## LEIÐBEININGAR VEGNA NÝRRA PERSÓNUVERNDARREGLNA

## FYRSTA SKREF - Kortlagning gagna

### **Útfylling eyðublaðs um kortlagningu gagna**

Fyrirtækið verður að hafa yfirsýn yfir hvaða persónuupplýsingar unnið er með, um hverja upplýsingarnar eru, í hvaða tilgangi þær eru unnar og á hvaða lagalegum grundvelli vinnsla þeirra er byggð á. Þá verður það jafnframt að hafa yfirsýn yfir alla viðtakendur sem fengið hafa eða munu fá upplýsingarnar í hendur, hvenær eyða skuli mismunandi flokkum gagna og til hvaða skipulögðu öryggisráðstafana verði gripið o.s.frv.

Mælt er með því að fyllt sé út neðangreint skjal og svarað þeim spurningum sem þar koma fram til að unnt sé að öðlast nauðsynlega yfirsýn. Það gefur einnig vísbendingu um hvort fyrirtækið uppfyllir lögbundnar kröfur um vinnslu persónuupplýsinga.

Gott er að kortleggja hvern og einn flokk vinnslustarfsemi hjá fyrirtækinu. Til dæmis væri sérstakt skjal fyrir mannauðsmál, annað fyrir sölu- og markaðsmál, reikningshald, þjónustu við viðskiptavini, kaup á vörum og þjónustu, skattamálefni og fjármálastjórn, eignir og upplýsingaöryggi, flotastýringu o.s.frv. Æskilegt getur verið að fylla út fleiri en eitt skjal fyrir sama flokk vinnslustarfsemi, t.d. eitt fyrir starfsumsóknir, annað fyrir starfsmenn og það þriðja fyrir fyrrverandi starfsmenn.

Ef ekki er hægt að svara tiltekinni spurningu, er í lagi að viðkomandi reitur sé auður en bregðast þarf við honum við gerð vinnsluskrár í skrefi 2 sem er lögboðin. Í svarreitnum (til vinstri) er svarað viðkomandi spurningu en (til hægri) er hægt að setja sérstaka athugasemd við svarið.

