

Lögmannafélag Íslands

# Leiðbeiningar fyrir lögmennt um hvernig uppfylla má kröfur nýrra laga um persónuvernd

Hörður Helgi Helgason, lögmaður

Samið að fyrirmynd norska lögmannafélagsins, *Advokatforeningens veileder om advokatvirksomhetens etterlevelse av GDPR*, eftir Thomas Olsen, Rune Opdahl, Christopher Sparre-Enger Clausen

Útgáfa 1.0, 15. júlí 2018

## Efnisyfirlit

1.	Útdráttur.....	3
2.	Almennt um ný persónuverndarlög í starfsemi lögmanna.....	4
3.	Ábyrgðarskylda .....	6
4.	Skrá yfir vinnlustarfsemi .....	9
5.	Takmörkun vegna tilgangs.....	11
6.	Vinnsluheimildir .....	12
7.	Upplýsingaréttur .....	16
8.	Réttindi hins skráða.....	18
9.	Öryggi persónuupplýsinga .....	20
10.	Vinnslusamningar.....	21
11.	Eyðing persónuupplýsinga.....	23
12.	Persónuverndarfulltrúar.....	24
13.	Mat á áhrifum á persónuvernd (MÁP) .....	25
14.	Markaðssetning .....	26
15.	Skoðun tölvupósts starfsmanna o.fl.....	27

## 1. Útdráttur

Ný lög um persónuvernd og vinnslu persónuupplýsinga tóku gildi 15. júlí 2018. Með lögnum er innleidd ný reglugerð ESB um persónuvernd. Kjarni þeirra er að mestu óbreyttur frá eldri lögum en nú liggja stjórnvaldssektir við brotum, skerpt hefur verið á efnisreglum og þeim fjölgað:

- *Persónuupplýsingar* eru upplýsingar um persónugreindan eða persónugreinanlegan einstakling sem er jafnan nefndur *hinn skráði*. *Vinnsla* persónuupplýsinga er hvers kyns aðgerð þar sem slíkar upplýsingar eru unnar, allt frá skráningu til eyðingar.
- *Meginreglur um vinnslu persónuupplýsinga*: Einungis má vinna með persónuupplýsingar með lögmætum sanngjörnum og gagnsæjum hætti; þeirra skal aflað í skýrum og málefnalegum tilgangi og ekki vinna frekar með í öðrum og ósamrýmanlegum tilgangi; gæta skal að því að þær séu ávallt nægilegar, viðeigandi og ekki umfram það sem nauðsynlegt er; að þær séu áreiðanlegar og uppfærðar eftir þörfum; að þær séu ekki varðveittar á persónugreinanlegu formi lengur en þörf krefur og að gætt sé að öryggi þeirra, sbr. 8. gr. laganna.
- *Vinnsluheimildir*: Ekki má vinna með persónuupplýsingar nema fyrir hendi sé einhver af svonefndum vinnsluheimildum, sbr. 9. gr. laganna og ef um viðkvæmar persónuupplýsingar er að ræða, einnig einhver af sérstökum skilyrðum, sbr. 11. gr.
- *Réttindi hinna skráðu*: Hinir skráðu njóta margs kyns réttinda samkvæmt lögnum, svo sem til upplýsinga um þá vinnslu sem fram fer með persónuupplýsingar þeirra, til aðgangs að þeim upplýsingum, til að fá upplýsingar um sig leiðréttar eða að þeim verði eytt, til að andmæla vinnslu og til að kvarta til Persónuverndar, sbr. III. k. laganna.
- *Skyldur ábyrgðar- og vinnsluaðila*: Þeim sem bera ábyrgð á vinnslu og þeim sem stunda hana fyrir þeirra hönd ber að fullnægja ýmiss konar skyldum, að uppfylltum nánar tilteknum skilyrðum, svo sem að gera samkomulag sameiginlegra ábyrgðaraðila eða vinnslusamninga við vinnsluaðila sbr. 23. og 24. gr. laganna, halda skrá yfir vinnslustarfsemi sína, sbr. 26. gr., framkvæma mat á áhrifum á persónuvernd og leita fyrirframsamráðs, sbr. 29. og 30. gr. og tilnefna persónuverndarfulltrúa, sbr. 35. gr.

Í leiðbeiningum þessum er leitast við að veita lögmönnum yfirlit yfir hvernig ákvæði laganna snúa að starfsemi þeirra og rekstri lögmannsstofa og praktísk ráð um hvernig uppfylla megi þær skyldur sem löggin leggja á þá sem sýsla með persónuupplýsingar.

## 2. Almennt um ný persónuverndarlög í starfsemi lögmanna

Ný lög um persónuvernd og vinnslu persónuupplýsinga, nr. 90/2018, tóku gildi 15. júlí 2018. Með lögnum eru felld úr gildi lög um persónuvernd og meðferð persónuupplýsinga nr. 77/2000 sem innleiddu ákvæði Evróputilskipunar 95/46/EB. Með hinum nýju lögum er innleidd í íslenskan rétt reglugerð ESB 2016/679 um persónuvernd sem leysti tilskipunina af hólmi. Reglugerðin er nefnd *almenna persónuverndarreglugerðin*. Hún gengur einnig undir skammstöfuninni GDPR sem stendur fyrir enska heiti hennar, General Data Protection Regulation.

Samhliða setningu laganna var samþykkt þingsályktun um að staðfesta fyrirhugaða ákvörðun sameiginlegu EES-nefndarinnar um að fella reglugerðina inn í samninginn um Evrópska efnahagssvæðið. Fyrirhugað er að taka þá ákvörðun á fundi nefndarinnar 6. júlí 2018.

Hin nýju lög innihalda að töluverðu leyti sams konar réttarreglur og hin eldri lög en þær eru nú ítarlegri og hafa verið uppfærðar, meðal annars með hliðsjón af nýrri tækni. Þá er með hinum nýju lögum gerð sú breyting að lagðar eru stjórnábyrgðarreglur við brotum gegn þeim.

Innleiðing almennu persónuverndarreglugerðarinnar hér á landi er að því leyti frábrugðin innleiðingunni í mörgum öðrum Evrópuríkjum að innleiðingarlögin innihalda að meginstefnu *útdrátt úr reglugerðinni* með öllum helstu efnisreglum hennar. Í einstökum greinum laganna er svo jafnan vísað til þeirra ákvæða reglugerðarinnar þar sem finna má nánari umfjöllun um viðkomandi efni. Áréttað er í lögnum að ákvæði reglugerðarinnar ganga framar ákvæðum þeirra. Í þessu leiðbeiningarriti er jafnan vísað til ákvæða hinna nýju laga en þar sem fjallað er ítarlega um tiltekin atriði er frekar vísað viðeigandi ákvæða í reglugerðinni heldur en í lögnum.

Öll starfsemi lögmanna sem varða persónuupplýsingar fellur undir hin nýju persónuverndarlög og almennu persónuverndarreglugerðina. Þetta á við óháð umfangi starfseminnar en eðli starfseminnar getur haft áhrif. Til dæmis má búast við að strangari kröfur verði gerðar til stærri lögmannsstofa sem sinna til dæmis sakamállum eða að sækja slysabætur heldur en til einyrkja sem fara með hagsmuni sem lúta nær einungis að lögaðilum.

### Helstu hugtök og efnislegt gildissvið

Persónuverndarlögin leggja skyldur á svonefnda *ábyrgðaraðila* og *vinnsluaðila*. Ábyrgðaraðilar eru þeir sem ákveða tilgang og aðferðir við vinnslu persónuupplýsinga en vinnsluaðilar eru þeir sem koma að vinnslunni en inna störf sín af hendi með aðferðum sem ábyrgðaraðilar mæla fyrir um. Lögmenn teljast allajafna til ábyrgðaraðila.

Með *vinnslu* er í lögnum átt við hvers kyns meðferð persónuupplýsinga, til dæmis skráningu þeirra, geymslu, sendingu eða eyðingu. Hugtakið er því afar vítt.

*Persónuupplýsingar* eru sömuleiðis víðtækt hugtak sem tekur til allra upplýsinga um persónugreindan eða persónugreinanlegan einstakling. Með því er átt við upplýsingar sem hægt er að rekja til tiltekins einstaklings, annað hvort með hjálp auðkennis, svo sem nafns, kennitölu, heimilisfangs, símanúmers, netfangs o.þ.h., eða með því að safn ópersónugreinanlegra upplýsinga um hann er nægilega ítarlegt til að hægt sé að persónugreina hann. Sem dæmi má nefna að ef fyrir liggja upplýsingar um starfsheiti, aldur, kyn og hjúskaparstöðu einstaklings og við hvaða götu hann býr væri jafnan hægt leikur að persónugreina viðkomandi og því um persónuupplýsingar að ræða. Í starfsemi lögmanna felst jafnan alls kyns umsýsla með persónuupplýsingar á borð við upplýsingar um tengiliði umbjóðenda sem eru lögaðilar eða um umbjóðendur sjálfa þegar um einstaklinga er að ræða, upplýsingar um aðra einstaklinga sem koma við sögu í máli, svo sem gagnaðila, vitni eða félagsmanna, auk upplýsinga um starfsfólk lögmanna sjálfra.

Lögin taka annars vegar til allrar vinnslu persónuupplýsinga sem er sjálfvirk og hins vegar til annarrar vinnslu ef þær upplýsingar sem unnið er með eru eða eiga að verða hluti af skrá. Öll stafræn vinnsla upplýsinga telst vera sjálfvirk í þessum skilningi, til dæmis þegar sýslað er með upplýsingar í hugbúnaðarkerfum. Þá teljast upplýsingar í pappírsgögnum vera hluti af skrá ef hægt er með einhverju móti að leita skipulega í safni slíkra gagna, til dæmis í tímaröð, eftir málsnúmeri eða í stafrófsröð.

