notkunarleiðbeiningar við þriðja skref – innra eftirlitskerfi: skjal yfir innra eftirlitskerfi með skýringum

**INNRA EFTIRLITSKERFI UM VINNSLU PERSÓNUUPPLÝSINGA– SA FÉLAGSMENN**

**EFNISYFIRLIT**

1 inngangur 4

1.1 Stutt samantekt um innra eftirlit 4

1.2 Skýringar/forsendur 4

1.3 Uppbygging innra eftirlits 4

I skipulag 6

2 ábyrgð á vinnslu persónuupplýsinga í fyrirtækinu 6

2.1 Vinnsluábyrgð 6

3 YFIRLIT YFIR vinnslu PERSÓNUUPPLÝSINGA OG MAT Á Lögmæti 6

3.1 Almennar persónuupplýsingar um starfsmenn 6

3.1.1 Yfirlit 6

3.1.2 Tilgangur vinnslu og lögmæti 6

3.1.3 Sérstaklega um rafræna vöktun 6

3.1.4 Sérstaklega um kennitölu 6

3.2 Viðkvæmar persónuupplýsingar um starfsmenn 6

3.2.1 Yfirlit 6

3.2.2 Tilgangur vinnslu og lögmæti 7

3.2.3 Mat á þörf fyrir tilkynningu til starfsmanna 7

3.2.4 Andmæli, aðgangur, leiðrétting, eyðing og flutningur 7

3.3 Persónuupplýsingar um viðskiptavini 7

3.3.1 Yfirlit 7

3.3.2 Mat á þörf fyrir tilkynningu til viðskiptavina. 7

3.4 Persónuupplýsingar um starfsmenn birgja og aðra viðskiptamenn 7

3.4.1 Yfirlit 7

3.4.2 Mat á þörf fyrir tilkynningu til tengiliða starfsmanna birgja og annarra viðskiptamanna. 8

II FRAMKVÆMD 9

4 verklagsreglur VIÐ vinnslu persónuupplýsinga 9

4.1 Yfirlit yfir verklagsreglur sem þarf að uppfylla við vinnslu persónuupplýsinga 9

4.1.1 Tilgangur verklagsreglana 9

4.1.2 Verklagsreglur við vinnslu persónuupplýsinga 9

4.2 Krafa um lögmætan tilgang 9

4.2.1 Almennt um lögmætan tilgang 9

4.2.2 Lögmætur tilgangur vinnslu persónuupplýsinga um starfsmenn 9

4.2.3 Lögmætur tilgangur vinnslu persónuupplýsinga um viðskiptavini 10

4.2.4 Lögmætur tilgangur vinnslu persónuupplýsinga um tengiliði starfsmanna birgja og annarra viðskiptamanna 10

4.3 Kröfur til vinnslu persónuupplýsinga 10

4.3.1 Almennt um kröfur til vinnslu persónuupplýsinga 10

4.3.2 Kröfur til vinnslu (almennra) persónuupplýsinga 10

4.3.3 Kröfur til vinnslu viðkvæmra persónuupplýsinga 11

4.4 Mat á áhrifum á persónuvernd 11

4.4.1 Tilgangur verklagsreglunnar 11

4.4.2 Verklagsreglur í tengslum við mat á áhrifum á persónuvernd 11

4.5 Eyðing og takmörkun persónuupplýsinga 12

4.5.1 Tilgangur verklagsreglunnar 12

4.5.2 Skilyrði eyðslu og takmörkunar persónuupplýsinga 12

4.5.2.1 Upplýsingar um starfsmenn 12

4.5.2.2 Upplýsingar um tengiliði eða aðra einstaklinga hjá birgjum eða viðskiptamönnum 12

4.5.2.3 Undantekningar 13

4.6 Skylda til að veita upplýsingar 13

4.6.1 Tilgangur verklagsreglunnar 13

4.6.2 Skilyrði þess að veita upplýsingar 13

4.7 Aðgangsréttur 14

4.7.1 Tilgangur verklagsreglunnar 14

4.7.2 Skilyrði þess að fá að vita um vinnslu 14

4.8 Réttur til að flytja eigin gögn 15

4.8.1 Tilgangur verklagsreglunnar 15

4.8.2 Skilyrði flutnings eigin gagna 15

4.9 Leiðrétting og uppfærsla 15

4.9.1 Tilgangur verklagsreglunnar 15

4.9.2 Skilyrði leiðréttingar og uppfærsla 15

4.10 Miðlun persónuupplýsinga til annarra 15

4.10.1 Tilgangur verklagsreglunnar 15

4.10.2 Skilyrði miðlunar persónuupplýsinga til annarra 15

4.11 Réttur til að skoða einkatölvupóst og netnotkun 16

4.11.1 Tilgangur verklagsreglunnar 16

4.11.2 Verklagsreglur um skoðun einkatölvupósts og netnotkun 16

4.12 Sjálfvirk og einstaklingsmiðuð ákvarðanataka 16

4.12.1 Tilgangur verklagsreglunnar 16

4.12.2 Verklagsreglur um sjálfvirka og einstaklingsmiðaða ákvarðanatöku 17

4.13 Innbyggð og sjálfgefin persónuvernd 17

4.13.1 Tilgangur verklagsreglunnar 17

4.13.2 Verklagsreglur um innbyggða og sjálfgefna persónuvernd 17

4.14 Persónuverndarfulltrúi 17

4.14.1 Tilgangur verklagsreglunnar 17

4.14.2 Verklagsreglur um persónuverndarfulltrúa 17

5 öryggismARKMIÐ og öryggisáætlun 18

5.1 Inngangur 18

5.2 Öryggismarkmið 18

5.3 Öryggisáætlun 19

5.4 Skipulag 19

6 áhættumat 20

6.1 Leiðir við að framkvæma áhættumat 20

6.2 Mat á afleiðingum 20

6.3 Eftirfylgni áhættumats 20

III EFTIRLIT 21

7 meðhöndlun frávika 21

8 verklag um kerfisbundnar uppfærslur 21

8.1 Inngangur 21

8.2 Reglur um uppfærslu og endurskoðun 21

# inngangur

## Stutt samantekt um innra eftirlit

Fyrirtæki sem vinna persónuupplýsingar, til dæmis safna, skrá, geyma eða miðla persónuupplýsingum þurfa að uppfylla vissar kröfur samkvæmt persónuverndarlöggjöfinni. Fyrirtækið þarf að hafa innra eftirlitskerfi til að geta staðið vörð um að uppfylltar séu kröfur persónuverndarlaganna. Markmið þessa skjals er að aðstoða fyrirtæki við að uppfylla kröfur sínar um innra eftirlit.

Innra eftirlitskerfi fyrirtækisins þarf að vera aðgengilegt starfsmönnum ásamt fulltrúum Persónuverndar.

## Skýringar/forsendur

Með „fyrirtæki“ í skjali þessu og viðaukum við það er átt við [setja inn nafn fyrirtækis þíns].

|  |
| --- |
| ***Ath.!***  Skjalið er hægt að laga til eftir þörfum ef fyrirtækið hefur nú þegar gögn undir höndum sem staðfesta að uppfylltar séu kröfur um vinnslu persónuupplýsinga, sbr. skref 2) Vinnsluskrá.  Það er einnig mikilvægt að hafa í huga að hér er skipulag innra eftirlits miðað við lítil og meðalstór fyrirtæki en ekki stór og tæknilega flókin fyrirtæki. Skjalið þarf að yfirfara og aðlaga að þínum rekstri. Til dæmis ef fyrirtækið er ekki með neina starfsmenn, má sleppa þeim atriðum.  Ákvæði um verkaskiptingu og ábyrgð eru miðuð við það sem almennt ætti að reynast vel. Það er nauðsynlegt að skipan mála sé skoðuð og aðlöguð að uppbyggingu og þörfum fyrirtækis þíns. |

## Uppbygging innra eftirlits

Innra eftirlit er skipt í þrjá mismunandi hluta:

I hluti Skipulag  
  
Hluti I lýsir almennt vinnslu persónuupplýsinga í fyrirtækinu, hver/hverjir bera ábyrgð og hvernig vinnsla persónuupplýsinga fer fram. Þar er auk þess fjallað um lögmæti vinnslunnar og lagt mat á hvernig fyrirtækið hefur fullnægt og aðlagað sig að skyldum sínum.

|  |
| --- |
| ***Ath.!***  Við mat á því hvort vinnslan sé lögmæt eða ekki er litið til ákvæða persónuverndarlaga og þess sem fram kemur í skrefi 2) Vinnsluskrá. |

2 Hluti Framkvæmd

Í 2. hluta eru ákveðnar verklagsreglur og yfirsýn yfir þær skyldur sem fyrirtækið verður að uppfylla vegna vinnslu persónuupplýsinga. Þegar vinnslu er breytt eða ný vinnsla hefst þarf að fara eftir þessum verklagsreglum.