| **Tegund vinnslustarfsemi: [Fylltu inn]** | **Athugasemdir við útfyllinguna:** |
| --- | --- |
| *Um hverja eru upplýsingarnar sem eru skráðar?*  *Til dæmis: Starfsmenn, fyrrverandi starfsmenn, fjölskylda / nánustu ættingjar, viðskiptavinir, hugsanlegir viðskiptamenn, birgjar eða aðrir aðilar*  *[VALKVÆTT: Á hvaða lagalega grundvelli skv. 6. gr. persónuverndarreglugerðarinnar byggist vinnslan?*  *Til dæmis: Hún byggist á samþykki en er einnig að hluta til nauðsynleg til að unnt sé að veita viðskiptavini pantaða þjónustu og uppfylla lögboðnar skyldur m.a. skv. bókhaldslögum.]* | Fyllið út flokkunina, eins og lýst er í dæminu. |
| *Hvers kyns persónuupplýsingar eru skráðar?*  *Inniheldur sú vinnslustarfsemi sem fellur undir flokkinn viðkvæmar persónuupplýsingar í skilningi persónuverndarlaga?[[1]](#footnote-1)* | Lýsa skal almennum persónuupplýsingum stutt og hnitmiðað en viðkvæmum persónuupplýsingum nánar. |
| *Hvaðan eru upplýsingarnar fengnar / hvernig er þeim safnað?* | Tilgreina hvort starfsmenn / aðrir veiti sjálfir upplýsingarnar eða hvort upplýsingarnar séu fengnar frá þriðja aðila og ef svo er frá hverjum / hvaðan. |
| *Hver er tilgangurinn með þessari tegund vinnslustarfsemi?* | Lýsið með almennum hætti  Tilgangur starfsmannaskrár er til dæmis mannauðsstjórnun. |
| *Eru einstaklingarnar sem persónuupplýsingarnar varða upplýstir um í hvaða tilgangi upplýsingarnar eru unnar?* | Fylltu út með já eða nei.  Ef já, til dæmis: Já, öllum umsækjendum um starf er birt persónuverndarstefna félagsins á heimasíðu okkar.  Ef nei, þarf að fylgja þessu eftir vinnsluskrá. |
| *Er til verklag um leiðréttingu upplýsinga þegar þess er þörf?*  *Hver hefur umsjón með að upplýsingarnar séu réttar og uppfærðar?* | Lýsið stuttlega gildandi verklagsreglum. |
| *Eru persónuupplýsingarnar afhentar þriðja aðila (utan fyrirtækisins)?*  *Ef já: hvers kyns aðilum eru afhentar upplýsingarnar? hver er tilgangurinn með afhendingunni?* | Lýsið stuttlega afhendingunni og tilganginum með því. |
| *Er öðrum fyrirtækjum (vinnsluaðila) veittur aðgangur að persónuupplýsingum sem fyrirtækið vinnur í tengslum við einstök verkefni?*  *Ef já: hefur samkomulag verið gert /eru í gildi verklagsreglur um hvenær slíkur aðgangur skuli veittur (vinnslusamningur)?* | Lýsið í stuttu máli þeim tilvikum þar sem önnur fyrirtæki fá aðgang að persónuupplýsingum. Þetta gæti t.d. verið ef fyrirtæki felur öðrum aðila að sjá um launavinnslu eða hýsingu á gögnum.  Þriðji aðili sem annast persónuupplýsingar fyrir hönd fyrirtækisins er svokallaður vinnsluaðili. Þess er krafist að gerður sé skriflegur samningur milli fyrirtækisins og vinnsluaðila.[[2]](#footnote-2) Gerðu hér grein fyrir því hvort slíkur samningur hafi verið gerður og tilgreindu ef við á heiti allra vinnsluaðila.  Ef samningur hefur ekki verið gerður þarf að bregðast við því. |
| *Eru upplýsingarnar sendar út fyrir ESB/EES svæðið og ef svo er hvert og til hvaða flokks viðtakenda?* | Fylltu út já eða nei.  Ef já, verður að bregðast við því. |
| *Hefur verið gert áhættumat um vinnslu persónuupplýsinga sem falla undir flokkinn?* | Fylltu út já eða nei.  Ef nei, verður að bregðast við því. |
| *Er við ákvörðun um vinnslu og við vinnsluna sem slíka gerðar viðeigandi tæknilegar og skipulagslegar verndarráðstafanir og tryggt að einungis sé unnið með þær persónuupplýsingar sem eru nauðsynlegar vegna tilgangs vinnslunnar hverju sinni (innbyggð og sjálfgefin persónuvernd)? Hvaða öryggisráðstafanir hafa verið gerðar til að tryggja innbyggða og sjálfgefna persónuvernd og vernda persónuupplýsingar? Eru ráðstafanirnar skjalfestar?* | Lýstu ráðstöfununum stuttlega  Ef engar ráðstafanir hafa verið gerðar og / eða verkferlar skráðir, verður að bregðast við því. |