Undan gildissviði laganna fellur vinnsla einstaklinga sem varða einungis einkahagi hans og fjölskyldu hans eða er einungis til persónulegra nota, sbr. 1. mgr. 4. gr. laganna. Þá falla upplýsingar um einstaklinga jafnan undan gildissviði laganna þegar 5 ár eru liðin frá andláti þeirra. Að auki segir í lögnum að þau gildi ekki um vinnslu sem fer fram „þegar dómstólar fara með dómsvald sitt“ eða „í tengslum við lögbundin verkefni Alþingis“. Þá taka lögin ekki til starfsemi hins opinbera á sviði refsivörslu, sbr. þó að hluti laganna mun gilda um slíka vinnslu þar til svonefnd löggæslutilskipun ESB hefur verið lögleidd hér á landi, sbr. bráðabirgðaákvæði III við lögin.

Persónuverndarlögin eru almenn lög og sérákvæði annarra laga um vinnslu ganga þeim því framár. Þá er rétt eins og í eldri lögum heimilt að víkja frá ákvæðum laganna „í þágu fjölmiðlunar, lista eða bókmennta“, sbr. nánar 6. gr. laganna. Hefur Persónuvernd jafnan túlkað þetta undantekningarákvæði fremur vítt. Umfjöllun fjölmiðla til dæmis um dómsmál myndi því oftast en ekki falla undan gildissviði laganna.

#### Trúnaðarskylda lögmanna

Lögmenn og starfsfólk þeirra bera þagnarskyldu um það sem þeim er trúað fyrir í starfi sínu, sbr. 1. mgr. 22. gr. laga nr. 77/1998 um lögmenn og t.d. 3. mgr. 35. gr. laga nr. 88/2008 um meðferð sakamála. Þessar skyldur eru ekki bundnar við persónuupplýsingar. Í persónuverndarlöggjöfinni er kveðið á um að tryggja skuli viðunandi öryggi persónuupplýsinga en í því felst meðal annars að verja þær gegn óheimilum aðgangi. Trúnaðarbrot lögmanna geta því bæði falist í brotum gegn lögum sem eiga við um lögmenn og gegn lögum um persónuvernd.

Þær skyldur sem persónuverndarlögin leggja á ábyrgðar- og vinnsluaðila eru hins vegar ekki takmarkaðar við trúnaðarskyldur. Til dæmis takmarka þær einnig hvað nýta má persónuupplýsingar í annað en það sem upphaflega stóð til að gera við þær, hve lengi má halda þeim áður en þeim skal eyða og hver réttindi hinna skráðu eru til vitneskju um vinnsluna og til aðgangs að persónuupplýsingunum. Því nægir ekki að lögmenn gæti einungis að þagnarskyldu sinni um þær persónuupplýsingar sem þeir búa yfir heldur hvíla á þeim fleiri skyldur um hvernig skuli standa að vinnslu þeirra.

#### Tilgangur þessara leiðbeininga

Í þessum leiðbeiningum er leitast við að útskýra hvernig stórar og smáar lögmennsstofur geta með sem einföldustum hætti uppfyllt kröfur hinnar nýju persónuverndarlöggjafar. Leiðbeiningarnar eru ekki tæmandi lýsing þeim kröfur sem settar eru fram í réttarreglunum. Þess í stað er ætlun höfunda að með því að fara að þeim ráðum sem leiðbeiningarnar geyma megi mynda traustan grunn sem lögmennsstofur geti svo notað til að byggja ofan á sitt starf til að verja persónuvernd þeirra sem þær búa yfir persónuupplýsingar um.

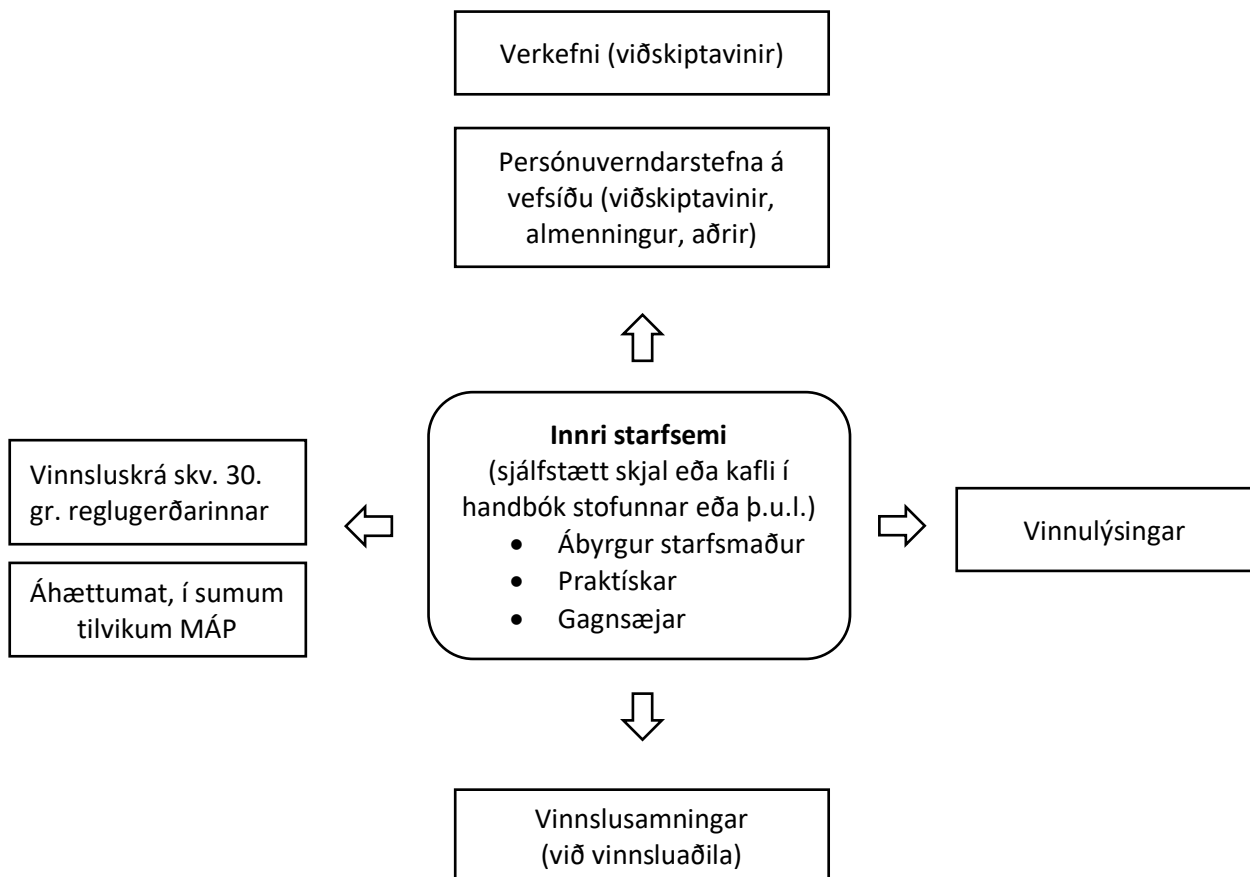
### 3. Ábyrgðarskylda

Með hinum nýju lögum er ábyrgðaraðili bæði gerður ábyrgur fyrir því að vinnsla hans á persónuupplýsingum uppfylli meginreglur um meðferð slíkra upplýsinga og fyrir því að hægt sé að sýna fram á það, sbr. 2. mgr. 8. gr. laganna. Þetta þýðir í raun að ábyrgðaraðili þarf að koma sér upp góðri, *skjalfestri og rekjanlegri yfirsýn* yfir alla starfsemi sína, meðal annars með því að semja og viðhalda skrá yfir vinnlustarfsemi í samræmi við 26. gr. og framkvæma mat á áhrifum á persónuvernd skv. 29. gr. þegar líklegt er að vinnslan geti haft í för með sér hættu fyrir réttindi og frelsi einstaklinga.

Lögin og almenna persónuverndarreglugerðin veita takmarkaða leiðsögn um hversu ítarlega skuli skjalfesta starfshætti ábyrgðaraðila. Þó er búist við að gerðar verði strangari kröfur til lögmannsstofa sem sýsla með umfangsmeiri og viðkvæmari gögn um einstaklinga en til þeirra sem aðallega fjalla um upplýsingar um lögaðila. Samkvæmt 24. gr. reglugerðarinnar skulu þær ráðstafanir sem gripið er til í því skyni að framfylgja meginreglum um persónuvernd meðal annars valdar með hliðsjón af eðli og umfangi vinnslunnar og þeirri áhættu sem hún hefur í för með sér.

Lögmannafélagið mælir með því að allar lögmannsstofur skjalfesti starfshætti sína í samræmi við hin nýju lög.

Fyrir flestar stofur væri hagræði af því að í þeim skjölum sé starfseminni skipt gróflga í tvennt, svo sem lýst er hér síðar.



Í lögnum er ekki gerð krafa um tiltekið fyrirkomulag eða skipulag á þeirri skjölun sem ábyrgðaraðilar skulu koma sér upp og viðhalda samkvæmt framangreindri ábyrgðarskyldu. Hér er sett fram, einungis til leiðbeiningar, tillaga að einu slíku fyrirkomulagi:

### Skjöl um innri starfsemi

Skipta mætti þeim hlutverkum í þrennt sem þarf að gegna á lögmannsstofum til að uppfylla kröfur laganna:

- Ábyrgð

Lögmannsstofa ætti að tilnefna þann sem ber ábyrgð á persónuvernd. Slík ábyrgð ætti jafnan að fara saman við ábyrgð á rekstrinum og því að vera hjá t.d. stjórn eða framkvæmdastjóra.

- Rekstur

Einhverjum starfsmanni stofunnar ætti að fela daglega umsjón þeirra mála sem snúa að persónuvernd, t.d.