Í 2. hluta er einnig að finna ákvæði um þær öryggisráðstafanir sem hafa verið innleiddar í fyrirtækinu.

|  |
| --- |
| ***Ath!***  Við mat á skyldu fyrirtækisins við vinnslu persónuupplýsinga er rétt að líta til skrefs 2) Vinnsluskrá |

3 Hluti Eftirlit

3. hluti tekur á því hvernig fyrirtækið meðhöndlar frávik frá verklagi um vinnslu persónuupplýsinga og grun um öryggisbrot.

Í 3. hluta eru einnig ákvæði sem ætluð eru að staðfesta að vinnsla hafa átt sér stað í samræmi við samþykkt verklag og fyrirmæli.

# I skipulag

# ábyrgð á vinnslu persónuupplýsinga í fyrirtækinu

## Vinnsluábyrgð

Fyrirtækið ber samkvæmt persónuverndarlögunum ábyrgð á vinnslu persónuupplýsinga um starfsmenn, viðskiptavini og aðra tengiliði.

|  |
| --- |
| ***Ath.!***  *Fyrirtækið getur fengið annan aðila eða svokallaðan „vinnsluaðila“ til að annast í heild eða að hluta vinnslu persónuupplýsinga sem fyrirtækið ber ábyrgð á. Aðlaga þarf þá eftirlitsskjalið og viðhengi þess í samræmi við það.* |

# YFIRLIT YFIR vinnslu PERSÓNUUPPLÝSINGA OG MAT Á Lögmæti

## Almennar persónuupplýsingar um starfsmenn

### Yfirlit

Fyrirtækið vinnur persónuupplýsingar um starfmenn sína og uppfærir reglulega skrá yfir vinnsluna. Yfirlitið er aðgengilegt [*skráðu inn hvar niðurstöður úr Skrefi 2) Vinnsluskrá er aðgengilegt*].

### Tilgangur vinnslu og lögmæti

Tilgangur fyrirtækisins með vinnslu persónuupplýsinga um starfsmenn sína er mannauðsstjórnun. Þar á meðal felst skylda fyrirtækisins að standa við samnings- og kjarasamningsbundnar skuldbindingar sínar gagnvart einstökum starfsmönnum, framkvæma verkefni sem lögð eru fyrir það af opinberu yfirvaldi og uppfylla lagaskyldur sem tengjast vinnusambandinu, t.d. skv. bókhaldslögum. Það er því stoð fyrir vinnslunni í persónuverndarlögum.

### Sérstaklega um rafræna vöktun

[Fyrirtækið hefur málefnalegar ástæður fyrir því að vinna persónuupplýsingar með myndavélakerfi þar sem vinnsla er nauðsynleg í öryggis- og eignavörsluskyni. Fyrirtækið hefur jafnframt málefnalegar ástæður til að skoða einkatölvupóst þegar brýna nauðsyn ber til vegna tölvuveiru eða sambærilegs tæknilegs atviks. Jafnframt upplýsingar um netvafur, tengingar og gagnamagn starfsmanns liggi fyrir rökstuddur grunur um að hann hafi brotið gegn gildandi lögum og reglum eða fyrirmælum fyrirtækisins. Þá hefur fyrirtækið málefnalegar ástæður til að annast vinnslu persónuupplýsinga með ökurita og rafrænum staðsetningarbúnaði vegna veigamikilla öryggissjónarmiða.]

## Viðkvæmar persónuupplýsingar um starfsmenn

### Yfirlit

Í ákveðnum tilfellum kann fyrirtækið að vinna persónuupplýsingar um starfsmenn vegna refsiverðs verknaðar sem þeir hafa framið eða grunur leikur á að þeir hafi framið í starfi sínu. Enn fremur vinnur fyrirtækið upplýsingar um stéttarfélagsaðild og heilsufar starfsmanna í tengslum við framkvæmd vinnu. Yfirlit um slíka vinnslu er aðgengilegt [*skráðu inn hvar niðurstöður úr Skrefi 2) Vinnsluskrá er aðgengilegt*].

### Tilgangur vinnslu og lögmæti

Þar sem vinnsla upplýsinga um (meintan) refsiverðan verknað í starfi getur verið afar þýðingarmikil við að upplýsa, koma í veg fyrir og færa sönnur á slík brot hefur fyrirtækið skýran og lögmætan tilgang fyrir vinnslu persónuupplýsinganna.

Vinnsla upplýsinga um stéttarfélagsaðild og heilsufar starfsmanna er notuð til að framfylgja ráðningarsambandinu.

Tilgangur vinnslunnar er því í samræmi við persónuverndarlög.

### Mat á þörf fyrir tilkynningu til starfsmanna

Almennt þarf ekki að veita starfsmönnum fræðslu um vinnslu persónuupplýsinga um þá þar sem þeir eru meðvitaðir um vinnsluna. Þess fyrir utan fullnægir fyrirtækið fræðsluskyldu sinni í öllum almennum tilvikum með aðgangi að innra eftirlitsskjali og/eða með almennri persónuverndarstefnu sem birt er á innra neti fyrirtækisins eða samsvarandi tiltækum aðgerðum. Í öðrum tilvikum þegar það er talið nauðsynlegt mun fyrirtækið veita starfsmönnum sérstakar upplýsingar.

### Andmæli, aðgangur, leiðrétting, eyðing og flutningur

Starfsmenn geta andmælt vinnslu upplýsinga um sig og afturkallað samþykki sitt til vinnslu þegar það á við með því að senda skriflega fyrirspurn á [...]. Starfsmanni er þó bent á að afturköllun samþykkis hefur ekki afturvirk áhrif. Þá geta starfsmenn sent fyrirspurn á sama netfang óski þeir eftir að fá aðgang að, fá afrit, leiðrétta eða óska eftir flutningi persónuupplýsinga um sig. Beiðni starfsmanna verður tekin til greina og þeim afhentar upplýsingarnar (þegar það á við) innan hæfilegs tíma, þó með þeim takmörkunum sem réttindi og frelsi annarra gera, þ.m.t. viðskiptaleyndarmál og hugverkaréttindi. Starfsmanni er jafnframt bent á rétt sinn til að kvarta til Persónuverndar.

## Persónuupplýsingar um viðskiptavini

### Yfirlit

Fyrirtækið vinnur persónuupplýsingar um viðskiptavini sína. Yfirlitið er aðgengilegt [*skráðu inn hvar niðurstöður úr Skrefi 2) Vinnsluskrá er aðgengilegt*]. Viðskiptavinir geta nálgast upplýsingar um vinnsluna, þ. á m. hvaða upplýsingum er safnað, í hvaða tilgangi þær eru nýttar, hvert þeim er miðlað og hvernig nálgast megi aðgang að þeim í persónuverndarstefnu fyrirtækisins. Persónuverndarstefnan er aðgengileg [*skráðu inn hvar niðurstaða úr Skrefi 4) Persónuverndarstefna er aðgengilegt*].

