MAT Á ÁHRIFUM Á PERSÓNUVERND (MÁP)

Almennt

Um vinnslu persónuupplýsinga gilda lög nr. 90/2018 um persónuvernd og vinnslu persónuupplýsinga (pvl.) sem tóku gildi 15. júlí 2018. Lögin leysa af hólmi eldri lög nr. 77/2000 um persónuvernd og meðferð persónuupplýsinga. Þau lögfesta jafnframt reglugerð (ESB) 2016/679 um persónuvernd (pvrg./reglugerðin), eins og hún var aðlöguð og tekin upp í EES-samninginn. Leiðbeiningar þessar byggja að hluta til á leiðbeiningum þáverandi 29. gr. vinnuhópsins um mat á áhrifum á persónuvernd[i].

Ein af þeim nýjungum, sem kynntar voru til sögunnar með persónuverndarreglugerð ESB er skylda ábyrgðaraðila til að framkvæma mat á áhrifum á persónuvernd (MÁP) hvenær sem verkefni felur í sér mikla áhættu fyrir persónuvernd einstaklinga.

MÁP er tól til að meta og lágmarka áhættu fyrir persónuvernd einstaklinga við framkvæmd nýrra verkefna. Matið er hluti af nýjum skyldum fyrirtækja og stofnana samkvæmt persónuverndarlöggjöfinni og mikilvægur hluti af „innbyggðri og sjálfgefinni persónuvernd“ sem er eitt af grundvallaratriðunum í nýju löggjöfinni.

Persónuvernd vinnur að nánari leiðbeiningum um framkvæmd MÁP og verða leiðbeiningarnar uppfærðar í samræmi við það.

1. útgáfa, september 2018

Efnisyfirlit

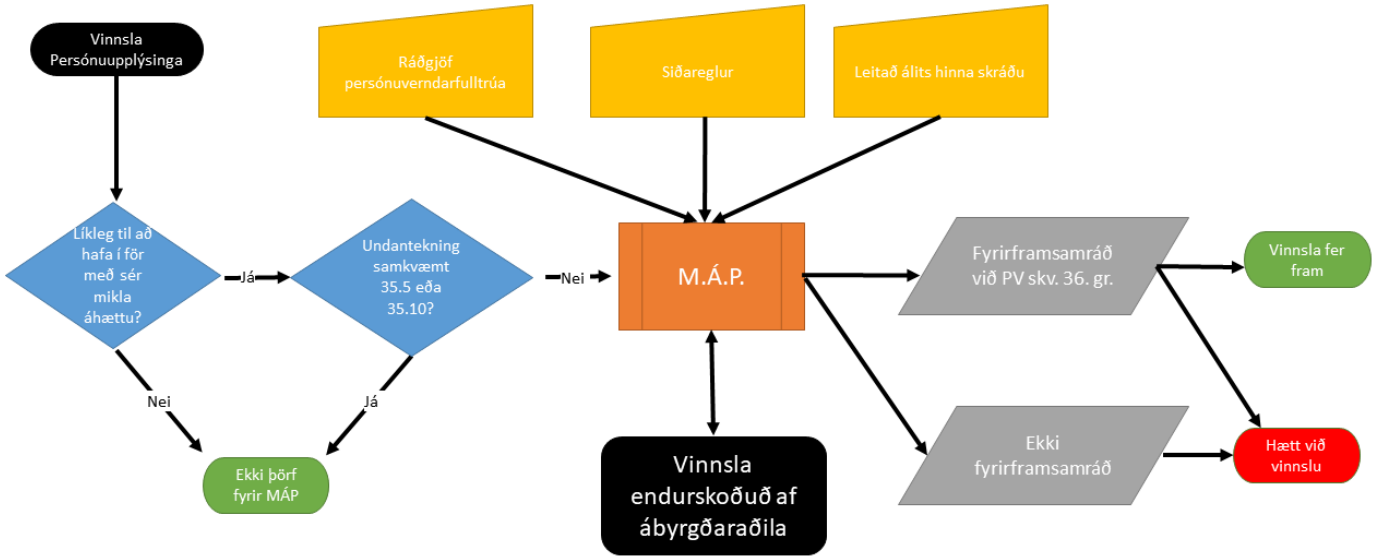
1. Hvað er MÁP?