- samráð fyrir starfsfólk áður en ráðist er í breytingar á vinnslu persónuupplýsinga;
- gerð vinnulýsingar um meðferð upplýsinga um viðskiptavina og um starfsmenn;
- viðmið um hvenær samstarfsaðilar teljist vinnsluaðilar og hvenær sameiginlegir ábyrgðaraðilar;
- áhættumat á vinnsluaðilum;
- setning verklagsreglna um hvernig gætt sé að réttindum hinna skráðu, svo sem upplýsinga- og aðgangsrétt, leiðréttingu og eyðingu;
- setning reglna um meðferð tölvupósts og rafræna vöktun, sbr. kafla 14 hér síðar; og
- gerð vinnulýsingar um eyðingu gagna.

- Eftirlit

Í rekstrinum ætti að vera stundað innra eftirlit með starfseminni, þar á meðal um:

- Meðferð frávika frá verklagsreglum um starfsemina og
- árlega yfirferð yfir og uppfærslu á verklagsreglum og vinnulýsingum um persónuvernd.

### Ytri skjöl

Auk innra verklags þurfa lögmannsstofur að viðhalda ýmsum skjölum varðandi persónuvernd sem snúa út á við, sbr. einkum:

- Auðskiljanleg persónuverndarstefna, þar sem koma mætti m.a. á framfæri eitthvað af þeim upplýsingum sem ber að veita hinum skráðu samkvæmt upplýsingarétti þeirra, sbr. kafla 6 hér síðar.

- Lýsing á því hvernig hinir skráðu geta nýtt sér aðgangsrétt sinn og jafnvel eyðublað fyrir þá sem vilja nýta sér þann rétt.
- Sniðmát að vinnslusamningum við vinnsluaðila og að samkomulagi milli sameiginlegra ábyrgðaraðila.



#### 4. Skrá yfir vinnlustarfsemi

##### Tilgangur skrárinnar

Fyrsta skrefið í átt að því að uppfylla kröfur persónuverndarlaganna er að gera *skrá yfir vinnlustarfsemi*, einnig nefnd *vinnsluskrá*. Tilgangurinn er þrjúþættur:

- 1) Vinnsluskráin veitir ábyrgðaraðilanum yfirsýn yfir þá vinnslu persónuupplýsinga sem hann hefur með höndum, leiðir í ljós hvaða hlutar starfseminnar samrýmast ekki lögnum og gerir kleift að taka upplýstar ákvarðanir um hvernig megi lagfæra það með sem viðurhlutaminnstum hætti. Með „vinnlustarfsemi“ er ekki átt við að skráð sé niður hvert handtak sem unnið er, heldur þess í stað þau helstu verkefni eða viðfangsefni sem unnið er að, t.d. samningagerð við viðskiptavinum, rekstur einstakra tegunda mála, löginheimta, ráðning starfsmanna og útreikningur launa.
- 2) Vinnsluskráin er það skjal sem viðbúið er að Persónuvernd muni óska eftir aðgangi að, telji hún tilefni til að ganga úr skugga um að farið sé að lögnum, svo sem í reglubundnu eftirliti sínu eða ef upp koma kvartanir.
- 3) Mörg fyrirtæki nýta vinnsluskrárnar til að halda utan um fleiri upplýsingar um starfsemi sína en þær sem gerð er krafa um í 26. gr. laganna. Þannig getur vinnsluskráin stutt við gæðakerfi og upplýsingaöryggiskerfi fyrirtækisins og auðveldað stjórnendum og eigendum að taka ákvarðanir um breytingar í rekstrinum.

##### Gerð vinnsluskrárinnar

Hægt er að standa að gerð skrár yfir vinnlustarfsemi á nokkra mismunandi vegu. Fyrir marga er einfaldast að setja upp töflu í töflureikni eða ritvinnsluforriti og skýra dálkana í samræmi við þau efnisatriði sem tiltekin eru í 30. gr. reglugerðarinnar.

Til þess að vinnsluskráin endurspegli sem réttast þá starfsemi sem fram fer á lögmannsstofunni er nauðsynlegt að þeir sem þekkja gleggst til hvers hluta af starfseminni fyrir sig séu kallaðir til við skrásetninguna. Oft er einfaldast og fljótlegast að afla upplýsinga í skrána á stuttum vinnufundum þar sem þeir sem næst standa viðkomandi hluta starfseminnar eru spurðir hvernig hann fari fram og svörin eru jafnóðum skráð í vinnsluskránnu. Bestur árangur fæst ef einhver sem þekkir vel til laganna leiðir fundina/viðtölin.

Gerð vinnsluskrár þarf að ná til allra þeirra þátta sem tilteknir eru í 1. mgr. 30. gr. reglugerðarinnar:

- a) Nafn og tengiliðaupplýsingar lögmannsstofunnar og persónuverndarfulltrúa, ef stofan hefur slíkan fulltrúa.
- b) Lýsing á tilgangi hvernar vinnslu fyrir sig (t.d. verja hagsmuni umbjóðanda, afla hæfs starfsfólks eða tryggja rétta launaafgreiðslu).
- c) Tegundir persónuupplýsinga sem hver vinnsla tekur til (t.d. heilbrigðisupplýsingar, tengiliðaupplýsingar eða starfsmannaupplýsingar) og flokkar þeirra einstaklinga sem þær eiga við um (t.d. viðskiptavinir, vitni eða starfsfólk).
- d) Hvert afurðum vinnslunnar er miðlað (t.d. kröfulýsing í þrotabú er send skiptastjóra, greinargerð og skjöl í eru lögð fram í héraðsdómi eða færslulisti er sendur til banka að greiða út laun).

- e) Hvort upplýsingum í vinnslunni sé miðlað út fyrir EES og á grundvelli hvaða heimildar.
- f) Hvað verður um þær persónuupplýsingar sem vinnslan tekur til, þ.á m. hvort og hvenær þeim verður eytt (t.d. málum er pakkað og vistuð í skjalageymslu í 10 ár en eytt að því loknu eða tilteknum upplýsingum um fyrrverandi starfsmenn er eytt ári eftir starfslok en aðrar upplýsingar geymdar til staðfestingar á vinnusambandi).
- g) Öryggisráðstafanir sem beitt er í vinnslunni til að verja viðkomandi persónuupplýsingar, sbr. reglur nr. 299/2001.

Þá er afar æskilegt að skrá í vinnsluskrána eftirtaldar upplýsingar:

- *Tilgreining* á hverri vinnslu, svo sem það heiti sem viðkomandi starfsmenn nota til að vísa til hennar (t.d. eignakönnun, starfsmannaviðtal eða ágrípsgerð)
- *Lýsing* á því sem felst í hverri vinnslu, þ.e. hver sé kjarni hennar (t.d. upplýsingar A móttækna frá B, samkeyrðar við upplýsingar frá C og sendar til móttakendanna D og E).
- Sú heimild, þ.e. svonefnd *vinnsluheimild*, sem er fyrir að stunda viðkomandi vinnslu (t.d. upplýst samþykki, nauðsyn vegna samnings við hinn skráða, lagaskylda eða lögmætir hagsmunir lögmannsstofunnar).
- *Nafn þess sem ber ábyrgð* innan stofunnar á viðkomandi vinnslu.
- *Upplýsingakerfi* sem notuð eru til að stunda viðkomandi vinnslu persónuupplýsingar (t.d. Microsoft Word, Sharepoint, GoPro, Navision eða tölvupóstur).

Loks getur verið hjálplegt að vinnsluskráin innihaldi einnig eftirtaldar upplýsingar:

- Hvort vinnsluaðila hafi verið falið að sjá um hluta af vinnslunni og ef svo er að vísa til vinnslusamnings við hann.
- Hvort áhættumat hafi farið fram á vinnslunni og, ef niðurstaða þess hafi verið að líkur séu á að friðhelgi einkalífs hinna skráðu sé stefnt í hættu, hvort mat á áhrifum á persónuvernd (MÁP) hafi farið fram.
- Hvort til séu nánari verklagsreglur um framkvæmd vinnslunnar.

Almenn skyldu ábyrgðaraðila til að gera vinnsluskrá á ekki við um fyrirtæki sem hjá starfa færri en 250 starfsmenn, sbr. 2. mgr. 26. gr. laganna. Í því ljósi mætti spyrja hvers vegna íslenskar lögmannsstofur ættu að semja sér vinnsluskrár? Því er til að svara að 250 starfsmanna undantekningin á ekki við ef viðkomandi vinnsla persónuupplýsinga:

- er líkleg til að leiða af sér áhættu fyrir réttindi og frelsi skráðra einstaklinga,
- er ekki tilfallandi eða
- tekur til viðkvæmra persónuupplýsinga eða persónuupplýsinga er varða sakfellingar í refsímálum.

Þar sem vinnsla persónuupplýsinga hjá lögmannsstofum er jafnan ekki tilfallandi má telja víst að 250 starfsmanna undantekningin eigi þegar af þeirri ástæðu ekki við um þá starfsemi.

## 5. Takmörkun vegna tilgangs

Ein af meginreglum um vinnslu persónuupplýsingar er að slíkar upplýsingar skuli einungis fengnar í *skýrt tilgreindum, lögmætum og málefnalegum tilgangi*, sbr. 2. tl. 1. mgr. 8. gr. laganna. Tilgang hverrar vinnslu skal getið í umfjöllun um hana í vinnsluskrá og skal tilkynnt hinum skráða þegar honum er veittur upplýsingaréttur samkvæmt 2. mgr. 17. gr. laganna.

Tilgangur vinnslu persónuupplýsinga hjá lögmannsstofum getur til dæmis verið:

- Að verja hagsmuni umbjóðanda.
- Gæðaeftirlit með störfum lögmannna og starfsmanna.
- Öflun og viðhald þekkingar (t.d. söfnun og rýni fordæma úr úrskurðum og dómum)
- Uppfylla kröfur viðskiptavina.
- Að fá hæft starfsfólk til starfa.
- Tryggja rétta launaafgreiðslu.
- Kortlagning hagsmuna aðila í dómsmálum.
- Markaðssetning stofunnar.
- Tryggja jöfn launakjör starfsfólks.
- Eftirlit með réttum tímaskráningum og reikningagerð.
- Gæta að upplýsingaöryggi.