### Mat á þörf fyrir tilkynningu til viðskiptavina.

Ekki þarf að tilkynna viðskiptavinum um vinnslu persónuupplýsinga ef þeir eru meðvitaðir um vinnsluna.

## Persónuupplýsingar um starfsmenn birgja og aðra viðskiptamenn

### Yfirlit

Fyrirtækið vinnur einhverjar persónuupplýsingar um starfsmenn birgja og aðra viðskiptamenn. Yfirlit er aðgengilegt [*skráðu inn hvar niðurstöður úr Skrefi 2) Vinnsluskrá er aðgengilegt*]. Starfsmenn birgja og aðrir viðskiptamenn geta nálgast upplýsingar um vinnsluna, þ. á m. hvaða upplýsingum er safnað, í hvaða tilgangi þær eru nýttar, hvert þeim er miðlað og hvernig nálgast megi aðgang að þeim í persónuverndarstefnu fyrirtækisins. Persónuverndarstefnan er aðgengileg [*skráðu inn hvar niðurstaða úr Skrefi 4) Persónuverndarstefna er aðgengilegt*].

### Mat á þörf fyrir tilkynningu til tengiliða starfsmanna birgja og annarra viðskiptamanna.

Ekki þarf að tilkynna tengiliðum starfsmanna birgja eða öðrum viðskiptamönnum um vinnslu persónuupplýsinga ef þeir eru meðvitaðir um vinnsluna.

# II FRAMKVÆMD

# verklagsreglur VIÐ vinnslu persónuupplýsinga

## Yfirlit yfir verklagsreglur sem þarf að uppfylla við vinnslu persónuupplýsinga

### Tilgangur verklagsreglana

Tilgangur verklagsreglana er að tryggja að fyrirtækið vinni aðeins með persónuupplýsingar að uppfylltum skilyrðum persónuverndarlaga og að gripið sé til nauðsynlegra öryggisráðstafana.

### Verklagsreglur við vinnslu persónuupplýsinga

Fyrirtækið skal:

* Meta hvort núverandi vinnsla uppfylli skilyrðið um lögmætan tilgang (sjá kafla 4.2),
* Meta hvort uppfylltar séu kröfur til vinnslu persónuupplýsinga (sjá kafla 4.3),
* Meta hvort fullnægt hafi verið kröfum um mat á áhrifum á persónuvernd og um fyrirframsamráð við Persónuvernd (sjá kafla 4.4),
* Ganga úr skugga um að persónuupplýsingar séu ekki geymdar lengur og að meira umfangi en nauðsyn krefur (sjá kafla 4.5)
* Uppfylla upplýsingaskyldu fyrirtækisins (sjá kafla 4.6)
* Uppfylla aðgangsskyldu fyrirtækisins (sjá kafla 4.7)
* Uppfylla skyldu fyrirtækisins til að flytja eigin gögn (sjá kafla 4.8)
* Framkvæma nauðsynlegar lagfæringar og viðbætur á persónuupplýsingum (sjá kafla 4.9)
* Ganga úr skugga um að persónuupplýsingum sé ekki miðlað til annarra nema heimild standi til þess (sjá kafla 4.10)
* Ganga úr skugga um að einkatölvupóstur og netnotkun starfsmanns sé aðeins skoðuð þegar lagaheimild stendur til þess og þá eftir lögboðnum aðferðum (sjá kafla 4.11)
* Ganga úr skugga um að ákvörðun verði ekki eingöngu tekin á grundvelli sjálfvirkrar og einstaklingsbundinnar ákvarðanatöku í öðrum tilvikum en þegar það er heimilt (sjá kafla 4.12)
* Ganga úr skugga um að áhættumat sem tengist núverandi vinnslu sé framkvæmt að því marki sem nauðsyn krefur (sjá kafla 6) og
* Ganga úr skugga um að gripið sé til nauðsynlegra öryggisráðstafana (sjá kafla 5 og 6).
* Framkvæma reglulegar kerfisbundnar uppfærslur (sjá kafla 8).

## Krafa um lögmætan tilgang

### Almennt um lögmætan tilgang

Einungis er heimilt að vinna persónuupplýsingar þegar lögmætur tilgangur stendur til vinnslunnar.

Í kafla 4.2.2, 4.2.3 og 4.2.4 hér að neðan er fjallað um hvenær lögmætur tilgangur er fyrir vinnslu persónuupplýsinga. Vinnsla persónuupplýsinga í öðrum tilgangi kann þó að vera lögmæt en það verður að meta í hverju tilviki fyrir sig. Ef vafi leikur á því hvort vinnsla telst framkvæmd í lögmætum tilgangi er rétt að leita sér lögfræðiráðgjafar áður en vinnsla hefst.

Tilgangurinn með vinnslu á alltaf að vera skýrt afmarkaður og hægt að rökstyðja hann áður en vinnsla hefst. Tilgangurinn setur takmarkanir á því hvaða upplýsingar má nota. Auk þess er þá ekki heimilt að nota þær upplýsingar í öðrum og ósamrýmanlegum tilgangi.

### Lögmætur tilgangur vinnslu persónuupplýsinga um starfsmenn

Fyrirtækið vinnur persónuupplýsingar um starfsmenn sína í eftirfarandi lögmætum tilgangi:

* Vinnsla er nauðsynleg til að efna ráðningarsamninga við einstaka starfsmenn.

Undir framangreindan tilgang fellur m.a. vinnsla persónuupplýsinga í tengslum við ráðningu, þjálfun, mat og þróun, launavinnslu, vinnuskipulag, ferðalög, útlagðan kostnað og samskipti innan fyrirtækisins.

* Vinnsla er nauðsynleg til verndar heilsu og öryggi starfsmanna.

Undir þennan tilgang fellur vinnsla heilsufarsupplýsinga, þ. á m. um ættingja sem er nauðsynleg til að gera vinnuveitanda kleift að efna ráðningarsamninginn.

* Vinnsla persónuupplýsinga vegna ýmissa skipulags- og eftirlitsráðstafana.

Undir þennan tilgang fellur starfsemi sem tengist skipulagningu og framkvæmd vinnu, rannsókna, athugunum og innra eftirliti.

* Vinnsla er nauðsynleg til að uppfylla lagaskyldu.

Tilgangur vinnslunnar er m.a. vinnsla persónuupplýsinga í tengslum við dómsmál.

* Vinnsla er nauðsynleg til að unnt sé að uppræta brot á skyldum samkvæmt ráðningarsambandi.

### Lögmætur tilgangur vinnslu persónuupplýsinga um viðskiptavini

Fyrirtækið vinnur persónuupplýsingar um viðskiptavini til að geta sinnt sambandi sínu við viðskiptavini og uppfyllt samningsbundnar skyldur sínar. Sjá nánar persónuverndarstefnu fyrirtækisins sem er aðgengileg [*skráðu inn hvar niðurstaða úr Skrefi 4) Persónuverndarstefna er aðgengilegt*].

### Lögmætur tilgangur vinnslu persónuupplýsinga um tengiliði starfsmanna birgja og annarra viðskiptamanna

Fyrirtækið vinnur persónuupplýsingar um tengiliði starfsmanna birgja og annarra viðskiptamanna til að geta sinnt sambandi sínu við birgja og aðra viðskiptamenn og til að geta uppfyllt samningsbundnar skyldur sínar. Sjá nánar persónuverndarstefnu fyrirtækisins sem er aðgengileg [*skráðu inn hvar niðurstaða úr Skrefi 4) Persónuverndarstefna er aðgengilegt*].

## Kröfur til vinnslu persónuupplýsinga

### Almennt um kröfur til vinnslu persónuupplýsinga

Einungis er heimilt að vinna persónuupplýsingar þegar lögmætur tilgangur stendur til vinnslu, sbr. kafla 4.2 og að fullnægðum lámarkskröfum til vinnslu. Nánar er gerð grein fyrir kröfum til vinnslu persónuupplýsinga hér að neðan. Óheimilt er að vinna persónuupplýsingar standi ekki sérstök heimild til vinnslu.