Mat á áhrifum á persónuvernd er kerfisbundið ferli sem hjálpar þér að greina, bera kennsl á og lágmarka persónuverndaráhættu verkefnis eða kerfis.

Yfirleitt er ekki hægt að koma í veg fyrir alla áhættu en það ætti að vera hægt að lágmarka hana og ákveða hvort áhættan sé ásættanleg miðað við ávinning.

MÁP er ekki bara æfing. Það að framkvæma matið getur greint möguleg vandamál áður en þau verða, aukið traust og tiltrú þeirra sem verkefnið nær til og getur auk þess leitt til sparnaðar ef verkefnið er gert einfaldara og minna af persónuupplýsingum er safnað.

Að gera ekki mat á áhrifum á persónuvernd þar sem kringumstæður krefjast þess getur auk þess leitt til álagningar stjórnvaldssekta eða annarra valdheimilda Persónuverndar.



1.1 Hvernig er MÁP notað?

MÁP er hægt að framkvæma fyrir einstök verkefni eða safn skyldra verkefna. Það má jafnvel nýta sér MÁP sem áður var gert fyrir samsvarandi verkefni. Hópur vinnsluaðila getur líka gert sameiginlegt MÁP fyrir mörg svipuð eða tengd verkefni.

Fyrir ný verkefni er MÁP hluti af innbyggðri og sjálfgefinni persónuvernd. Best er að byggja persónuvernd inn í verkefni frá upphafi þegar mestir möguleikar eru að hafa áhrif á virknina.

Þó má ekki gleyma því að gera MÁP ef stórfelldar breytingar eru gerðar á langtímavinnslu.

MÁP má ekki bara vera eyðublað sem fyllt er út og geymt. Það er ferli sem þarf alltaf að hafa í huga frá upphafi til enda verkefnis. Til dæmis þarf að endurskoða áhættu ef ákveðið er að safna frekari upplýsingum, gildissviðið er víkkað, öryggisgallar uppgötvast eða breytingar verða á afstöðu almennings eða löggjafa til tiltekinnar áhættu.

1.2 Nánar um MÁP

Persónuverndarreglugerðin gerir kröfu til þess að MÁP sé gert við ákveðnar aðstæður áður en vinnsla fer fram.

1.2.1 Hver er meginreglan?

Meginreglan er sú að MÁP skuli framkvæmt þegar tiltekin vinnsla er líkleg til að fela í sér verulega áhættu fyrir rétt einstaklinga til persónuverndar.

1.2.2 Hvað þýðir „veruleg áhætta“?

Áhætta í þessu samhengi vísar til þess að hætta sé á verulegum skaða fyrir einstaklinga. Það þarf bæði að taka til þess hversu miklar líkur eru á skaða og þess hversu mikill skaðinn gæti orðið. ‘Veruleg áhætta’ getur þýtt annað hvort að meiri líkur séu á að skaðinn verði eða að skaðinn sé meiri eða hvort tveggja.

1.2.3 Hvenær þarf að framkvæma MÁP?

Reglugerðin tekur þrjú dæmi um vinnslu sem sjálfkrafa krefst mats á áhrifum á persónuvernd.

- Vinnsla sem felur í sér umfangsmikla söfnun persónuupplýsinga, gerð persónusniðs og notkun þess til ákvarðanatöku sem hefur lagalegar afleiðingar fyrir einstaklinga
- Umfangsmikil vinnsla viðkvæmra upplýsinga svo sem um heilsufar, fjárhag, erfðaupplýsingar eða sakaferil
- Umfangsmikil vöktun svæða sem eru opin almenningi

Hér ekki um tæmandi lista að ræða. Þannig getur verið um að ræða vinnsluaðgerðir sem fylgir mikil áhætta og eru ekki tilteknar í upptalningunni og þarf þess vegna að framkvæma MÁP.