Þessi listi er einungis settur fram í dæmaskyni og er ekki ætlað að vera notaður sem forskrift. Það er afar mikilvægt að lögmennt *greini sjálfir tilganginn* með hverri vinnslu persónuupplýsinga sem þeir bera ábyrgð á og tryggi þar með rétta skráningu vinnslustarfsemi sinnar. Ábyrgðaraðili skal enda ávallt geta sýnt fram á að vinnsla hans uppfylli meginreglurnar um vinnslu persónuupplýsinga, sbr. 2. mgr. 8. gr. laganna.

Persónuupplýsinga sem aflað hefur verið í tilteknum tilgangi *má ekki nota í öðrum og óskyldum tilgangi* nema til slíks standi sérstök vinnsluheimild. Í því sambandi má vísa til norsks dóms, Rt. 2013, bls. 143. Málið laut að einkabílstjóra sem hafði verið sagt upp störfum vegna misræmis milli tímaskráninga hans og gagna í ökurita þeirrar bifreiðar sem hann ók. Yfirlýstur tilgangur með vinnslu upplýsinga úr ökuritanum var flotastýring. Dæmt var að það væri ósamrýmanlegt hinum upphaflega tilgangi að nota upplýsingar úr ökuritanum til rafrænnar vöktunar, enda hafði starfsfólki ekki verið tilkynnt fyrirfram um að upplýsingarnar kynnu að verða notaðar í hinum síðarnefnda tilgangi.

## 6. Vinnsluheimildir

### Inngangur

Ekki má vinna með persónuupplýsinga nema fyrir slíkri vinnslu sé heimild, svonefnd *vinnsluheimild*. Reglur nýju laganna um vinnsluheimildir eru að stórum hluta óbreyttar frá eldri lögum.

Hinar almennu vinnsluheimildir eru taldar upp í 9. gr. laganna. Einhver þeirra verður ávallt að vera til staðar meðan á vinnslu stendur og allt frá því áður en vinnsla hefst. Þegar unnið er með svonefndar „viðkvæmar“ persónuupplýsingar þarf að auki að uppfylla eitthvert af sérstöku skilyrðunum sem talin eru upp í 11. gr. laganna.

Lögmenn teljast jafnan vera ábyrgðaraðilar fyrir allri vinnslu persónuupplýsingar sem þeir standa að og það er því skýlaus skylda þeirra að tryggja að engin slík vinnsla fari fram nema áður liggi fyrir vinnsluheimild. Í þeim undantekningartilvikum þar sem lögmenn vinna með persónuupplýsingar sem vinnsluáðilar, samkvæmt leiðbeiningum frá óskyldum ábyrgðaraðila í vinnslusamningi þeirra, þá sækir sá lögmaður heimild sína til að vinna með upplýsingarnar til vinnsluheimildar ábyrgðaraðilans og þess vinnslusamnings sem þeir gera með sér.

### Lögmætisgrundvöllur fyrir vinnslu lögmanna á persónuupplýsingum

Í töflunni hér fyrir neðan er að finna yfirlit yfir þær vinnsluheimildir sem jafnan koma helst til greina vegna nokkurra af algengari tegundum af vinnslu persónuupplýsinga sem lögmenn hafa með höndum:

<b>Tegund vinnslu</b>	<b>Almenn vinnsluheimild</b>	<b>Sérstök viðbótarvinnsluheimild fyrir viðkvæmar persónuupplýsingar</b>
Stofnun viðskiptasambands	1. tl. 9. gr. laganna (samþykki hins skráða)  2. tl. 9. gr. laganna (nauðsynleg til að efna samning við hinn skráða)  3. tl. 9. gr. laganna (lagaskylda sem hvílir á lögmanni, t.d. f-liður 1. mgr. 2. gr. sbr. 5., 6. og 17. gr. l. nr. 64/2006 um peningabætti)	1. tl. 1. mgr. 11. gr. laganna (afdráttarlaust samþykki hins skráða)  6. tl. 1. mgr. 11. gr. laganna (nauðsynleg til að unnt sé að stofna, hafa uppi eða verja réttarkröfur)
Meðferð mála fyrir dómi	6. tl. 9. gr. laganna (lögmætir hagsmunir sem gangi frammar hagsmunum hins skráða)  2. tl. 9. gr. laganna (nauðsynleg til að efna samning við hinn skráða)  1. tl. 9. gr. laganna (samþykki hins skráða)	1. tl. 1. mgr. 11. gr. laganna (afdráttarlaust samþykki hins skráða)  5. tl. 1. mgr. 11. gr. laganna (upplýsingar sem hinn skráði hefur augsljóslega sjálfur gert opinberar)  6. tl. 1. mgr. 11. gr. laganna (nauðsynleg til að unnt sé að stofna, hafa uppi eða verja réttarkröfur)
Seminar innan stofu, farið yfir nýleg mál / mál í vinnslu	5. tl. 9. gr. laganna (lögmætir hagsmunir sem gangi frammar hagsmunum hins skráða)	1. tl. 1. mgr. 11. gr. laganna (afdráttarlaust samþykki hins skráða)  5. tl. 1. mgr. 11. gr. laganna

Tegund vinnslu	Almenn vinnsluheimild	Sérstök viðbótarvinnsluheimild fyrir viðkvæmar persónuupplýsingar
		(upplýsingar sem hinn skráði hefur augsljóslega sjálfur gert opinberar)
Skjalavistun, t.d. varðveisla gagna úr dómsmálum eða skjala úr búum sem ekki voru lögð fram í dómi	<p>2. tl. 9. gr. laganna (nauðsynleg til að efna samning við hinn skráða)</p> <p>6. tl. 9. gr. laganna (lögmætir hagsmunir sem gangi frammar hagsmunum hins skráða)</p> <p>3. tl. 9. gr. laganna (lagaskylda sem hvílir á lögmanni, t.d. 5. mgr. 14. gr. laga nr. 77/2014 um opinber skjalasöfn)</p>	<p>1. tl. 1. mgr. 11. gr. laganna (afdráttarlaust samþykki hins skráða)</p> <p>5. tl. 1. mgr. 11. gr. laganna (upplýsingar sem hinn skráði hefur augsljóslega sjálfur gert opinberar)</p> <p>6. tl. 1. mgr. 11. gr. laganna (nauðsynleg til að unnt sé að stofna, hafa uppi eða verja réttarkröfur)</p> <p>11. tl. 1. mgr. 11. gr. laganna (nauðsyn vegna skjalavistunar í þágu alm.hagsm. og á grundvelli laga)</p>
Vinnslur vegna viðskiptasambands	<p>2. tl. 9. gr. laganna (nauðsynleg til að efna samning við hinn skráða)</p> <p>6. tl. 9. gr. laganna (lögmætir hagsmunir sem gangi frammar hagsmunum hins skráða)</p>	6. tl. 1. mgr. 11. gr. laganna (nauðsynleg til að unnt sé að stofna, hafa uppi eða verja réttarkröfur)
Markaðssetning	<p>1. tl. 9. gr. laganna (samþykki hins skráða)</p> <p>6. tl. 9. gr. laganna (lögmætir hagsmunir sem gangi frammar hagsmunum hins skráða)</p>	
Vinnslur varðandi starfsmannahald	<p>2. tl. 9. gr. laganna (nauðsynleg til að efna samning við hinn skráða)</p> <p>3. tl. 9. gr. laganna (lagaskylda sem hvílir á lögmanni sem vinnuveitanda, sbr. t.d. lög um orlof, um lífeyrissjóði, um tekjuskatt, jafnréttislög o.fl.)</p> <p>6. tl. 9. gr. laganna (lögmætir hagsmunir sem gangi frammar hagsmunum hins skráða)</p> <p>1. tl. 9. gr. laganna (samþykki hins skráða, en það á sjaldan við þar sem samþykki starfsmanna til vinnuveitenda telst jafnan ekki „gefið af fúsum og frjálsum vilja“, sem er áskilið)</p>	2. tl. 1. mgr. 11. gr. laganna (vinnulöggjöf, almannatryggingar og félagsleg vernd)

Tegund vinnslu	Almenn vinnsluheimild	Sérstök viðbótarvinnsluheimild fyrir viðkvæmar persónuupplýsingar
Reikningagerð og innheimta	2. tl. 9. gr. laganna (nauðsynleg til að efna samning við hinn skráða)  3. tl. 9. gr. laganna (lagaskylda sem hvílir á lögmanni sem vinnuveitanda, t.d. lög um bókhald)  6. tl. 9. gr. laganna (lögmætir hagsmunir sem gangi framur hagsmunum hins skráða)	6. tl. 1. mgr. 11. gr. laganna (nauðsynleg til að unnt sé að stofna, hafa uppi eða verja réttarkröfur)
Aðgerðir til að tryggja öryggi persónuupplýsinga	3. tl. 9. gr. laganna (lagaskylda, t.d. 27. gr. laganna um persónuvernd og reglur nr. 299/2001)  6. tl. 9. gr. laganna (lögmætir hagsmunir sem gangi framur hagsmunum hins skráða)	6. tl. 1. mgr. 11. gr. laganna (nauðsynleg til að unnt sé að stofna, hafa uppi eða verja réttarkröfur)

Svo sem fram kemur í töflunni hér að ofan kunna fleiri en ein vinnsluheimild að koma til skoðunar þegar fundin er stoð fyrir lögmæti vinnslu persónuupplýsinga. Hins vegar leggur Persónuvernd á það áherslu að í stað þess að byggja á fleiri en einni vinnsluheimild þurfi ábyrgðaraðili að ákvarða hvaða vinnsluheimild sé rétt að byggja á varðandi sérhverja vinnslu, sbr. *Leiðbeiningar um samþykki*, 1. útg. 2018, bls. 10-11.