### Kröfur til vinnslu (almennra) persónuupplýsinga

Ólíkar kröfur eru gerðar til vinnslu almennra persónuupplýsinga og viðkvæmra persónuupplýsinga, sjá kröfur til vinnslu viðkvæmra persónuupplýsinga í kafla 4.3.3:

* (A) Samþykki frá þeim aðila sem upplýsingarnar varða,
  + Samþykki felur í sér frjálsa og sjálfsviljuga yfirlýsingu sem gefin er með upplýstum og ótvíræðum hætti. Samþykki má því aldrei vera þvingað eða gefið undir pressu. Enn fremur er alltaf heimilt að afturkalla samþykki. Ef samþykki fyrir vinnslu er afturkallað skal fyrirtæki þar með hætta þeirri vinnslu nema annað sé sérstaklega tekið fram en afturköllunin hefur ekki afturvirk áhrif. Ekki eru gerðar sérstakar formkröfur til samþykkis en mælt er með því að það sé gefið með skriflegum hætti svo dregið sé úr sönnunarerfiðleikum á tilvist þess.
* (B) Nauðsynleg til að fullnægja lagaskyldu, og
* Vinnsla persónuupplýsinga getur verið nauðsynleg til að:
  + (C) Uppfylla samning við þann sem upplýsingarnar varða – til dæmis í ráðningarsamningi, samningi við viðskiptavin, birgja eða annan viðskiptamann, eða til að sinna verkefnum að ósk tilgreinds starfsmanns.

Stór hluti þeirra upplýsinga sem fyrirtækið vinnur um starfsmenn sína byggist á þessari heimild (C).

* + (D) Gæta lögmætra hagsmuna,
  + (E) Vernda brýna hagsmuni þess sem upplýsingarnar varða eða annars einstaklings.
  + Mikilvægt er að ganga úr skugga um að þörf fyrirtækisins eða annars aðila fyrir vinnslunni sé ekki minni en persónuverndarréttur þess sem upplýsingarnar varðar af því að upplýsingarnar séu ekki unnar.

### Kröfur til vinnslu viðkvæmra persónuupplýsinga

Ef unnið er með viðkvæmar persónuupplýsingar (sjá viðkvæmar persónuupplýsingar sem fyrirtækið vinnur með í tengslum við skref 2) Vinnsluskrá), er vinnsla jafnframt heimil í öðrum tilvikum en þeim sem koma fram í kafla 4.3.2 þegar hún er nauðsynleg til að;

* Vernda verulega hagsmuni einstaklings eða annars sem getur ekki veitt samþykki sitt fyrir vinnslunni t.d. sökum veikinda- eða lögræðisskorts,
* Stofna, hafa uppi eða verja réttarkröfur, eða
* Verja almannahagsmuni á sviði lýðheilsu.

## Mat á áhrifum á persónuvernd

### Tilgangur verklagsreglunnar

Tilgangur þessarar greinar er að tryggja að fyrirtæki láti fara fram mat á áhrifum á persónuvernd ef tiltekin tegund vinnslu getur haft í för með sér mikla áhættu fyrir réttindi og frelsi einstaklinga og afli sérstaks leyfis þegar þess er krafist.

Ef óljóst er hvort vinnsla krefjist mats á áhrifum á persónuvernd er rétt að leita lögfræðilegrar ráðgjafar áður en vinnslan hefst.

Upplýsingar um mat á áhrifum á persónuvernd má einnig finna á heimasíðu Persónuverndar (https://www.personuvernd.is/fyrirtaeki-og-stjornsysla/fraedsluefni/leidbeiningar-fra-evropska-personuverndarradinu-edpb )

### Verklagsreglur í tengslum við mat á áhrifum á persónuvernd

Einungis þarf að framkvæma mat á áhrifum á persónuvernd þegar það er skylt samkvæmt sérstakri skrá vinnsluaðgerða.

Þegar mat á áhrifum á persónuvernd á við skal [framkvæmdastjóri]:

* Sjá til þess að matið sé framkvæmt áður en vinnsla hefst.

Eiga fyrirframsamráð við Persónuvernd ef mat á áhrifum á persónuvernd gefur til kynna að vinnsla muni hafa mikla áhættu í för með sér áður en vinnsla hefst, nema fyrirtækið geti gripið til nauðsynlegra ráðstafana til að draga úr áhættunni.

## Eyðing og takmörkun persónuupplýsinga

### Tilgangur verklagsreglunnar

Tilgangur verklagsreglunnar er að tryggja að brugðist verði við kröfum einstaklinga um eyðingu eða takmörkun persónuupplýsinga í samræmi við kröfur 17. og 18. gr. persónuverndarreglugerðarinnar og að persónuupplýsingar séu ekki geymdar lengur eða að meira umfangi en nauðsyn ber til.

### Skilyrði eyðslu og takmörkunar persónuupplýsinga

#### Upplýsingar um starfsmenn

Vinnsla persónuupplýsinga um starfsmenn er að meginstefnu til heimil á meðan ráðningarsambandið varir. Á hinn bóginn á ekki að geyma neinar persónuupplýsingar lengur en nauðsyn er á til að ná tilgangi vinnslunnar. Nauðsynlegt kann að vera að geyma ákveðnar upplýsingar í tiltekinn tíma eftir starfslok þannig að unnt sé að svara fyrirspurnum frá opinberum aðilum. [Framkvæmdastjóri/mannauðsstjóri] verður að leggja mat á það sérstaklega hvort fyrirtækið hafi lögmætan tilgang til frekari vinnslu skv. kafla 4.2 og hvort vinnsla sé nauðsynleg.

[Framkvæmdastjóri/mannauðsstjóri] fyrirtækis skal:

* Uppfæra yfirlit yfir vinnslu persónuupplýsinga (vinnsluskrá) þegar þörf krefur,
* Fjarlægja óþarfa upplýsingar úr skýrslum og öðrum sambærilegum gögnum þegar lokið er viðtali við starfsmann vegna veikindafjarvista,
* Fjarlægja óþarfa upplýsingar í tengslum við starfslok,
* Endurskoða þörf fyrir áframhaldandi geymslu persónuupplýsinga um starfsmann ári eftir starfslok,
* Ganga úr skugga um að persónuupplýsingar sem tengjast ekki vinnuréttarsambandinu séu ekki geymdar um starfsmenn og
* Tryggja að persónuupplýsingum sé reglulega eytt þegar þeirra er ekki lengur þörf eða þegar heimild til vinnslu er ekki lengur til staðar og að þær séu takmarkaðar þegar skráður einstaklingur fer fram á það skv. nánari fyrirmælum 17. og 18. gr. persónuverndarreglugerðarinnar.

#### Upplýsingar um tengiliði eða aðra einstaklinga hjá birgjum eða viðskiptamönnum

Vinnsla persónuupplýsinga um tengiliði eða aðra einstaklinga hjá birgjum eða viðskiptamönnum er heimil svo lengi sem tengsl eru á milli vinnslunnar og viðskiptasambandsins. Þá kann einnig að vera nauðsynlegt að geyma persónuupplýsingarnar í tiltekinn tíma eftir að viðskiptasambandi lýkur. [Framkvæmdastjóri] verður að leggja mat á það sérstaklega hvort fyrirtækið hafi lögmætan tilgang til frekari vinnslu skv. kafla 4.2 og hvort vinnsla sé nauðsynleg.