Við mat á því hvort MÁP þurfi að fara fram má líta til þess hvort vinnslan felur í sér eitthvað af eftirfarandi atriðum:

1. Mat á einstaklingum, þ.m.t. notkun persónusniðs, einkum til að greina eða spá fyrir um þætti er varða frammistöðu í starfi, fjárhagsstöðu, heilsufar, smekk, áhugamál, áreiðanleika eða hegðun, staðsetningu eða hreyfanleika. Dæmi um þetta gæti t.d. verið þegar lánastofnun framkvæmir lánshæfismat einstaklings með því að bera upplýsingar saman við vanskilaskrá, þegar líftæknifyrirtæki býður erfðaefnisrannsóknir beint til neytenda í þeim tilgangi að leggja mat á og setja fram líkur á tilteknum áhættuþáttum, eða fyrirtæki sem býr til persónusnið í markaðssetningartilgangi á grundvelli upplýsinga um hegðun viðkomandi einstaklings inn á vefsíðu fyrirtækisins.
2. Sjálfvirk ákvarðanataka sem hefur réttaráhrif að því er varðar einstaklinginn sjálfan eða snertir hann á sambærilegan hátt að verulegu leyti. Slík ákvarðanataka má eingöngu fara fram við vissar aðstæður, t.d. þegar einstaklingur hefur veitt samþykki eða samið um það. Slík vinnsla getur leitt til þess að einstaklingum sé mismunað og þarf þess vegna að fara í MÁP.

3. Kerfisbundið eftirlit.
    - Hér falla meðal annars undir vinnsluaðgerðir sem taka til kerfisbundins og umfangsmikils eftirlits með svæði sem er aðgengilegt almenningi, t.d. notkun eftirlitsmyndavéla eða þegar fylgst er með hegðun og staðsetningu einstaklinga á þráðlausu neti (e. wi-fi tracking).
    - Þessi tegund vinnslu er háð mati á áhrifum vegna þess að í tilvikum sem þessum geta persónuupplýsingum verið safnað í aðstæðum þar sem einstaklingar gera sér ekki grein fyrir því hver er að safna upplýsingunum, og hvernig upplýsingarnar verða notaðar eða unnar. Þar að auki getur verið ómögulegt fyrir einstaklinga að forðast slíka vinnslu, ef hún fer fram á almennum svæðum, eða svæðum sem eru aðgengileg almenningi.
4. Viðkvæmar persónuupplýsingar eða upplýsingar persónulegs eðlis
    - Hér undir falla viðkvæmar persónuupplýsingar, t.d. upplýsingar um heilsufar, uppruna, kynhneigð og kynlíf og persónuupplýsingar er varða sakfellingar í refsimálum og refsiverð brot.
    - Sem dæmi má nefna hér varðveislu heilbrigðisstofnana á sjúkraskrám eða rannsakanda sem hefur undir höndum persónuupplýsingar einstaklinga í refsimálum. Jafnframt eru nokkrir flokkar persónuupplýsinga þess eðlis að vinnsla þeirra getur haft í för með sér aukna áhættu. Þessar upplýsingar teljast til viðkvæmra upplýsinga þar sem þær tengjast heimilis- og einkalífi þeirra einstaklinga sem í hlut eiga, s.s. rafrænar samskiptaupplýsingar, staðsetningarupplýsingar og fjárhagsupplýsingar. Hér getur þó skipt máli hvort upplýsingarnar hafa verið gerðar opinberar af einstaklingnum sjálfum eða öðrum honum óviðkomandi. Þá geta jafnframt fallið hér undir gögn er taka til persónulegra skjala, dagbókafærslna, tölvupósta o.fl.
5. Umfangsmiklar vinnsluaðgerðir
    - Taka ætti tillit til eftirfarandi þátta við mat á því hvort vinnsluaðgerð teljist umfangsmikil:
        - Fjöldi skráðra einstaklinga
        - Magn þeirra upplýsinga sem á að vinna með
        - Lengd eða varanleiki vinnslunnar
        - Landfræðilegt eða svæðisbundið umfang vinnslunnar
6. Samkeyrsla
    - Hér má nefna samkeyrslu sem á uppruna sinn að rekja í tvær eða fleiri vinnsluaðgerðir, sem eru framkvæmdar í mismunandi tilgangi og/eða af mismunandi ábyrgðaraðilum á þann hátt, að vinnslan færi fram úr raunhæfum væntingum einstaklingsins.
7. Persónuupplýsingar um viðkvæma hópa einstaklinga
    - Vinnsla þeirra persónuupplýsinga sem hér er um ræðir er háð MÁP vegna þess aðstöðumunar sem hugsanlega getur verið á milli ábyrgðaraðila og einstaklingsins sem vinnslan lýtur að. Þessi aðstöðumunur getur þýtt að einstaklingarnir eru eftir atvikum ekki færir um að veita samþykki fyrir vinnslu persónuupplýsinga, mótmæla vinnslunni, eða nýta réttindi sín. Til „viðkvæmra einstaklinga“ í þessum skilningi geta fallið hér undir börn, launþegar, einstaklingar sem þurfa sérstaka vernd (t.d. andlega veikir