Hér fyrir neðan er að finna nokkrar ábendingar varðandi algengustu vinnsluheimildir persónuupplýsinga:

- *Samþykki* (1. tl. 9. gr. laganna) hentar ekki vel sem vinnsluheimild í hefðbundinni starfsemi lögmanna. Kröfur laganna, svo sem um að afla þurfi samþykkis beint frá sérhverjum hinna skráðra fyrir sig og að það kunni að verða afturkallað fyrirvaralaust, geta farið illa saman við þá starfsemi að veita lögmannsþjónustu.
- *Nauðsyn vegna samnings* (2. tl. 9. gr. laganna) á að jafnaði oftast við sem vinnsluheimild. Sé ætlunin að byggja lögmæti vinnslu á slíkri heimild er hins vegar mikilvægt að lýsa í þeim samningi eins skýrt og snöfurmannalega og frekast er unnt hinni fyrirhuguðu vinnslu og hvað fyrirhugað er að gera við þær upplýsingar sem hún tekur til. Þá verður að gæta sín á að blanda ekki öðrum og óskyldum persónuupplýsingum eða tilgangi inn í þá vinnslu.
- Sé lögmæti vinnslu byggt á að fyrir liggi *lagaskylda* (3. tl. 9. gr. laganna) þá þarf slíkt lagaákvæði jafnan að gera skýrlega grein fyrir hinni fyrirhuguðu vinnslu persónuupplýsinga sem hún veitir stoð.
- Þær vinnsluheimildir sem felst í nauðsyn til að *vernda brýna hagsmuni einstaklinga* (4. tl. 9. gr. laganna) og nauðsyn vegna verks sem er unnið í *almannaþágu eða vegna beiting opinbers valds* (5. tl. 9. gr. laganna) eru túlkaðar með þröngum hætti og eiga sjaldan við um starfsemi lögmanna.
- Loks kann í sumum tilvikum að vera hægt að sækja almenna vinnsluheimild í *lögmæta hagsmuni lögmannsstofunnar* sem gangi framur einkalífshagsmunum hins skráða (6. tl. 9. gr.

laganna). Algengt dæmi eru öryggismyndavélar í húsnæði stofunnar. Úr slíkum kerfum þarf hins vegar að eyða efni reglulega, gæta að öryggi o.s.frv.

- Hvað varðar sérstöku skilyrðin, fyrir vinnslu viðkvæmra persónuupplýsinga hjá lögmannsstofum, þá væri vinnsluheimildina oft að finna í nauðsyn til að unnt sé að *stofna, hafa uppi eða verja réttarkröfur* (6. tl. 1. mgr. 11. gr. laganna).

#### Vinnsla persónuupplýsinga um refsiverða háttsemi

Í lögnum er fjallað sérstaklega um meðferð upplýsinga sem lúta að refiverðri háttsemi, sbr. 12. gr. þeirra.

Stjórnvöld mega vinna með slíkar upplýsingar ef það er nauðsynlegt í þágu lögbundinna verkefna þeirra, sbr. 1. mgr. Telja má víst að þetta ákvæði taki til starfsemi saksóknara, að svo miklu sem slík starfsemi fellur undir lögin, sbr. 6. mgr. 4. gr. sem undanskilur meðal annars saksókn fyrir refsiverð brot frá efnislegu gildissviði laganna.

Þá er í 3. mgr. 12. gr. laganna áskilið að til þess að einkaaðilar megi vinna með upplýsingar um refsiverða háttsemi þurfi annað hvort hinn skráði að veita sjálfur sitt afdráttarlaust samþykki fyrir vinnslunni eða vinnslan verði talin nauðsynleg í þágu lögmætra hagsmuna sem auðsjáanlega vega þyngra en grundvallarréttindi og frelsi hins skráða.

## 7. Upplýsingaréttur

### Almennt

*Gagnsæi* er ein af meingreglum um vinnslu persónuupplýsinga, sbr. 1. tl. 1. mgr. 8. gr. og 1. mgr. 17. gr. laganna. Krafa endurspeglast einnig í svonefndum *upplýsingarétti hinna skráðu*. Samkvæmt upplýsingaréttinum á hinn skráði rétt á upplýsingum um vinnslu, hvort sem persónuupplýsinga er aflað hjá honum sjálfum eða annars staðar frá, eða hann óskar eftir þeim að eigin frumkvæði, sbr. 2. mgr. 17. gr.

Návar er fjallað í 13. gr. almennu persónuverndarreglugerðarinnar um þær upplýsingar sem ber að veita hinum skráða um fyrirhugaða vinnslu þegar persónuupplýsinganna er aflað beint frá honum sjálfum (t.d. þegar hann leitar beint til lögmanns eftir þjónustu) en í 14. gr. er fjallað um hvernig upplýsingarétturinn horfir við þegar persónuupplýsinga er aflað annars staðar frá (t.d. uppfletting skuldara í vanskilaskrá). Þá er að finna nokkrar almennar reglur í 12. gr. reglugerðarinnar um með hvaða hætti skuli reiða fram upplýsingar til hins skráða. Loks eru í 4. mgr. 17. gr. laganna tilgreind tilvik þar sem heimilt er að víkja frá upplýsingarétti hins skráða (m.a. til verndar grundvallarréttindum annarra einstaklinga, til þess að fullnægja einkaréttarlegum kröfum eða vegna lagaákvæða um þagnarskyldu).

### Hvaða upplýsingar ber að veita og hverjum?

Upplýsingar um vinnsluna skal veita hinum skráða óumbeðnar. Í því felst að honum skal annað hvort sendar eða birtar upplýsingarnar eða honum skal vísað á hvar þær megi greiðlega finna. Upplýsingarnar má veita hvort sem er bréflega eða í rafrænu formi.

Lögmannsstofur geta veitt starfsfólki sínu umræddar upplýsingar á Netinu, í starfsmannahandbók, útprentaðar eða með öðrum skýrum hætti sem notaður er venjulega innan stofunnar til að koma upplýsingum til starfsmanna.

Þegar upplýsingum er komið til umbjóðenda sem eru einstaklingar þá mætti til dæmis gera það í meginmáli eða viðauka við samning um þjónustuna eða að þar sé vísað til upplýsinga á vefsíðu lögmannsstofunnar.

Í sumum tilvikum getur verið sérstaklega erfitt fyrir lögmannsstofu að koma við beinum tilkynningum til hinna skráðu um fyrirhugaða vinnslu persónuupplýsinga um þá. Þegar persónuupplýsinga um hinn skráða er aflað frá öðrum en honum sjálfum (t.d. með því að fletta honum upp í opinberum skrá) og ekki er unnt að veita hinum skráða upplýsingar um vinnsluna eða slíkt kostar óhóflega fyrirhöfn þá kann að vera að vinnslan sé undanþegin upplýsingarétti, sbr. b)-lið 5. mgr. 14. gr. reglugerðarinnar. Í þeim tilvikum væri þó í það minnsta rétt að sem gagnsæjastar upplýsingar um vinnsluna væri að finna á vefsetri stofunnar.

Loks má nefna að í þeim tilvikum sem lögmennt bera þagnarskyldu um persónuupplýsingar, sbr. 1. mgr. 22. gr. laga nr. 77/1998 um lögmennt, sbr. kafla 1 hér að framan, þá á upplýsingaréttur hins skráða samkvæmt 14. gr. persónuverndarlaga ekki við.

Í stuttu máli er mælt með að lögmennt noti þessar leiðir til að veita öðrum en starfsmönnum sínum upplýsingar um vinnslu sína á persónuupplýsingum:

- Í auðskiljanlegri persónuverndarstefnu á *vefsíðu* lögmannsstofu sinnar eða útprentaða í *afgreiðslu* stofunnar.



- Í *samningum* sem gerðir er við viðskiptavini um lögfræðiþjónustuna.

#### Hvaða upplýsingar á að veita?

Upplýsingaréttur hins skráða tekur einkum til eftirtaldrá upplýsinga:

- Heiti/nafn og tengiliðaupplýsingar lögmansstofunnar og persónuverndarfulltrúa, ef stofan hefur slíkan fulltrúa.
- Tilgangur og vinnsluheimild hinnar fyrirhuguðu vinnslu.
- Tegundir persónuupplýsinga sem vinnslan tekur til.
- Hvort og hvert upplýsingunum verði miðlað.
- Hversu lengi persónuupplýsingarnar verði vistaðar.
- Hver séu réttindi hinna skráðu (þ.e. réttur til aðgangs, leiðréttingar, eyðingar, takmörkunar vinnslu og andmæla, auk réttar til að kvarta til Persónuverndar).

Æskilegt er að láta fylgja hvenær upplýsingatextinn hafi verið birtur eða síðast uppfærður og hverju hafi verið breytt.

#### Hvernig á að veita upplýsingarnar?

Þegar hinum skráða eru veittar upplýsingar um vinnsluna skal gera það á „gagnorðu, gagnsæju, skiljanlegu og aðgengilegu formi og skýru og einföldu máli“, sbr. 12. gr. reglugerðarinnar. Það er því mikilvægt, ekki síst fyrir lögmenn, þegar saminn er slíkur upplýsingatexti um vinnslu persónuupplýsinga, að gætt sé að því að hann verði ekki á flóknu lögfræðimáli eða að öðru leyti torskilinn.

## 8. Réttindi hins skráða

Í III. kafla laganna er að finna kröfur sem lúta að ýmiss konar réttindum hinna skráðu. Mörg þessara réttinda voru þegar lögfest í eldri lögum um persónuvernd og meðferð persónuupplýsinga en sum eru ný. Nánar er svo fjallað í reglugerðinni um hver þessara réttinda fyrir sig.

Það er einkum ábyrgðaraðila vinnslunnar að uppfylla þessar kröfur en oft þarf hann aðstoð vinnsluaðila til að geta gert það. Af þeim sökum er mælt fyrir um það, í e-lið 3. mgr. 28. gr. reglugerðarinnar, að í samningum ábyrgðar- og vinnsluaðila, þ.e. svonefndum vinnslusamningum, sé áréttuð skylda vinnsluaðila til að aðstoða ábyrgðaraðila við að mæta þessum kröfum.

