ÍSLENSK útgáfa

EES-viðbætir

við Stjórnartíðindi Evrópusambandsins

ISSN 1022-9337

Nr. 46

25. árgangur

19.7.2018

EES-STOFNANIR

SAMEIGINLEGA EES-NEFNDIN

ÁKVÖRÐUN SAMEIGINLEGU EES-NEFNDARINNAR **2018/EES/46/01**
nr. 154/2018

frá 6. júlí 2018

um breytingu á XI. viðauka (Rafræn fjarskipti, hljóð- og myndmiðlun og upplýsingasamfélagið) og bókun 37 (sem inniheldur skrána sem kveðið er á um í 101. gr.) við EES-samninginn

SAMEIGINLEGA EES-NEFNDIN HEFUR,

með vísan til samningsins um Evrópska efnahagssvæðið, („EES-samningurinn“), einkum 98. gr.,

og að teknu tilliti til eftirfarandi:

1) Fella ber inn í EES-samninginn reglugerð Evrópuþingsins og ráðsins (ESB) 2016/679 frá 27. apríl 2016 um vernd einstaklinga í tengslum við vinnslu persónuupplýsinga og um frjálsa miðlun slíkra upplýsinga og niðurfellingu tilskipunar 95/46/EB (almenna persónuverndar-reglugerðin) ([1]).

2) Sameiginlega EES-nefndin viðurkennir að gagnavernd er grundvallarréttindi sem varin eru í ýmsum alþjóðlegum mannréttindasamningum.

3) Sameiginlega EES-nefndin viðurkennir mikilvægi jafnra réttinda og skyldna þeirra sem annast eftirlit með gagnavinnslu og gagnavinnslu á EES-svæðinu.

4) Ákvörðun þessi kveður á um að eftirlitsyfirvöld EFTA-ríkjanna skuli taka fullan þátt í fyrirkomulaginu sem varðar „afgreiðslu á einum stað“ og samræmingarkerfið og hafa sömu réttindi og skyldur og eftirlitsyfirvöld aðildarríkja ESB í Evrópska persónuverndarráðinu („persónuverndar-ráðið“), sem komið er á fót með reglugerð (ESB) 2016/679, án þess þó að eiga rétt á að greiða atkvæði og bjóða sig fram til embættis formanns eða varaformanns. Því skulu eftirlitsyfirvöld EFTA-ríkjanna taka þátt í starfsemi persónuverndarráðsins, m.a. starfi hvers konar undirhóps sem persónuverndarráðið kann að setja á laggirnar til þess að sinna starfi sínu, og fá allar upplýsingar sem nauðsynlegar eru fyrir skilvirka þátttöku, þ.m.t., eftir því sem nauðsyn krefur, með fullum aðgangi að hvers konar rafrænum kerfum fyrir upplýsingaskipti sem persónuverndarráðið kann að setja upp.

5) Reglugerð (ESB) 2016/679 fellir úr gildi tilskipun Evrópuþingsins og ráðsins 95/46/EB ([2]), sem hefur verið felld inn í EES-samninginn, og ber því að fella gerðina brott úr samningnum.

6) XI. viðauki og bókun 37 við EES-samninginn breytist því í samræmi við það.

TEKIÐ EFTIRFARANDI ÁKVÖRÐUN:

1. gr.

Eftirfarandi kemur í stað texta liðar 5e (tilskipun Evrópuþingsins og ráðsins 95/46/EB) í XI. viðauka við EES-samninginn:

„32016 R 0679: Reglugerð Evrópuþingsins og ráðsins (ESB) 2016/679 frá 27. apríl 2016 um vernd einstaklinga í tengslum við vinnslu persónuupplýsinga og um frjálsa miðlun slíkra upplýsinga og niðurfellingu tilskipunar 95/46/EB (almenna persónuverndarreglugerðin) (Stjtíð. ESB L 119, 4.5.2016, bls. 1).

([1]) Stjtíð. ESB L 119, 4.5.2016, bls. 1.
([2]) Stjtíð. ESB L 281, 23.11.1995, bls. 31.

Ákvæði reglugerðarinnar skulu, að því er samning þennan varðar, aðlöguð sem hér segir:

a) Eftirlitsyfirvöld EFTA-ríkjanna skulu taka þátt í starfsemi Evrópska persónuverndarráðsins, hér á eftir nefnt „persónuverndarráðið“. Því skulu þau hafa sömu réttindi og skyldur og eftirlitsyfirvöld aðildarríkja ESB í persónuverndarráðinu, án þess þó að eiga rétt á að neyta atkvæðisréttar og bjóða sig fram til embættis formanns eða varaformanns persónuverndarráðsins, nema kveðið sé á um annað í samningi þessum. Persónuverndarráðið skal skrá afstöðu eftirlitsyfirvalda EFTA-ríkjanna sérstaklega.

   Haga skal starfsreglum persónuverndarráðsins þannig að eftirlitsyfirvöld EFTA-ríkjanna og Eftirlitsstofnun EFTA geti tekið fullan þátt í því, að undanskildum rétti á að neyta atkvæðisréttar og bjóða sig fram til embættis formanns eða varaformanns persónuverndarráðsins.

b) Þrátt fyrir ákvæði bókunar 1 við samning þennan, og nema kveðið sé á um annað í samningi þessum, ber að skilja hugtökin „aðildarríki (-n)“ og „eftirlitsyfirvöld“ þannig að þau taki til EFTA-ríkjanna og eftirlitsyfirvalda þeirra til viðbótar við merkingu þeirra í reglugerðinni, í þeirri röð.

c) Skilja ber tilvísanir til laga Sambandsins eða ákvæða Sambandsins um gagnavernd sem tilvísanir til EES-samningsins eða ákvæða um gagnavernd sem í honum eru, í þeirri röð.

d) Í f-lið 1. mgr. 13. gr. og f-lið 1. mgr. 14. gr. er, hvað EFTA-ríkin varðar, orðunum „sem gildir samkvæmt EES-samningnum“ bætt við á eftir orðunum „ákvörðun framkvæmdastjórnarinnar um það hvort vernd sé fullnægjandi“.

e) Að því er EFTA-ríkin varðar er eftirfarandi bætt við á eftir 1. mgr. 45. gr.:

   „1a. Þar til sameiginlega EES-nefndin hefur ákveðið að fella inn í EES-samninginn framkvæmdargerð, sem samþykkt er í samræmi við 3. eða 5. mgr. þessarar greinar, getur EFTA-ríki ákveðið að beita ráðstöfunum sem þar er kveðið á um.

   Hvert EFTA-ríki skal ákveða og upplýsa framkvæmdastjórnina og Eftirlitsstofnun EFTA, áður en allar framkvæmdargerðir, sem samþykktar eru í samræmi við 3. eða 5. mgr. þessarar greinar, öðlast gildi, um hvort það muni, þar til sameiginlega EES-nefndin hefur ákveðið að fella framkvæmdargerðina inn í EES-samninginn, beita ráðstöfununum, sem þar er kveðið á um, á sama tíma og aðildarríki ESB eða ekki. Ef ekki hefur verið tekin ákvörðun um hið gagnstæða skal hvert EFTA-ríki beita ráðstöfununum, sem eru í framkvæmdargerðinni sem samþykkt er í samræmi við 3. eða 5. mgr. þessarar greinar, á sama tíma og aðildarríki ESB.

   Þrátt fyrir ákvæði 102. gr. samningsins getur EFTA-ríki hætt beitingu slíkra ráðstafana ef samningur um að fella inn í EES-samninginn framkvæmdargerð, sem samþykkt er í samræmi við 3. eða 5. mgr., næst ekki í sameiginlegu EES-nefndinni innan tólf mánaða frá því að sú framkvæmdargerð öðlast gildi, og skal tilkynna það til framkvæmdastjórnarinnar og Eftirlitsstofnunar EFTA án tafar.

   Aðrir aðilar að EES-samningnum skulu, þrátt fyrir 3. mgr. 1. gr., takmarka eða banna frjálst flæði persónuupplýsinga til EFTA-ríkis sem ekki beitir ráðstöfununum í framkvæmdargerðinni, sem samþykkt er í samræmi við 5. mgr. þessarar greinar, á sama hátt og þessar ráðstafanir koma í veg fyrir miðlun persónuupplýsinga til þriðja lands eða alþjóðastofnunar.“

f) Hvenær sem ESB hefur viðræður við þriðju lönd eða alþjóðastofnanir, í því skyni að samþykkja ákvörðun um fullnægjandi vernd í samræmi við 45. gr., skulu EFTA-ríkin upplýst um það með tilhlýðilegum hætti. Í þeim tilvikum þar sem þriðja landið eða alþjóðastofnunin tekst á hendur tilteknar skuldbindingar að því er varðar vinnslu persónuupplýsinga frá aðildarríkjunum, mun ESB taka tillit til aðstæðna EFTA-ríkjanna og ræða við þriðju lönd eða alþjóðastofnanir um mögulegt fyrirkomulag hugsanlegrar beitingar í kjölfarið af hálfu EFTA-ríkjanna.

g) Eftirfarandi er bætt við d-lið 2. mgr. 46. gr.:

   „Eftirlitsyfirvöld EFTA-ríkjanna skulu hafa sama rétt og eftirlitsyfirvöld ESB til þess að senda stöðluð ákvæði um persónuvernd til framkvæmdastjórnarinnar til samþykkis í samræmi við rannsóknarmálsmeðferðina sem um getur í 2. mgr. 93. gr.“

h) Að því er EFTA-ríkin varðar er eftirfarandi málsgrein bætt við á eftir 2. mgr. 46. gr.:

„2a. Þar til sameiginlega EES-nefndin hefur ákveðið að fella framkvæmdargerð inn í EES-samninginn er unnt að kveða á um viðeigandi verndarráðstafanir, sem um getur í fyrstu málsgrein, með stöðluðum ákvæðum um persónuvernd, sem um getur í c- og d-lið 2. mgr. 46. gr., þar sem EFTA-ríki beitir ráðstöfununum sem þar er kveðið á um.

Hvert EFTA-ríki skal ákveða og upplýsa framkvæmdastjórnina og Eftirlitsstofnun EFTA, áður en framkvæmdargerðirnar, sem samþykktar eru í samræmi við c- og d-lið 2. mgr. 46. gr., öðlast gildi, um hvort það muni, þar til sameiginlega EES-nefndin hefur ákveðið að fella framkvæmdargerðina inn í EES-samninginn, beita ráðstöfununum, sem þar er kveðið á um, á sama tíma og aðildarríki ESB eða ekki. Ef ekki hefur verið tekin ákvörðun um hið gagnstæða skal hvert EFTA-ríki beita ráðstöfununum, sem eru í framkvæmdargerðinni sem samþykkt er í samræmi við c- og d-lið 2. mgr. 46. gr., á sama tíma og aðildarríki ESB.

Þrátt fyrir ákvæði 102. gr. samningsins getur EFTA-ríki hætt beitingu slíkra ráðstafana ef samningur um að fella framkvæmdargerðina, sem samþykkt er í samræmi við c- og d-lið 2. mgr. 46. gr., inn í EES-samninginn næst ekki í sameiginlegu EES-nefndinni innan tólf mánaða frá því að sú framkvæmdargerð öðlast gildi, og skal tilkynna það til framkvæmdastjórnarinnar og Eftirlitsstofnunar EFTA án tafar.“

i) Í 4. mgr. 58. gr. gilda orðin „í samræmi við sáttmálann um grundvallarréttindi“ ekki að því er EFTA-ríkin varðar.

j) Í 59. gr. er orðunum „, Eftirlitsstofnun EFTA“ bætt við á eftir orðinu „framkvæmdastjórninni“.

k) Eftirlitsstofnun EFTA skal hafa rétt til þátttöku í fundum persónuverndarráðsins, þó án atkvæðisréttar. Eftirlitsstofnun EFTA skal tilnefna fulltrúa sinn.

l) Þegar við á, að því er varðar framkvæmd þeirra starfa sem Eftirlitsstofnun EFTA annast skv. 109. gr. samnings þessa, skal stofnunin hafa rétt á að óska eftir ráðgjöf eða áliti persónuverndarráðsins og skiptast á upplýsingum við það í samræmi við 63. gr., 2. mgr. 64. gr., c-lið 1. mgr. 65. gr. og e-lið 1. mgr. 70. gr. Orðunum „og, ef við á, Eftirlitsstofnun EFTA“ er bætt við á eftir orðinu „framkvæmdastjórnina“ í 63. gr., orðinu „framkvæmdastjórnin“ í 2. mgr. 64. gr., orðinu „framkvæmdastjórnin“ í c-lið 1. mgr. 65. gr. og orðunum „og, ef við á, Eftirlitsstofnunar EFTA“ er bætt við á eftir orðinu „framkvæmdastjórnarinnar“ í e-lið 1. mgr. 70. gr.

m) Formaður persónuverndarráðsins eða skrifstofa þess skal tilkynna Eftirlitsstofnun EFTA um starfsemi persónuverndarráðsins, ef við á, í samræmi við a- og b-lið 5. mgr. 64. gr., 5. mgr. 65. gr. og b-lið 6. mgr. 75. gr. Orðunum „og, ef við á, Eftirlitsstofnun EFTA“ er bætt við á eftir orðinu „framkvæmdastjórninni“ í a- og b-lið 5. mgr. 64. gr. og 5. mgr. 65. gr. og orðunum „og, ef við á, Eftirlitsstofnunar EFTA“ er bætt við á eftir orðinu „framkvæmdastjórnarinnar“ í b-lið 6. mgr. 75. gr.

Þegar við á, að því er varðar framkvæmd þeirra starfa sem Eftirlitsstofnun EFTA annast skv. 109. gr. samnings þessa, skal stofnunin hafa rétt á að fá afhentar upplýsingar frá eftirlitsstofnun þess EFTA-ríkis sem um er að ræða í samræmi við 1. mgr. 66. gr. Í 1. mgr. 66. gr. er orðunum „og, ef við á, Eftirlitsstofnun EFTA“ bætt við á eftir orðinu „framkvæmdastjórninni“.

n) Í 1. mgr. 71. gr. er orðunum „, fastanefndar EFTA-ríkjanna, Eftirlitsstofnunar EFTA“ bætt við á eftir orðinu „ráðsins“.

o) Í 1. mgr. 73. gr. er eftirfarandi setningu bætt við:

„Fulltrúar persónuverndarráðsins frá EFTA-ríkjunum eru ekki kjörgengir til embættis formanns eða varaformanns.“

2. gr.

Texti 13. liðar bókunar 37 við EES-samninginn (Starfshópur um vernd einstaklinga í tengslum við vinnslu persónuupplýsinga) fellur brott.

3. gr.

Íslenskur og norskur texti reglugerðar (ESB) 2016/679, sem verður birtur í EES-viðbæti við *Stjórnartíðindi Evrópusambandsins*, telst fullgiltur.

4. gr.

Ákvörðun þessi öðlast gildi daginn eftir að síðasta tilkynning, samkvæmt 1. mgr. 103. gr. EES-samningsins, hefur farið fram (*).

5. gr.

Ákvörðun þessi skal birt í EES-deild *Stjórnartíðinda Evrópusambandsins* og EES-viðbæti við þau.

Gjört í Brussel 6. júlí 2018.

Fyrir hönd sameiginlegu EES-nefndarinnar

Oda Helen Sletnes

formaður.

(*) Stjórnskipuleg skilyrði gefin til kynna.

Sameiginleg yfirlýsing samningsaðila

vegna ákvörðunar sameiginlegu EES-nefndarinnar nr. 154/2018 frá 6. júlí 2018 um að fella reglugerð Evrópuþingsins og ráðsins (ESB) 2016/679 frá 27. apríl 2016 um vernd einstaklinga í tengslum við vinnslu persónuupplýsinga og um frjálsa miðlun slíkra upplýsinga og niðurfellingu tilskipunar 95/46/EB (almenna persónuverndarreglugerðin) inn í EES-samninginn.

Samningsaðilarnir, með tveggja stoða kerfi EES-samningsins í huga og með tilliti til beinna og bindandi áhrifa ákvarðana Evrópska persónuverndarráðsins fyrir innlend eftirlitsyfirvöld í EFTA-ríkjunum innan EES:

– taka mið af þeirri staðreynd að ákvörðunum Evrópska persónuverndarráðsins er beint að innlendum eftirlitsyfirvöldum,

– viðurkenna að þessi lausn hefur ekki fordæmisgildi fyrir aðlögun gerða ESB sem verða felldar inn í EES-samninginn í framtíðinni.

REGLUGERÐ EVRÓPUÞINGSINS OG RÁÐSINS (ESB) 2016/679 **2018/EES/46/02**

frá 27. apríl 2016

um vernd einstaklinga í tengslum við vinnslu persónuupplýsinga og um frjálsa miðlun slíkra upplýsinga og niðurfellingu tilskipunar 95/46/EB (almenna persónuverndarreglugerðin) (*)

EVRÓPUÞINGIÐ OG RÁÐ EVRÓPUSAMBANDSINS HAFA,

með hliðsjón af sáttmálanum um starfshætti Evrópusambandsins, einkum 16. gr.,

með hliðsjón af tillögu framkvæmdastjórnar Evrópusambandsins,

eftir að hafa lagt drög að lagagerð fyrir þjóðþingin,

með hliðsjón af áliti efnahags- og félagsmálanefndar Evrópusambandsins ([1]),

með hliðsjón af áliti svæðanefndarinnar ([2]),

í samræmi við almenna lagasetningarmeðferð ([3]),

og að teknu tilliti til eftirfarandi:

1) Vernd einstaklinga í tengslum við vinnslu persónuupplýsinga telst til grundvallarréttinda. Í 1. mgr. 8. gr. sáttmála Evrópusambandsins um grundvallarréttindi („sáttmálanum um grundvallarréttindi“) og í 1. mgr. 16. gr. sáttmálans um starfshætti Evrópusambandsins er kveðið á um að sérhver einstaklingur eigi rétt á að persónuupplýsingar um hann njóti verndar.

2) Meginreglur og reglur um vernd einstaklinga í tengslum við vinnslu persónuupplýsinga þeirra ættu að virða grundvallarréttindi og frelsi einstaklinga án tillits til ríkisfangs þeirra eða búsetu, einkum rétt þeirra til verndar persónuupplýsingum. Reglugerð þessari er ætlað að stuðla að því að koma á svæði frelsis, öryggis og réttlætis og efnahagsbandalagi, að efnahagslegri og félagslegri þróun, að styrkingu og aukinni samleitni efnahagskerfa sem mynda innri markaðinn og að velferð einstaklinga.

3) Í tilskipun Evrópuþingsins og ráðsins 95/46/EB ([4]) er leitast við að samræma vernd grundvallarréttinda og frelsis einstaklinga í tengslum við vinnslustarfsemi og tryggja frjálst flæði persónuupplýsinga milli aðildarríkja.

(*) Þessi ESB-gerð birtist í Stjtíð. ESB L 119, 4.5.2016, bls. 1. Hennar var getið í ákvörðun sameiginlegu EES-nefndarinnar nr. 154/2018 frá 6. júlí 2018 um breytingu á XI. viðauka (Rafræn fjarskipti, hljóð- og myndmiðlun og upplýsingasamfélagið) og bókun 37 við EES-samninginn með skrá sem kveðið er á um í 101. gr. (bíður birtingar).

([1]) Stjtíð. ESB C 229, 31.7.2012, bls. 90.

([2]) Stjtíð. ESB C 391, 18.12.2012, bls. 127.