einstaklingar, hælisleitendur, aldraðir, sjúklingar o.fl.). Það sem skiptir hér máli er að unnt sé að greina þann aðstöðumun sem ríkir milli einstaklingsins og ábyrgðaraðila.

8. Tækninýjungar eða nýstárlegar aðferðir við vinnslu persónuupplýsinga, t.d. notkun fingrafaralesara eða andlitsgreiningartækni til að stýra aðgangi að húsnæði, notkun á internet allra hluta (e. internet of things), gervigreind o.fl. Athuga skal þó að tæknin þarf að vera ný í tækniheiminum, ekki bara fyrir þér.
9. Þegar komið er í veg fyrir að einstaklingar njóti réttinda sinna, eða nýti sér þjónustu eða geri samninga
    - Hér má nefna vinnsluaðgerðir sem miða að því að leyfa, breyta eða neita hinum skráðu aðgangi að þjónustu eða samningi, t.d. gerð lánshæfismats eða synjun á bótarétti.

Eftir því sem fleiri af þessum viðmiðum eiga við um þá vinnslu sem á sér stað, því líklegra er að vinnslan hafi í för með sér mikla áhættu fyrir réttindi og frelsi einstaklinga.

Í flestum tilvikum geta fyrirtæki og stofnanir metið sem svo að vinnsla sem fellur undir tvö fyrrgreindra viðmiða þarfnist MÁP. Í einhverjum tilvikum getur þó niðurstaðan verið sú að vinnsla sem tekur til eins af viðmiðunum, þarfnist mats.

Eftirfarandi tafla sýnir hvernig unnt er að nota viðmiðin til þess að meta hvort tiltekin vinnsluaðgerð þarfnist MÁP:

Dæmi um vinnsluaðgerðir	Viðmið sem gætu átt við	Er þörf á MÁP?
Vinnsla heilsufars- og erfðafræðilega upplýsinga hjá heilbrigðisstofnun.	- Viðkvæmar persónuupplýsingar eða upplýsingar persónulega eðlis - Upplýsingar sem varða viðkvæma einstaklinga - Umfangsmiklar vinnsluaðgerðir	Já
Notkun eftirlitsmyndavéla til þess að vakta ökuhegðun á þjóðvegum. Ábyrgðaraðili hyggst nota greiningarkerfi sem getur numið bifreiðaplötur og aðgreint þær.	- Skipulagt eftirlit - Nýjar aðferðir eða nýjar lausnir	Já
Fyrirtæki sem viðhefur vöktun með vinnuskilum, þ. á m. vöktum með netnotkun og vinnuaðstöðu.	- Skipulagt eftirlit - Upplýsingar sem varða viðkvæma einstaklinga	Já
Söfnun félagslegra upplýsinga til þess að útbúa persónusnið.	- Mat/hæfni - Umfangsmiklar vinnsluaðgerðir	Já

	- Samkeyrsla - Viðkvæmar upplýsingar eða upplýsingar persónulegs eðlis	
Stofnun framkvæmir mat á lánshæfni.	- Mat/hæfni - Sjálfvirk ákvarðanataka sem hefur lagaleg eða önnur sambærileg, áhrif.	Já
Varðveisla viðkvæmra persónuupplýsinga sem hafa verið gerviauðkennd, þeirra viðkvæmu einstaklinga, vegna skjalavistunar, sem eru andlag rannsóknarverkefna og klínískra rannsókna.)	- Viðkvæmar upplýsingar - Gögn sem varða viðkvæma einstaklinga - Komið í veg fyrir að hinir skráðu njóti réttinda, eða gangi til samninga eða nýti sér þjónustu	Já
Vinnsla persónuupplýsinga frá einstökum lækni, öðrum faglærðum heilbrigðisstarfsmanni eða lögfræðingi um sjúklinga eða viðskiptavini. (91. gr. aðfararorðanna)	- Viðkvæmar upplýsingar eða upplýsingar persónulegs eðlis - Upplýsingar um viðkvæma einstaklinga	Nei
Tímarit sem notar póstlista til þess að senda almennt (e. *daily digest*?) til áskrifenda sinna.	- Umfangsmikil vinnsluaðgerð	Nei
Rafræn verslun birtir á Internetinu auglýsingar um varahluti í fornbíla, en auglýsingarnar birtast á grundvelli gerðrar persónusniðs með vísan til þeirra vara sem eru skoðaðar eða keyptar á vefsíðunni.	- Mat/hæfni	Nei