Hér er að finna yfirlit yfir þau réttindi hins skráða sem telja má mikilvægast að lögmannsstofur viti af og sjái til þess að hinn skráði geti notið:

### Upplýsingaréttur (13. og 14. gr. reglugerðarinnar)

Hinn skráði á rétt til upplýsinga frá ábyrgðaraðila um vinnslu persónuupplýsinga sinna. Um þennan upplýsingarétt er fjallað í kafla 6 hér að framan.

### Aðgangsréttur (15. gr. reglugerðarinnar)

Svonefndur aðgangsréttur hins skráða, sem lýst er í 15. gr. reglugerðarinnar, er tvíþættur.

Annars vegar á hinn skráði, þegar hann óskar eftir því frá ábyrgðaraðila, rétt á að fá *upplýsingar um vinnsluna*, þ.e. hvort og þá hvernig sé unnið með persónuupplýsingar hans af hálfu ábyrgðaraðilans. Þessi réttur er sambærilegur við upplýsingarétt hins skráða sem lýst er hér að framan.

Hins vegar á hinn skráði rétt á því, ef hann óskar eftir, að fá *aðgang að persónuupplýsingum* sem unnið er með um hann. Ef beiðnin er lögð fram rafrænt skulu upplýsingarnar afhentar á rafrænu formi.

Víkja má frá upplýsinga- og aðgangsrétti hins skráða í ákveðum tilvikum, sbr. 4. mgr. 17. gr. laganna, þ.e. vegna:

- þjóðaröryggis, landvarna eða almannaoöryggis;
- starfsemi hins opinbera á sviði refsivörslu og til að koma í veg fyrir ógnir við almannaoöryggi;
- almannahagsmuna (t.d. vegna gjaldeyrismála, fjárlaga og skattamála, lýðheilsu og almannatrygginga);
- verndar skráðs einstaklings eða grundvallarréttinda annarra;
- tillits til þess að einkaréttarlegum kröfum verði fullnægt; auk
- lagaákvæða um þagnarskyldu.

Allar þessar undanþágur kunna að koma við sögu í starfi málflytjenda, sbr. t.d. þagnarskylda ákæranda skv. 4. mgr. 18. gr. laga nr. 88/2008 um meðferð sakamála. Eins og sjá má af upptalningunni eru það þó einkum seinni þrjár undanþágurnar sem eiga við um lögmennt og vinnslu þeirra á persónuupplýsingum. Einkum eiga hér við fyrrnefnd lagaákvæði um þagnarskyldur lögmannna, sbr. kafla 1. Í raun leiðir hún til þess að lögmanni er jafnan hvorki heimilt að veita öðrum en umbjóðanda sjálfum upplýsingar um né aðgang að persónuupplýsingum sem lögmanninum hefur

verið trúað fyrir. Lögmenn þurfa því einkum að huga að upplýsinga- og aðgangsréttinum gagnvart umbjóðendum og starfsmönnum sínum, núverandi og fyrrverandi.

Réttur til leiðréttinga (16. gr. reglugerðarinnar)

Hinn skráði á rétt á því, ef hann óskar eftir, að rangar eða villandi persónuupplýsingar um sig verði leiðréttar eða uppfærðar.

Réttur til eyðingar (17. gr. reglugerðarinnar)

Hinn skráði á að auki rétt á því, með ákveðnum undantekningum, að persónuupplýsingum um hann verði eytt, sbr. nánar kafla 10 hér síðar.

## 9. Öryggi persónuupplýsinga

Bæði lögmenn og vinnsluaðilar þeirra skulu gera ráðstafanir til að tryggja viðunandi öryggi persónuupplýsinga, sbr. 27. gr. laganna. Í gildi eru reglur nr. 299/2001 um öryggi persónuupplýsinga, sbr. bráðabirgðaákvæði II við lögina, þar sem nánar er mælt fyrir um hvernig skuli bera sig að við að tryggja öryggi persónuupplýsinga.

Lögmenn nota í miklum mæli alls kyns tölvubúnað og rafrænan samskiptabúnað í störfum sínum og samskiptum við dómstóla, yfirvöld og umbjóðendur. Þessi búnaður hefur í för með sér margvíslegar hættur fyrir öryggi þeirra persónuupplýsinga sem lögmenn sýsla með. Því er brýnt að lögmenn fari skipulega yfir starfsemi sína og greini heildstætt, í samræmi við framangreindar reglur, hvaða öryggiráðstafanir sé rétt að grípa til í vinnslunni.

Af þeim öryggisráðstöfunum sem nýta má til að stuðla að öruggum samskiptum má meðal annars nefna þessi örfáu dæmi:

- Þegar hefðbundinn tölvupóstur er sendur ætti að hafa í huga að efni hans nýtur gjarnan svipaðrar leyndar og það sem sent er á póstkorti. Slík samskipti með viðkvæmar persónuupplýsingar ætti því jafnan að *dulkóða með einhverju móti*. Hægt er að nota virkni sem er innbyggð í algeng tölvupóstforrit, til dæmis Microsoft Outlook, til að dulkóða tölvupóstsamskipti en slíkt getur verið flókið í framkvæmd. Þá eru til þjónustur upplýsingatæknifyrirtækja, til dæmis hÉrlendra, sem gera til dæmis lögmönnum kleift að leggja skrár, svo sem ritvinnsluskrár eða pdf-skrár, inn á læst vefsvæði og senda viðtakendum einungis hlekk á þau. Þjónustuna má einnig nota til að taka á móti skjölum. Til þess að sækja skjölin skrá móttakendur sig inn með rafrænum skilríkjum eða annarri öruggri auðkenningu. Þá veita mörg ritvinnsluforrit og hugbúnaður til að búa til pdf-skrár möguleika á læsa skránum með lykilorði. Skrárnar má svo senda sem viðhengi í tölvupósti og lykilorðið með smáskilaboðum (SMS).
- Binda aðgang að upplýsingakerfum lögmennsstofunnar við vélar sem eru *aðgangsstýrðar* og eftirlit haft með hvaða hugbúnaður sé á þeim. Ef leyft er að hafa samband við upplýsingakerfin úr tölvum annars staðar frá en innan úr stofunni þá sé hann einungis um svonefndar VPN-tengingar eða eftir öðrum slíkum fyrirfram skilgreindum, *dulkóðuðum samskiptaleiðum*.
- Ef aðgangur er veittur úr snjallsímum eða spjalddölvum inn í upplýsingakerfi stofunnar, t.d. tölvupóstkerfi, sé slíkt einungis heimilað ef viðkomandi *snjalltæki er læst* t.d. með talnarunu og læsist sjálft eftir að hafa ekki verið notað í skamman tíma.
- Farið sé reglulega yfir öryggisráðstafanir og þær sem reynast úreltar verði annað hvort *uppfærðar eða skipt út* fyrir aðrar vænlegri.

Þá er mikilvægt að lögmenn haldi skjalfest yfirlit, í samræmi við ábyrgðarskyldu laganna, yfir allar upplýsingaöryggisráðstafanir.

Ef upp kemur öryggisbrot, eða öryggisbrestur, þá ber ábyrgðaraðila að tilkynna Persónuvernd um slíkt brot innan einungis 72 klst. frá því að þeirra verður vart, sbr. 2. mgr. 27. gr. laganna. Þá ber ábyrgðaraðila einnig að tilkynna hinum skráðu um öryggisbrotið án tafar ef líklegt er talið að það leiði af sér mikla hættu fyrir réttindi og frelsi viðkomandi einstaklinga.

## 10. Vinnslusamningar

### Samband lögmanns og umbjóðanda

Almennar reglur um samband ábyrgðar- og vinnsluaðila er að finna í 25. gr. laganna.

Eins og fram kom í kafla 1 hér að framan *teljast lögmennt jafnan vera ábyrgðaraðilar* þeirrar vinnslu persónuupplýsinga sem þeir hafa með höndum. Ekki er unnið með upplýsingarnar með þeim hætti sem umbjóðandinn veitir leiðbeiningar um heldur veitir hann jafnan einungis almenn fyrirmæli og umboð. Lögmanninum ber að fara með upplýsingarnar í samræmi við góða lögmannshætti, menntun sína og starfsreynslu, þau skilyrði sem liggja til grundvallar málflutningsleyfi hans, siðareglur lögmannna og þau lög og aðrar réttarreglur sem gilda um starfsemina. Honum ber með öðrum orðum að taka sjálfur flestar þær ákvarðanir sem þarf að taka um vinnsluna og meðferð þeirra persónuupplýsinga sem honum er treyst fyrir. Svonefndur 29. gr. starfshópur, sem er samstarfsvettvangur evrópskra persónuverndarstofnana, kemst að sömu niðurstöðu í leiðbeiningarriti sínu um hugtökin „ábyrgðaraðili“ og „vinnsluaðili“ (wp169), bls. 28. Til hliðsjónar má einnig vísa til úrskurðar Persónuverndar í máli 2016/266 (sálfræðingur).

### Samband lögmannna og birgja eða þjónustuaðila

Reglurnar um vinnsluaðila skipta lögmennt helst máli þegar kemur að þjónustuaðilum og birgjum lögmannna, svo sem veitendum upplýsingatækniþjónustu. Hvað varðar slíka aðila hafa lögmennt tvö meginverkefni:

1. Að ganga úr skugga um að *vinnsluaðilinn veiti nægilegar tryggingar* fyrir því að þeir geri öryggisráðstafanir til að vinnslan uppfylli kröfur laganna og að réttindi hinna skráðu séu tryggð. Til þess að geta sýnt fram á að hæfur vinnsluaðili hafi verið valinn er lögmenntum ráðlagt að skjalfesta hvað felist í þjónustu vinnsluaðilans, hvaða vottanir eða aðra staðfestingu vinnsluaðilinn leggur fram til að staðfesta að hann gæti að öryggi þeirra persónuupplýsinga sem hann vinnur með, hvaða gögn liggi fyrir um úttektir á starfsemi vinnsluaðilans og öryggi vinnslu hans, hvort vinnsluaðilinn nýti sér þjónustu undirverktaka eða þjónustuaðila og hvort í vinnslunni kunni að felast að þær persónuupplýsingar sem viðkomandi lögmanni hefur verið treyst fyrir verði fluttar út fyrir EES en slíkt er háð sérstökum skilyrðum sbr. 16. gr. laganna og nánar í V. kafla reglugerðarinnar. Oftar en ekki kann að þurfa að spyrja vinnsluaðilann viðbótarspurninga til að fá upplýsingar um öll framangreind atriði.