[Framkvæmdastjóri] skal:

* Fjarlægja óþarfa persónuupplýsingar þegar viðskiptasamband við viðkomandi birgja eða viðskiptamann rennur út,
* Gera nýtt mat á þörf fyrir áframhaldandi geymslu einu ári eftir að viðskiptasambandinu lýkur,
* Ganga úr skugga um að ekki séu geymdar persónuupplýsingar um tengiliði birgja eða viðskiptamanna sem tengjast ekki viðskiptasambandinu og
* Tryggja að persónuupplýsingum sé reglulega eytt þegar þeirra er ekki lengur þörf eða heimild til vinnslu er ekki lengur til staðar og að þær séu takmarkaðar þegar skráður einstaklingur fer fram á það skv. nánari fyrirmælum 18. gr. persónuverndarreglugerðarinnar.

#### Undantekningar

Ef skylt er að geyma upplýsingar í samræmi við ákvæði bókhaldslaga eða annarra laga eiga ákvæði 4.5.2.1 – 4.5.2.2 ekki við. Slíkum upplýsingum er óheimilt að eyða fyrr en lögboðinn geymsluréttur er liðinn.

## Skylda til að veita upplýsingar

### Tilgangur verklagsreglunnar

Tilgangur verklagsreglunnar er að uppfylla upplýsingaskyldu persónuverndarlaga.

Einstaklingur sem fyrirtækið býr yfir persónuupplýsingum um skal fá eftirfarandi upplýsingar áður en vinnsla persónuupplýsinga hefst:

* Nafn og aðrar nauðsynlegar samskiptaupplýsingar frá fyrirtækinu og vinnsluaðila þess, ef við á (þ.e. þess fyrirtækis sem vinnur persónuupplýsingarnar),
* upplýsingar um tilgang vinnslunnar og lagagrundvöll hennar,
* upplýsingar um hvort upplýsingunum verði miðlað og flokkum viðtakanda, ef einhverjir eru,
* upplýsingar um hvaðan upplýsingarnar koma og, ef við á, hvort um hafi verið að ræða upplýsingar sem eru aðgengilegar almenningi,
* upplýsingar um hvort til standi að miðla upplýsingunum til lands utan ESB/EES ásamt því hvort það land sé meðal ríkja sem tryggi fullnægjandi vernd ásamt tilvísun til viðeigandi eða hæfilegra verndarráðstafana,
* samskiptaupplýsingar persónuverndarfulltrúa, ef við á,
* upplýsingar um hversu lengi persónuupplýsingarnar verði geymdar eða sé það ekki mögulegt þær viðmiðanir sem notaðar eru til að ákveða það,
* hvaða lögmætu hagsmunir standi til þess að vinnsla sé nauðsynleg, ef við á,
* að heimilt sé að draga samþykki til baka hvenær sem er, ef við á,
* upplýsingar um hvort það að veita persónuupplýsingar sé krafa samkvæmt lögum eða samningi eða forsenda þess að hægt sé að gera samning og einnig hvort einstaklingi sé skylt að láta persónuupplýsingarnar í té og mögulegar afleiðingar þess ef viðkomandi veitir ekki upplýsingarnar,
* upplýsingar um hvort fram fari sjálfvirk ákvarðanataka, þ.m.t. gerð persónusniðs og þau rök sem þar liggja að baki og einnig þýðingu og fyrirhugaðar afleiðingar slíkrar vinnslu og
* annað sem getur gert einstaklingnum kleift að nýta sér réttindi sín samkvæmt persónuverndarlögum, svo sem réttur hans til þess að andmæla vinnslu, leggja fram kvörtun til Persónuverndar eða annars eftirlitsyfirvalds, ef við á ásamt því að krefjast aðgangs, leiðréttingar, takmörkunar, eyðingar og til að flytja eigin gögn.

Ekki er nauðsynlegt að veita upplýsingar um vinnslu persónuupplýsinga ef ljóst má vera að viðkomandi hefur þegar upplýsingarnar undir höndum, það fæli í sér óhóflega fyrirhöfn þegar vinnsla er framkvæmd í tölfræðilegum tilgangi, skýrt er mælt fyrir um öflun og miðlun upplýsinganna í lögum eða óheimilt er að veita upplýsingarnar á grundvelli lögbundinna þagnarskylduákvæða.

### Skilyrði þess að veita upplýsingar

Áður en vinnsla hefst á nýjum eða breyttum persónuupplýsingum, skal [framkvæmdastjóri] huga að því hvort veita skuli upplýsingar um vinnsluna eða hvort það sé óþarft þar sem slíkar upplýsingar hafa þegar verið veittar eða ljóst má vera að þeir sem upplýsingarnar varða hafa þegar nauðsynlegar upplýsingar undir höndum.

## Aðgangsréttur

### Tilgangur verklagsreglunnar

Tilgangurinn með verklagsreglunni er að uppfylla kröfu persónuverndarlaga um rétt einstaklings til að fá að vita hvers konar persónuupplýsingar fyrirtækið er að vinna um hann. Eftirfarandi upplýsingar skal veita samkvæmt beiðni:

* Nafn og aðrar samskiptaupplýsingar frá fyrirtækinu og vinnsluaðila, ef við á (þ.e. þess fyrirtækis sem vinnur persónuupplýsingarnar),
* Tilgang og lagagrundvöll vinnslunnar,
* upplýsingar um viðtakendur þ. á m. í landi utan ESB/EES og flokk viðtakanda sem hafa fengið eða munu fá persónuupplýsingarnar í hendur,
* upplýsingar um þær verndarráðstafanir sem gripið hefur verið til vegna miðlunar upplýsinga til lands utan ESB/EES,
* upplýsingar um hversu lengi persónuupplýsingar verði geymdar eða, sé það ekki mögulegt, þær viðmiðanir sem notaðar eru til að ákveða það,
* upplýsingar um uppruna upplýsinganna sé þeirra ekki aflað hjá viðkomandi einstaklingi,
* upplýsingar um hvort fram fari sjálfvirk ákvarðanataka, þ.m.t. gerð persónusniðs þegar marktækar upplýsingar um þau rök sem þar liggja að baki og einnig þýðingu og fyrirhugaðar afleiðingar slíkrar vinnslu og
* annað sem getur gert einstaklingnum kleift að nýta sér réttindi sín samkvæmt persónuverndarlögum, svo sem réttur hans til þess að andmæla vinnslu, leggja fram kvörtun til Persónuverndar eða annars eftirlitsyfirvalds, ef við á ásamt því að krefjast aðgangs, leiðréttingar, takmörkunar, eyðingar og til að flytja eigin gögn.

Enn fremur skal verklagsreglan leitast við að tryggja að fyrirtækið veiti frekari upplýsingar en taldar eru upp hér að framan af því marki sem það kann að vera nauðsynlegt til að einstaklingurinn sem upplýsingarnar varða geti tryggt hagsmuni sína.

### Skilyrði þess að fá að vita um vinnslu

[Framkvæmdastjóri] skal þegar beiðni kemur fram

* Ef nauðsyn krefur, óska eftir skriflegri staðfestingu á beiðninni,
* Senda beiðnina til eiganda hugbúnaðarkerfisins og
* Staðfesta móttöku beiðninnar.

Ef sá sem óskar eftir upplýsingum um vinnsluna er sá aðili sem upplýsingarnar varða (hinn skráði), skal [framkvæmdastjóri]:

* Prenta afrit og, ef nauðsyn krefur, vinna úr þeim upplýsingum sem skylt er að veita að teknu tilliti til réttinda og frelsi annarra og
* Safna upplýsingum frá núverandi kerfum um viðkomandi og senda þær skv. beiðninni án ótilhlýðilegrar tafar, þó ekki seinna en innan mánaðar frá viðtöku beiðninnar nema fjöldi flókinna beiðna gera það að verkum að ekki sé unnt að verða við henni innan þess tíma. Skal þá tilkynna um seinkunina og afgreiða beiðnina innan tveggja mánaða frá viðtöku hennar.

## Réttur til að flytja eigin gögn

### Tilgangur verklagsreglunnar

Tilgangur verklagsreglunnar er að tryggja að kröfur persónuverndarlaga varðandi flutning eigin gagna sé fullnægt.

