geymsluáætlunum:   * Daglegt afrit er geymt í 35 daga * Vikulegt afrit er geymt í 4 vikur * Mánaðarlegt afrit er geymt í 3 mánuði * Ársfjórðungs afrit er geymt í 9 mánuði   Öll gögn sem Microsoft vinnur fyrir hönd stofnana sem vinnsluaðili eru geymd og unnið með á ESS-svæðinu, nánar tiltekið á Írlandi.  Upplýsingar um notendur í notendaumsjónarkerfi eru geymdar í 30 daga frá því að notanda var eytt.  Upplýsingar í atburðaskrám eru geymdar í 90 daga. Upplýsingar sem er safnað í tengslum við notkun og afköst þjónusta og vara eru geymdar í 180 daga.  Upplýsingum í verkbeiðnakerfinu Freshdesk er ekki eytt þar sem Umbra er afhendingarskyldur aðili samkvæmt lögum nr. 77/2014 um opinber skjalasöfn. Upplýsingarnar eru varðveittar innan EES-svæðisins í samræmi við samninga aðila. | |
| **3. Tilgangur vinnslu, lögmæti og meginreglur** | |
| **Hver er tilgangur vinnslunnar og ávinningur?**  Smelltu hér til að færa inn texta.  Markmið með innleiðingu Office 365 er einkum að auðvelda starfsmönnum stofnana ríkisins að sinna vinnu sinni, óháð staðsetningu en á sama tíma auka öryggi notendaauðkenningar og þeirra upplýsinga sem unnið er með.  Starfsmenn munu nota umræddan hugbúnað í störfum sínum og vinnsla persónuupplýsinga mun eiga sér stað í tengslum við lögbundin hlutverk ábyrgðaraðila. Tilgangurinn með vinnslu persónuupplýsinga með þjónustum og vörum Microsoft er ákveðinn af stofnun hverju sinni.  Þegar Microsoft kemur fram sem vinnsluaðili þá er tilgangurinn vinnslunnar að standa við samning við þjónustukaupendur og veita þeim umsamda þjónustu hverju sinni í samræmi við samning. Microsoft vinnur einnig persónuupplýsingar í eigin ábyrgð í lögmætum viðskiptahagsmunum, svo sem til að innheimta gjöld fyrir leyfi, greiða þóknanir, upplýsingagjöf og áætlanagerð innanhús, þróa og bæta þjónustur, veita upplýsingar um fjárhag fyrirtækisins og uppfylla lagaskyldur. Microsoft mun ekki nota gögn stofnunar í markaðstilgangi.  Umbra vinnur með upplýsingar um tengiliði stofnunar til að geta afgreitt verkbeiðnir og átt í samskiptum við stofnun. Nauðsynlegt er að vinna með upplýsingar um notendur í notendaumsjón í þeim tilgangi að stofna notendur í umhverfinu þannig að þeir hafi aðgang að sínu vinnuumhverfi.  Gögnin verða ekki notuð í öðrum og ósamrýmanlegum tilgangi nema slík notkun teljist heimil samkvæmt ákvæðum persónuverndarlaga. | |
| **Hagsmunir einstaklings og ávinningur af verkefninu** *[Hér skal í stuttu máli fara yfir það hvaða áhrif vinnslan getur haft af þá einstaklinga sem persónuupplýsingarnar eru um og hver ávinningur samfélagsins er af vinnslunni. Þessi liður á helst við þegar vinnsla byggist á lögmætum hagsmunum eða almannahagsmunum.]*  Smelltu hér til að færa inn texta. | |