Í lögnum er ekki gerð almenn krafa um að ábyrgðaraðili framkvæmi *áhættumat* þegar hann velur sér vinnsluaðila eða ákveður fyrirkomulag vinnslu að öðru leyti. Þá skyldu er hins vegar að finna í fyrrnefndum reglum nr. 299/2001 um öryggi persónuupplýsinga auk þess sem í 27. gr. laganna kemur fram að við ákvörðun um öryggisráðstafanir skuli meðal annars taka með hliðsjón af þeirri áhættu sem henni fylgir fyrir réttindi og frelsi einstaklinga. Þá er að auki lögð sú skylda á ábyrgðaraðila að ef talið verði líklegt að fyrirhuguð vinnsla geti haft í för með sér mikla áhættu fyrir réttindi og frelsi einstaklinga skuli ábyrgðaraðili, áður en vinnslan hefst, láta fara fram mat á áhrifum hennar á vernd persónuupplýsinga, sbr. kafli 12 hér síðar. Þegar áhættumat er framkvæmt er rétt að það nái til þeirrar hættu sem steðjar að *leynd* persónuupplýsinganna (þ.e. hættu á óheimilum aðgangi), *heilleika* (þ.e. hættu á að upplýsingar brenglist eða í þær komi villur) og *aðgengileika* (þ.e. hættu á að þeir sem þurfi að komast í upplýsingarnar geti það ekki, svo sem ef ekki er nægilega hugsað fyrir afritatöku). Margt kyns tæki má nota til að framkvæma áhættumat á upplýsingaöryggi, til dæmis alþjóðlega staðalinn ISO/IEC 27005:2018. Til fróðleiks má um kröfur Persónuverndar til áhættumats sjá nýlega ákvörðun stofnunarinnar í máli 2017/1195 (landlæknir) þar sem

komist var að þeirri niðurstöðu að ábyrgðaraðili hefði vanrækt þá skyldu sína að framkvæma áhættumat áður en persónuupplýsingar sem hann bar ábyrgð á voru fluttar til vinnsluaðila.

2. Að gera *vinnslusamning* við vinnsluaðilann. Form samningsins getur verið hvort sem er sjálfstæður samningur, viðauki við þegar gerða eða aðra samninga aðila eða ákvæði sem felld eru inn í slíkan samning. Slíkur viðauki gæti haft eftirtalda efnisskipan:
- Bakgrunnur, tilgangur samningsviðaukans (tenging við meginsamning aðila).
  - Lýsing á vinnslunni sem samningurinn lýtur að og tilgangi hennar, flokkar hinna skráðu og tegundir persónuupplýsinga.
  - Almennar meginreglur um vinnsluna sem vinnsluaðilinn skal fara eftir (t.d. að hann skuli ekki nýta persónuupplýsingarnar í öðrum og óskyldum tilgangi).
  - Stuðningur vinnsluaðilans við ábyrgðaraðilann (t.d. að hann skuli aðstoða ábyrgðaraðilann við að uppfylla skyldur sínar gagnvart réttindum hinna skráðu).
  - Kröfur gagnvart vinnsluaðilanum varðandi öryggi vinnslunnar (t.d. að hann skuli innleiða upplýsingaöryggisráðstafanir í samræmi við kröfur 1. mgr. 27. gr. laganna).
  - Hvort og að hve miklu leyti vinnsluaðila sé heimilt að fela undir-vinnsluaðila þau verkefni sem hann ber ábyrgð á samkvæmt samningnum. Í 4. mgr. 28. gr. reglugerðarinnar er kveðið á um að samþykki ábyrgðaraðil fyrir slíku þurfi annað hvort að vera almennt, þannig að vinnsluaðili láti nægja að tilkynna ábyrgðaraðila ef hann skiptir um eða bætir við undirvinnsluaðila, eða að það verði sérstakt, þannig að sækja þurfi sérstakt samþykki í hvert samþykki og skipt er um vinnsluaðila.
  - Hvort og með hvaða skilyrðum megi flytja persónuupplýsingar út fyrir EES.
  - Sameiginleg skilgreining aðila á „öryggisbrotum“ og vel skilgreint í hvaða tilvikum vinnsluaðili skuli tilkynna ábyrgðaraðila um slík brot: Mikilvægt atriði í ljósi framangreindrar tilkynningarskyldu ábyrgðaraðila um öryggisbrot.
  - Úttekt ábyrgðaraðila á því hversu vel vinnsluaðili fer að ákvæðum vinnslusamningsins og laganna.
  - Gildistími og uppsögn (t.d. ákvæði um að vinnsluaðili skuli við samningslok skila og síðan eyða öllum gögnum sem hann hefur unnið með á vegum ábyrgðaraðila).

Fyrir lögmenn er mikilvægt að gætt sé öryggis allra upplýsinga sem vinnsluaðili vinnur með. Því kann það að tryggja hagsmuni lögmannsstofu betur ef samningurinn er látinn taka til allra upplýsinga sem vinnsluaðilinn sýslar með fyrir stofuna, ekki einungis persónuupplýsinga.

### Flutningur persónuupplýsinga úr landi

Heimilt er að flytja persónuupplýsingar jafn ótakmarkað milli EES-ríkja eins og innan eins þeirra. Hins vegar þarf sérstaka heimild til að flytja megi persónuupplýsingar eða veita aðgang að þeim utan EES, sbr. augl. 228/2010 um flutning persónuupplýsinga til annarra landa.

Helstu heimildir fyrir slíku má nefna svonefnd stöðluð samningsákvæði, útgefin af framkvæmdastjórn ESB, svonefndar bindandi fyrirtækjareglur (á ensku Binding Corporate Rules, BCR) og svonefndur „öryggisskjöldur“ (e. Privacy Shield) um flutning persónuupplýsinga til margra fyrirtækja í Bandaríkjunum.

## 11. Eyðing persónuupplýsinga

Svo sem að framan greinir er óheimilt að vinna með persónuupplýsingar nema fyrir hendi sé vinnsluheimild. Þá eru meðal meginreglna um vinnslu persónuupplýsinga skyldur til að gæta þess að persónuupplýsingar séu ekki umfram það sem nauðsynlegt er miðað við tilgang vinnslunnar, að óáreiðanlegum eða ófullkomnum upplýsingum sé eytt ef þær verða ekki leiðréttar og að þær séu ekki varðveittar á persónugreinanlegu formi lengur en þörf krefur, sbr. 8. gr. laganna.

Á hinn bóginn er lögmönnum í sumum tilvikum skylt að vista upplýsingar sem þeir búa yfir í ákveðinn tíma. Til dæmis þjóða bókhaldslög að geyma skuli meðal annars bókhaldsgögn og fylgiskjöl í 7 ár frá lokum viðkomandi reikningsárs.

Af þessu leiðir að lögmenn eiga, án dráttar, að *eyða eða gera varanlega ópersónugreinanlegar* þær persónuupplýsingar sem þeir sýsla með ef þá breytur vinnsluheimild svo sem í þeim undantekningartilvikum þar sem byggt er á samþykki hins skráða og hann afturkallar það, til dæmis samþykki til að vera á póstlista sem lögmannsstofan heldur úti. Þá leiðir einnig af framangöngu að eyða skal persónuupplýsingum ef þær eru ekki lengur nauðsynlegar í þeim tilgangi sem lá að baki vinnslunni, til dæmis upplýsingar um innheimtukuröfu ef fyrningartími hennar og lögbundinn geymslutími þeirra bókhaldsgagna sem geyma upplýsingar um hana eru hvorir tveggja liðnir.

Í 17. gr. reglugerðarinnar er settur fram réttur hins skráða til að krefjast eyðingar upplýsinga. Sá réttur er nefndur „rétturinn til að gleymast“. Hafi lögmaður farið að framangreindum skyldum hefur hann þegar eytt þeim upplýsingum sem hann hefur ekki lengur heimild til að vinna með. Í þeim tilvikum verður svar lögmanns við óskum hins skráða, um að hann eyði gögnum um hann, í meginatriðum einfaldlega það að þeim upplýsingum sem beri að eyða hafi þegar verið eytt.

## 12. Persónuverndarfulltrúar

Mörgum ábyrgðaraðilum og vinnsluaðilum ber að tilnefna svonefnda persónuverndarfulltrúa. Persónuverndarfulltrúi skal hafa sérþekkingu á persónuverndarrétti, hafa innra eftirlit með persónuverndarmálum hjá ábyrgðaraðilanum og vera honum til ráðgjafar um persónuverndarmál.

Þessi skyldan tekur til allra opinberra aðila og til annarra lögaðila ef meginstarfsemi þeirra felst í:

- umfangsmiklu, reglubundnu og kerfisbundnu eftirliti með skráðum einstaklingum eða
- umfangsmikilli vinnslu viðkvæmra persónuupplýsinga eða upplýsinga sem varða sakfellingar í refsimálum og refsiverð brot.

Hefbundnar lögmansstofur falla jafnan utan þessarar skyldu. Hins vegar falla hér undir lögmansstofur sem hafa með höndum umsvifamikla starfsemi á sviði refsiréttar eða réttarsviðum þar sem reglulega er sýslað með mikið magn viðkvæmra persónuupplýsinga, til dæmis á sviði vinnuréttar eða varðandi slysabætur. Mikilvægt er að lögmansstofur taki meðvitaða og skjalfesta ákvörðun um hvort þær telji sér bera að tilnefna persónuverndarfulltrúa og ef ekki, hver séu rökin fyrir því.