### Skilyrði flutnings eigin gagna

[Framkvæmdastjóri] skal sjá til þess að einstaklingi séu afhentar persónuupplýsingar er varða hann sjálfan og sem hann hefur látið fyrirtækinu í té, á skipulegu, algengu, tölvulesanlegu sniði eða þær séu sendar beint til annars aðila, enda:

* Byggist vinnslan á samþykki,
* Byggist vinnslan á samningi,
* Er vinnslan sjálfvirk.

Rétturinn til flutnings eigin gagna skal ekki takmarka réttindi og frelsi annarra.

## Leiðrétting og uppfærsla

### Tilgangur verklagsreglunnar

Tilgangur verklagsreglunnar er að tryggja að kröfur persónuverndarlaga varðandi leiðréttingu og uppfærslu sé fullnægt. Í samræmi við persónuverndarlögin skal fyrirtækið tryggja að gætt sé að meðalhófi og áreiðanleika við vinnslu persónuupplýsinga. Enn fremur skal fyrirtækið að eigin frumkvæði eða að beiðni þess einstaklings sem upplýsingarnar varða leiðrétta ófullnægjandi upplýsingar.

### Skilyrði leiðréttingar og uppfærsla

[Framkvæmdastjóri] skal:

* Uppfæra persónuupplýsingar sem reynast rangar,
* Meta fyrirspurnir um leiðréttingu og uppfærslu frá þeim sem upplýsingarnar eiga við,
* Meta hvort nauðsyn sé á að breyta upplýsingum af öðrum ástæðum,
* Ef nauðsyn krefur, gefa fyrirmæli um að breyta upplýsingum,
* Veita skriflega tilkynningu til einstaklinga sem hafa óskað eftir leiðréttingu eða uppfærslu, ef slík fyrirspurn hefur valdið breytingum á upplýsingunum og
* Tilkynna sérhverjum aðila sem fengið hefur persónuupplýsingar í hendur, um hvers kyns leiðréttingu eða eyðingu, nema það sé ekki unnt eða feli í sér óhóflega fyrirhöfn.

## Miðlun persónuupplýsinga til annarra

### Tilgangur verklagsreglunnar

Tilgangur verklagsreglunnar er að tryggja að persónuupplýsingar sem unnar eru af fyrirtækinu sé ekki miðlað áfram til annarra án lögmætrar heimildar.

### Skilyrði miðlunar persónuupplýsinga til annarra

Komi fram beiðni um miðlun persónuupplýsinga, skal [framkvæmdastjóri]:

* Meta hvort fallast skuli á beiðnina, m.a. að undangengnu mati á því hvort uppfyllt séu skilyrði um lögmætan tilgang og vinnslu persónuupplýsinga, skv. gr. 4.2 og 4.3 hér að ofan.
* Sjá til þess að gripið sé til fullnægjandi verndarráðstafana ef miðla á upplýsingum til lands utan ESB/EES svæðisins sem ekki er talið veita fullnægjandi vernd að mati ákvörðun framkvæmdastjórnar Evrópusambandsins.
* Sjá til þess að tilnefnt sé forystueftirlitsvald ef vinnsla persónuupplýsinga á sér stað yfir landamæri í tengslum við starfsemi starfstöðva fyrirtækisins í fleiri en einu ríki ESB/EES svæðisins, eða þegar vinnsla persónuupplýsinga sem fram fer í tengslum við starfsemi einnar starfstöðvar hefur veruleg áhrif eða er líklegt er að hafi veruleg áhrif á einstaklinga í fleiri en einu ríki ESB/EES svæðisins.

## Réttur til að skoða einkatölvupóst og netnotkun

### Tilgangur verklagsreglunnar

Tilgangur verklagsreglunnar er að tryggja að einungis sé skoðað einkapósthólf og netnotkun starfsmanns þegar lagaheimild stendur til þess og þá eftir lögboðnum aðferðum.

Ef vafi er fyrir hendi er rétt að leita sér lögfræðilegrar ráðgjafar áður en ákvörðun er tekin.

### Verklagsreglur um skoðun einkatölvupósts og netnotkun

[Framkvæmdastjóri] skal meta hvort grundvöllur sé fyrir skoðun. Einungis er heimilt að skoða einkatölvupóst

* Þegar það er nauðsynlegt vegna tölvuveiru eða sambærilegs tæknilegs atviks eða að uppfylltum skilyrðum 8. – 11. gr. persónuverndarlaga, einkum vegna gruns starfsmanns um brots gegn trúnaðar- eða vinnuskyldum.

Einungis er heimilt að skoða upplýsingar um netvafur, tengingar og gagnamagn starfsmanns

* Liggi fyrir rökstuddur grunur um að hann hafi brotið gegn gildandi lögum og reglum eða fyrirmælum vinnuveitanda.

Eftir þessa skoðun er ráðlagt að fylgja eftirfarandi verklagsreglum.

[Framkvæmdastjóri] skal:

* Ganga úr skugga um að starfsmanni sé tilkynnt um skoðunina eins fljótt og hægt er og honum veittur kostur á að játa meint brot (ef við á) án þess að skoðun þurfi þá að fara fram. Í tilkynningunni skal koma fram hvers vegna fyrirtækið telji skilyrði til aðgangs vera fyrir hendi. Í tilkynningunni skal jafnframt upplýst um rétt starfsmanns til að vera viðstaddur skoðunina eða tilnefna fulltrúa fyrir sína hönd,
* Ganga úr skugga um að starfsmanni, sé eins og unnt er, gefinn raunverulegur kostur á að vera viðstaddur skoðunina. Starfsmenn eiga rétt á að njóta aðstoðar trúnaðarmanns eða annars fulltrúa við skoðunina,
* Óska atbeini lögreglu sé tilefni skoðunarinnar grunur um refsiverðan verknað,
* Tryggja að fyrirtækið hafi ekki lengur aðgang að upplýsingunum og að afrit af þeim sé eytt ef skoðun sýnir að ekkert bendi til brots í starfi,
* Ganga úr skugga um að skráðar séu niðurstöður skoðunarinnar.

## Sjálfvirk og einstaklingsmiðuð ákvarðanataka

### Tilgangur verklagsreglunnar

Tilgangur verklagsreglunnar er að tryggja að ákvörðun verði ekki tekin eingöngu á grundvelli sjálfvirkar gagnavinnslu, þ.m.t. gerðar persónusniðs, nema í undantekningartilvikum, enda hafi ákvörðunin réttaráhrif að því er hann sjálfan varðar eða snertir hann að verulegu leyti á sambærilegan hátt.

### Verklagsreglur um sjálfvirka og einstaklingsmiðaða ákvarðanatöku

[Framkvæmdastjóri] skal sjá til þess að ákvörðun sem hefur réttaráhrif á einstaklinga eða snertir þá að verulegu leyti verði ekki tekin eingöngu á grundvelli sjálfvirkar ákvarðanatöku nema ákvörðunin:

* Sé forsenda þess að unnt sé að gera eða framkvæma samning á milli einstaklingsins og fyrirtækisins,
* Sé heimiluð í lögum, eða
* Byggist á afdráttarlausu samþykki einstaklingsins.

Í þeim tilvikum sem ákvörðun getur byggst á sjálfvirkri ákvarðanatöku er skilyrði að gerðar séu viðeigandi ráðstafanir til að vernda rétt, frelsi og lögmæta hagsmuni viðkomandi einstaklinga.

## Innbyggð og sjálfgefin persónuvernd

### Tilgangur verklagsreglunnar

Tilgangur verklagsreglunnar er að tryggja að við ákvörðun um aðferð við vinnslu og við vinnsluna sjálfa séu gerðar viðeigandi tæknilegar og skipulagslegar öryggisráðstafanir í skilningi 24. gr. persónuverndarlaganna.