([3]) Afstaða Evrópuþingsins frá 12. mars 2014 (hefur enn ekki verið birt í Stjórnartíðindunum) og afstaða ráðsins eftir fyrstu umræðu frá 8. apríl 2016 (hefur enn ekki verið birt í Stjórnartíðindunum). Afstaða Evrópuþingsins frá 14. apríl 2016.

([4]) Tilskipun Evrópuþingsins og ráðsins 95/46/EB frá 24. október 1995 um vernd einstaklinga í tengslum við vinnslu persónuupplýsinga og um frjálsa miðlun slíkra upplýsinga (Stjtíð. EB L 281, 23.11.1995, bls. 31).

4) Vinnsla persónuupplýsinga ætti að hafa það að markmiði að þjóna mannkyninu. Rétturinn til verndar persónuupplýsingum er ekki ófrávíkjanlegur, hann þarf að ígrunda í tengslum við hlutverk hans í samfélaginu og vega hann og meta gagnvart öðrum grundvallarréttindum í samræmi við meðalhófsregluna. Í þessari reglugerð eru öll grundvallarréttindi og mannfrelsi virt og þeim meginreglum fylgt sem eru viðurkenndar í sáttmálanum um grundvallarréttindi eins og þær koma fram í sáttmálunum, einkum varðandi friðhelgi einkalífs og fjölskyldu, heimilis og samskipta, vernd persónuupplýsinga, hugsana-, samvisku- og trúfrelsi, tjáningar- og upplýsingafrelsi, frelsi til atvinnurekstrar, rétt til skilvirks úrræðis til að leita réttar síns og réttlátrar málsmeðferðar fyrir dómi og fjölbreytni menningar, trúarbragða og tungumála.

5) Með þeirri efnahagslegu og félagslegu aðlögun, sem fylgir starfsemi innri markaðarins, hefur flæði persónuupplýsinga yfir landamæri aukist verulega. Skipti á persónuupplýsingum milli opinberra aðila og einkaaðila, þ.m.t. einstaklinga, samtaka og fyrirtækja í Sambandinu, hafa farið vaxandi. Samkvæmt lögum Sambandsins ber yfirvöldum í aðildarríkjunum að starfa saman og skiptast á persónuupplýsingum til að þau geti rækt skyldur sínar og framkvæmt verkefni fyrir hönd yfirvalda í öðru aðildarríki.

6) Hröð tækniþróun og hnattvæðing hafa leitt til nýrra viðfangsefna varðandi vernd persónuupplýsinga. Umfang söfnunar og miðlunar persónuupplýsinga hefur aukist verulega. Tæknin gerir jafnt einkafyrirtækjum sem opinberum yfirvöldum kleift að nýta persónuupplýsingar við starfsemi sína í áður óþekktum mæli. Einstaklingar gera í auknum mæli persónuupplýsingar aðgengilegar öllum og á alþjóðavísu. Tæknin hefur breytt bæði efnahagskerfinu og félagslífi fólks og ætti að greiða enn frekar fyrir frjálsu flæði persónuupplýsinga innan Sambandsins og miðlun þeirra til þriðju landa og alþjóðastofnana, jafnframt því að tryggja öfluga vernd upplýsinganna.

7) Þessi þróun kallar á að komið verði á fót öflugum og heildstæðari ramma um persónuvernd í Sambandinu og honum fylgt kröftuglega eftir, með hliðsjón af mikilvægi þess að skapa traust sem gerir hinu stafræna hagkerfi kleift að þróast á öllum innri markaðnum. Einstaklingar ættu að stjórna eigin persónuupplýsingum. Efla ætti réttarvissu og fyrirsjáanleika gagnvart einstaklingum, rekstraraðilum og opinberum yfirvöldum.

8) Þegar kveðið er á um það í þessari reglugerð að setja megi fram í lögum aðildarríkja skýringar eða takmarkanir á reglum hennar er aðildarríkjum heimilt að fella inn í landslög sín þætti úr þessari reglugerð að því marki sem nauðsynlegt er vegna samræmis og til þess að gera ákvæði landslaga skiljanleg þeim sem þau eiga við um.

9) Markmið og meginreglur tilskipunar 95/46/EB standa enn fyrir sínu en hún hefur ekki náð að sporna gegn sundurlausri framkvæmd persónuverndar innan Sambandsins, réttaróvissu eða þeim útbreiddu hugmyndum meðal almennings að fyrir hendi sé veruleg áhætta fyrir vernd einstaklinga, einkum í tengslum við Netnotkun. Réttindi og frelsi einstaklinga, einkum rétturinn til verndar persónuupplýsingum, njóta mismikillar verndar í aðildarríkjunum í tengslum við vinnslu persónuupplýsinga og getur það hindrað frjálst flæði persónuupplýsinga um Sambandið. Þessi munur getur því orðið hindrun í vegi ýmiss konar atvinnustarfsemi á vettvangi Sambandsins, raskað samkeppni og komið í veg fyrir að yfirvöld sinni skyldustörfum sínum samkvæmt lögum Sambandsins. Þennan mun á vernd má rekja til þess mismunar sem er á framkvæmd og beitingu tilskipunar 95/46/EB.

10) Til þess að tryggja einstaklingum samræmda og öfluga vernd og ryðja úr vegi hindrunum á flæði persónuupplýsinga innan Sambandsins ætti vernd réttinda og frelsis einstaklinga í tengslum við vinnslu slíkra upplýsinga að vera sambærileg í öllum aðildarríkjunum. Tryggja ætti alls staðar í Sambandinu samræmda og einsleita beitingu reglna um vernd grundvallarréttinda og frelsis einstaklinga í tengslum við vinnslu persónuupplýsinga. Að því er varðar vinnslu persónuupplýsinga til þess að fullnægja lagaskyldu ætti aðildarríkjunum að vera heimilt, vegna framkvæmdar á verkefni sem unnið er í þágu almannahagsmuna eða við beitingu opinbers valds sem ábyrgðaraðili fer með, að viðhalda eða innleiða ný ákvæði í landslög til að tilgreina nánar hvernig þessari reglugerð skuli beitt. Auk almennrar og láréttrar löggjafar um persónuvernd, sem sett er til framkvæmdar tilskipun 95/46/EB, hafa aðildarríkin ýmsa geirabundna löggjöf á sviðum þar sem þörf er á sértækari ákvæðum. Þessi reglugerð veitir aðildarríkjunum einnig ákveðið svigrúm til að skilgreina reglur sínar, m.a. varðandi vinnslu sérstakra flokka persónuupplýsinga („viðkvæmra upplýsinga“). Hvað þetta varðar útilokar þessi reglugerð ekki að í lögum aðildarríkjanna sé mælt fyrir um aðstæður sem réttlæta sérstaka vinnslu, þar sem m.a. er skilgreint nánar með hvaða skilyrðum vinnsla persónuupplýsinga sé lögmæt.

11) Til að tryggja skilvirka vernd persónuupplýsinga alls staðar í Sambandinu þarf að styrkja og setja fram með ítarlegum hætti réttindi skráðra einstaklinga og skyldur þeirra sem vinna persónuupplýsingar og taka ákvarðanir um vinnslu þeirra, svo og samsvarandi heimildir til að hafa eftirlit með og tryggja að farið sé að reglum um vernd persónuupplýsinga, og setja fram sambærileg viðurlög vegna brota í aðildarríkjunum.

12) Í 2. mgr. 16. gr. sáttmálans um starfshætti Evrópusambandsins er Evrópuþinginu og ráðinu veitt heimild til að mæla fyrir um reglur er varða vernd einstaklinga með tilliti til vinnslu persónuupplýsinga og um reglur er varða frjálsa miðlun slíkra upplýsinga.

13) Til að tryggja samræmda vernd einstaklinga alls staðar í Sambandinu og koma í veg fyrir að misræmi hamli frjálsri miðlun persónuupplýsinga á innri markaðnum er þörf á reglugerð sem skapar réttarvissu og gagnsæi gagnvart rekstraraðilum, þ.m.t. örfyrirtækjum, litlum og meðalstórum fyrirtækjum, tryggir einstaklingum í öllum aðildarríkjum sömu lagalega framfylgjanlegu réttindi og skyldur og leggur samsvarandi ábyrgð á herðar ábyrgðaraðilum og vinnsluaðilum, og tryggir samræmt eftirlit með vinnslu persónuupplýsinga og sambærileg viðurlög í öllum aðildarríkjum, sem og skilvirkt samstarf milli eftirlitsyfirvalda einstakra aðildarríkja. Eðlileg starfsemi innri markaðarins krefst þess að ekki séu settar takmarkanir eða lagt bann við frjálsri miðlun persónuupplýsinga innan Sambandsins af ástæðum sem varða vernd einstaklinga í tengslum við vinnslu persónuupplýsinga. Með hliðsjón af sérstökum aðstæðum örfyrirtækja, lítilla og meðalstórra fyrirtækja er sett fram undanþága í þessari reglugerð varðandi skráahald fyrirtækja með færri en 250 starfsmenn. Enn fremur eru stofnanir og aðilar Sambandsins og aðildarríkin og eftirlitsyfirvöld þeirra hvött til að taka tillit til sérstakra þarfa örfyrirtækja, lítilla og meðalstórra fyrirtækja við beitingu þessarar reglugerðar. Hugtökin örfyrirtæki, lítið og meðalstórt fyrirtæki ættu að byggjast á 2. gr. viðaukans við tilmæli framkvæmdastjórnarinnar 2003/361/EB ([1]).

14) Sú vernd, sem þessi reglugerð veitir í tengslum við vinnslu persónuupplýsinga, ætti að gilda um einstaklinga án tillits til ríkisfangs eða búsetu. Þessi reglugerð nær ekki yfir vinnslu persónuupplýsinga er varða lögaðila, einkum fyrirtæki sem stofnuð eru sem lögaðilar, þ.m.t. upplýsinga um heiti lögaðila, rekstrarform hans og samskiptaupplýsingar.

15) Til að komast hjá því að fram komi alvarleg hætta á að reglur verði sniðgengnar ætti vernd einstaklinga að vera tæknilega hlutlaus og ekki háð þeim aðferðum sem notaðar eru. Vernd einstaklinga ætti að eiga við um sjálfvirka jafnt sem handvirka vinnslu persónuupplýsinga ef upplýsingarnar eru varðveittar eða ráðgert er að varðveita þær í skráningarkerfi. Skjöl eða skjalaraðir, sem og forsíður þeirra, sem eru ekki skipulagðar samkvæmt tilteknum viðmiðunum, ættu ekki að falla undir gildissvið þessarar reglugerðar.

16) Þessi reglugerð á ekki við um vernd grundvallarréttinda og mannfrelsis eða frjálst flæði persónuupplýsinga í tengslum við starfsemi sem fellur utan gildissviðs laga Sambandsins, s.s. starfsemi er varðar þjóðaröryggi. Þessi reglugerð á ekki við um vinnslu aðildarríkjanna á persónuupplýsingum vegna starfsemi í tengslum við sameiginlega stefnu Sambandsins í utanríkis- og öryggismálum.

17) Reglugerð Evrópuþingsins og ráðsins (EB) nr. 45/2001 ([2]) gildir um vinnslu stofnana, aðila, skrifstofa og sérstofnana Sambandsins á persónuupplýsingum. Laga ætti reglugerð (EB) nr. 45/2001 og aðrar réttargerðir Sambandsins, sem eiga við um slíka vinnslu persónuupplýsinga, að þeim meginreglum og reglum sem komið er á með þessari reglugerð og beitt er í ljósi þessarar reglugerðar. Í því skyni að setja öflugan og samræmdan ramma um persónuvernd í Sambandinu ættu nauðsynlegar aðlaganir á reglugerð (EB) nr. 45/2001 að fylgja í kjölfar samþykktar þessarar reglugerðar til þess að þær geti komið til framkvæmda á sama tíma og hún.

18) Þessi reglugerð á ekki við um vinnslu einstaklings á persónuupplýsingum ef hún er einungis í þágu hans sjálfs eða fjölskyldu hans og hefur þannig engin tengsl við atvinnu- eða viðskiptastarfsemi. Vinnsla, sem er einungis í þágu

([1]) Tilmæli framkvæmdastjórnarinnar frá 6. maí 2003 um skilgreininguna á örfyrirtækjum, litlum fyrirtækjum og meðalstórum fyrirtækjum (Stjtíð. ESB L 124, 20.5.2003, bls. 36).

([2]) Reglugerð Evrópuþingsins og ráðsins (EB) nr. 45/2001 frá 18. desember 2000 um vernd einstaklinga í tengslum við vinnslu persónuupplýsinga, sem stofnanir og aðilar Bandalagsins hafa unnið, og um frjálsa miðlun slíkra upplýsinga (Stjtíð. EB L 8, 12.1.2001, bls. 1).

einstaklings eða fjölskyldu hans, getur t.d. tekið til bréfaskrifta og þess að halda skrár yfir heimilisföng, notkunar samfélagsmiðla og Netnotkunar sem fram fer í tengslum við slíka vinnslu. Hins vegar á þessi reglugerð við um ábyrgðaraðila eða vinnsluaðila sem setja fram leiðir til að vinna persónuupplýsingar í þágu einstaklings eða fjölskyldu hans.

19) Vernd einstaklinga að því er varðar vinnslu lögbærra yfirvalda á persónuupplýsingum í þeim tilgangi að koma í veg fyrir, rannsaka, koma upp um eða saksækja fyrir refsiverð brot eða fullnægja refsiviðurlögum, þ.m.t. að vernda gegn og koma í veg fyrir ógnir við almannaöryggi og frjálsa miðlun slíkra upplýsinga, er efni í sérstaka réttargerð Sambandsins. Þessi reglugerð ætti því ekki að gilda um vinnslustarfsemi í þessum tilgangi. Persónuupplýsingar, sem opinber yfirvöld taka til vinnslu samkvæmt þessari reglugerð, ættu hins vegar að heyra undir sértækari réttargerð Sambandsins þegar þær eru notaðar í þessum tilgangi, þ.e. tilskipun Evrópuþingsins og ráðsins (ESB) 2016/680 ([1]). Aðildarríkin geta falið lögbærum yfirvöldum í skilningi tilskipunar (ESB) 2016/680 verkefni, sem ekki eru endilega unnin í þeim tilgangi að koma í veg fyrir, rannsaka, koma upp um eða saksækja fyrir refsiverð brot eða fullnægja refsiviðurlögum, þ.m.t. að vernda gegn og koma í veg fyrir ógnir við almannaöryggi, þannig að vinnsla persónuupplýsinga í þessum öðrum tilgangi falli, að svo miklu leyti sem hún fellur undir lög Sambandsins, innan gildissviðs þessarar reglugerðar.

Að því er varðar vinnslu þessara lögbæru yfirvalda á persónuupplýsingum í þeim tilgangi sem fellur innan gildissviðs þessarar reglugerðar ætti aðildarríkjunum að vera heimilt að viðhalda eða innleiða sértækari ákvæði til að aðlaga beitingu reglna þessarar reglugerðar. Í slíkum ákvæðum mætti tilgreina nánar sértækar kröfur um vinnslu þessara lögbæru yfirvalda á persónuupplýsingum í þessum öðrum tilgangi, með hliðsjón af stjórnskipan, stjórnskipulagi og skipulagi stjórnsýslu í viðkomandi aðildarríki. Þegar vinnsla einkaaðila á persónuupplýsingum fellur innan gildissviðs þessarar reglugerðar ætti hún að veita aðildarríkjunum kost á að takmarka að lögum, við sérstakar aðstæður, tilteknar skyldur og réttindi þegar slík takmörkun telst nauðsynleg og hófleg ráðstöfun í lýðræðisþjóðfélagi til að standa vörð um tiltekna mikilvæga hagsmuni, m.a. almannaöryggi, og koma í veg fyrir, rannsaka, koma upp um eða saksækja fyrir refsiverð brot eða fullnægja refsiviðurlögum, þ.m.t. að vernda gegn og koma í veg fyrir ógnir við almannaöryggi. Þetta á m.a. við innan ramma baráttu gegn peningaþvætti eða í starfsemi réttarrannsóknarstofa.

20) Enda þótt þessi reglugerð gildi m.a. um starfsemi dómstóla og annarra dómsyfirvalda mætti í lögum Sambandsins eða lögum aðildarríkis tilgreina vinnsluaðgerðir og verklagsreglur í tengslum við vinnslu dómstóla og annarra dómsyfirvalda á persónuupplýsingum. Til að standa vörð um sjálfstæði dómskerfisins við framkvæmd verkefna þess á sviði dómsmála, m.a. ákvarðanatöku, ætti valdsvið eftirlitsyfirvalda ekki að ná til vinnslu dómstóla á persónuupplýsingum þegar þeir fara með dómsvald sitt. Mögulegt ætti að vera að fela eftirlit með slíkri gagnavinnslu sérstökum aðilum innan dómskerfis aðildarríkisins sem ættu einkum að tryggja að farið sé að reglum þessarar reglugerðar, efla vitund dómara um skyldur sínar samkvæmt henni og annast meðferð kvartana í tengslum við slíka gagnavinnslu.

21) Þessi reglugerð hefur ekki áhrif á beitingu tilskipunar Evrópuþingsins og ráðsins 2000/31/EB ([2]), einkum reglur í 12.-15. gr. hennar um bótaábyrgð þjónustuveitenda sem eru milliliðir. Með þeirri tilskipun er leitast við að stuðla að eðlilegri starfsemi innri markaðarins með því að tryggja frjálsa þjónustustarfsemi milli aðildarríkjanna á sviði upplýsingasamfélagsins.

22) Hvers kyns vinnsla persónuupplýsinga í tengslum við starfsemi starfsstöðvar ábyrgðaraðila eða vinnsluaðila í Sambandinu ætti að fara fram í samræmi við þessa reglugerð, án tillits til þess hvort vinnslan sjálf fer fram í Sambandinu. Með staðfestu er átt við virka og raunverulega starfsemi með föstu fyrirkomulagi. Lögákveðið rekstrarform slíks fyrirkomulags, hvort sem um er að ræða útibú eða dótturfélag með réttarstöðu lögaðila, ræður ekki úrslitum að því er þetta varðar.

([1]) Tilskipun Evrópuþingsins og ráðsins (ESB) 2016/680 frá 27. apríl 2016 um vernd einstaklinga að því er varðar vinnslu lögbærra yfirvalda á persónuupplýsingum í tengslum við að koma í veg fyrir, rannsaka, koma upp um eða saksækja fyrir refsiverð brot eða fullnægja refsiviðurlögum og frjálsa miðlun slíkra upplýsinga og um niðurfellingu rammaákvörðunar ráðsins 2008/977/DIM (Stjtíð. ESB L 119, 4.5.2016, bls. 89).

([2]) Tilskipun Evrópuþingsins og ráðsins 2000/31/EB frá 8. júní 2000 um tiltekna lagalega þætti þjónustu, einkum rafrænna viðskipta, í tengslum við upplýsingasamfélagið á innri markaðnum (tilskipun um rafræn viðskipti) (Stjtíð. EB L 178, 17.7.2000, bls. 1).