Vinnsluaðgerð getur fallið undir einhverra framangreindra atriða, en þó gæti niðurstaðan verið sú að vinnslan sé ekki líkleg til að hafa mikla áhættu í för með sér. Í slíkum aðstæðum þarf að réttlæta og skjalfesta ástæðuna fyrir því að mat á áhrifum eigi ekki að fara fram. Þá þarf einnig að tiltaka þau sjónarmið sem persónuverndarfulltrúinn hefur viðhaft, þar að lútandi, ef hann er til staðar.

1.3 Hvað þýðir „ný tækni“?

Reglugerðin skilgreinir ekki hvað er ný tækni. Þó er átt við tækni sem er nýjung í tækniheiminum í heild, ekki bara ný fyrir þér. Ákvæði reglugerðarinnar taka skýrt fram að beiting nýrrar tækni getur leitt

til þess að MÁP verður að fara fram. Þegar fyrirtæki og stofnanir nota nýja tækni til að safna eða vinna með persónuupplýsingar er líklegt til framkvæma MÁP. Einnig getur það átt við þegar eldri tækni er notuð á nýstárlegan hátt. Þetta er nauðsynlegt vegna þess að ný tækni getur haft í för með sér nýstárlegar aðferðir við gagnaöflun og –notkun, sem getur haft í för með sér mikla áhættu fyrir réttindi og frelsi skráðra einstaklinga. Að sjálfsögðu getur sú áhætta sem stafar af nýrri tækni eða nýjum lausnum, og/eða aðferðum við gagnaöflun eða vinnslu persónuupplýsinga verið óþekktar, en MÁP getur aðstoðað fyrirtæki og stofnanir að greina og takast á við slíka áhættu.

1.4 Hvað þýðir „kerfisbundin og umfangsmikil“?

Reglugerðin skilgreinir ekki með beinum hætti hvað sé kerfisbundið og umfangsmikið en ef miðað er við eldri reglugerðir má skilgreina vinnslu sem „kerfisbundna“ ef hún fer fram samkvæmt fyrirfram gerðri áætlun, er skipulögð og hluti af reglulegri starfsemi. „Umfangsmikil“ felur í sér að vinnslan nái til stórra landssvæða, mikils magns af persónuupplýsingum eða margra einstaklinga. Hér getur einnig þurft að taka mið af stærð viðkomandi lands, t.d. gæti vinnsla sem almennt væri ekki talin umfangsmikil í Evrópu talist mjög umfangsmikil á Íslandi þar sem um er að ræða fámenna þjóð.

2. Eru undantekningar frá kröfunni um MÁP?

Mat á áhrifum er ekki nauðsynlegt í eftirfarandi tilvikum:

- Ef ekki er líklegt að tiltekin tegund vinnslu hafi í för með sér mikla áhættu fyrir réttindi og frelsi einstaklinga
- Þegar eðli, umfang, samhengi og tilgangur vinnslunnar eru mjög svipaðir vinnslu sem þegar hefur farið í gegnum MÁP
- Þegar vinnsluaðgerðirnar hafa verið athugaðar af Persónuvernd fyrir gildistöku nýrra persónuverndarlaga.
- Þegar mælt er fyrir um vinnsluaðgerðina í lögum og MÁP var framkvæmt sem hluti af almennu áhrifamati við frumvarpsgerð. Hins vegar getur löggjafinn ákveðið að MÁP skuli engu að síður fara fram áður en formleg vinnsla hefst.
- Ef vinnsluaðgerð er á lista yfir þær tegundir vinnsluaðgerða þar sem ekki er krafist mats á áhrifum, sem Persónuvernd er heimilt að gefa út. Fyrirhugað er að birta slíkan lista fyrir lok árs 2018.