### Verklagsreglur um innbyggða og sjálfgefna persónuvernd

[Framkvæmdastjóri] skal sjá til þess að við ákvörðun um vinnslu og við vinnsluna sjálfa séu gerðar viðeigandi tæknilegar og skipulagslegar öryggisráðstafanir, með hliðsjón af nýjustu tækni, kostnaði við framkvæmd og eðli, umfangi, samhengi og tilgangi vinnslunnar, sem skulu tryggja:

* Lágmörkun gagna, með skilvirkum hætti,
* Að ekki sé unnið meira með persónuupplýsingar en nauðsynlegt er vegna tilgangs vinnslunnar,
* Að persónuupplýsingar séu ekki varðveittar lengur en nauðsyn krefur,
* Að persónuupplýsingar séu ekki gerðar aðgengilegar ótakmörkuðum fjölda fólks án íhlutunar viðkomandi einstaklings,
* Að inn í vinnsluna séu innbyggðar nauðsynlegar verndarráðstafanir til að uppfylla kröfur persónuverndarlaga og vernda réttindi einstaklinga.

## Persónuverndarfulltrúi

### Tilgangur verklagsreglunnar

Tilgangur verklagsreglunnar er að tryggja að mat á því hvort tilnefna eigi persónuverndarfulltrúa fari fram og að það sé endurskoðað við endurskoðun á eftirlitskerfinu. Þá er tilgangur verklagsreglunnar jafnframt að tryggja að tilnefndur sé persónuverndarfulltrúi þegar á við sem uppfyllir hæfisskilyrði 4. þáttar persónuverndarreglugerðarinnar varðandi faglega hæfni og sjálfstæði og skapa umhverfi fyrir hann til að rækja hlutverk sitt í samræmi við persónuverndarlög.

### Verklagsreglur um persónuverndarfulltrúa

[Framkvæmdastjóri] skal sjá til þess að fram fari mat á því hvort tilnefna eigi persónuverndarfulltrúa og leitað sé álits sérfróðra aðila ef vafi leikur á því hvort skylt sé að tilnefna hann. Mat á því hvort tilnefna þurfi persónuverndarfulltrúa skal tekið til endurskoðunar við endurskoðun á innra eftirlitskerfi skv. grein 8.2.

Ef niðurstaða fyrirtækisins er sú að tilnefna þurfi persónuverndarfulltrúa skal [framkvæmdastjóri] sjá til þess að:

* Tilnefndur sé án nokkurs dráttar aðili í verkefnið, starfsmaður eða utanaðkomandi verktaki, sem uppfyllir kröfu um faglega hæfni, einkum á sviði laga og lagaframkvæmdar á sviði persónuverndar og getu til að sinna þeim verkefnum sem honum eru falin skv. 39. gr. persónuverndarreglugerðarinnar, ásamt kröfum um hlutleysi,
* Tryggt sé að persónuverndarfulltrúi komi, með viðeigandi hætti og tímanlega, að öllum málum sem tengjast vernd persónuupplýsinga,
* Persónuverndarfulltrúi fái nauðsynlegan stuðning við framkvæmd þeirra verkefna sem starfinu fylgja með því að láta honum í té nauðsynleg úrræði til að inna þau af hendi, auk aðgangs að persónuupplýsingum og vinnsluaðgerðum, og gera honum kleift að viðhalda sérþekkingu sinni,
* Sjálfstæði persónuverndarfulltrúa sé tryggt og að hann fái engin fyrirmæli varðandi framkvæmd verkefna sinna og að honum sé ekki vikið úr starfi né refsað vegna þeirra og heyri ekki undir annan varðandi verkefni sitt en æðstu stjórn fyrirtækisins,
* Önnur verkefni sem fyrirtækið felur persónuverndarfulltrúa leiði ekki til hagsmunaáreksturs.

# öryggismARKMIÐ og öryggisáætlun

## Inngangur

Öryggismarkmið og öryggisáætlun fyrirtækis setja ramma utan um upplýsingaöryggi þess. Öryggismarkmiðin lýsa þeim markmiðum um öryggi sem að er stefnt, en öryggisstefnan lýsir því hvernig leitast skuli við að ná öryggismarkmiðunum.

|  |
| --- |
| ***Ath.!***  Textinn hér að neðan er dæmi um öryggismarkmið -og áætlun. Nauðsynlegt getur verið að aðlaga öryggismarkmiðin -og áætlunina eftir þörfum og eðli hvers fyrirtækis. |

## Öryggismarkmið

Eftirfarandi öryggismarkmið eru skilgreind:

* Gengið skal úr skugga um að persónuupplýsingar um einstaka starfsmenn fyrirtækisins eða viðskiptavini þess séu aðeins aðgengilegar fyrir einstaklinga sem þarfnast upplýsinganna í starfi sínu og gætt skal að því að óviðkomandi hafi ekki aðgang að gögnunum (trúnaður),
* Gengið skal úr skugga um að persónuupplýsingar um starfsmenn fyrirtækisins og viðskiptavini þess séu uppfærðar og aðgengilegar þeim notendum sem eiga lögmætan aðgang að þeim (aðgangur),
* Gengið skal úr skugga um áreiðanleika gagna og að þeim sé ekki breytt án heimildar eða fyrir mistök (áreiðanleiki),
* Gengið skal úr skugga um að persónuupplýsingarnar séu vel varðveittar þannig að óviðkomandi aðili hafi ekki aðgang að þeim (varðveisla).

Dæmi um atriði sem fyrirtækið vill vernda sig gegn:

* Algeng brot á trúnaði, heilindum og aðgengi.
  + Innbrot í fyrirtækið eða netkerfi þess.
  + Óheimil notkun notendareikninga.
  + Tölvuárás.
* Trúnaðarbrot
  + Tap á flytjanlegum búnaði.
  + Tap á geymslumiðli.
  + Útprentun sem liggur í prentara.
  + Óviljandi miðlun starfsmannaupplýsinga með tölvupósti.
* Brot á heilindum
  + Mismunandi útgáfur af skjölum.
  + Rangfærsla.
* Brot á tiltækileika
  + Netkerfi eða kerfi úr vinnslu.
  + Eldur, vatnsskemmdir og rafmagnsskemmdir.
  + Skemmdarverk.
  + Miðlunarsynjun (Denial of Service).

## Öryggisáætlun

Til að ná framangreindum öryggismarkmiðum hefur eftirfarandi öryggisráðstöfunum verið komið á fót:

* [Skipa [...] sem persónuverndarfulltrúa ásamt því að] skipa[...] sem öryggisfulltrúa,
* Komið skal í veg fyrir að óviðkomandi aðili hafi aðgang að persónuupplýsingum eða stöðum þar sem þær eru geymdar,
* Tryggt skal með aðgangstakmörkunum að aðgangur að persónuupplýsingum sé takmarkaður við þá sem eiga lögmætan tilgang til aðgangs að gögnunum störfum sinna vegna,
* Gengið skal úr skugga um að netkerfi fyrirtækisins sé varið gegn áhrifum utanaðkomandi netkerfa með eldvegg sem heimilar aðeins nauðsynlega gagnaumferð,
* Gengið skal úr skugga um að netkerfi fyrirtækisins sé varið gegn óleyfilegri notkun, svo sem með þráðlausum netum,
* Gera þarf sérstakar ráðstafanir til varnar ákveðnum upplýsingum, svo sem veikindaskrá starfsmanna, upplýsingar um vinnuskipulag, umsagnir um starfsmenn og áminningar.
* Allir starfsmenn sem eru með aðgang að upplýsingakerfum verða að undirrita leiðbeiningar um öryggi (sjá viðauka A),
* Starfsmenn og aðrir aðilar, sem hafa aðgang að trúnaðarupplýsingum um fyrirtækið skuli skrifa undir þagnaryfirlýsingu (sjá viðauka B „Ábyrgðaryfirlýsing um þagnarskyldu“),
* Gera skal vinnslusamning við alla þriðju aðila sem annast í heild eða að hluta vinnslu persónuupplýsinga sem fyrirtækið ber ábyrgð á (sjá viðauka G),
* Upplýsingar um uppsetningu (netteikningar, lýsingar á tækjum og hugbúnaði ásamt uppsetningu hugbúnaðar) skal vera uppfært og endurspegla núverandi stillingar, (sjá viðauka C „Lýsing á uppsetningu“). Aðgangur að viðhenginu er takmarkaður.
* Verklagsreglur um rekstur upplýsingakerfisins og lýsing á öryggisráðstöfunum er skjalfest (sjá viðauka E „Öryggisafrit“). *[Vinsamlegast fylltu inn upplýsingar um hvernig fyrirtækið tengist hugbúnaðarsérfræðingi – innanhúsmanni eða utanaðkomandi].*