| *Hefur mat á áhrifum á persónuvernd farið fram?*   * *Ef nei: hefur farið fram mat og hvers vegna er það ekki talið nauðsynlegt?* * *Ef já: hefur verið haft samráð við Persónuvernd?* | Lýsið stuttlega.   * Ef ekki hefur verið tekið til skoðunar hvort mat á áhrifum á persónuvernd eigi að fara fram og hvort samráð við Persónuvernd eigi að fara fram áður en vinnsla hefst, þarf að bregðast við því með endurskoðun á verkferlum. |
| *Er við ákvörðun um aðferðir við vinnsluna og þegar vinnslan sjálf fer fram, gerðar viðeigandi tæknilegar og skipulagslegar ráðstafanir, sem hannaðar eru til að framfylgja meginreglum um persónuvernd og felldar nauðsynlegar verndarráðstafanir inn í vinnsluna til að uppfylla kröfur persónuverndarlaga?*  *Eru gerðar viðeigandi tæknilegar og skipulagslegar ráðstafanir til að tryggja að sjálfgefið sé að einungis þær persónuupplýsingar séu unnar sem nauðsynlegar eru vegna tilgangs vinnslunnar hverju sinni?* | Lýsið stuttlega.  Ef ekki hafa verið framkvæmdar viðeigandi tæknilegar og skipulagslegar ráðstafanir til samræmis við kröfur 25. gr. persónuverndarreglugerðarinnar um innbyggða og sjálfgefna persónuvernd, þarf að bregðast við því með endurskoðun á verkferlum. |
| *Eru til verkferlar vegna frávika, þ.e. tilvik þar sem persónuupplýsingar eru rangar, þær fara á rangan stað, eru misnotaðar eða annað álíka?*  *Eru til verkferlar vegna öryggisbrota og um tilkynningar vegna þeirra til Persónuverndar? Eru reglurnar skráðar?* | Lýstu verkferlunum stuttlega  Ef engir verkferlar eru til þarf að bregðast við því. |
| *Hversu lengi eru upplýsingarnar geymdar?*  *Hver eru skilyrðin fyrir eyðingu upplýsinganna?*  *Hver ákveður hvort / hvenær upplýsingunum skuli eytt?*  *Hvernig er upplýsingunum eytt?* | Lýsið stuttlega.  Ef engir verkferlar eru til þarf að bregðast við því. |
| *Eru í gildi verklagsreglur í fyrirtækinu um hvernig eigi að afgreiða beiðnir frá einstaklingum sem fyrirtækið vinnur/safnar persónuupplýsingum um?*  *Hvert er verklagið vegna slíkra beiðna; þ. á m.:*   * *um aðgang að persónuupplýsingum* * *um upplýsingar um söfnun og vinnslu persónuupplýsinga* * *um leiðréttingu, takmörkun og / eða eyðingu upplýsinga* * *um flutning eigin gagna* | Lýstu verklagi stuttlega Ef engar verklagsreglur gilda og /eða eru skráðar, þarf að bregðast við því. |
| *Eru í gildi verklagsreglur í fyrirtækinu sem tryggja að ekki sé tekin mikilsverð ákvörðun eingöngu á grundvelli sjálfvirkrar gagnavinnslu, þ.m.t. gerðar persónusniðs, nema að til staðar séu þær undantekningar sem 22. gr. persónuverndarreglugerðarinnar mælir fyrir um?* | Lýstu verklagi stuttlega. Ef engar verklagsreglur gilda og /eða eru skráðar, þarf að bregðast við því. |

1. Til viðkvæmra persónuupplýsinga teljast þær upplýsingar sem við í daglegu tali teljum til dæmigerðra persónuupplýsinga. Dæmi um slíkar upplýsingar eru þær sem varða uppruna, litarhátt, pólitískar skoðanir, trúar- eða aðrar lífsskoðanir eða aðild að stéttarfélagi. Einnig teljast upplýsingar um heilbrigði (svo sem ónæmi, veikindi, óléttu), kynlíf og kynhneigð til viðkvæmra persónuupplýsinga. Sama gildir um erfðafræðilegar og líffræðilegar upplýsingar þegar tilgangur þeirra er að bera kennsl á mann. [↑](#footnote-ref-1)
2. Nálgast má sniðmát að vinnslusamningi á heimasíðu Persónuverndar: (<https://www.personuvernd.is/media/leidbeiningar-personuverndar/Leidbeiningar-fyrir-vinnsluadila_16.2.2018.pdf>). [↑](#footnote-ref-2)