23) Til að tryggja að einstaklingar séu ekki sviptir þeirri vernd, sem þeir eiga rétt á samkvæmt þessari reglugerð, ætti vinnsla ábyrgðaraðila eða vinnsluaðila, sem ekki hefur staðfestu í Sambandinu, á persónuupplýsingum um skráða einstaklinga, sem eru í Sambandinu, að heyra undir þessa reglugerð ef vinnslustarfsemin tengist því að bjóða hinum skráðu vörur eða þjónustu, án tillits til þess hvort það er gegn greiðslu. Til að ákvarða hvort slíkur ábyrgðaraðili eða vinnsluaðili bjóði skráðum einstaklingum í Sambandinu vörur og þjónustu ætti að ganga úr skugga um hvort ljóst sé að ábyrgðaraðilinn eða vinnsluaðilinn hafi í hyggju að bjóða skráðum einstaklingum þjónustu í einu eða fleiri aðildarríkjum Sambandsins. Enda þótt aðgangurinn einn og sér að vefsetri ábyrgðaraðila, vinnsluaðila eða milliliðar í Sambandinu, netfangi hans eða öðrum upplýsingum um hvernig megi nálgast viðkomandi, eða notkun tungumáls, sem almennt er notað í þriðja landinu þar sem ábyrgðaraðili hefur staðfestu, nægi ekki til að staðfesta að um slíka fyrirætlan sé að ræða, geta þættir eins og að nota tungumál eða gjaldmiðil, sem er almennt notaður í einu eða fleiri aðildarríkjum, og möguleikinn á að panta vörur og þjónustu á því tungumáli eða að nefna viðskiptavini eða notendur í Sambandinu, gert það ljóst að ábyrgðaraðili hefur í hyggju að bjóða skráðum einstaklingum í Sambandinu vörur eða þjónustu.

24) Vinnsla ábyrgðaraðila eða vinnsluaðila, sem ekki hefur staðfestu í Sambandinu, á persónuupplýsingum um skráða einstaklinga, sem eru í Sambandinu, ætti einnig að falla undir þessa reglugerð ef hún tengist því að vakta hegðun hinna skráðu, að því marki sem slík hegðun á sér stað innan Sambandsins. Til að ákvarða hvort vinnslustarfsemi geti talist vera vöktun á hegðun skráðra einstaklinga ætti að ganga úr skugga um hvort slóð einstaklinga sé rakin á Netinu, m.a. hvort í kjölfarið séu notaðar vinnsluaðferðir á persónuupplýsingum sem felast í gerð persónusniðs um einstakling, einkum í því skyni að taka ákvarðanir varðandi viðkomandi eða til að greina eða spá fyrir um smekk hans, hegðun og viðhorf.

25) Þegar lög aðildarríkis gilda í krafti þjóðaréttar ætti þessi reglugerð einnig að gilda um ábyrgðaraðila sem hefur ekki staðfestu í Sambandinu, s.s. í sendiskrifstofu eða ræðisstofnun aðildarríkis.

26) Meginreglur um persónuvernd ættu að gilda um hvers kyns upplýsingar varðandi persónugreindan eða persónugreinanlegan einstakling. Persónuupplýsingar sem hafa verið færðar undir gerviauðkenni, sem kann að vera hægt að rekja til einstaklings með notkun viðbótarupplýsinga, skulu teljast upplýsingar um persónugreinanlegan einstakling. Til þess að ákvarða hvort einstaklingur er persónugreinanlegur ætti að taka mið af öllum þeim aðferðum sem ástæða er til að ætla að annaðhvort ábyrgðaraðili eða annar aðili geti beitt til að bera kennsl á viðkomandi einstakling með beinum eða óbeinum hætti. Til að ganga úr skugga um hvort fremur líklegt megi telja að aðferðum verði beitt til að bera kennsl á einstakling ætti að taka tillit til allra hlutlægra þátta, s.s. kostnaðar við það og þess tíma sem það tæki, að teknu tilliti til þeirrar tækni sem fyrir hendi er þegar vinnslan fer fram og til tækniþróunar. Meginreglur um persónuvernd ættu því ekki að eiga við um nafnlausar upplýsingar, þ.e. upplýsingar sem tengjast ekki persónugreindum eða persónugreinanlegum einstaklingi, eða persónuupplýsingar sem hafa verið aftengdar persónuauðkennum þannig að ekki er lengur unnt að persónugreina hinn skráða. Þessi reglugerð varðar því ekki vinnslu slíkra nafnlausra upplýsinga, s.s. í tölfræðilegum tilgangi eða vegna rannsókna.

27) Þessi reglugerð á ekki við um persónuupplýsingar látinna einstaklinga. Aðildarríkjunum er heimilt að kveða á um reglur um vinnslu persónuupplýsinga látinna einstaklinga.

28) Notkun gerviauðkenna fyrir persónuupplýsingar getur dregið úr áhættu viðkomandi skráðra einstaklinga og auðveldað ábyrgðaraðilum og vinnsluaðilum að uppfylla persónuverndarskyldur sínar. Sérstakri innleiðingu á „notkun gerviauðkenna“ í þessari reglugerð er ekki ætlað að útiloka aðrar persónuverndarráðstafanir.

29) Til þess að skapa hvata til notkunar gerviauðkenna við vinnslu persónuupplýsinga ættu ráðstafanir vegna gerviauðkennanotkunar, sem leyfa jafnframt almenna greiningu, að vera mögulegar hjá sama ábyrgðaraðila þegar hann hefur gert nauðsynlegar tæknilegar og skipulagslegar ráðstafanir til að tryggja, vegna viðkomandi vinnslu, að þessari reglugerð sé komið til framkvæmda og að viðbótarupplýsingum, sem gera það kleift að rekja persónuupplýsingarnar til tiltekins skráðs einstaklings, sé haldið aðgreindum. Ábyrgðaraðili, sem vinnur persónuupplýsingarnar, ætti að gefa upp hvaða aðilar í starfsemi hans hafa tilskildar heimildir.

30) Tæki og tól, forrit og samskiptareglur, sem einstaklingar nota, geta tengt Netauðkenni við þá, s.s. IP-tölur (e. internet protocol addresses), smygildaauðkenni (e. cookie identifiers) eða önnur auðkenni, s.s. fjarskiptatíðniauðkenningar. Þetta getur skilið eftir spor sem hægt er að nota til að útbúa persónusnið um einstaklinga og bera kennsl á þá, einkum þegar sporunum er bætt við einkvæm auðkenni og aðrar upplýsingar sem berast netþjónum.

31) Ekki ætti að líta á opinber yfirvöld, sem fá í hendur persónuupplýsingar á grundvelli lagaskyldu í tengslum við opinber störf sín, s.s. skatta- og tollyfirvöld, einingar sem fara með rannsóknir á sviði fjármála, sjálfstæð stjórnsýsluyfirvöld eða yfirvöld fjármálamarkaða, sem bera ábyrgð á reglusetningu og eftirliti með verðbréfamörkuðum, sem viðtakendur ef þau fá í hendur persónuupplýsingar sem eru nauðsynlegur þáttur í tiltekinni fyrirspurn í þágu almennra hagsmuna, í samræmi við lög Sambandsins eða lög aðildarríkis. Beiðnir opinberra yfirvalda um afhendingu upplýsinga ættu ætíð að vera skriflegar, rökstuddar og tilvikabundnar og ættu ekki að varða skráningarkerfi í heild eða leiða til samtengingar á milli skráningarkerfa. Vinnsla þessara opinberu yfirvalda á persónuupplýsingum ætti að samrýmast gildandi reglum um persónuvernd samkvæmt tilgangi vinnslunnar.

32) Veita ætti samþykki með skýrri staðfestingu, s.s. skriflegri yfirlýsingu, þ.m.t. með rafrænum hætti, eða munnlegri yfirlýsingu, á því að fyrir liggi óþvinguð, afmörkuð, upplýst og ótvíræð viljayfirlýsing hins skráða um að hann samþykki vinnslu persónuupplýsinga sem varða hann sjálfan. Þetta gæti falið í sér að haka við reit þegar farið er inn á vefsetur á Netinu, velja tæknilegar stillingar fyrir þjónustu í upplýsingasamfélaginu eða aðra yfirlýsingu eða athöfn sem gefur skýrt til kynna í þessu samhengi að skráður einstaklingur samþykki fyrirhugaða vinnslu á persónuupplýsingum um sig. Þögn, reitir sem þegar er búið að haka við eða aðgerðarleysi ættu því ekki að fela í sér samþykki. Samþykki ætti að ná til allrar vinnslustarfsemi sem fram fer í sama tilgangi, einum eða fleiri. Þegar vinnslan er í margvíslegum tilgangi ætti að gefa samþykki fyrir hverjum og einum þeirra. Ef hinn skráði á að veita samþykki sitt við rafrænni beiðni verður beiðnin að vera skýr og skilmerkileg og má ekki raska óþarflega notkun þjónustunnar sem það er veitt fyrir.

33) Oft er ekki hægt að greina tilgang með vinnslu persónuupplýsinga í þágu vísindarannsókna að fullu þegar upplýsingunum er safnað. Því ættu skráðir einstaklingar að geta gefið samþykki sitt fyrir tilteknum sviðum vísindarannsókna þegar þær samrýmast viðurkenndum, siðferðislegum viðmiðunum fyrir vísindarannsóknir. Skráðir einstaklingar ættu að hafa tækifæri til að veita samþykki sitt einungis á tilteknum sviðum rannsókna eða fyrir hlutum rannsóknarverkefna, að því marki sem fyrirhugaður tilgangur leyfir.

34) Skilgreina ætti erfðafræðilegar upplýsingar sem persónuupplýsingar sem varða arfgenga eða áunna erfðaeiginleika einstaklings, sem fást með greiningu á líffræðilegu sýni frá viðkomandi einstaklingi, einkum litningagreiningu, greiningu á deoxýríbósakjarnsýru (DNA) eða ríbósakjarnsýru (RNA), eða með greiningu á öðrum þætti sem gerir kleift að fá fram jafngildar upplýsingar.

35) Persónuupplýsingar sem varða heilsufar ættu að taka til allra gagna tengdra heilsufari skráðs einstaklings og veita upplýsingar um líkamlegt eða andlegt heilsufar hans í fortíð, nútíð eða framtíð. Þar á meðal eru upplýsingar um einstaklinginn sem safnað er við skráningu hans vegna heilbrigðisþjónustu eða við veitingu hennar, eins og um getur í tilskipun Evrópuþingsins og ráðsins 2011/24/ESB ([1]); númer, tákn eða atriði sem einstaklingi er úthlutað til að auðkenna hann með einkvæmum hætti í tengslum við heilsufar; upplýsingar sem má rekja til prófunar eða rannsóknar á líkamshluta eða líkamsefni, þ.m.t. erfðafræðilegar upplýsingar og líffræðileg sýni; og hvers kyns upplýsingar um t.d. sjúkdóm, fötlun, hættu á sjúkdómi, heilsufarssögu, klíníska meðferð eða lífeðlisfræðilegt eða líf- og læknisfræðilegt ástand hins skráða, án tillits til uppruna þeirra, s.s. hvort sem þær koma frá lækni eða öðrum heilbrigðisstarfsmanni, sjúkrahúsi, úr lækningatæki eða með greiningarprófun í glasi.

36) Höfuðstöðvar ábyrgðaraðila í Sambandinu ættu að vera sá staður þar sem hann hefur yfirstjórn sína í Sambandinu nema ákvarðanir um tilgang með og aðferðir við vinnslu persónuupplýsinga séu teknar í annarri starfsstöð ábyrgðaraðila í Sambandinu en í því tilviki ætti síðarnefnda starfsstöðin að teljast vera höfuðstöðvar. Ákvarða ætti hverjar höfuðstöðvar

([1]) Tilskipun Evrópuþingsins og ráðsins 2011/24/ESB frá 9. mars 2011 um réttindi sjúklinga varðandi heilbrigðisþjónustu yfir landamæri (Stjtíð. ESB L 88, 4.4.2011, bls. 45).

ábyrgðaraðila eru í Sambandinu í samræmi við hlutlægar viðmiðanir og ætti þar að fara fram virk og raunveruleg stjórnun með föstu fyrirkomulagi þar sem helstu ákvarðanir eru teknar um tilgang og aðferðir við vinnsluna. Sú viðmiðun ætti ekki að velta á því hvort vinnsla persónuupplýsinga fer fram á þeim stað. Tilvist og notkun nauðsynlegra tæknilegra aðferða og tækni við vinnslu persónuupplýsinga eða vinnslustarfsemi jafngildir ekki höfuðstöðvum í sjálfu sér og er því ekki ákvarðandi viðmiðun um hvað telst vera höfuðstöðvar. Höfuðstöðvar vinnsluaðila ættu að vera sá staður þar sem hann hefur yfirstjórn sína í Sambandinu eða, hafi hann enga yfirstjórn í Sambandinu, sá staður þar sem helsta vinnslustarfsemi fer fram í Sambandinu. Í tilvikum þar sem bæði ábyrgðaraðili og vinnsluaðili koma við sögu ætti leiðandi lögbært eftirlitsyfirvald áfram að vera eftirlitsyfirvald aðildarríkisins þar sem ábyrgðaraðili hefur höfuðstöðvar sínar en eftirlitsyfirvald vinnsluaðila ætti að teljast hlutaðeigandi eftirlitsyfirvald og það eftirlitsyfirvald ætti að taka þátt í samstarfsferlinu sem kveðið er á um í þessari reglugerð. Þó ættu eftirlitsyfirvöld aðildarríkis eða aðildarríkja þar sem vinnsluaðili hefur eina starfsstöð eða fleiri aldrei að teljast hlutaðeigandi eftirlitsyfirvöld ef drög að ákvörðun varða einungis ábyrgðaraðilann. Ef fyrirtækjasamstæða annast vinnsluna ættu höfuðstöðvar ráðandi fyrirtækis að teljast höfuðstöðvar samstæðunnar nema ákvarðanataka um tilgang og aðferðir við vinnslu persónuupplýsinganna sé á hendi annars fyrirtækis.

37) Fyrirtækjasamstæða ætti að taka til ráðandi fyrirtækis og undirfyrirtækja þess þar sem ráðandi fyrirtækið ætti að vera það fyrirtæki sem hefur ráðandi áhrif á hin fyrirtækin, s.s. í krafti eignarhalds, fjárhagslegrar þátttöku eða reglna sem gilda um fyrirtækið eða valds til að koma reglum um vernd persónuupplýsinga til framkvæmda. Fyrirtæki, sem stjórnar vinnslu persónuupplýsinga í fyrirtækjum sem eru í eignartengslum við það, ætti, ásamt þeim fyrirtækjum, að teljast fyrirtækjasamstæða.

38) Persónuupplýsingar barna ættu að njóta sérstakrar verndar þar sem þau kunna að vera síður meðvituð um áhættu, afleiðingar og viðkomandi verndarráðstafanir og réttindi sín í tengslum við vinnslu persónuupplýsinga. Þessi sérstaka vernd ætti einkum að eiga við um notkun persónuupplýsinga barna í markaðssetningarskyni eða þegar búin eru til persónu- eða notendasnið og um söfnun persónuupplýsinga er varða börn þegar þau nota þjónustu sem börnum er boðin beint. Samþykki forsjáraðila ætti ekki að vera nauðsynlegt þegar um er að ræða forvarnar- eða ráðgjafarþjónustu sem barni er boðin beint.

39) Hvers kyns vinnsla persónuupplýsinga ætti að vera lögmæt og sanngjörn. Það ætti að vera einstaklingum ljóst þegar persónuupplýsingum um þá er safnað, þær eru notaðar, skoðaðar eða unnar á annan hátt, og að hvaða marki persónuupplýsingar eru eða munu verða unnar. Meginreglan um gagnsæi krefst þess að hvers kyns upplýsingar og samskipti, sem tengjast vinnslu þessara persónuupplýsinga, séu auðveldlega aðgengileg og auðskiljanleg og á skýru og einföldu máli. Sú meginregla á einkum við um upplýsingar til skráðra einstaklinga um það hver ábyrgðaraðilinn er og tilganginn með vinnslunni og frekari upplýsingar til að tryggja sanngjarna og gagnsæja vinnslu gagnvart viðkomandi einstaklingum og rétt þeirra til að fá staðfestingu og tilkynningu um vinnslu á persónuupplýsingum um sig. Gera ætti einstaklingum ljósa áhættu, reglur, verndarráðstafanir og réttindi í tengslum við vinnslu persónuupplýsinga og hvernig þeir geta neytt réttar síns í tengslum við slíka vinnslu. Einkum ætti tilgangurinn með vinnslu persónuupplýsinganna að vera skýr og lögmætur og liggja fyrir við söfnun þeirra. Persónuupplýsingarnar ættu að vera nægilegar, viðeigandi og takmarkaðar við það sem nauðsynlegt er miðað við tilganginn með vinnslunni. Þetta krefst þess einkum að geymslutími persónuupplýsinganna sé takmarkaður við algjört lágmark. Því aðeins ætti að vinna persónuupplýsingar að ekki sé unnt að ná tilganginum með vinnslunni á annan aðgengilegan hátt. Til að tryggja að persónuupplýsingar séu ekki varðveittar lengur en nauðsynlegt er ætti ábyrgðaraðilinn að setja tímafresti varðandi eyðingu eða reglulega endurskoðun þeirra. Gera verður hóflegar ráðstafanir til að tryggja að óáreiðanlegar persónuupplýsingar verði leiðréttar eða þeim eytt. Vinnsla persónuupplýsinga ætti að vera með þeim hætti að viðeigandi öryggi og trúnaður um upplýsingarnar sé tryggt, m.a. að komið sé í veg fyrir óheimilan aðgang eða notkun á persónuupplýsingum og þeim búnaði sem notaður er við vinnsluna.

40) Til að vinnsla persónuupplýsinga teljist lögmæt ætti hún að fara fram með samþykki hlutaðeigandi skráðs einstaklings eða á einhverjum öðrum lögmætum grundvelli, sem mælt er fyrir um í lögum, annaðhvort í þessari reglugerð eða í

öðrum lögum Sambandsins eða lögum aðildarríkis, eins og um getur í þessari reglugerð, þ. á m. þegar hún er nauðsynleg til að fara að ákvæðum um lagaskyldu sem hvílir á ábyrgðaraðilanum eða vegna framkvæmdar samnings sem hinn skráði á aðild að eða með hliðsjón af ráðstöfunum sem eru gerðar að beiðni hans áður en samningur er gerður.

41) Þegar vísað er til lagagrundvallar eða löggjafarráðstöfunar í þessari reglugerð er ekki endilega gerð sú krafa að þing samþykki lagagerð, með fyrirvara um kröfur samkvæmt stjórnskipan hlutaðeigandi aðildarríkis. Slíkur lagagrundvöllur eða löggjafarráðstöfun ætti þó að vera skýr og nákvæm og beitingin fyrirsjáanleg þeim sem falla þar undir, eins og krafist er í dómaframkvæmd Evrópudómstólsins („Dómstólsins“) og Mannréttindadómstóls Evrópu.

42) Þegar vinnsla er byggð á samþykki skráðs einstaklings ætti ábyrgðaraðilinn að geta sýnt fram á að hinn skráði hafi samþykkt vinnsluaðgerðina. Verndarráðstafanir ættu að tryggja, einkum í tengslum við skriflega yfirlýsingu um annað málefni, að hinum skráða sé kunnugt um að samþykki hafi verið veitt og að hvaða marki. Í samræmi við tilskipun ráðsins 93/13/EB ([1]) ætti ábyrgðaraðilinn að setja fram yfirlýsingu um samþykki á skiljanlegu og aðgengilegu formi og á skýru og einföldu máli sem ætti ekki að fela í sér óréttmæta skilmála. Til þess að samþykki teljist upplýst ætti skráður einstaklingur að vita deili á a.m.k. ábyrgðaraðilanum og vera kunnugt um tilgang þeirrar vinnslu sem persónuupplýsingunum er ætlað að þjóna. Ekki ætti að telja að samþykki hafi verið veitt af fúsum og frjálsum vilja ef hinn skráði hefur ekki raunverulegt eða frjálst val eða getur ekki neitað eða dregið til baka samþykki án þess að verða fyrir tjóni.