| **Á hvaða heimild í lögum nr. 90/2018 um persónuvernd og vinnslu persónuupplýsinga byggist vinnslan á?** *[Samþykki, samningur, lagaskylda, almannahagsmunir, lögmætir hagsmunir o.s.frv., sbr. 9. og 11. gr. laga nr. 90/2018 og 6. og 9. gr. reglugerðar (ESB) nr. 2016/679.]*  Smelltu hér til að færa inn texta.  Atburðaskrár eru haldnar á grundvelli lögmætra hagsmuna, til að tryggja rekjanleika aðgerða. Upplýsingar í Azure notendaumsjón (e. Azure Active Directory) eru haldnar til að framkvæma samning milli aðila og reka skýjageirann. | |
| **Hvernig er gætt að því að persónuupplýsingar sem unnið er með séu nægilegar, viðeigandi og takmarkast við það sem nauðsynlegt er?**  Smelltu hér til að færa inn texta.  Í Azure notendaumsjón (e. Azure Active Directory) eru eingöngu geymdar upplýsingar sem nauðsynlegar eru til að auðkenna notendur og starfsfólk, og samskipti sín og milli og við önnur kerfi.  Vinnslan af hálfu Microsoft fyrir hönd stofnunar er nauðsynleg til að veita umsanda þjónustu hverju sinni.  Hvað varðar vinnslu Microsoft í tengslum við atburðaskrár þá eru almennt ekki hægt að rekja slík gögn til tiltekinna einstaklinga. | |
| **4. Réttindi einstaklinga** | |
| **Hvernig er fræðslu til hinna skráðu háttað?** *[Sbr. 12., 13. og 14. gr. pvrg.]*  Smelltu hér til að færa inn texta.  Microsoft birtir fræðslu um vinnslu persónuupplýsinga á vef sínum:   * <https://privacy.microsoft.com/en-US/privacystatement> * <https://privacy.microsoft.com/en-US/privacy-report>   Fræðsla um vinnslu persónuupplýsinga hjá Umbru verður birt á sér vef sem er í vinnslu. | |
| **Hvernig eru réttindi einstaklinga samkvæmt 3. kafla laga nr. 90/2018 um persónuvernd og vinnslu persónuupplýsinga tryggð?** *[Svo sem réttur til aðgangs, til að flytja gögn, leiðréttingar, til að gleymast, andmæla og takmarka vinnslu.]*  Smelltu hér til að færa inn nánari umfjöllun um hvernig réttindi einstaklinga verða tryggð.  Þegar Microsoft vinnur persónuupplýsingar fyrir hönd stofnunar sem vinnsluaðili mun Microsoft veita stofnun og rekstraraðila skýjageira aðstoð við að uppfylla beiðni einstaklinga um að beita réttindum sínum samkvæmt persónuverndarlögum. Beiðnir einstaklinga til Microsoft eru áframsendar til  stofnunar eða rekstraraðila skýjageira.  Þegar Microsoft vinnur persónuupplýsingar sem ábyrgðaraðili ber einstaklingum að senda beiðni til Microsoft í samræmi við [persónuverndarstefnu](https://privacy.microsoft.com/en-ca/privacystatement) þess. | |
| **5. Samráð við hlutaðeigandi aðila** | |
| **Var haft samráð við einstaklingana sem upplýsingarnar varða?** *[Ef ekki, rökstyddu þá hvers vegna.]*  Smelltu hér til að færa inn texta. | |
| **Hver var ráðgjöf persónuverndarfulltrúa við gerð matsins?** *[Hér skal stuttlega gera grein fyrir ráðgjöf persónuverndarfulltrúa nema þess teljist ekki þörf. Ef ráðgjöf persónuverndarfulltrúa er ekki fylgt skal gera grein fyrir ástæðum þess.]*  Smelltu hér til að færa inn texta. | |
| **Hefur verið haft samráð við aðra innan stofnunar?**  Smelltu hér til að færa inn texta. | |