3. Hvernig á að framkvæma MÁP?

Mat á áhrifum á að framkvæma áður en vinnslan hefst. Það er fyrst og fremst fyrirtækið sjálft eða stofnunin sem ber ábyrgð á að framkvæma matið, ekki þjónustuaðili eða persónuverndarfulltrúinn. Það er þó hægt að útvista matinu en ábyrgðin liggur áfram hjá ábyrgðaraðilanum. Þá þarf að leita ráða hjá persónuverndarfulltrúa, sé hann til staðar, þegar matið er framkvæmt og er nauðsynlegt að skjalfesta í matinu þau ráð sem hann gefur.

Ef vinnsla er að hluta eða í heild unnin af þjónustuaðila eða vinnsluaðila, ber honum að aðstoða ábyrgðaraðila við að tryggja að skyldur samkvæmt löggjöfinni séu uppfylltar og veita nauðsynlegar upplýsingar.

Þá getur verið nauðsynlegt að leita álits einstaklinga sem vinna á upplýsingar um eða fulltrúa þeirra. Hægt er að afla álits þeirra t.d. með því að beina spurningum til fulltrúa starfsfólks eða senda könnun á viðskiptavini. Ef ábyrgðaraðili ákveður að ekki þurfi að leita álits þeirra einstaklinga sem vinnslan varðar þá getur hann þurft að skjalfesta það, t.d. ef það er talið skerða viðskiptaáætlanir fyrirtækis að upplýsa um fyrirhugaða vinnslu. Þá getur það líka einfaldlega verið úr hófi, óhagkvæmt og of kostnaðarsamt.

Þegar sérstakar rekstrareiningar leggja sérstaklega til að MÁP fari fram, ættu þær að vera viðloðandi matið og leggja fram tillögur. Þá getur verið viðeigandi að leita álits utanaðkomandi sérfræðinga sem tilheyra mismunandi starfsstéttum (lögfræðinga, upplýsingatæknifræðinga, öryggisfræðinga, siðfræðinga, félagsfræðinga o.fl.)

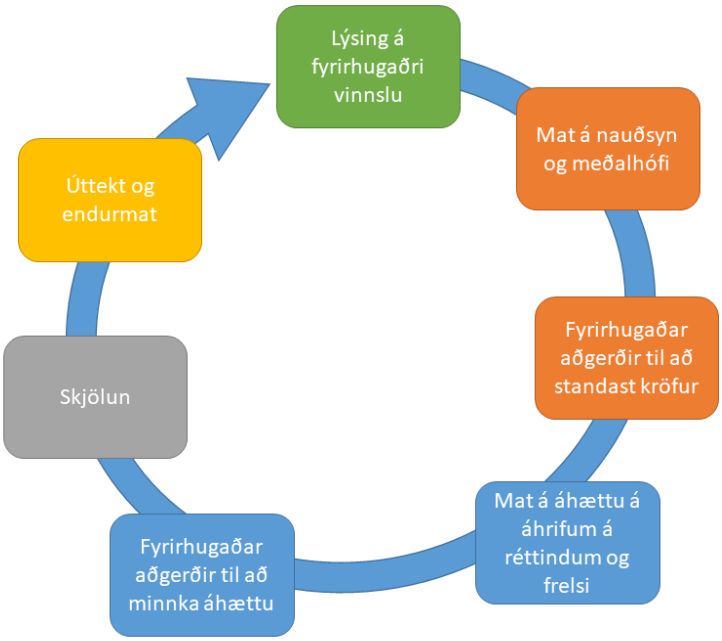
Öryggisstjórar og persónuverndarfulltrúar geta einnig lagt til að MÁP sé framkvæmt á tiltekinni vinnsluaðgerð. Þá ættu þessir aðilar einnig að aðstoða og hafa eftirlit með gerð matsins, þ.á m. til að meta gæði þess og hvort áhætta sem enn er til staðar er viðunandi.

Ábyrgðaraðilar geta tileinkað sér mismunandi aðferðafræði við framkvæmd matsins, en viðmiðin eru þau hin sömu.