43) Til þess að tryggja að samþykki sé veitt af fúsum og frjálsum vilja ætti það ekki að teljast gildur lagagrundvöllur fyrir vinnslu persónuupplýsinga í tilteknu tilviki þar sem skýr aðstöðumunur er milli hins skráða og ábyrgðaraðilans, einkum þegar ábyrgðaraðilinn er opinbert yfirvald og því ólíklegt að samþykki hafi verið veitt af fúsum og frjálsum vilja við allar aðstæður í því tiltekna tilviki. Samþykki telst ekki veitt af fúsum og frjálsum vilja ef ekki er hægt að veita sérstakt samþykki fyrir aðskildum aðgerðum við vinnslu persónuupplýsinga, þótt slíkt ætti við í því einstaka tilviki, eða ef framkvæmd samnings, m.a. veiting þjónustu, er komin undir samþykkinu þótt samþykkið sé ekki nauðsynlegt vegna framkvæmdar samningsins.

44) Vinnsla ætti að teljast lögmæt þegar hún er nauðsynleg í tengslum við samning eða fyrirætlun um að gera samning.

45) Þegar vinnsla fer fram í samræmi við lagaskyldu sem hvílir á ábyrgðaraðilanum eða er nauðsynleg vegna verkefnis sem unnið er í þágu almannahagsmuna eða við beitingu opinbers valds ætti vinnslan að byggjast á lögum Sambandsins eða lögum aðildarríkis. Þess er ekki krafist í þessari reglugerð að sett verði sérstök lög um hverja einstaka vinnslu. Það kann að vera nægilegt að hafa lög sem grundvöll fyrir ýmsum vinnsluaðgerðum, sem byggjast á lagaskyldu sem hvílir á ábyrgðaraðilanum, eða þegar vinnslan er nauðsynleg vegna verkefnis sem unnið er í þágu almannahagsmuna eða við beitingu opinbers valds. Einnig ættu lög Sambandsins eða lög aðildarríkis að ákvarða tilgang vinnslunnar. Í þeim lögum mætti enn fremur tilgreina almenn skilyrði þessarar reglugerðar um lögmæta vinnslu persónuupplýsinga og hvernig skuli ákvarða hver ábyrgðaraðilinn er, hvaða tegund persónuupplýsinga unnið verður með, þá skráðu einstaklinga sem í hlut eiga, hvaða aðilar mega fá persónuupplýsingarnar, hvaða takmarkanir eiga við vegna tilgangs, varðveislutímabil og aðrar ráðstafanir til að tryggja að vinnslan fari fram á lögmætan og sanngjarnan hátt. Einnig ætti að ákvarða í lögum Sambandsins eða lögum aðildarríkis hvort ábyrgðaraðili, sem annast framkvæmd verkefnis sem er unnið í þágu almannahagsmuna eða við beitingu opinbers valds, ætti að vera opinbert yfirvald eða annar einstaklingur eða lögaðili sem fellur undir opinberan rétt eða, þegar slíkt er í þágu almannahagsmuna, m.a. heilbrigðismála á borð við lýðheilsu og félagslega vernd og við stjórnun heilbrigðisþjónustu, undir einkarétt, s.s. fagfélag.

46) Einnig verður að telja vinnslu persónuupplýsinga lögmæta ef hún er nauðsynleg til að vernda hagsmuni sem skipta sköpum fyrir líf skráðs einstaklings eða annars einstaklings. Vinnsla persónuupplýsinga á grundvelli brýnna hagsmuna

([1]) Tilskipun ráðsins 93/13/EBE frá 5. apríl 1993 um óréttmæta skilmála í neytendasamningum (Stjtíð. EB L 95, 21.4.1993, bls. 29).

annars einstaklings ætti að meginreglu til aðeins að fara fram þegar greinilegt er að hún getur ekki byggst á öðrum lagagrundvelli. Sumar tegundir vinnslu geta bæði þjónað mikilvægum almannahagsmunum og brýnum hagsmunum skráðs einstaklings, t.d. þegar vinnsla er nauðsynleg í mannúðarskyni, s.s. við að fylgjast með farsóttum og útbreiðslu þeirra eða vegna neyðarástands sem kallar á mannúðaraðstoð, einkum þegar um er að ræða náttúruhamfarir eða stóráföll af mannavöldum.

47) Lögmætir hagsmunir ábyrgðaraðila, þ.m.t. hagsmunir ábyrgðaraðila sem fá persónuupplýsingarnar í hendur, eða þriðja aðila geta verið lagagrundvöllur fyrir vinnslu þeirra, að því tilskildu að hagsmunir eða grundvallarréttindi og frelsi hins skráða vegi ekki þyngra, að teknu tilliti til eðlilegra væntinga skráðra einstaklinga á grundvelli tengsla þeirra við ábyrgðaraðilann. Um lögmæta hagsmuni gæti m.a. verið að ræða þegar viðeigandi tengsl sem máli skipta eru milli hins skráða og ábyrgðaraðilans, t.d. í tilvikum þar sem hinn skráði er viðskiptavinur ábyrgðaraðilans eða í þjónustu hans. Hvað sem öðru líður þyrfti að meta af kostgæfni hvort um lögmæta hagsmuni er að ræða, m.a. hvort skráður einstaklingur getur, þegar söfnun persónuupplýsinganna fer fram og í samhengi við hana, haft gilda ástæðu til að ætla að vinnsla muni fara fram í þeim tilgangi. Hagsmunir hins skráða og grundvallarréttindi hans gætu einkum gengið framar hagsmunum ábyrgðaraðila gagna þegar vinnsla persónuupplýsinga fer fram við aðstæður þar sem skráðir einstaklingar hafa ekki ástæðu til að ætla að um frekari vinnslu verði að ræða. Að því gefnu að það sé í höndum löggjafans að kveða á um lagagrundvöll vegna vinnslu opinberra yfirvalda á persónuupplýsingum ætti sá lagagrundvöllur ekki að eiga við um vinnslu opinberra yfirvalda þegar þau sinna verkefnum sínum. Vinnsla persónuupplýsinga, sem er beinlínis nauðsynleg í þeim tilgangi að koma í veg fyrir svik, telst einnig til lögmætra hagsmuna hlutaðeigandi ábyrgðaraðila gagna. Líta má svo á að vinnsla persónuupplýsinga vegna beinnar markaðssetningar sé í þágu lögmætra hagsmuna.

48) Ábyrgðaraðilar, sem eru hluti af fyrirtækjasamstæðu eða stofnunum sem tengjast miðlægri stofnun, geta haft lögmæta hagsmuni af því að miðla persónuupplýsingum innan fyrirtækjasamstæðunnar í þágu innri stjórnunar, m.a. vegna vinnslu persónuupplýsinga um viðskiptavini eða starfsmenn. Þetta hefur engin áhrif á almennar meginreglur um miðlun persónuupplýsinga, innan fyrirtækjasamstæðu, til fyrirtækis sem er staðsett í þriðja landi.

49) Vinnsla persónuupplýsinga, að því marki sem hún er beinlínis nauðsynleg og hófleg til að tryggja net- og upplýsingaöryggi, þ.e. getu nets eða upplýsingakerfis til að standast, á tilteknu öryggisstigi, atburði sem verða fyrir slysni eða aðgerðir sem eru ólögmætar eða skaðlegar og stofna í hættu aðgengileika, sannvottuðum uppruna, heilleika og leynd vistaðra eða sendra persónuupplýsinga, og öryggi tengdrar þjónustu sem boðin er eða er aðgengileg um þessi net og kerfi, af hálfu opinberra yfirvalda, viðbragðsteymis vegna neyðartilvika er varða tölvuöryggi (CERT), viðbragðsteymis vegna váatvika er varða tölvuöryggi (CSIRT), þeirra sem reka rafræn fjarskiptanet og -þjónustu og þeirra sem útvega öryggistækni og -þjónustu, telst til lögmætra hagsmuna hlutaðeigandi ábyrgðaraðila gagna. Þetta gæti t.d. falið í sér að komið sé í veg fyrir óheimilan aðgang að rafrænum fjarskiptanetum og dreifingu spilliforrita og til að stöðvaðar séu atlögur að þjónustumiðlun (e. „denial of service“ attacks) og skemmdir á tölvum og rafrænum fjarskiptakerfum.

50) Heimila ætti vinnslu persónuupplýsinga í öðrum tilgangi en þeim sem var upphaflega markmiðið með söfnun þeirra því aðeins að vinnslan samrýmist þeim tilgangi sem var forsenda söfnunarinnar í upphafi. Í því tilviki er ekki krafist annars lagagrundvallar en þess sem heimilaði söfnun persónuupplýsinganna. Ef vinnslan er nauðsynleg vegna verkefnis sem unnið er í þágu almannahagsmuna eða við beitingu opinbers valds, sem ábyrgðaraðili fer með, má í lögum Sambandsins eða lögum aðildarríkis ákvarða og tilgreina hvenær frekari vinnsla telst samrýmanleg og lögmæt með tilliti til tiltekinna verkefna og tilgangs. Frekari vinnsla vegna skjalavistunar í þágu almannahagsmuna, rannsókna á sviði vísinda eða sagnfræði eða í tölfræðilegum tilgangi ætti að teljast til samrýmanlegra, lögmætra vinnsluaðgerða. Lagagrundvöllur samkvæmt lögum Sambandsins eða lögum aðildarríkis vegna vinnslu persónuupplýsinga getur einnig verið lagagrundvöllur frekari vinnslu. Til þess að ganga úr skugga um hvort tilgangur með frekari vinnslu samrýmist þeim tilgangi sem var forsenda söfnunarinnar í upphafi ætti ábyrgðaraðilinn, þegar hann hefur fullnægt öllum kröfum um lögmæti vinnslunnar í upphafi, að taka tillit til m.a.: hvers kyns tengsla milli þessa tilgangs og tilgangsins með fyrirhugaðri frekari vinnslu, þess í hvaða samhengi persónuupplýsingunum var safnað, einkum eðlilegra væntinga

skráðra einstaklinga um frekari notkun þeirra á grundvelli tengsla þeirra við ábyrgðaraðilann, eðlis persónuupplýsinganna, afleiðinga fyrirhugaðrar frekari vinnslu þeirra fyrir skráða einstaklinga og þess hvort viðeigandi verndarráðstafanir hafi verið eða séu gerðar, bæði í upphaflegu vinnsluaðgerðunum og fyrirhuguðum frekari aðgerðum.

Þegar skráður einstaklingur hefur veitt samþykki sitt eða vinnslan byggist á lögum Sambandsins eða lögum aðildarríkis, sem fela í sér nauðsynlega og hóflega ráðstöfun í lýðræðisþjóðfélagi og sem er einkum ætlað að standa vörð um mikilvæg markmið sem þjóna almannahagsmunum, ætti ábyrgðaraðilanum að vera heimil frekari vinnsla persónuupplýsinganna án tillits til þess hvort tilgangurinn telst samrýmanlegur. Hvað sem öðru líður ætti að tryggja beitingu meginreglnanna sem settar eru fram í þessari reglugerð, einkum um að upplýsa hinn skráða um þennan viðbótartilgang og réttindi hans, m.a. andmælaréttinn. Ef ábyrgðaraðilinn bendir á mögulega refsiverða háttsemi eða ógnanir við almannaöryggi og sendir lögbæru yfirvaldi viðeigandi persónuupplýsingar í stökum eða fleiri tilvikum, sem snerta sama refsiverða verknað eða ógnanir við almannaöryggi, ætti að telja slíkt í þágu lögmætra hagsmuna ábyrgðaraðilans. Þó ætti að banna slíka sendingu í þágu lögmætra hagsmuna ábyrgðaraðilans eða vegna frekari vinnslu persónuupplýsinga ef vinnslan samrýmist ekki lagalegri, faglegri eða annars konar bindandi þagnarskyldu.

51) Persónuupplýsingar, sem eru í eðli sínu sérlega viðkvæmar að því er varðar grundvallarréttindi og mannfrelsi, eiga að njóta sérstakrar verndar þar sem vinnsla þeirra gæti haft í för með sér umtalsverða áhættu fyrir grundvallarréttindi og mannfrelsi. Til þessara persónuupplýsinga ætti að telja upplýsingar um kynþátt eða þjóðernislegan uppruna, en ekki ber að skilja notkun hugtaksins „kynþáttur“ í þessari reglugerð sem viðurkenningu Sambandsins á kenningum sem reyna að sanna tilvist mismunandi kynþátta manna. Ekki ætti kerfisbundið að telja vinnslu ljósmynda til vinnslu sérstakra flokka persónuupplýsinga þar sem þær falla eingöngu undir skilgreiningu á lífkennaupplýsingum þegar vinnsla þeirra fer fram með sérstakri tæknilegri aðferð sem gerir kleift að greina eða staðfesta deili á einstaklingi með ótvíræðum hætti. Vinnsla slíkra persónuupplýsinga ætti ekki að fara fram nema hún sé heimiluð í sérstökum tilvikum, eins og sett er fram í þessari reglugerð, að teknu tilliti til þess að í lögum aðildarríkjanna er heimilt að mæla fyrir um sértæk ákvæði um persónuvernd til þess að aðlaga beitingu reglna þessarar reglugerðar svo að þær samrýmist lagaskyldu eða vegna verkefnis sem unnið er í þágu almannahagsmuna eða við beitingu opinbers valds sem ábyrgðaraðili fer með. Almennar meginreglur og aðrar reglur þessarar reglugerðar ættu að gilda, auk hinna sértæku krafna vegna slíkrar vinnslu, einkum að því er varðar skilyrði fyrir lögmæti vinnslunnar. Veita ætti með skýrum hætti undanþágur frá almennu banni við vinnslu slíkra sérstakra flokka persónuupplýsinga, t.d. þegar hinn skráði gefur ótvírætt samþykki sitt eða með hliðsjón af sérstökum þörfum, einkum þegar vinnslan fer fram sem hluti af lögmætri starfsemi tiltekinna samtaka eða stofnana sem hafa það að markmiði að tryggja mannfrelsi.

52) Einnig ætti að heimila undanþágu frá banni við vinnslu sérstakra flokka persónuupplýsinga ef kveðið er á um það í lögum Sambandsins eða lögum aðildarríkis og með fyrirvara um viðeigandi verndarráðstafanir, svo að vernda megi persónuupplýsingar og önnur grundvallarréttindi, þegar það þjónar almannahagsmunum, einkum vinnslu persónuupplýsinga á sviði vinnulöggjafar, löggjafar um félagslega vernd, m.a. lífeyri, og með hliðsjón af heilbrigðisöryggi, vöktun og viðvörunum, forvörnum og vörnum gegn smitsjúkdómum og annarri alvarlegri heilsufarsógn. Heimilt er að veita slíka undanþágu af heilbrigðisástæðum, s.s. vegna lýðheilsu og stjórnunar heilbrigðisþjónustu, einkum til að tryggja gæði og kostnaðarhagkvæmni þeirra verklagsreglna sem notaðar eru við uppgjör á kröfum um bætur og þjónustu sjúkratryggingakerfisins, eða vegna skjalavistunar í þágu almannahagsmuna, rannsókna á sviði vísinda eða sagnfræði eða í tölfræðilegum tilgangi. Með undanþágu ætti líka að vera heimilt að vinna slíkar persónuupplýsingar þegar það er nauðsynlegt til að unnt sé að stofna, hafa uppi eða verja réttarkröfur, hvort heldur er fyrir dómstól eða við stjórnsýslumeðferð eða málsmeðferð utan réttar.

53) Vinnsla sérstakra flokka persónuupplýsinga, sem þurfa að njóta aukinnar verndar, ætti aðeins að fara fram í þágu heilsutengdra markmiða þegar það er nauðsynlegt til að ná þessum markmiðum í þágu einstaklinga og samfélagsins alls, einkum í tengslum við stjórnun heilbrigðis- eða félagsþjónustu og -kerfa, þ.m.t. vinnslu slíkra upplýsinga á vegum stjórnsýslunnar og miðlægra landsbundinna heilbrigðisyfirvalda í þágu gæðastýringar, gagnaumsýslu stjórnsýslunnar og almenns eftirlits með heilbrigðis- og félagsþjónustu á lands- og staðarvísu og til að tryggja samfellu í heilbrigðis- og félagsþjónustu og heilbrigðisþjónustu eða heilbrigðisöryggi yfir landamæri, vegna vöktunar og viðvörunar, eða vegna skjalavistunar í þágu almannahagsmuna, rannsókna á sviði vísinda eða sagnfræði eða í tölfræðilegum tilgangi, á grundvelli laga Sambandsins eða laga aðildarríkis, sem verða að þjóna hagsmunum almennings, sem og vegna rannsókna sem fara fram í þágu almannahagsmuna á sviði lýðheilsu. Þessi reglugerð ætti því að kveða á um samræmd skilyrði fyrir vinnslu sérstakra flokka persónuupplýsinga sem varða heilbrigðismál, með hliðsjón af sérstökum þörfum, einkum þegar vinnsla slíkra upplýsinga fer fram í þágu tiltekinna heilsutengdra markmiða af hálfu aðila sem falla undir

þagnarskyldu samkvæmt lögum. Lög Sambandsins eða lög aðildarríkis ættu að kveða á um sértækar og viðeigandi ráðstafanir til að vernda grundvallarréttindi og persónuupplýsingar einstaklinga. Aðildarríkjum ætti að vera heimilt að viðhalda eða setja frekari skilyrði, m.a. takmarkanir, að því er varðar vinnslu erfðafræðilegra upplýsinga, lífkennaupplýsinga eða heilsufarsupplýsinga. Þetta ætti þó ekki að standa í vegi fyrir frjálsu flæði persónuupplýsinga innan Sambandsins þegar þessi skilyrði eiga við um vinnslu slíkra upplýsinga yfir landamæri.

54) Vinnsla sérstakra flokka persónuupplýsinga kann að vera nauðsynleg vegna almannahagsmuna á sviði lýðheilsu án samþykkis hins skráða. Slík vinnsla ætti að vera með fyrirvara um viðeigandi og sértækar ráðstafanir til að standa vörð um réttindi og frelsi einstaklinga. Í þessu samhengi ætti að túlka hugtakið „lýðheilsa“ eins og það er skilgreint í reglugerð Evrópuþingsins og ráðsins (EB) nr. 1338/2008 ([1]), þ.e. sem allir heilsufarstengdir þættir, nánar tiltekið heilsufar, m.a. sjúkdómstilvik og fötlun, ákvarðandi þættir sem hafa áhrif á heilsufar, þörf fyrir heilbrigðisþjónustu, fjármagn sem veitt er til heilbrigðisþjónustu, veiting og almennur aðgangur að heilbrigðisþjónustu og kostnaður og fjármögnun heilbrigðisþjónustu, sem og dánarorsakir. Slík vinnsla heilsufarsupplýsinga í þágu almannahagsmuna ætti ekki að leiða til vinnslu persónuupplýsinga í öðrum tilgangi af hálfu þriðju aðila, s.s. vinnuveitenda eða tryggingafélaga og bankastofnana.