| **Hver er aðkoma vinnsluaðila við gerð matsins?**  Smelltu hér til að færa inn texta.  Sniðmátið fyrir þetta mat á áhrifum á persónuvernd var útbúið af Umbra – þjónustumiðstöð Stjórnarráðsins og persónuverndarfulltrúa Stjórnarráðsins. Stöðluð svör um vinnslu persónuupplýsinga Umbru, Microsoft og annarra undirvinnsluaðila voru útbúinn á grunni upplýsinga úr vinnsluskrám, vinnslusamningum og upplýsingaveitum aðila. | |
| **Var leitað ráðgjafar sérfræðinga í upplýsingaöryggi eða annarra sérfræðinga?**  Smelltu eða pikkaðu hér til að færa inn texta. | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **6. Áhætta fyrir réttindi og frelsi einstaklinga** | | | | |
| Í töflunni að neðan skal tilgreina helstu ógnir sem einstaklingum getur stafað af vinnslunni. Líta þarf til allra tegunda ógna, svo sem tæknilegra, lagalegra, samningslegra og rekstrarlegra. Dæmi um ógnir er innbrot í kerfi, persónuupplýsingar óvart birtar, kerfi liggur niðri vegna bilana, gögnum er safnað umfram lagaheimild, skyldur aðila samkvæmt lögum um opinber skjalasöfn eru ekki uppfylltar.  Líkur skulu metnar á skalanum 1-4; (1) mjög ólíklegt, (2) frekar ólíklegt, (3) frekar líklegt og (4) mjög líklegt. Afleiðingu skal meta á skalanum 1-4; (1) litlar afleiðingar, (2) frekar litlar afleiðingar, (3) frekar miklar afleiðingar og (4) miklar afleiðingar. Margfaldað skor fyrir hvort tveggja myndar áhættuna af ógninni (L\*A=Á). Að lokum skal tilgreina þær ráðstafanir sem gripið hefur verið til, fyrirhugað eða mögulegt er að grípa til. Nauðsynlegt er að grípa til ráðstafanna vegna áhætta sem fá skor 8 eða hærra.   |  |  |  |  |  | | --- | --- | --- | --- | --- | |  | **Afleiðing** | | | | | **Líkur** | 1 | 2 | 3 | 4 | | 2 | 4 | 6 | 8 | | 3 | 6 | 9 | 12 | | 4 | 8 | 12 | 16 |   Í stað þessarar áhættugreiningar er hægt að nota [sniðmát netöryggisráðs fyrir áhættumat](https://www.stjornarradid.is/efst-a-baugi/frettir/stok-frett/2017/01/06/Upplysingaoryggi-samningsvidauki-leidbeiningar-og-eydublod-fyrir-gerd-ahaettumats/) sem verður þá viðauki við þetta skjal. Þá er hægt að nálgast frekari upplýsingar um áhættumat, áreiðanleikakannanir, öryggi og úttektir hjá Microsoft hér:   * Áhættumat: <https://docs.microsoft.com/en-us/compliance/assurance/assurance-risk-assessment-guide> * Öryggi hjá Microsoft: <https://www.microsoft.com/en-ww/security> * Áreiðanleikakönnun: <https://www.microsoft.com/en-ww/trust-center/compliance/due-diligence-checklist> * Útgefnar úttektarskýrslur á Microsoft: <https://servicetrust.microsoft.com/> * Öryggisbrestir og tilkynning þeirra: <https://learn.microsoft.com/en-us/compliance/regulatory/gdpr-breach-notification> | | | | |
| **Ógn** | **Líkur** | **Afleiðing** | **Áhætta** | **Ráðstöfun** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

|  |
| --- |
| **7. Samþykki og niðurstaða** |
| **Mat samþykkt af:**  Nafn, titill og dagsetning. |
| **Niðurstaða:** Veldu atriði. |
| **Var leitað ráðgjafar persónuverndarfulltrúa?** Já  Nei  Undirritun persónuverndarfulltrúa; nafn, titill og dagsetning. |
| Þetta MÁP verður endurskoðað við lok innleiðingar af persónuverndarfulltrúm. Persónuverndarfulltrúar skulu fylgjast með hvort vinnsla samræmist MÁP-inu. |