### 13. Mat á áhrifum á persónuvernd (MÁP)

Ábyrgðaraðili skal láta fara fram *mat á áhrifum fyrirhugaðrar vinnslu á vernd persónuupplýsinga (MÁP)* ef líklegt er að hún geti haft í för með sér „mikla hættu fyrir réttindi og frelsi einstaklinga“, sbr. 29. gr. laganna.

Í almennu persónuverndarreglugerðinni eru nánar tilgreindar þær tegundir vinnslu sem skulu sæta slíku mati, sbr. 3. mgr. 35. gr.:

- a) Kerfisbundið og umfangsmikið mat, sem byggist á sjálfvirkri vinnslu, á persónulegum þáttum einstaklinga og leiðir til ákvarðana um réttindi eða skyldur þeirra eða um önnur atriði sem snerta þá verulega.
- b) Umfangsmikil vinnsla viðkvæmra persónuupplýsinga eða upplýsinga sem varða sakfellingar í refsimálum og refsiverð brot.
- c) Kerfisbundið og umfangsmikið eftirlit með svæði sem er aðgengilegt almenningi.

Eins og sjá má af þessari upptalningu á hér hið sama við og um persónuverndarfulltrúa, sbr. kafla 11 hér að framan, að einkum kynni að koma til þess að lögmannsstofur þurfi að láta fara fram MÁP ef liður b) á við og þær stunda umfangsmikla starfsemi á nánar tilteknum réttarsviðum, svo sem á sviði refsiréttar eða vinnuréttar. Á móti má benda á að samkvæmt inngangsákvæði 91) í reglugerðinni ætti vinnsla persónuupplýsinga ekki að teljast „umfangsmikil“ ef hún varðar „persónuupplýsingar frá einstökum lækni, öðrum faglærðum heilbrigðisstarfsmanni eða lögfræðingi um sjúklinga eða viðskiptavini. Í þeim tilvikum ætti mat á áhrifum á persónuvernd ekki að vera skyldubundið“, eins og segir í ákvæðinu.

Af framangreindu leiðir að jafnan myndu lögmannsstofur ekki að þurfa að láta fara fram mat á áhrifum á persónuvernd í starfsemi sinni. Nánari leiðsögn um hvenær nauðsynlegt er að láta slíkt mat fara fram og hvernig megi bera sig að við það má finna í leiðbeiningarriti sem fyrrnefndur 29. gr. starfshópur gaf út um MÁP (wp248).

## 14. Markaðssetning

Ef lögmannsstofa hyggst senda viðskiptavinum sínum viðskiptaboð er mikilvægt að fara að ákvæðum fjarskiptalaga nr. 81/2003 um óumbeðin fjarskipti, sbr. 46. gr.

- Í 1. mgr. er sett fram sú meginregla að bannað sé að nota tölvupóst, smáskilaboð eða önnur rafræn skilaboð til beinnar markaðssetningar nema að fyrirfram fengnu samþykki hins skráða.
- Frá banninu eru gerðar undanþágur í 2. mgr., þar sem heimilað er að nota netfang hins skráða í beina markaðssetningu á öðrum vörum eða þjónustu sama söluaðila ef hinum skráða er gefinn kosur á að andmæla slíku þegar skráning á sér stað og í hvert sinn sem slíkur póstur er sendur, hafi hinn skráði ekki andmælt þegar í upphafi.

Af þessu leiðir að hafi lögmannsstofa hug á að geta stundað beina markaðssetningu til viðskiptavina sinna er rétt að huga að því þegar í upphafi viðskiptasambands með því að gefa viðskiptavininum þá þegar kost á að taka afstöðu til þess hvort hann myndi vilja geta fengið slík boð send.

Þá er rétt að hafa í huga að fyrrnefnd undanþága frá banni við beinni markaðssetningu á einungis við um aðrar vörur og þjónustur frá sama söluaðila. Því nægir hún ekki lögmannsstofu sem myndi vilja stunda beina markaðssetningu til viðskiptavina sinna á vörum eða þjónustu frá öðrum en stofunni sjálfri.

Þá er rétt að hafa í huga að sjálft viðskiptasambandið milli lögmanns og umbjóðanda er háð trúnaði og því þarf jafnan að afla fyrirfram samþykkis umbjóðanda ef lögmaður hyggst vísa til hans í markaðssetningu sinni.

Loks má nefna að í 5. mgr. 46. gr. fjarskiptalaga er mælt fyrir um að þeir sem nota almenna tal- og fjarskiptaþjónustu sem lið í markaðssetningu skuli virða merkingu í símaskrá sem gefur til kynna að áskrifandi vilji ekki slíkar símhringingar. Sambærilegt ákvæði er að finna í 2. mgr. 21. gr. persónuverndarlaganna þar sem segir að Þjóðskrá Íslands haldi skrá yfir þá sem andmæla því að nöfn þeirra séu notuð í markaðssetningarstarfsemi. Þeir sem stunda slíka starfsemi skulu gæta þess að beina markpósti og marksímtölum ekki að þeim sem eru á þeirri skrá. Nánari skilyrði fyrir beinni markaðssetningu er að finna í ákvæðinu og í reglum nr. 36/2005.

## 15. Skoðun tölvupósts starfsmanna o.fl.

### Inngangur

Fjallað er um rafræna vöktun í 14. gr. laganna. Þar eru sett þau skilyrði fyrir slíkri vöktun að hún fari fram í málefnalegum tilgangi. Þá kemur meðal annars fram að Persónuvernd setji reglur og gefi fyrirmæli um rafræna vöktun og vinnslu efnis sem verður til við vöktunina.

Í frumvarpi til hinna nýju laga um persónuvernd kemur fram að því hafi ekki verið ætlað að breyta efnislega ákvæðum gildandi laga um rafræna vöktun eða reglna settra á grundvelli þeirra, þar á meðal reglna nr. 837/2006 um rafræna vöktun, með áorðnum breytingum. Í þeim koma meðal annars fram sérreglur um tölvupóst og netnotkun starfsmanna á vinnustöðum.

Samkvæmt reglunum er einkatölvupóstur starfsmanna skilgreindur sem póstur sem lýtur að einkalífi hans en varðar hvorki hagsmuni ábyrgðaraðila né starfsemi hans. Til viðmiðunar um hvort um einkatölvupóst sé að ræða segir í reglunum að líta megi til þess hvort hann sé auðkenndur sem einkamál t.d. í efnislínu eða vistaður í sérstakri möppu sem auðkennd er sem einkamál eða með sambærilegum hætti.

Þá segir í reglunum að óheimilt sé að skoða einkatölvupóst eða upplýsingar um netnotkun nema brýna nauðsyn beri til, t.d. vegna „tölvuveiru eða sambærilegs tæknilegs atviks“. Þá segir að heimilt sé að skoða upplýsingar um „netvafur, tengingar og gagnamagn“ starfsmanns liggja fyrir rökstuddur grunur um að hann hafi brotið gegn lögum og reglum eða fyrirmælum vinnuveitanda. Við slíka skoðun skal þess gætt að gera starfsmanni fyrst grein fyrir því og veita honum eða fulltrúa hans tækifæri á að vera viðstaddur skoðun, ef þess er kostur.

Loks segir í reglunum að við starfslok skuli starfsmanni gefinn kostur á að eyða eða taka afrit af þeim tölvupósti sem ekki tengist starfsemi vinnuveitanda. Við starfslok skuli starfsmanni leiðbeint um að virkja sjálfvirka svörun úr sínu pósthólfi um að hann hafi látið af störfum. Loka skuli pósthólfinu eigi síðar en að tveimur vikum liðnum. Sérstaklega er tekið fram að óheimilt sé að senda tölvupóst fyrirverandi starfsmanns á nýjan starfsmann nema um annað hafi verið samið.

### Reglur ábyrgðaraðila

Í 10. gr. fyrrnefndra reglna kemur fram að ábyrgðaraðili að rafrænni vöktun skuli setja reglur og veita fræðslu til þeirra sem henni sæta og að kynna skuli þær með sannanlegum hætti áður en þeim verði beitt.

Í slíkum reglum ábyrgðaraðila skulu koma fram upplýsingar um eftirfarandi:

- Tilgang vöktunarinnar.
- Þá sem hafa eða kunna að fá aðgang að upplýsingum sem safnast og hversu lengi þær verða varðveittar.
- Hvaða búnaður er notaður, t.d. stafrænar myndavélar, ökusíritar eða hljóðupptökutæki.
- Rétt til að andmæla vöktuninni og hverjar geti verið afleiðingar þess.
- Rétt viðkomandi til að fá að vita hvaða upplýsingar verða til um hann og um rétt hans til að fá upplýsingar leiðréttar eða þeim eytt.

- Að hvaða marki netnotkun sé heimil, s.s. hvort bannað sé að sækja á netið ólöglegt og/eða kynlífstengt efni og/eða senda slíkt með tölvupósti.
- Hvernig farið sé með einkatölvupóst og annan tölvupóst.
- Hvort símvöktun fari fram og hvort takmarkanir, og þá hvaða, séu á heimild til einkanota á tilgreindum símtækjum.
- Afleiðingar þess ef brotið er gegn fyrirmælum, s.s. um notkun síma eða internets.
- Önnur atriði, að því marki sem þörf krefur með hliðsjón af aðstæðum hverju sinni, svo að starfsmenn geti gætt hagsmuna sinna.

Þá kemur fram í 12. gr. að sá sem sætt hefur rafrænni vöktun skuli eiga rétt á að skoða gögn sem verða til við vöktunina, svo sem að fá að hlusta á hljóðupptökur, að nánar tilteknum skilyrðum uppfylltum.