Reglugerðin tiltekur ákveðna lágmarksþætti sem matið þarf að geyma:

- Kerfisbundin lýsing á fyrirhugðum vinnsluaðgerðum og tilganginum með vinnslunni
- Mat á því hvort vinnsluaðgerðirnar eru nauðsynlegar og hóflegar
- Mat á áhættu fyrir réttindi og frelsi skráðra einstaklinga
- Ráðstafanir sem fyrirhugað er að grípa til gegn slíkri áhættu og fyrirkomulag við að sýna fram á að farið sé að þessari reglugerð

Eftirfarandi skýringarmynd sýnir með myndrænum hætti það almenna ferli sem stöðugt þarf að viðhafa við framkvæmd MÁP:



Taka skal tilhlýðilegt tillit til þess hvort hlutaðeigandi ábyrgðaraðilar eða vinnsluaðilar fylgja samþykktum hátternisreglum þegar áhrif vinnsluaðgerða téðra ábyrgðaraðila eða vinnsluaðila eru metin. Þetta getur verið nytsamlegt fyrir ábyrgðaraðila til þess að sýna fram á að hann hafi gert fullnægjandi ráðstafanir, að því gefnu að hátternisreglurnar eru viðeigandi miðað við vinnsluaðgerðina.

Þá ætti einnig að taka tillit til vottana, innsigla, merkja, og bindandi fyrirtækjareglna við mat á því hvort þær vinnsluaðgerðir sem ábyrgðaraðilar eða vinnsluaðilar bera ábyrgð á, séu í samræmi við ákvæði reglugerðarinnar.

Þær kröfur sem reglugerðin gerir til mats á áhrifum veita á vissan hátt breiðan og almennan ramma fyrir hönnun og framkvæmd matsins. Reglugerðin veitir ábyrgðaraðilum sveigjanleika til þess að ákveða hvernig þeir vilja nákvæmlega haga uppbyggingu og tegund mats á áhrifum á persónuvernd. Óháð því hvaða tegund eða gerð mats verður fyrir valinu, þá verður mat á áhrifum að vera raunverulegt mat á þeirri áhættu sem stafar af vinnsluaðgerð, svo ábyrgðaraðilar geti viðhaft þær ráðstafanir til þess að koma til móts við áhættuna.

Það er hlutverk ábyrgðaraðila að velja þá aðferðafræði sem notast er við framkvæmd mats á áhrifum, en að lágmarki að farið sé eftir þeim viðmiðum sem Persónuvernd hefur sett fram:

3.1 Athugunarlisti vegna framkvæmdar mats á áhrifum á persónuvernd

1. <u>Kerfisbundin lýsing á fyrirhuguðum vinnsluaðgerðum, sem inniheldur:</u>
    - Eðli, umfang, samhengi og tilgang vinnslunnar;
    - Um hvaða persónuupplýsingar er að ræða, hverjir séu viðtakendur og varðveislutími;
    - Lýsingu á fyrirhuguðum vinnsluaðgerðum;

- Lýsingu á þeim upplýsingaeignum (vélbúnaður, hugbúnaður, net, fólk, pappír) sem nota á til vinnslunnar.
- Upplýsingar um hvort fylgt sé samþykktum hátternisreglum