## Skipulag

[Framkvæmdastjóri/Öryggisstjóri/Persónuverndarfulltrúi] hefur umsjón með öllum öryggismálum er snúa að persónuvernd. Hann skal hafa yfirsýn yfir vinnslu persónuupplýsinga og í hvaða tilgangi það sé gert. Þá skal hann ganga úr skugga um að fyrirtækið sé ávallt með til staðar nauðsynlegar verklagsreglur við vinnslu persónuupplýsinga, sem og undirbúa, kalla eftir og skrá niður niðurstöður úr áhættumati og innra eftirliti.

Hugbúnaður og upplýsingakerfi skulu vera þannig uppbyggð að tryggt sé að kröfum sem byggjast á framangreindu öryggismarkmiði og öryggisáætlun sé mætt. Þetta felur í sér ráðstafanir eins og:

* Innbyggt öryggi í hugbúnaði gegn þjófnaði, skemmdarverkum og rafmagnsleysi.
* Yfirlit yfir upplýsingakerfi fyrirtækisins.
* Gengið sé úr skugga um að upplýsingakerfi séu flokkuð eftir tegund þeirra upplýsinga sem unnið er með.
* Öryggisafrit og örugg geymsla öryggisafrita.

Að því marki sem rekstur upplýsingakerfisins hefur verið útvistað til þriðja aðila (vinnsluaðila) skal vinnsluaðili fá nauðsynlegar upplýsingar eins og þeim er lýst í þessum kafla svo hann geti sinnt hlutverki sínu.

# áhættumat

## Leiðir við að framkvæma áhættumat

Gera skal áhættumat til að meta hvort persónuupplýsingar sem unnar eru af fyrirtækinu eru tryggðar með fullnægjandi hætti varðandi trúnað, áreiðanleika og aðgengi.

Áhættumat er framkvæmt eftir þörfum og þegar breytingar eiga sér stað sem geta haft áhrif á upplýsingaöryggi, svo sem breytingar á upplýsingakerfum eða þegar breytingar eiga sér stað á áhættuþáttum.

Niðurstöður áhættumats af kerfum þar sem vinnsla persónuupplýsinga fer fram á grundvelli vinnslusamnings, milli fyrirtækis og þriðja aðila (vinnsluaðila) þarf að vera staðfest af vinnsluaðila og ábyrgðaraðila.

## Mat á afleiðingum

Áhættumat byggist á mati á áhrifum og líkindum þar sem:

Áhætta = Áhrif \* Líkindi

Áhætta er stærð sem gefur til kynna möguleg áhrif tiltekins atburðar á fyrirtæki ef hann liggur ljós fyrir. Líkindi er aftur stærð sem miðast við þekkingu á því hvernig ógn eða ógnunarvaldur getur nýtt sér varnarleysi eða veikleika. Hægt er að velja á milli þess að nýta sér hreina líkindamælikvarða, líkindi byggt á reynslu, hvata / hvötum eða samsetningu af hvoru tveggja.

Ef áhættuþátturinn er meiri en samþykkt áhætta er þörf á að láta framkvæma öryggisráðstafanir til að draga úr áhættu. Hægt er að draga úr áhættu með með því að draga úr áhrifum eða líkindum.

Dæmi um einfalt áhættumat er að finna í fyrri hluta viðauka D.

## Eftirfylgni áhættumats

Dæmi um aðgerðir sem hægt er að grípa til við að fylgja eftir niðurstöðum áhættumats þegar niðurstaða þess er ekki viðunandi er að finna í síðari hluta viðauka D.

# III EFTIRLIT

# meðhöndlun frávika

Samkvæmt persónuverndarlögum telst það frávik sem skylt er að meðhöndla ef:

* persónuupplýsingar eru meðhöndlaðar í andstöðu við verklagsreglur eða
* ef um öryggisbrot er að ræða eða
* grunur leikur á því.

Tilgangur meðhöndlunar frávika er að endurheimta eðlilegt ástand og koma í veg fyrir að frávikið endurtaki sig.

Meðhöndlun frávika felur í sér:

* Greiningu á frávikinu,
* Skýrslugerð þess sem greinir frávik. Fráviki skal tilkynna til [persónuverndarfulltrúa / öryggisstjóra],
* Framkvæmd á ráðstöfunum til aðhaldsaðgerða meðal annars með það fyrir augum að takmarka hugsanlega afleitt tjón,
* Framkvæmd úrbótaaðgerða til að endurheimta eðlilegt ástand. Það er venjulega gert af [kerfisstjóra / gæðastjóra / framkvæmdastjóra] og
* Mat á hvort úrbótaaðgerðir virki í samræmi við tilgang þeirra. Mat á því skal fara fram fljótlega í kjölfarið af [kerfisstjóra / gæðastjóra / framkvæmdastjóra].

Meðhöndlun frávika skal skjalfest í samræmi við skýrslu um öryggisbrot (sjá viðauka F).

Ef frávikið hefur leitt til öryggisbrots eða meints öryggisbrots skal tilkynna um það til Persónuverndar án ótilhlýðilegrar tafar þó eigi síðar en 72 klst. eftir að fyrirtæki verður vart við öryggisbrotið nema ólíklegt þyki að brotið leiði til áhættu fyrir réttindi og frelsi einstaklinga.

# verklag um kerfisbundnar uppfærslur

## Inngangur

Innra eftirlitskerfi líkt og þetta krefst reglulegrar uppfærslu og endurskoðunar. Það er í höfuðatriðum vegna þess að

* reglur laga og reglugerða geta breyst,
* vinnsla persónuupplýsinga getur breyst eða
* reynsla af verklagsreglunum getur leitt til þess að breyta verði verklagsreglum

Í ljósi þessa hafa verið settar nánari reglur um uppfærslu og endurskoðun á innra eftirlitskerfi þannig að það geti virkað sem lifandi tól og tryggt á hverjum tíma að það standist kröfur laga og reglugerða.

## Reglur um uppfærslu og endurskoðun

[Framkvæmdastjóri] er ábyrgur fyrir því að innra eftirlitskerfið sé uppfært og endurskoðað þegar breytinga gerist þörf eins skjótt og hægt er.

[Framkvæmdastjóri] skal láta framkvæma mat og endurskoðun á innra eftirlitskerfi fyrir [skrifa inn dagsetningu] ár hvert. Matið ætti að gefa svör við eftirfarandi spurningum:

* Hefur fyrirtækið frá fyrri endurskoðun hafið nýja vinnslu persónuupplýsinga sem ekki er stýrt með innra eftirlitskerfi?
* Hefur fyrirtækið frá því að endurskoðun fór fram síðast lokið við tiltekna vinnslu persónuupplýsinga sem hægt er að fjarlægja úr innra eftirlitskerfi?
* Hafa breytingar á lögum eða reglugerðum kallað á endurskoðun á innra eftirlitskerfinu?
* Hefur fyrirtækið frá því að fyrri endurskoðun fór fram uppgötvað nýjar leiðir sem geta bætt innra eftirlitskerfið eða þær verklagsreglur sem í gildi eru?

Þegar matið hefur farið fram verður að gera nauðsynlegar breytingar á innra eftirlitskerfinu og, ef nauðsyn krefur, tilkynna hlutaðeigandi aðilum.