55) Vinnsla persónuupplýsinga af hálfu opinberra yfirvalda í þeim tilgangi að vinna að markmiðum opinberlega viðurkenndra trúarsamtaka, eins og mælt er fyrir um í stjórnskipunarlögum eða samkvæmt þjóðarétti, fer einnig fram með vísan til almannahagsmuna.

56) Þegar nauðsynlegt reynist fyrir starfsemi lýðræðislegs stjórnkerfis í aðildarríki, í tengslum við kosningar, að stjórnmálaflokkar taki saman persónuupplýsingar um stjórnmálaskoðanir fólks má heimila vinnslu slíkra upplýsinga í þágu almannahagsmuna, að því tilskildu að gerðar séu viðeigandi verndarráðstafanir.

57) Ef persónuupplýsingar sem ábyrgðaraðili vinnur gera honum ekki kleift að persónugreina einstakling ætti honum ekki að vera skylt að afla viðbótarupplýsinga til að greina skráðan einstakling eingöngu í þeim tilgangi að uppfylla eitthvert ákvæðanna í þessari reglugerð. Þó ætti ábyrgðaraðili ekki að neita að taka við viðbótarupplýsingum sem hinn skráði lætur í té til þess að ná fram rétti sínum. Í persónugreiningu ætti að felast stafræn auðkenning á skráðum einstaklingi, m.a. með hjálp sannvottunaraðferðar á borð við sömu skilríki og hann notar við innskráningu á þjónustu á vegum ábyrgðaraðila gagna á Netinu.

58) Meginreglan um gagnsæi krefst þess að hvers kyns upplýsingar, sem ætlaðar eru almenningi eða skráðum einstaklingi, séu gagnorðar, aðgengilegar og auðskiljanlegar, að þær séu á skýru og einföldu máli og að auki að sjónrænum aðferðum sé beitt, eftir því sem við á. Veita mætti slíkar upplýsingar á rafrænu formi, t.d. á vefsetri, þegar þær eru ætlaðar almenningi. Þetta á einkum við í tilvikum þar sem erfitt er fyrir skráðan einstakling að vita og skilja, vegna hins mikla fjölda aðila sem koma að máli og flókinnar tækni sem notuð er, hvort, af hverjum og í hvaða tilgangi upplýsingum er safnað um hann, s.s. þegar um er að ræða auglýsingar á Netinu. Þar sem börn þurfa að njóta sérstakrar verndar ættu hvers kyns upplýsingar og tilkynningar, þegar vinnsla beinist að barni, að vera á skýru og einföldu máli sem barnið getur auðveldlega skilið.

59) Koma ætti á nánari reglum til að greiða fyrir því að skráður einstaklingur geti neytt réttar síns samkvæmt þessari reglugerð, m.a. ráðstöfunum sem gera honum kleift að fara fram á og, ef við á, fá því endurgjaldslaust framgengt að honum sé veittur aðgangur að persónuupplýsingum, þær séu leiðréttar eða þeim eytt, sem og að hann geti neytt andmælaréttar síns. Ábyrgðaraðili ætti einnig að sjá til þess að hægt sé að leggja fram beiðnir rafrænt, einkum þegar vinnsla persónuupplýsinga fer fram með rafrænum hætti. Ábyrgðaraðila ætti að vera skylt að svara beiðnum skráðs einstaklings án ótilhlýðilegrar tafar og innan eins mánaðar hið mesta og færa fram rök ef hann hyggst ekki taka slíkar beiðnir til greina.

([1]) Reglugerð Evrópuþingsins og ráðsins (EB) nr. 1338/2008 frá 16. desember 2008 um hagskýrslur Bandalagsins um lýðheilsu og heilbrigði og öryggi á vinnustað (Stjtíð. ESB L 354, 31.12.2008, bls. 70).

60) Meginreglurnar um sanngirni og gagnsæi við vinnslu krefjast þess að skráðum einstaklingi sé tilkynnt um að vinnsluaðgerð standi yfir og hver sé tilgangur hennar. Ábyrgðaraðili ætti að veita hinum skráða frekari upplýsingar sem nauðsynlegar eru til að tryggja að gætt sé sanngirni og gagnsæi við vinnslu persónuupplýsinga með tilliti til þeirra sérstöku aðstæðna og samhengis sem eiga við vinnslu þeirra. Enn fremur ætti að upplýsa hinn skráða um að gert hafi verið persónusnið og um afleiðingar þess. Þegar persónuupplýsingar eru fengnar hjá skráðum einstaklingi ætti einnig að upplýsa hann um hvort honum sé skylt að láta persónuupplýsingarnar í té og um það hvaða afleiðingar það hefur að veita þær ekki. Hægt er að láta staðlaðar táknmyndir fylgja þessum upplýsingum til að veita greinargott yfirlit yfir fyrirhugaða vinnslu á auðsýnilegan, skiljanlegan og auðlæsilegan hátt. Táknmyndirnar ættu að vera á tölvulesanlegu sniði þegar þær eru settar fram rafrænt.

61) Veita ætti skráðum einstaklingi upplýsingar í tengslum við vinnslu persónuupplýsinga um hann á þeim tíma þegar upplýsinganna er aflað hjá honum eða, þegar persónuupplýsinganna er aflað frá öðrum heimildum, innan hæfilegs tíma, með hliðsjón af aðstæðum í hverju tilviki fyrir sig. Ef fá má öðrum viðtakanda persónuupplýsingar í hendur með lögmætum hætti ætti að tilkynna það hinum skráða þegar viðtakandinn fær persónuupplýsingarnar í fyrsta sinn. Ef ábyrgðaraðili hyggst vinna persónuupplýsingarnar í öðrum tilgangi en þeim sem er að baki söfnun þeirra ætti hann að láta hinum skráða í té upplýsingar um þennan nýja tilgang áður en sú frekari vinnsla hefst, ásamt öðrum nauðsynlegum upplýsingum. Ef ekki er hægt að skýra hinum skráða frá uppruna persónuupplýsinganna vegna þess að þær koma frá mismunandi heimildum ætti að veita almennar upplýsingar.

62) Þó er ekki nauðsynlegt að setja fram skyldu til að veita upplýsingar ef skráður einstaklingur hefur þær þegar undir höndum, ef sérstaklega er mælt fyrir um skráningu eða birtingu persónuupplýsinganna í lögum, ef ómögulegt reynist að veita hinum skráða upplýsingar eða það hefði í för með sér óhóflega fyrirhöfn. Það síðasttalda gæti einkum átt við þegar vinnslan fer fram vegna skjalavistunar í þágu almannahagsmuna, rannsókna á sviði vísinda eða sagnfræði eða í tölfræðilegum tilgangi. Í því sambandi ætti að taka tillit til fjölda skráðra einstaklinga, þess hversu gamlar upplýsingarnar eru og viðeigandi verndarráðstafana sem gerðar hafa verið.

63) Skráður einstaklingur ætti að hafa rétt til aðgangs að persónuupplýsingum sem hefur verið safnað um hann og til að neyta þessa réttar með auðveldum hætti og hæfilegum hléum til þess að hann geti gert sér grein fyrir því hvort vinnslan fari fram með lögmætum hætti og sannreynt það. Þetta felur í sér rétt skráðra einstaklinga til aðgangs að upplýsingum sem varða heilsufar þeirra, t.d. upplýsingum í sjúkraskrám á borð við sjúkdómsgreiningu, niðurstöður rannsókna, mat meðhöndlandi lækna og hvers kyns meðferðir eða inngrip. Sérhver skráður einstaklingur ætti því einkum að hafa rétt til að fá vitneskju og tilkynningu um tilganginn með vinnslu persónuupplýsinganna, vinnslutímabil upplýsinganna ef unnt er, viðtakendur þeirra, hvaða rök liggja að baki sjálfvirkri vinnslu persónuupplýsinga og afleiðingar slíkrar vinnslu, einkum þegar hún er byggð á gerð persónusniðs. Ábyrgðaraðilinn ætti, ef mögulegt er, að vera fær um að veita hinum skráða fjaraðgang að öruggu kerfi sem myndi veita honum beinan aðgang að persónuupplýsingum um sig. Sá réttur ætti ekki að hafa neikvæð áhrif á réttindi eða frelsi annarra, þ.m.t. viðskiptaleyndarmál eða hugverkaréttindi og þá einkum höfundarrétt til verndar hugbúnaðinum. Niðurstaða þessara atriða ætti þó ekki að vera sú að skráðum einstaklingi sé neitað um allar upplýsingar. Þegar ábyrgðaraðili vinnur með mikið magn upplýsinga sem varða skráðan einstakling ætti hann að geta óskað eftir því að hinn skráði tilgreini nánar um hvaða upplýsingar eða vinnsluaðgerðir beiðnin snýst, áður en upplýsingarnar eru veittar.

64) Ábyrgðaraðilinn ætti að gera allar eðlilegar ráðstafanir til að sannreyna deili á skráðum einstaklingi sem óskar eftir aðgangi, einkum í tengslum við þjónustu á Netinu og netauðkenni. Ábyrgðaraðili ætti ekki að halda eftir persónuupplýsingum í þeim tilgangi einum að geta brugðist við hugsanlegum beiðnum.

65) Skráður einstaklingur ætti að hafa rétt til leiðréttingar á persónuupplýsingum er varða hann sjálfan og „rétt til að gleymast“ ef varðveisla slíkra upplýsinga brýtur í bága við þessa reglugerð, lög Sambandsins eða lög aðildarríkis sem ábyrgðaraðilinn fellur undir. Skráður einstaklingur ætti einkum að hafa rétt til þess að fá persónuupplýsingum er varða hann sjálfan eytt og að vinnslu með þær sé hætt ef upplýsingarnar eru ekki lengur nauðsynlegar í tengslum við tilganginn með söfnun eða vinnslu þeirra að öðru leyti, ef hann hefur afturkallað samþykki sitt eða andmælir vinnslu persónuupplýsinga um sig eða ef vinnsla persónuupplýsinga um hann samrýmist ekki þessari reglugerð að öðru leyti. Þessi réttur á einkum við þegar hinn skráði hefur veitt samþykki sitt sem barn og gerir sér ekki fulla grein fyrir

áhættunni sem vinnslan felur í sér og óskar eftir því síðar að persónuupplýsingunum verði eytt, einkum á Netinu. Skráður einstaklingur ætti að geta neytt þessa réttar þrátt fyrir að hann sé ekki lengur barn. Þó ætti frekari varðveisla persónuupplýsinganna að vera lögmæt, ef nauðsyn krefur, til að neyta réttar til tjáningar- og upplýsingafrelsis, til að uppfylla lagaskyldu, vegna verkefnis sem er unnið í þágu almannahagsmuna eða við beitingu opinbers valds sem ábyrgðaraðili fer með, í þágu almannahagsmuna á sviði lýðheilsu, vegna skjalavistunar í þágu almannahagsmuna, rannsókna á sviði vísinda eða sagnfræði eða í tölfræðilegum tilgangi eða til að unnt sé að stofna, hafa uppi eða verja réttarkröfur.

66) Til að efla megi réttinn til að gleymast í netumhverfinu ætti einnig að víkka réttinn til eyðingar þannig að ábyrgðaraðila, sem gerði persónuupplýsingarnar opinberar, sé skylt að upplýsa þá ábyrgðaraðila sem vinna slíkar upplýsingar um að afmá beri alla tengla á þessar persónuupplýsingar eða afrit af þeim eða endurgerðir þeirra. Í því sambandi ætti viðkomandi ábyrgðaraðili að gera eðlilegar ráðstafanir með tilliti til þeirrar tækni sem er fyrir hendi og aðferða sem honum eru aðgengilegar, þ.m.t. tæknilegar ráðstafanir til að upplýsa ábyrgðaraðilana, sem vinna persónuupplýsingar um hinn skráða, um beiðni hans.

67) Aðferðir til að takmarka vinnslu persónuupplýsinga gætu m.a. falið í sér að færa valdar upplýsingar tímabundið í annað vinnslukerfi, gera valdar persónuupplýsingar óaðgengilegar notendum eða fjarlægja birtar upplýsingar tímabundið af vefsetri. Í sjálfvirkum skráningarkerfum ætti að jafnaði að tryggja takmörkun vinnslunnar með tæknilegum aðferðum á þann hátt að ekki verði um frekari vinnslu persónuupplýsinganna að ræða og ekki sé hægt að breyta þeim. Tilgreina ætti með skýrum hætti í kerfinu að vinnsla persónuupplýsinga sé takmörkuð.

68) Til að styrkja enn frekar stjórn skráðs einstaklings á upplýsingum er varða hann sjálfan þegar vinnsla persónuupplýsinga fer fram með sjálfvirkum aðferðum ætti hann einnig að hafa rétt til að fá persónuupplýsingar er varða hann sjálfan, sem hann hefur látið ábyrgðaraðila í té, á skipulegu, algengu, tölvulesanlegu og samvirkandi sniði og senda þær öðrum ábyrgðaraðila. Hvetja ætti ábyrgðaraðila gagna til að þróa samvirkandi snið sem gera það mögulegt að flytja eigin gögn. Þessi réttur ætti að gilda þegar hinn skráði lét persónuupplýsingarnar í té á grundvelli eigin samþykkis eða ef vinnslan er nauðsynleg vegna framkvæmdar samnings. Hann ætti ekki að eiga við þegar vinnslan byggist á öðrum lagagrundvelli en samþykki eða samningi. Eðli málsins samkvæmt ætti ekki að beita þessum rétti gagnvart ábyrgðaraðilum sem vinna persónuupplýsingar við opinber skyldustörf sín. Hann ætti því ekki að gilda þegar vinnsla persónuupplýsinga er nauðsynleg til að uppfylla lagaskyldu sem hvílir á ábyrgðaraðilanum eða vegna verkefnis sem er unnið í þágu almannahagsmuna eða við beitingu opinbers valds sem ábyrgðaraðili fer með. Réttur skráðs einstaklings til að senda eða taka á móti persónuupplýsingum er varða hann sjálfan ætti ekki að verða til þess að ábyrgðaraðilum sé skylt að taka upp eða viðhalda vinnslukerfum sem eru tæknilega samhæfð. Ef tiltekið mengi persónuupplýsinga varðar fleiri en einn skráðan einstakling ætti réttur þeirra til að fá persónuupplýsingarnar að vera með fyrirvara um réttindi og frelsi annarra skráðra einstaklinga í samræmi við þessa reglugerð. Þessi réttur ætti enn fremur ekki að hafa áhrif á rétt skráðs einstaklings til að láta eyða persónuupplýsingum og takmarkanir á þeim rétti eins og sett er fram í þessari reglugerð, einkum ætti hann ekki að gefa til kynna að persónuupplýsingum, sem varða hinn skráða, sem hann hefur látið af hendi vegna efndar á samningi, verði eytt, að því marki og svo lengi sem persónuupplýsingarnar eru nauðsynlegar til að efna samninginn. Ef það er tæknilega gerlegt ætti skráður einstaklingur að hafa rétt til að láta senda persónuupplýsingarnar beint frá einum ábyrgðaraðila til annars.

69) Þegar vinnsla persónuupplýsinga gæti verið lögmæt vegna þess að hún er nauðsynleg vegna verkefnis, sem er unnið í þágu almannahagsmuna eða við beitingu opinbers valds sem ábyrgðaraðili fer með eða vegna lögmætra hagsmuna ábyrgðaraðila eða þriðja aðila, ætti skráður einstaklingur engu að síður að hafa rétt til að andmæla vinnslu persónuupplýsinga sem varða hans tilteknu aðstæður. Það ætti að vera á hendi ábyrgðaraðila að sýna fram á að mikilvægir lögmætir hagsmunir hans gangi framar hagsmunum eða grundvallarréttindum og frelsi hins skráða.

70) Þegar persónuupplýsingar eru unnar í þágu beinnar markaðssetningar ætti skráður einstaklingur að hafa rétt til að andmæla slíkri vinnslu, m.a. gerð persónusniðs, að því marki sem hún tengist slíkri beinni markaðssetningu, hvort sem um er að ræða upphaflega eða frekari vinnslu eða ekki, hvenær sem er og endurgjaldslaust. Gera ætti hinum skráða sérstaklega grein fyrir þessum rétti með skýrum hætti og aðgreint frá öðrum upplýsingum.

71) Skráður einstaklingur ætti að eiga rétt á því að sæta ekki ákvörðun sem kann að fela í sér ráðstöfun þar sem persónulegir þættir hans eru metnir eingöngu á grundvelli sjálfvirkrar gagnavinnslu og hefur réttaráhrif gagnvart honum sjálfum eða veruleg sambærileg áhrif, s.s. sjálfvirka höfnun lánsumsóknar á Netinu eða rafrænt ráðningarferli án mannlegrar íhlutunar. Til slíkrar vinnslu telst „gerð persónusniðs“ sem felur í sér hvers kyns sjálfvirka vinnslu persónuupplýsinga til að meta persónulega þætti er varða hagi einstaklings, einkum að greina eða spá fyrir um þætti er varða frammistöðu hans í starfi, fjárhagsstöðu, heilsufar, smekk, áhugamál, áreiðanleika eða hegðun, staðsetningu eða hreyfanleika, þegar hún hefur réttaráhrif hvað hann sjálfan varðar eða veruleg sambærileg áhrif. Ákvarðanataka, sem byggist á slíkri vinnslu, þ.m.t. gerð persónusniðs, ætti að vera leyfileg samkvæmt sérstakri heimild í lögum Sambandsins eða lögum aðildarríkis sem ábyrgðaraðilinn fellur undir, m.a. í þeim tilgangi að fylgjast með og koma í veg fyrir svindl og skattsvik í samræmi við reglur, staðla og tilmæli stofnana Sambandsins eða landsbundinna eftirlitsaðila og til að tryggja öryggi og áreiðanleika þjónustu sem ábyrgðaraðili veitir eða, þegar nauðsyn krefur, vegna gerðar eða framkvæmdar samnings milli skráðs einstaklings og ábyrgðaraðila eða þegar hinn skráði hefur veitt ótvírætt samþykki sitt. Hvað sem öðru líður ætti við slíka vinnslu að gera viðeigandi verndarráðstafanir, þ. á m. að veita hinum skráða skilmerkilegar upplýsingar og rétt til mannlegrar íhlutunar, að láta skoðun sína í ljós, fá útskýringar á ákvörðun sem tekin er að loknu slíku mati og vefengja ákvörðunina. Slík ráðstöfun ætti ekki að varða barn.

Til að tryggja að vinnslan sé sanngjörn og gagnsæ gagnvart skráðum einstaklingi, að teknu tilliti til sérstakra aðstæðna og samhengis við vinnslu persónuupplýsinganna, ætti ábyrgðaraðilinn að nota viðeigandi stærðfræðilegar eða tölfræðilegar aðferðir við gerð persónusniðs, gera viðeigandi tæknilegar og skipulagslegar ráðstafanir, einkum til að tryggja að þættir sem gera persónuupplýsingar óáreiðanlegar séu leiðréttir og dregið sé úr hættu á mistökum, að tryggja öryggi persónuupplýsinga þannig að tekið sé tillit til mögulegrar áhættu fyrir hagsmuni og réttindi hins skráða og m.a. komið í veg fyrir að einstaklingum sé mismunað á grundvelli kynþáttar eða þjóðernislegs uppruna, stjórnmálaskoðana, trúarbragða eða trúar, þátttöku í stéttarfélagi, erfðaeiginleika eða heilsuhaga eða kynhneigðar, eða vinnslu sem leiðir til ráðstafana sem hafa samsvarandi áhrif. Sjálfvirka ákvarðanatöku og gerð persónusniðs, sem byggist á sérstökum flokkum persónuupplýsinga, ætti einungis að heimila með sérstökum skilyrðum.