2. Eru vinnsluaðgerðirnar nauðsynlegar og hóflegar miðað við tilgang?:
   - Ákveðnar hafa verið ráðstafanir sem miða að því að sýna fram á að farið sé að reglugerðinni:
     - Rökstudd lýsing á ráðstöfunum sem stuðla að nauðsyn og meðalhófi vinnslunnar og taka til eftirfarandi atriða:
       - Er tilgangurinn skýrt tilgreindur og lögmætur?
       - Er til staðar fullnægjandi heimild fyrir vinnslunni (samþykki, samningur, lagaskylda, almannahagsmunir, lögmætir hagsmunir o.s.frv.)? Sjá nánar 6.-9. gr. pvrg.
       - Eru upplýsingarnar sem vinna á með sem nægilegar, viðeigandi og takmarkast við það sem nauðsynlegt er?
       - Hefur verið tekin afstaða til þess hvenær eyða eigi upplýsingum (í tilviki stjórnvalda þarf að taka tillit til skilaskyldu til skjalasafna).
     - Rökstudd lýsing á ráðstöfunum sem stuðla að réttindum hinna skráðu og taka að lágmarki til eftirfarandi atriða:
       - Hvernig er fræðslu til hinna skráðu háttað? Sjá 12., 13. og 14. gr. pvrg.
       - Hvernig er tryggður réttur einstaklinga til aðgangs að persónuupplýsingum og réttur til að flytja eigin gögn, ef það á við? Sjá 15. og 20. gr. pvrg.
       - Hvernig er tryggður réttur til leiðréttingar og rétturinn til að gleymast? Sjá 16., 17. og 19. gr. pvrg.
       - Hvernig er tryggður andmælaréttur og réttur til takmörkunar á vinnslu Sjá 18., 19., og 21. gr. pvrg.
       - Lýsing á sambandi við vinnsluaðila, sé hann til staðar. Sjá 28. gr. pvrg.
       - Er fyrirhugað að flytja upplýsingar út fyrir EES-svæðið? Hvaða verndarráðstafana á að grípa til, s.s. að viðtakandi sé innan öruggs þriðja ríkis, búið sé að staðfesta bindandi fyrirtækjareglur eða gera staðlaða samningsskilmála? Sjá V. kafla pvrg.
       - Fyrirframsamráð við Persónuvernd
3. Áhætta og ógnir fyrir réttindi og frelsi skráðra einstaklinga skilgreindar
   - Uppruni, eðli, sérkenni og alvarleiki áhættunnar eru metin frá sjónarhóli hinna skráðu (s.s. ólögmætur aðgangur, óumbeðnar breytingar og eyðing upplýsinga).
     - Uppruni áhættunnar er skilgreindur. Sjá 90. lið formálsorða pvrg.
     - Möguleg áhrif á réttindi og frelsi hinna skráðu eru skilgreind í þeim tilvikum sem geta leitt til ólögmæts aðgangs, breytinga og eyðingar upplýsinga.
     - Ógnir sem geta leitt til ólögmæts aðgangs, breytinga eða eyðingar séu skilgreindar.

- Metnar séu líkur og alvarleiki. Sjá 90. lið formálsorða pvrg.

4. Hvaða ráðstafanir eru fyrirhugaðar til þess að draga úr áhættu.
   - Dæmi: Dulkóðun, gerviauðkenni, aðgangsstýring o.fl.
5. Samráð við hlutaðeigandi aðila:
   - Leita ráðgjafar hjá persónuverndarfulltrúar og skjalfesta ráðgjöf hans og af hverju ekki er farið að ráðum hans, ef við á.
   - Leita álits hjá þeim einstaklingum sem vinnslan lýtur að eða fulltrúa þeirra á fyrirhugaðri vinnslu, þegar við á.
6. Niðurstaða MÁP
   - Ef áhættan er enn of mikil miðað við skilgreind viðmið eru þrjár leiðir í boði:
     - Hætta við fyrirhugaða vinnslu persónuupplýsinga.
     - Grípa til frekari ráðstafana, t.d. sterkari dulkóðun, að dregið sé úr magni persónuupplýsinga sem safnað er, aðgangur starfsmanna sé takmarkaður við tiltekna starfsmenn o.fl.
     - Leita fyrirframsamráðs við Persónuvernd, ef ábyrgðaraðili getur ekki dregið úr áhættunni á viðunandi hátt.

3.2 Er til staðall um framkvæmd MÁP?

Nei, en fyrirhugað er að slíkur staðall verði gefinn út á vegum ISO: ISO/IEC 29134 (project), *Information technology – Security techniques – Privacy impact assessment – Guidelines* .

4. Ítarefni

- Vurdering av personvernkonsekvenser (DPIA), Datatilsynet
- Standard Data Protection Model, V.1.0 – Trial version, 201631, Datenschutzzentrum.
- *Guía para una Evaluación de Impacto en la Protección de Datos Personales (EIPD)*, Agencia española de protección de datos (AGPD).
- *Privacy Impact Assessment (PIA)*, Commission nationale de l'informatique et des libertés (CNIL).
- *Conducting privacy impact assessments code of practice*, Information Commissioner's Office (ICO).

[i] Á fyrsta fundi evrópska persónuverndarráðsins þann 25. maí 2018 var lýst yfir fullum stuðningi við þær leiðbeiningar sem 29. gr. vinnuhópurinn hafði gefið út vegna nýju persónuverndarreglugerðarinnar.