72) Gerð persónusniðs fellur undir reglurnar um vinnslu persónuupplýsinga í þessari reglugerð, m.a. hvað varðar lagagrundvöll vinnslunnar eða meginreglur um persónuvernd. Evrópska persónuverndarráðið, sem komið er á fót með þessari reglugerð („persónuverndarráðið“), ætti að geta gefið út leiðbeiningar í því tilliti.

73) Lög Sambandsins eða lög aðildarríkis geta kveðið á um að takmarka megi sértækar meginreglur og rétt á upplýsingum, aðgang að persónuupplýsingum og leiðréttingu á þeim eða eyðingu þeirra, rétt til að flytja eigin gögn, rétt til andmæla, ákvarðanir sem byggjast á gerð persónusniðs, ásamt tilkynningum til skráðs einstaklings um öryggisbrest við meðferð persónuupplýsinga og tilteknar tengdar skyldur ábyrgðaraðila, að því marki sem nauðsynlegt er og hóflegt í lýðræðisþjóðfélagi til að vernda almannaöryggi, þ.m.t. mannslíf, einkum vegna viðbragða við náttúruhamförum og hamförum af mannavöldum, vegna forvarna, rannsókna og saksóknar í refsimálum eða fullnustu refsiviðurlaga, m.a. til að vernda gegn og koma í veg fyrir ógnir við almannaöryggi eða brot á siðareglum í lögvernduðum atvinnugreinum, vegna annarra mikilvægra markmiða sem þjóna almannahagsmunum Sambandsins eða aðildarríkis, einkum mikilvægum efnahagslegum eða fjárhagslegum hagsmunum Sambandsins eða aðildarríkis, vegna halds opinberra skráa í þágu almannahagsmuna, frekari vinnslu persónuupplýsinga í skjalasöfnum til að útvega sérstakar upplýsingar um stjórnmálahegðun undir stjórnum fyrrverandi einræðisríkja eða til að vernda hinn skráða eða réttindi og frelsi annarra, m.a. í þágu félagslegrar verndar, lýðheilsu og mannúðar. Þessar takmarkanir ættu að vera í samræmi við kröfurnar sem settar eru fram í sáttmálanum um grundvallarréttindi og Evrópusáttmálanum um verndun mannréttinda og mannfrelsis.

74) Setja ætti reglur um ábyrgð og bótaábyrgð ábyrgðaraðila vegna vinnslu persónuupplýsinga af hans hálfu eða fyrir hans hönd. Ábyrgðaraðilanum ætti einkum að vera skylt að gera viðeigandi og skilvirkar ráðstafanir og hann ætti að vera fær um að sýna fram á að vinnslan fari fram í samræmi við þessa reglugerð, þ.m.t. að því er varðar skilvirkni ráðstafananna. Ráðstafanirnar ættu að taka mið af eðli, umfangi, samhengi og tilgangi vinnslunnar og áhættu fyrir réttindi og frelsi einstaklinga.

75) Vinnsla persónuupplýsinga kann að leiða til misjafnlega líklegrar og alvarlegrar áhættu fyrir réttindi og frelsi einstaklinga sem getur leitt af sér efnislegt tjón, eignatjón og óefnislegt tjón, einkum þegar vinnslan getur haft í för með sér mismunun, auðkennisþjófnað eða svik, fjárhagstjón, skaða á orðstír, tapaðan trúnað um persónuupplýsingar sem njóta verndar á grundvelli þagnarskyldu, að notkun gerviauðkenna sé aflétt í leyfisleysi eða annað umtalsvert efnahagslegt eða félagslegt óhagræði, þegar skráðir einstaklingar gætu misst réttindi sín og frelsi eða verið hindraðir í að stjórna eigin persónuupplýsingum, þegar persónuupplýsingar eru unnar sem leiða í ljós kynþátt eða þjóðernislegan uppruna, stjórnmálaskoðanir, trúarbrögð eða heimspekilega sannfæringu, þátttöku í stéttarfélagi og vinnsla erfðafræðilegra upplýsinga, upplýsinga sem varða heilsu eða upplýsinga um kynlíf eða sakfellingu í refsimálum og refsiverð brot eða tengdar öryggisráðstafanir, þegar lagt er mat á persónulega þætti, einkum við að greina eða spá fyrir um þætti er varða frammistöðu í starfi, fjárhagsstöðu, heilsuhagi, smekk eða áhugamál, áreiðanleika eða hegðun, staðsetningu eða hreyfanleika, til þess að gera eða nota persónusnið, þegar persónuupplýsingar berskjaldaðra einstaklinga, einkum barna, eru unnar eða þegar vinnsla tekur til mikils magns persónuupplýsinga og hefur áhrif á marga skráða einstaklinga.

76) Ákvarða ætti hversu líkleg og alvarleg áhættan er fyrir réttindi og frelsi hins skráða með vísun til eðlis, umfangs, samhengis og tilgangs vinnslunnar. Meta ætti áhættu út frá hlutlægu mati þar sem leitt er í ljós hvort aðgerðir við vinnslu persónuupplýsinga feli í sér áhættu eða mikla áhættu.

77) Veita mætti ábyrgðaraðila eða vinnsluaðila leiðbeiningar um framkvæmd viðeigandi ráðstafana og um það hvernig sýna skuli fram á fylgni við reglur, einkum að því er varðar greiningu á áhættu í tengslum við vinnsluna, mat þeirra að því er varðar orsök áhættunnar, eðli hennar, hversu líkleg og alvarleg hún er og við að greina bestu starfsvenjur til að draga úr henni, einkum með því að nota viðurkenndar hátternisreglur, viðurkennda vottun, viðmiðunarreglur frá persónuverndarráðinu eða ábendingar frá persónuverndarfulltrúa. Persónuverndarráðið getur einnig gefið út viðmiðunarreglur um vinnsluaðgerðir sem ólíklegt er að leiði af sér mikla áhættu fyrir réttindi og frelsi skráðra einstaklinga og bent á ráðstafanir sem geta verið nægilegar í slíkum tilvikum til að bregðast við slíkri áhættu.

78) Til að vernda réttindi og frelsi einstaklinga að því er varðar vinnslu persónuupplýsinga er nauðsynlegt að gerðar séu viðeigandi tæknilegar og skipulagslegar ráðstafanir til að tryggja að kröfum þessarar reglugerðar sé fullnægt. Til að geta sýnt fram á farið sé að þessari reglugerð ætti ábyrgðaraðilinn að setja sér innri stefnu og innleiða ráðstafanir sem fylgja einkum meginreglunum um innbyggða persónuvernd og sjálfgefna persónuvernd. Slíkar ráðstafanir gætu m.a. falið það í sér að draga sem mest úr vinnslu persónuupplýsinga, færa persónuupplýsingar undir gerviauðkenni eins skjótt og unnt er, gagnsæi að því er varðar eiginleika persónuupplýsinga og vinnslu þeirra, gera skráðum einstaklingi kleift að fylgjast með vinnslu upplýsinganna, gera ábyrgðaraðila kleift að taka upp og bæta öryggisþætti. Þegar framleiðendur vöru, þjónustu og hugbúnaðar þróa, hanna, velja og nota hugbúnað, vöru og þjónustu, sem er byggð á vinnslu persónuupplýsinga, eða vinna persónuupplýsingar í störfum sínum ætti að hvetja þá til að taka tillit til réttarins til persónuverndar við þróun og hönnun á slíkum vörum, þjónustu og hugbúnaði og ganga úr skugga um, að teknu tilhlýðilegu tilliti til nýjustu tækniþekkingar, að ábyrgðaraðilar og vinnsluaðilar geti uppfyllt skyldur sínar um persónuvernd. Einnig ætti að taka tillit til meginreglnanna um innbyggða og sjálfgefna persónuvernd í tengslum við opinber útboð.

79) Vernd réttinda og frelsis skráðra einstaklinga, ásamt ábyrgð og bótaábyrgð ábyrgðaraðila og vinnsluaðila, einnig að því er varðar eftirlit og aðgerðir eftirlitsyfirvalda, krefst þess að skipting ábyrgðarsviða samkvæmt þessari reglugerð sé skýr, m.a. þegar ábyrgðaraðili ákvarðar, ásamt öðrum ábyrgðaraðilum, tilgang og aðferðir við vinnslu eða þegar vinnsluaðgerð er framkvæmd fyrir hönd ábyrgðaraðila.

80) Ef ábyrgðaraðili eða vinnsluaðili, sem ekki hefur staðfestu í Sambandinu, vinnur persónuupplýsingar um skráða einstaklinga sem eru í Sambandinu og vinnslustarfsemi hans tengist því að bjóða slíkum skráðum einstaklingum í Sambandinu vöru eða þjónustu, án tillits til þess hvort þeir verði krafðir um greiðslu, eða hafa eftirlit með hegðun þeirra, að svo miklu leyti sem hegðunin á sér stað innan Sambandsins, ætti ábyrgðaraðilinn eða vinnsluaðilinn að tilnefna fulltrúa nema því aðeins að vinnslan sé tilfallandi, feli ekki í sér stórfellda vinnslu sérstakra flokka persónuupplýsinga eða vinnslu persónuupplýsinga er varða sakfellingu í refsimálum og refsiverð brot, og ólíklegt teljist að hún leiði af sér áhættu fyrir réttindi og frelsi einstaklinga, með tilliti til eðlis, samhengis, umfangs og tilgangs vinnslunnar, eða ef

ábyrgðaraðilinn er opinbert yfirvald eða stofnun. Fulltrúinn ætti að koma fram fyrir hönd ábyrgðaraðilans eða vinnsluaðilans og getur hvaða eftirlitsyfirvald sem er haft samband við hann. Ábyrgðaraðilinn eða vinnsluaðilinn ætti að tilnefna fulltrúann sérstaklega með skriflegu umboði til að koma fram fyrir sína hönd með tilliti til skuldbindinga hans samkvæmt þessari reglugerð. Tilnefning slíks fulltrúa hefur ekki áhrif á ábyrgð eða bótaábyrgð ábyrgðaraðilans eða vinnsluaðilans samkvæmt þessari reglugerð. Slíkur fulltrúi ætti að inna verk sín af hendi í samræmi við fengið umboð frá ábyrgðaraðilanum eða vinnsluaðilanum, þ.m.t. starfa með lögbærum eftirlitsyfirvöldum með tilliti til hvers konar aðgerða sem gripið er til í því skyni að tryggja að farið sé að þessari reglugerð. Tilnefndur fulltrúi ætti að sæta framfylgdaraðgerð hafi ábyrgðaraðili eða vinnsluaðili ekki farið að reglugerðinni.

81) Til að tryggja að farið sé að kröfum þessarar reglugerðar að því er varðar þá vinnslu, sem vinnsluaðilinn á að annast fyrir hönd ábyrgðaraðilans, ætti ábyrgðaraðilinn, þegar hann felur vinnsluaðila vinnsluaðgerðir, einungis að leita til vinnsluaðila sem veita fullnægjandi tryggingar, einkum með tilliti til sérþekkingar, áreiðanleika og úrræða, fyrir því að koma til framkvæmda tæknilegum ráðstöfunum og skipulagsráðstöfunum sem samrýmast kröfum þessarar reglugerðar, m.a. að því er varðar öryggi vinnslunnar. Ef vinnsluaðili fylgir samþykktum hátternisreglum eða samþykktu vottunarfyrirkomulagi má nota það til að sýna fram á að ábyrgðaraðili uppfylli skuldbindingar sínar. Ákvæði um að vinnsla sé í höndum vinnsluaðila ætti að setja fram í samningi eða annarri réttargerð samkvæmt lögum Sambandsins eða lögum aðildarríkis, sem skuldbindur vinnsluaðilann gagnvart ábyrgðaraðilanum og tilgreinir viðfangsefni og lengd vinnslunnar, eðli og tilgang hennar, tegund persónuupplýsinga og flokka skráðra einstaklinga, með tilliti til sérstakra verkefna og ábyrgðar vinnsluaðilans í tengslum við vinnsluna sem á að fara fram og áhættu sem skapast varðandi réttindi og frelsi hins skráða. Ábyrgðaraðilinn og vinnsluaðilinn geta valið að nota stakan samning eða föst samningsákvæði sem annaðhvort framkvæmdastjórnin samþykkir beint eða eftirlitsyfirvald samþykkir í samræmi við samræmingarkerfið og framkvæmdastjórnin samþykkir síðan. Þegar vinnslu á vegum ábyrgðaraðilans er lokið ætti vinnsluaðilinn, eftir því sem ábyrgðaraðilinn ákveður, að skila eða eyða persónuupplýsingunum nema fyrir liggi krafa um varðveislu persónuupplýsinganna samkvæmt lögum Sambandsins eða lögum aðildarríkis sem vinnsluaðilanum ber að hlíta.

82) Til þess að sýna fram á að farið sé að þessari reglugerð ætti ábyrgðaraðilinn eða vinnsluaðilinn að halda skrár yfir vinnsluaðgerðir sem eru á hans ábyrgð. Hverjum ábyrgðaraðila og vinnsluaðila ætti að vera skylt að vinna með eftirlitsyfirvaldi og gera þessar skrár, að fenginni beiðni, aðgengilegar eftirlitsyfirvaldinu svo að nýta megi þær í þágu eftirlits með þessum vinnsluaðgerðum.

83) Til þess að viðhalda öryggi og koma í veg fyrir vinnslu, sem brýtur í bága við þessa reglugerð, ætti ábyrgðaraðili eða vinnsluaðili að meta þá áhættu sem fylgir vinnslunni og gera ráðstafanir til að draga úr slíkri áhættu, s.s. með dulkóðun. Þessar ráðstafanir ættu að tryggja viðeigandi öryggisstig, þ.m.t. trúnað, með tilliti til nýjustu tækni og kostnaðar við framkvæmd í tengslum við áhættu og eðli persónuupplýsinganna sem á að vernda. Við mat á áhættu fyrir gagnaöryggi ætti að líta til þeirrar áhættu sem fylgir vinnslu persónuupplýsinga, s.s. óviljandi eða ólögmætrar eyðingar persónuupplýsinga þegar þær eru sendar, geymdar eða unnar á annan hátt, s.s. að þær glatist, breytist, verði birtar eða aðgangur veittur að þeim í leyfisleysi, sem kann einkum að leiða til efnislegs tjóns, eignatjóns eða óefnislegs tjóns.

84) Til að stuðla að því að farið sé að þessari reglugerð þegar líklegt er að vinnsluaðgerðir leiði af sér mikla áhættu fyrir réttindi og frelsi einstaklinga ætti ábyrgðaraðilinn að vera ábyrgur fyrir að gert sé mat á áhrifum á persónuvernd, einkum til að meta uppruna, eðli, sérkenni og alvarleika þeirrar áhættu. Taka ætti tillit til niðurstöðu matsins þegar ákvarðaðar eru viðeigandi ráðstafanir sem grípa skal til þannig að hægt sé að sýna fram á að vinnsla persónuupplýsinga sé í samræmi við þessa reglugerð. Þegar mat á áhrifum á persónuvernd gefur til kynna að vinnsluaðgerðir feli í sér mikla áhættu, sem ábyrgðaraðilinn getur ekki dregið úr með viðeigandi ráðstöfunum með hliðsjón af tiltækri tækni og kostnaði við framkvæmd, ætti að hafa samráð við eftirlitsyfirvaldið áður en vinnslan hefst.

85) Öryggisbrestur við meðferð persónuupplýsinga getur, ef ekki er brugðist við honum á réttan hátt og tímanlega, valdið einstaklingum efnislegu tjóni, eignatjóni eða óefnislegu tjóni, s.s. missi yfirráða þeirra yfir persónuupplýsingum um sig eða takmörkun réttinda þeirra, mismunun, auðkennisþjófnaði eða svikum, fjárhagstjóni, að notkun gerviauðkenna sé aflétt í leyfisleysi, skaða á orðstír, töpuðum trúnaði um persónuupplýsingar sem njóta verndar samkvæmt þagnarskyldu eða öðru umtalsverðu efnahagslegu eða félagslegu óhagræði fyrir viðkomandi einstakling. Af þeim sökum ætti

ábyrgðaraðilinn, um leið og hann verður þess áskynja að öryggisbrestur hafi orðið við meðferð persónuupplýsinga, að tilkynna eftirlitsyfirvaldinu um hann án ótilhlýðilegrar tafar og, ef mögulegt er, eigi síðar en 72 klst. eftir að hann verður brestsins var nema ábyrgðaraðilinn geti sýnt fram á, í samræmi við meginregluna um ábyrgðarskyldu, að ekki sé líklegt að viðkomandi brestur leiði af sér áhættu fyrir réttindi og frelsi einstaklinga. Ef ekki er hægt að tilkynna slíkt innan 72 klst. ættu ástæður tafarinnar að fylgja tilkynningunni og veita má upplýsingar í áföngum án frekari ástæðulausrar tafar.

86) Ábyrgðaraðilinn ætti að tilkynna skráðum einstaklingi um öryggisbrest við meðferð persónuupplýsinga án ótilhlýðilegrar tafar ef líklegt má telja að bresturinn leiði af sér mikla áhættu fyrir réttindi og frelsi einstaklingsins og gefa viðkomandi þannig færi á að gera nauðsynlegar varúðarráðstafanir. Í tilkynningunni ætti að koma fram eðli öryggisbrestsins við meðferð persónuupplýsinga, auk tilmæla til viðkomandi einstaklings um að draga úr mögulegum skaðlegum áhrifum. Slíkar tilkynningar til skráðra einstaklinga ætti að senda eins fljótt og mögulegt er og í nánu samstarfi við eftirlitsyfirvaldið, í samræmi við leiðbeiningar frá því sjálfu eða öðrum viðeigandi yfirvöldum, s.s. löggæsluyfirvöldum. Þörf á að draga úr bráðri hættu á tjóni kallar eftir skjótum samskiptum við skráða einstaklinga, en þörf á að grípa til viðeigandi ráðstafana gagnvart áframhaldandi eða sambærilegum öryggisbrestum við meðferð persónuupplýsinga kann að réttlæta að meiri tími fari í samskipti.

87) Ganga ætti úr skugga um hvort allar viðeigandi tæknilegar verndarráðstafanir og skipulagsráðstafanir hafi verið gerðar til að staðfesta tafarlaust hvort öryggisbrestur við meðferð persónuupplýsinga hafi átt sér stað og til að upplýsa eftirlitsyfirvaldið og hinn skráða þegar í stað um það. Ganga ætti úr skugga um að tilkynningin hafi verið send án ótilhlýðilegrar tafar, einkum með tilliti til eðlis og alvarleika öryggisbrests við meðferð persónuupplýsinga, afleiðinga hans og skaðlegra áhrifa hans fyrir hinn skráða. Slík tilkynning getur leitt til inngripa af hálfu eftirlitsyfirvaldsins í samræmi við verkefni þess og valdsvið sem mælt er fyrir um í þessari reglugerð.

88) Þegar settar eru ítarlegar reglur um viðeigandi framsetningu og verklag við tilkynningu öryggisbrests við meðferð persónuupplýsinga ætti að taka tilhlýðilegt tillit til aðstæðna þegar viðkomandi brestur átti sér stað, m.a. hvort persónuupplýsingar hafi verið varðar með viðeigandi tæknilegum ráðstöfunum sem takmarka í reynd líkur á auðkennasvikum eða annars konar misnotkun. Enn fremur ættu slíkar reglur og málsmeðferð að taka tillit til lögmætra hagsmuna löggæsluyfirvalda þegar upplýsingagjöf snemma í ferlinu kann að ástæðulausu að standa í vegi fyrir rannsókn á aðstæðum þegar öryggisbrestur við meðferð persónuupplýsinga átti sér stað.

89) Í tilskipun 95/46/EB er kveðið á um almenna skyldu til að tilkynna eftirlitsyfirvöldum um vinnslu persónuupplýsinga. Þótt sú skylda leiði til stjórnsýslulegrar og fjárhagslegrar byrði leiddi hún ekki í öllum tilvikum til bættrar verndar persónuupplýsinga. Af þeim sökum ætti að afnema slíka tilviljanakennda almenna tilkynningarskyldu og þess í stað ættu að koma skilvirkar verklagsreglur og aðferðir sem leggja í staðinn áherslu á þær tegundir vinnsluaðgerða sem líklegt er að leiði af sér mikla áhættu fyrir réttindi og frelsi einstaklinga vegna eðlis þeirra, umfangs, samhengis og tilgangs. Slíkar tegundir vinnsluaðgerða geta verið þær sem fela einkum í sér notkun nýrrar tækni eða eru nýrrar gerðar og þar sem ábyrgðaraðilinn hefur ekki áður framkvæmt mat á áhrifum á persónuvernd eða þegar þær verða nauðsynlegar í ljósi þess tíma sem liðinn er frá upphaflegu vinnslunni.

90) Í þeim tilvikum ætti ábyrgðaraðilinn að láta fara fram mat á áhrifum á persónuvernd áður en vinnslan hefst til þess að meta líkur á og alvarleika mikillar áhættu með tilliti til eðlis, umfangs, samhengis og tilgangs vinnslunnar og uppruna áhættunnar. Þetta mat á áhrifum ætti einkum að fela í sér ráðstafanir, verndarráðstafanir og fyrirkomulag sem ætlað er að draga úr þeirri áhættu, tryggja vernd persónuupplýsinga og sýna fram á að farið sé að þessari reglugerð.

91) Þetta ætti einkum að eiga við um umfangsmiklar vinnsluaðgerðir sem miða að því að vinna verulegt magn persónuupplýsinga á svæðisbundnum, landsbundnum eða yfirþjóðlegum vettvangi og sem gætu haft áhrif á mikinn fjölda skráðra einstaklinga og sem líklegt má telja að leiði af sér mikla áhættu, t.d. vegna þess hversu viðkvæmar upplýsingarnar eru, þegar í samræmi við þá tækniþekkingu sem náðst hefur er notuð ný tækni í miklum mæli, svo og aðrar vinnsluaðgerðir sem leiða af sér mikla áhættu fyrir réttindi og frelsi skráðra einstaklinga, einkum þegar þessar aðgerðir gera hinum skráðu erfiðara fyrir með að neyta réttar síns. Einnig ætti að framkvæma mat á áhrifum á

persónuvernd þegar persónuupplýsingar eru unnar vegna töku ákvarðana er varða tiltekna einstaklinga í kjölfar kerfisbundins og umfangsmikils mats á persónubundnum þáttum sem tengjast einstaklingum og er byggt á gerð persónusniðs úr þessum upplýsingum eða í kjölfar vinnslu á sérstökum flokkum persónuupplýsinga, lífkennaupplýsinga eða upplýsinga um sakfellingar í refsimálum og refsiverð brot eða tengdar öryggisráðstafanir. Á sama hátt er krafist mats á áhrifum á persónuvernd þegar haft er umfangsmikið eftirlit með svæðum sem eru aðgengileg almenningi, einkum þegar notaður er ljósrafeindabúnaður eða vegna annarra aðgerða þar sem lögbært eftirlitsyfirvald telur að vinnslan leiði líklega af sér mikla áhættu fyrir réttindi og frelsi skráðra einstaklinga, einkum vegna þess að þær koma í veg fyrir að hinir skráðu neyti réttar síns, noti þjónustu eða byggi á samningi, eða vegna þess að þær eru umfangsmiklar og framkvæmdar kerfisbundið. Vinnsla persónuupplýsinga ætti ekki að teljast umfangsmikil ef vinnslan 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.

92) Við tilteknar aðstæður kann að vera skynsamlegt og hagkvæmt að hafa viðfangsefni mats á áhrifum á persónuvernd víðtækara en eitt verkefni, t.d. ef opinber yfirvöld eða stofnanir hafa í hyggju að koma á sameiginlegum vettvangi vegna notkunar eða vinnslu eða þegar margir ábyrgðaraðilar ráðgera að koma á sameiginlegu notkunar- eða vinnsluumhverfi innan atvinnugreinar eða -geira eða algengrar, þverlægrar starfsemi.

93) Í tengslum við samþykkt laga aðildarríkis, sem eru grundvöllur fyrir framkvæmd verkefna opinbera yfirvaldsins eða stofnunarinnar og gilda um sérstaka vinnsluaðgerð eða röð aðgerða sem um er að ræða, geta aðildarríki talið nauðsynlegt að framkvæma slíkt mat áður en vinnsluaðgerðirnar hefjast.

94) Þegar mat á áhrifum á persónuvernd bendir til þess að vinnslan myndi, vegna skorts á verndarráðstöfunum, öryggisráðstöfunum og aðgerðum til að draga úr áhættu, leiða til mikillar áhættu fyrir réttindi og frelsi einstaklinga og ábyrgðaraðilinn lítur svo á að ekki verði dregið úr henni með hóflegum aðferðum með tilliti til tiltækrar tækni og kostnaðar við framkvæmd, ætti að hafa samráð við eftirlitsyfirvaldið áður en hafist er handa við vinnsluaðgerðir. Líklegt er að tilteknar tegundir vinnslu og umfang og tíðni vinnslu hafi svo mikla áhættu í för með sér sem kann einnig að leiða til skaða eða röskunar á réttindum og frelsi einstaklingsins. Eftirlitsyfirvaldið ætti að bregðast við beiðni um samráð innan tilgreinds tíma. Ef engin viðbrögð koma frá eftirlitsyfirvaldinu innan þess tíma ætti það þó ekki að hafa áhrif á íhlutun eftirlitsyfirvaldsins í samræmi við verkefni þess og valdheimildir sem mælt er fyrir um í þessari reglugerð, m.a. heimild til að banna vinnsluaðgerðir. Liður í því samráðsferli er að heimilt er að leggja fyrir eftirlitsyfirvaldið niðurstöðu úr mati á áhrifum á persónuvernd sem framkvæmt er með tilliti til viðkomandi vinnslu, einkum fyrirhugaðar ráðstafanir til að draga úr áhættu fyrir réttindi og frelsi einstaklinga.

95) Vinnsluaðilinn ætti að aðstoða ábyrgðaraðilann, eftir því sem nauðsyn krefur og komi fram beiðni um það, við að tryggja að farið sé að þeim skuldbindingum sem leiðir af framkvæmd mats á áhrifum á persónuvernd og fyrirframsamráði við eftirlitsyfirvaldið.

96) Samráð við eftirlitsyfirvaldið ætti einnig að fara fram við undirbúning löggjafar- eða stjórnvaldsráðstöfunar sem varðar vinnslu persónuupplýsinga til þess að tryggja að fyrirhuguð vinnsla sé í samræmi við þessa reglugerð og einkum til að takmarka áhættu sem snertir skráðan einstakling.

97) Ef vinnslan er í höndum opinbers yfirvalds, að undanskildum dómstólum eða sjálfstæðum dómsyfirvöldum þegar þau fara með dómsvald sitt, ef vinnsla í einkageiranum er í höndum ábyrgðaraðila þar sem meginstarfsemin felst í vinnsluaðgerðum sem krefjast umfangsmikillar, reglubundinnar og kerfisbundinnar vöktunar á skráðum einstaklingum eða ef meginverkefni ábyrgðaraðilans eða vinnsluaðilans felast í umfangsmikilli vinnslu sérstakra flokka persónuupplýsinga og upplýsinga er varða sakfellingu í refsimálum og refsiverð brot, ætti aðili með sérþekkingu á löggjöf um persónuvernd að aðstoða ábyrgðaraðilann eða vinnsluaðilann við eftirlit með því að þessari reglugerð sé fylgt á innri vettvangi. Í einkageiranum varða meginverkefni ábyrgðaraðila aðalstarfsemi hans en ekki vinnslu persónuupplýsinga sem viðbótarstarfsemi. Ákvarða ætti nauðsynlega sérþekkingu einkum út frá þeim gagnavinnsluaðgerðum sem

framkvæmdar eru og þeirri vernd sem nauðsynleg er vegna þeirra persónuupplýsinga sem ábyrgðaraðili eða vinnsluaðili vinnur. Persónuverndarfulltrúar, hvort sem þeir eru starfsmenn ábyrgðaraðilans eða ekki, ættu að vera í aðstöðu til að sinna skyldustörfum sínum og verkefnum með óháðum hætti.

98) Hvetja ætti samtök eða aðra aðila, sem eru fulltrúar flokka ábyrgðaraðila eða vinnsluaðila, til að setja sér hátternisreglur, innan marka þessarar reglugerðar, í því skyni að auðvelda skilvirka beitingu hennar, með hliðsjón af sérstökum eiginleikum þeirrar vinnslu sem fer fram á tilteknum sviðum og í samræmi við sérstakar þarfir örfyrirtækja og lítilla og meðalstórra fyrirtækja. Slíkar hátternisreglur gætu einkum afmarkað skyldur ábyrgðaraðila og vinnsluaðila, með tilliti til þeirrar áhættu fyrir réttindi og frelsi einstaklinga sem líklegt er að vinnslan hafi í för með sér.

99) Þegar samtök og aðrir aðilar, sem eru fulltrúar flokka ábyrgðaraðila eða vinnsluaðila, setja sér hátternisreglur, breyta þeim eða rýmka gildissvið þeirra ættu þau að hafa samráð við viðeigandi hagsmunaaðila, m.a. skráða einstaklinga ef unnt er, og taka tillit til athugasemda og skoðana sem fram hafa komið í kjölfar slíks samráðs.

100) Til að bæta gagnsæi og fylgni við þessa reglugerð ætti að hvetja til þess að komið verði á vottunarfyrirkomulagi og persónuverndarinnsiglum og -merkjum sem gera skráðum einstaklingum kleift að meta fljótt persónuverndarstig viðkomandi vöru og þjónustu.

101) Flæði persónuupplýsinga til og frá löndum utan Sambandsins og til og frá alþjóðastofnunum er nauðsynlegt vegna vaxandi alþjóðaviðskipta og alþjóðlegrar samvinnu. Aukið flæði af þessu tagi hefur haft í för með sér ný viðfangsefni og vanda í tengslum við vernd persónuupplýsinga. Þegar persónuupplýsingum er miðlað frá Sambandinu til ábyrgðaraðila, vinnsluaðila eða annarra viðtakenda í þriðju löndum eða til alþjóðastofnana ætti það ekki að grafa undan þeirri vernd sem þessi reglugerð tryggir einstaklingum í Sambandinu, þ.m.t. við framsendingu persónuupplýsinga frá þriðja landinu eða alþjóðastofnuninni til ábyrgðaraðila eða vinnsluaðila í sama eða öðru þriðja landi eða hjá annarri alþjóðastofnun. Miðlun til þriðju landa eða alþjóðastofnana má þó aðeins fara fram með þeim hætti að þessari reglugerð sé fylgt í einu og öllu. Upplýsingunum má því aðeins miðla, með fyrirvara um önnur ákvæði þessar reglugerðar, að ábyrgðaraðili eða vinnsluaðili hafi farið að skilyrðunum sem mælt er fyrir um í ákvæðum þessarar reglugerðar um miðlun persónuupplýsinga til þriðja lands eða alþjóðastofnunar.

102) Þessi reglugerð hefur ekki áhrif á alþjóðasamninga sem Sambandið hefur gert við þriðju lönd um miðlun persónuupplýsinga, þ.m.t. um viðeigandi verndarráðstafanir í þágu skráðra einstaklinga. Aðildarríki geta gert alþjóðasamninga sem taka til miðlunar persónuupplýsinga til þriðju landa eða alþjóðastofnana, að svo miklu leyti sem slíkir samningar hafa ekki áhrif á þessa reglugerð eða önnur ákvæði í lögum Sambandsins og hafa að geyma ákvæði um viðeigandi vernd grundvallarréttinda skráðra einstaklinga.

103) Framkvæmdastjórnin getur ákveðið, þannig að gildi hafi alls staðar í Sambandinu, að þriðja land, yfirráðasvæði eða tilgreindur geiri innan þriðja lands eða alþjóðastofnun veiti fullnægjandi persónuvernd, og þannig skapað réttarvissu og einsleitni í öllu Sambandinu að því er varðar þriðja land eða alþjóðastofnun sem talin er veita slíka vernd. Í þeim tilvikum er leyfilegt að miðla persónuupplýsingum til umrædds þriðja lands eða alþjóðastofnunar án þess að afla frekari heimildar. Framkvæmdastjórnin getur einnig ákveðið að afturkalla slíka ákvörðun eftir að hún hefur tilkynnt þriðja landinu eða alþjóðastofnuninni um það og upplýst að fullu um ástæður.

104) Við mat framkvæmdastjórnarinnar á þriðja landi eða á yfirráðasvæði eða tilgreindum geira innan þriðja lands ætti hún, í samræmi við þau grundvallargildi sem Sambandið er byggt á, einkum vernd mannréttinda, að taka tillit til þess hvernig viðkomandi þriðja land virðir grunnreglur réttarríkisins, tryggir aðgang að réttarkerfinu og fer að alþjóðlegum reglum og viðmiðunum um mannréttindi, og til almennra laga og sérlaga, sem og til löggjafar um almannaöryggi, landvarnir og öryggi ríkisins, auk allsherjarreglu og refsiréttar. Við samþykkt ákvörðunar um það hvort vernd sé fullnægjandi að því er varðar yfirráðasvæði eða tilgreindan geira innan þriðja lands ætti að taka tillit til skýrra og hlutlægra viðmiðana, s.s. tiltekinna vinnsluaðgerða og gildissviðs viðkomandi lagareglna og löggjafar sem eru í gildi í þriðja landinu. Þriðja

landið ætti að ábyrgjast að tryggð sé fullnægjandi vernd sem er í meginatriðum sambærileg þeirri sem er tryggð í Sambandinu, einkum þegar vinnsla persónuupplýsinga fer fram í einum eða fleiri tilgreindum geirum. Þriðja landið ætti einkum að tryggja skilvirkt og sjálfstætt eftirlit með persónuvernd og móta verklag vegna samstarfs við persónuverndaryfirvöld í aðildarríkjunum og skráðir einstaklingar ættu að njóta skilvirkra og framfylgjanlegra réttinda og geta leitað réttar síns fyrir stjórnsýsluyfirvaldi og dómstólum með skilvirkum hætti.

105) Auk alþjóðlegra skuldbindinga, sem þriðja landið eða alþjóðastofnunin hefur gengist undir, ætti framkvæmdastjórnin að taka tillit til skuldbindinga sem leiðir af þátttöku þriðja landsins eða alþjóðastofnunarinnar í marghliða eða svæðisbundnum kerfum, einkum í tengslum við vernd persónuupplýsinga, svo og framkvæmdar slíkra skuldbindinga. Einkum ætti að taka tillit til aðildar þriðja lands að samningi Evrópuráðsins frá 28. janúar 1981 um vernd einstaklinga varðandi vélræna vinnslu persónuupplýsinga og viðbótarbókunar við hann. Framkvæmdastjórnin ætti að hafa samráð við persónuverndarráðið þegar hún leggur mat á umfang verndar í þriðju löndum eða hjá alþjóðastofnunum.

106) Framkvæmdastjórnin ætti að fylgjast með framkvæmd ákvarðana um umfang verndar í þriðja landi, á yfirráðasvæði eða í tilgreindum geira innan þriðja lands eða hjá alþjóðastofnun og ætti að fylgjast með framkvæmd ákvarðana sem samþykktar eru á grundvelli 6. mgr. 25. gr. eða 4. mgr. 26. gr. tilskipunar 95/46/EB. Þegar framkvæmdastjórnin tekur ákvarðanir um hvort vernd sé fullnægjandi ætti hún að sjá til þess að fyrir hendi sé fyrirkomulag vegna reglubundinnar endurskoðunar á framkvæmd þeirra. Þessi reglubundna endurskoðun ætti að fara fram í samráði við hlutaðeigandi þriðja land eða alþjóðastofnun og að teknu tilliti til viðeigandi þróunar í þriðja landinu eða hjá alþjóðastofnuninni. Að því er eftirlit og reglubundna endurskoðun varðar ætti framkvæmdastjórnin að taka tillit til sjónarmiða og niðurstaðna Evrópuþingsins og ráðsins, svo og annarra viðeigandi aðila og heimilda. Framkvæmdastjórnin ætti að meta, innan hæfilegs frests, framkvæmd síðarnefndu ákvarðananna og leggja skýrslu um viðeigandi niðurstöður fyrir nefndina í skilningi reglugerðar Evrópuþingsins og ráðsins (ESB) nr. 182/2011 ([1]), sem komið er á fót samkvæmt þessari reglugerð, og fyrir Evrópuþingið og ráðið.

107) Framkvæmdastjórnin getur staðfest að þriðja land, yfirráðasvæði eða tilgreindur geiri í þriðja landi eða alþjóðastofnun tryggi ekki lengur fullnægjandi persónuvernd. Af þessum sökum ætti að banna miðlun persónuupplýsinga til þessa þriðja lands eða alþjóðastofnunar nema fullnægt sé kröfum þessarar reglugerðar um miðlun með fyrirvara um viðeigandi verndarráðstafanir, þ.m.t. bindandi fyrirtækjareglur, og undanþágur vegna sérstakra aðstæðna. Í því tilviki ætti að gera ráð fyrir samráði milli framkvæmdastjórnarinnar og umræddra þriðju landa eða alþjóðastofnana. Framkvæmdastjórnin ætti að tilkynna þriðja landinu eða alþjóðastofnuninni tímanlega um ástæðurnar og hefja viðræður við það eða hana til þess að ráða bót á ástandinu.

108) Þegar ekki hefur verið tekin ákvörðun um það hvort fullnægjandi vernd er fyrir hendi ætti ábyrgðaraðili eða vinnsluaðili að gera ráðstafanir til að bæta upp skort á persónuvernd í þriðja landi með viðeigandi verndarráðstöfunum í þágu skráðs einstaklings. Viðeigandi verndarráðstafanir geta m.a. falist í því að nota bindandi fyrirtækjareglur, stöðluð ákvæði um persónuvernd sem framkvæmdastjórnin hefur samþykkt, stöðluð ákvæði um persónuvernd sem eftirlitsyfirvald hefur samþykkt eða samningsákvæði sem eftirlitsyfirvald hefur heimilað. Þessar verndarráðstafanir ættu að tryggja að farið sé að kröfum um persónuvernd og að virt séu réttindi skráðra einstaklinga sem varða vinnslu innan Sambandsins, þ.m.t. að fyrir liggi framfylgjanleg réttindi skráðra einstaklinga og skilvirk lagaleg úrræði, m.a. að hægt sé að leita réttar síns fyrir stjórnsýsluyfirvöldum eða dómstólum með skilvirkum hætti og að krefjast bóta, í Sambandinu eða í þriðja landi. Þær ættu einkum að varða fylgni við almennar meginreglur um vinnslu persónuupplýsinga og meginreglur um innbyggða og sjálfgefna persónuvernd. Opinber yfirvöld eða stofnanir geta einnig miðlað upplýsingum til opinberra yfirvalda eða stofnana í þriðju löndum eða til alþjóðastofnana sem hafa samsvarandi skyldur eða hlutverk, m.a. á grundvelli ákvæða sem eru felld inn í stjórnvaldsráðstafanir, s.s. samkomulag, sem veita skráðum einstaklingum framfylgjanleg og skilvirk réttindi. Afla ætti heimildar lögbærs eftirlitsyfirvalds ef gert er ráð fyrir verndarráðstöfunum í stjórnvaldsráðstöfunum sem eru ekki lagalega bindandi.

109) Möguleiki ábyrgðaraðila eða vinnsluaðila á að beita stöðluðum ákvæðum um persónuvernd, sem framkvæmdastjórnin eða eftirlitsyfirvald hefur samþykkt, ætti hvorki að hindra ábyrgðaraðila né vinnsluaðila í að fella stöðluð ákvæði um

([1]) Reglugerð Evrópuþingsins og ráðsins (ESB) nr. 182/2011 frá 16. febrúar 2011 um reglur og almennar meginreglur varðandi tilhögun eftirlits aðildarríkjanna með framkvæmdastjórninni þegar hún beitir framkvæmdavaldi sínu (Stjtíð. ESB L 55, 28.2.2011, bls. 13).

persónuvernd inn í víðtækari samning, s.s. samning milli ábyrgðaraðilans og annars ábyrgðaraðila, né heldur í að bæta við öðrum ákvæðum eða viðbótarverndarráðstöfunum, að því tilskildu að þau stangist ekki með beinum eða óbeinum hætti á við stöðluðu samningsákvæðin, sem framkvæmdastjórnin eða eftirlitsyfirvald hefur samþykkt, eða hafi áhrif á grundvallarréttindi eða frelsi skráðra einstaklinga. Hvetja ætti ábyrgðaraðila og vinnsluaðila til að gera frekari verndarráðstafanir með hjálp samningsbundinna skuldbindinga sem koma til viðbótar stöðluðum verndarákvæðum.

110) Fyrirtækjasamstæða eða hópur fyrirtækja í sameiginlegri atvinnustarfsemi ætti að geta notað viðurkenndar bindandi fyrirtækjareglur varðandi alþjóðlega miðlun sína frá Sambandinu til skipulagsheilda innan sömu fyrirtækjasamstæðu eða hóps fyrirtækja í sameiginlegri atvinnustarfsemi, að því tilskildu að þessar fyrirtækjareglur nái yfir allar mikilvægar meginreglur og framfylgjanleg réttindi til að tryggja viðeigandi verndarráðstafanir vegna miðlunar eða miðlunarflokka persónuupplýsinga.

111) Setja ætti ákvæði um möguleika á miðlun við sérstakar aðstæður þegar skráður einstaklingur hefur veitt ótvírætt samþykki sitt og miðlunin er tilfallandi og nauðsynleg í tengslum við samning eða réttarkröfu, hvort heldur er við dómsmeðferð eða stjórnsýslumeðferð eða aðra málsmeðferð utan dómstóla, þ.m.t. málsmeðferð hjá eftirlitsaðilum. Einnig ætti að gera ráð fyrir möguleika á miðlun þegar brýnir almannahagsmunir, sem mælt er fyrir um í lögum Sambandsins eða lögum aðildarríkis, krefjast þess eða þegar miðlunin er úr skrá sem komið var á fót samkvæmt lögum og ætluð er til þess að almenningur eða þeir sem hafa lögmætra hagsmuna að gæta geti skoðað hana. Í síðarnefnda tilvikinu ætti miðlunin ekki að ná til persónuupplýsinganna í heild sinni eða heilla flokka upplýsinga í skránni og miðlunin ætti, þegar gert er ráð fyrir að þeir sem hafa lögmætra hagsmuna að gæta geti skoðað skrána, aðeins að fara fram að beiðni þeirra eða, ef þeir eiga að vera viðtakendur upplýsinganna, að teknu fullu tilliti til hagsmuna og grundvallarréttinda hins skráða.

112) Undanþágurnar ættu einkum að gilda um miðlun upplýsinga sem eru nauðsynlegar vegna mikilvægra almannahagsmuna, t.d. þegar um er að ræða alþjóðleg upplýsingaskipti milli samkeppnisyfirvalda, skatta- eða tollyfirvalda, milli fjármálaeftirlitsstofnana, milli stofnana sem starfa á sviði almannatrygginga eða lýðheilsu, t.d. við að rekja smitleiðir vegna smitsjúkdóma eða í þeim tilgangi að draga úr og/eða útrýma lyfjamisnotkun í íþróttum. Einnig ætti miðlun persónuupplýsinga að teljast lögmæt þegar hún er nauðsynleg til að vernda hagsmuni sem skipta sköpum fyrir brýna hagsmuni skráðs einstaklings eða annars einstaklings, þ.m.t. líkamlega friðhelgi eða líf, ef hinn skráði er ekki fær um að veita samþykki sitt. Þegar ekki hefur verið tekin ákvörðun um hvort fullnægjandi vernd er fyrir hendi geta lög Sambandsins eða lög aðildarríkis takmarkað, í ljósi mikilvægra almannahagsmuna, sérstaklega miðlun tiltekinna flokka upplýsinga til þriðja lands eða alþjóðastofnunar. Aðildarríkin ættu að tilkynna framkvæmdastjórninni um slík ákvæði. Telja mætti miðlun persónuupplýsinga um skráðan einstakling, sem er líkamlega eða í lagalegum skilningi ófær um að veita samþykki sitt, til alþjóðlegrar stofnunar á sviði mannúðarmála vegna framkvæmdar verkefnis samkvæmt Genfarsamningunum eða til að framfylgja alþjóðlegum mannúðarlögum sem gilda um vopnuð átök, nauðsynlega í ljósi mikilvægra almannahagsmuna eða þess að það varðar brýna hagsmuni hins skráða.

113) Miðlun, sem telja má að verði ekki endurtekin og sem aðeins varðar takmarkaðan fjölda skráðra einstaklinga, gæti einnig verið möguleg með tilliti til mikilvægra lögmætra hagsmuna sem ábyrgðaraðili gætir þegar hagsmunir eða réttindi og frelsi skráðs einstaklings ganga þeim ekki framar og ef ábyrgðaraðilinn hefur kannað allar aðstæður í tengslum við miðlun upplýsinganna. Ábyrgðaraðilinn ætti einkum að skoða eðli persónuupplýsinganna, tilgang og tímalengd fyrirhugaðrar vinnsluaðgerðar eða -aðgerða, svo og aðstæður í upprunalandinu, þriðja landinu og endanlegu viðtökulandi og ætti að gera viðeigandi verndarráðstafanir til að vernda grundvallarréttindi og frelsi einstaklinga með tilliti til vinnslu persónuupplýsinga þeirra. Slík miðlun ætti aðeins að vera möguleg í einstaka tilvikum þegar engin annarra nefndra ástæðna til miðlunar á við. Taka ætti tillit til lögmætra væntinga samfélagsins um aukna þekkingu þegar um er að ræða vísindalegar eða sagnfræðilegar rannsóknir eða tölfræðilegan tilgang. Ábyrgðaraðilinn ætti að tilkynna eftirlitsyfirvaldinu og hinum skráða um miðlunina.

114) Hvað sem öðru líður ætti ábyrgðaraðili eða vinnsluaðili, ef framkvæmdastjórnin hefur ekki tekið ákvörðun um hvort persónuvernd sé fullnægjandi í þriðja landi, að nýta sér lausnir sem veita skráðum einstaklingum framfylgjanleg og skilvirk réttindi að því er varðar vinnslu persónuupplýsinga um þá í Sambandinu eftir að miðlun þessara upplýsinga hefur farið fram svo að þeir njóti áfram grundvallarréttinda og verndarráðstafana.

115) Sum þriðju lönd samþykkja lög, reglur og aðrar réttargerðir sem lúta að beinu eftirliti með vinnsluaðgerðum einstaklinga og lögaðila undir lögsögu aðildarríkjanna. Þetta kann að taka til dóma, sem dómstólar kveða upp eða ákvarðana stjórnvalda í þriðju löndum, sem krefjast þess að ábyrgðaraðili eða vinnsluaðili miðli persónuupplýsingum eða birti þær og sem byggjast ekki á alþjóðasamningi á borð við samning um gagnkvæma dómsmálaaðstoð, sem er í gildi milli þriðja landsins, sem leggur fram beiðni, og Sambandsins eða aðildarríkis. Ef beiting þessara laga, reglna og annarra réttargerða er ekki svæðisbundin getur það gengið gegn þjóðarétti og kann að standa í vegi fyrir þeirri vernd sem einstaklingum er tryggð í Sambandinu með þessari reglugerð. Aðeins ætti að heimila miðlun ef skilyrðum þessarar reglugerðar um miðlun til þriðju landa er fullnægt. Þetta getur m.a. átt við þegar birting er nauðsynleg vegna mikilvægra almannahagsmuna sem viðurkenndir eru í lögum Sambandsins eða lögum aðildarríkis sem ábyrgðaraðili heyrir undir.

116) Þegar persónuupplýsingar fara yfir landamæri utan Sambandsins getur það leitt til aukinnar áhættu fyrir getu einstaklinga til að neyta réttar síns til persónuverndar, einkum verja sig gegn ólögmætri notkun eða birtingu umræddra upplýsinga. Jafnframt geta eftirlitsyfirvöld komist að þeirri niðurstöðu að þau geti ekki fylgt eftir kvörtunum eða sinnt rannsóknum í tengslum við starfsemi utan landamæra sinna. Ófullnægjandi valdheimildir til forvarna eða úrbóta, misræmi milli lagareglna og hindranir sem lúta að framkvæmd á borð við takmarkað fjármagn geta staðið í vegi fyrir viðleitni þeirra til að vinna saman yfir landamæri. Þess vegna þarf að hvetja til nánara samstarfs meðal eftirlitsyfirvalda á sviði persónuverndar til að hjálpa þeim við að skiptast á upplýsingum og vinna að rannsóknum með samsvarandi alþjóðlegum aðilum. Í þeim tilgangi að móta fyrirkomulag alþjóðlegrar samvinnu til að greiða fyrir og veita gagnkvæma aðstoð á alþjóðavettvangi við framkvæmd löggjafar um vernd persónuupplýsinga ættu framkvæmdastjórnin og eftirlitsyfirvöldin að skiptast á upplýsingum og starfa með lögbærum yfirvöldum þriðju landa að verkefnum sem tengjast beitingu valdheimilda þeirra, á gagnkvæmum grundvelli og í samræmi við þessa reglugerð.

117) Þýðingarmikill þáttur í vernd einstaklinga að því er varðar vinnslu persónuupplýsinga þeirra felst í því að koma eftirlitsyfirvöldum á fót í aðildarríkjunum með umboð til að gegna störfum sínum og beita valdheimildum sínum algerlega óháð öðrum. Aðildarríkin ættu að geta komið á fót fleiri en einu eftirlitsyfirvaldi til að endurspegla stjórnskipan sína, stjórnunarhætti og skipulag stjórnsýslu.

118) Sjálfstæði eftirlitsyfirvalda ætti ekki að þýða að þau þurfi ekki að hlíta eftirlits- eða vöktunarkerfum í tengslum við útgjöld sín eða eftirliti dómstóla.

119) Ef aðildarríki kemur á fót fleiri en einu eftirlitsyfirvaldi ætti það að koma á kerfi samkvæmt lögum til að tryggja skilvirka þátttöku eftirlitsyfirvaldanna í samræmingarkerfinu. Umrætt aðildarríki ætti einkum að tilnefna það eftirlitsyfirvald sem gegnir hlutverki sameiginlegs tengiliðar vegna virkrar þátttöku þessara yfirvalda í kerfinu til þess að tryggja skjóta og snurðulausa samvinnu við önnur eftirlitsyfirvöld, persónuverndarráðið og framkvæmdastjórnina.

120) Sérhvert eftirlitsyfirvald ætti að hafa yfir að ráða því fjármagni, þeim mannauði, húsakosti og innviðum sem nauðsynleg eru til að þau geti sinnt verkefnum sínum með skilvirkum hætti, þ.m.t. þeim sem lúta að gagnkvæmri aðstoð og samvinnu við önnur eftirlitsyfirvöld alls staðar í Sambandinu. Sérhvert eftirlitsyfirvald ætti að hafa sérstaka, opinbera árlega fjárhagsáætlun sem getur verið hluti af heildarfjárlögum fylkisins eða ríkisins.

121) Mæla ætti fyrir um almenn skilyrði fyrir fulltrúa eftirlitsyfirvaldsins í lögum hvers aðildarríkis og í þeim ætti einkum að kveða á um að þing, ríkisstjórn eða þjóðhöfðingjar aðildarríkisins skipi þessa fulltrúa á grundvelli gagnsærrar málsmeðferðar, að fenginni tillögu ríkisstjórnarinnar, ráðherra hennar, þingsins eða þingdeildar, eða að sjálfstæðum aðila sé falið það verkefni samkvæmt lögum aðildarríkis. Til þess að tryggja sjálfstæði eftirlitsyfirvaldsins ættu fulltrúarnir að koma fram af heilindum, ekki aðhafast neitt það sem er ósamrýmanlegt skyldum þeirra og ekki að stunda önnur launuð eða ólaunuð ósamrýmanleg störf á skipunartíma sínum. Eftirlitsyfirvaldið ætti að hafa eigið starfslið, valið af því sjálfu eða sjálfstæðum aðila, sem er komið á fót samkvæmt lögum aðildarríkis, og ætti það eingöngu að lúta stjórn fulltrúa eftirlitsyfirvaldsins.

122) Sérhvert eftirlitsyfirvald ætti að vera til þess bært á yfirráðasvæði eigin aðildarríkis að beita þeim valdheimildum og vinna þau verkefni sem því eru falin samkvæmt þessari reglugerð. Þau ættu einkum að taka til vinnslu í tengslum við

starfsemi starfsstöðvar ábyrgðaraðila eða vinnsluaðila á yfirráðasvæði eigin aðildarríkis, vinnslu opinberra yfirvalda eða einkaaðila á persónuupplýsingum í þágu almannahagsmuna, vinnslu sem hefur áhrif á skráða einstaklinga á yfirráðasvæði þess eða vinnslu af hálfu ábyrgðaraðila eða vinnsluaðila, sem hefur ekki staðfestu í Sambandinu, þegar hún beinist að skráðum einstaklingum sem búa á yfirráðasvæði þess. Þar á meðal ætti að vera meðferð kvartana frá skráðum einstaklingi, framkvæmd rannsókna á beitingu þessarar reglugerðar og vitundarefling meðal almennings um áhættuþætti, reglur, verndarráðstafanir og réttindi í tengslum við vinnslu persónuupplýsinga.

123) Eftirlitsyfirvöldin ættu að hafa eftirlit með beitingu ákvæðanna samkvæmt þessari reglugerð og stuðla að samræmdri framkvæmd hennar í öllu Sambandinu, til að vernda einstaklinga í tengslum við vinnslu persónuupplýsinga um þá og greiða fyrir frjálsu flæði persónuupplýsinga á innri markaðnum. Í því skyni ættu eftirlitsyfirvöld að hafa samstarf sín á milli og við framkvæmdastjórnina, án þess að nauðsynlegt sé að gera samning milli aðildarríkjanna um gagnkvæma aðstoð eða slíka samvinnu.

124) Þegar vinnsla persónuupplýsinga fer fram innan ramma starfsemi starfsstöðvar ábyrgðaraðila eða vinnsluaðila í Sambandinu og ábyrgðaraðilinn eða vinnsluaðilinn hefur staðfestu í fleiru en einu aðildarríki, eða þegar vinnsla, sem fram fer innan ramma starfsemi stakrar starfsstöðvar ábyrgðaraðila eða vinnsluaðila í Sambandinu, hefur veruleg áhrif eða búast má við að hún hafi veruleg áhrif á skráða einstaklinga í fleiri en einu aðildarríki, ætti eftirlitsyfirvald yfir höfuðstöðvum ábyrgðaraðila eða vinnsluaðila eða þessari einu starfsstöð ábyrgðaraðila eða vinnsluaðila að gegna hlutverki forystuyfirvalds. Það ætti að hafa samstarf við önnur hlutaðeigandi yfirvöld þegar ábyrgðaraðili eða vinnsluaðili er með starfsstöð á yfirráðsvæði þeirra, skráðir einstaklingar á yfirráðasvæði þeirra verða fyrir verulegum áhrifum eða kvörtun er lögð fram hjá þeim. Ef skráður einstaklingur, sem býr ekki í því aðildarríki, leggur fram kvörtun ætti eftirlitsyfirvaldið, sem kvörtunin er lögð fram hjá, einnig að vera hlutaðeigandi eftirlitsyfirvald. Innan ramma þeirra verkefna sinna að gefa út viðmiðunarreglur varðandi álitaefni, sem upp kunna að koma varðandi beitingu þessarar reglugerðar, ætti persónuverndarráðið að geta gefið út viðmiðunarreglur, einkum um þær viðmiðanir sem taka ber tillit til þegar gengið er úr skugga um hvort viðkomandi vinnsla hafi veruleg áhrif á skráða einstaklinga í fleiri en einu aðildarríki og hvað teljast vera viðeigandi og rökstudd andmæli.

125) Forystuyfirvaldið ætti að vera til þess bært að samþykkja bindandi ákvarðanir um ráðstafanir og beita til þess þeim valdheimildum sem því eru fengnar í samræmi við þessa reglugerð. Í krafti hlutverks síns sem forystuyfirvald ætti eftirlitsyfirvaldið að virkja hlutaðeigandi eftirlitsyfirvöld til þátttöku í ákvarðanatökuferlinu og samhæfa þau. Ef ákveðið er að hafna kvörtun viðkomandi skráðs einstaklings, að öllu leyti eða að hluta til, ætti eftirlitsyfirvaldið, sem kvörtunin var lögð fram hjá, að taka þá ákvörðun.

126) Forystueftirlitsyfirvaldið og önnur hlutaðeigandi eftirlitsyfirvöld ættu að komast að samkomulagi um ákvörðunina og henni ætti að beina til höfuðstöðva eða hinnar einu starfsstöðvar ábyrgðaraðilans eða vinnsluaðilans og vera bindandi gagnvart honum. Ábyrgðaraðilinn eða vinnsluaðilinn ætti að grípa til nauðsynlegra ráðstafana til að tryggja að farið sé að þessari reglugerð og framkvæmd ákvörðunarinnar sem forystueftirlitsyfirvaldið tilkynnir um til höfuðstöðva ábyrgðaraðilans eða vinnsluaðilans að því er varðar vinnslustarfsemi í Sambandinu.

127) Eftirlitsyfirvald, sem gegnir ekki hlutverki forystueftirlitsyfirvalds, ætti að vera til þess bært að taka á staðbundnum málum þegar ábyrgðaraðili eða vinnsluaðili hefur staðfestu í fleiri en einu aðildarríki en viðfangsefni hinnar tilteknu vinnslu varðar einungis vinnslu sem fram fer í einu aðildarríki og tekur einungis til skráðra einstaklinga í því eina aðildarríki, t.d. þegar það varðar vinnslu persónuupplýsinga um starfsmenn í tilteknu atvinnutengdu samhengi í aðildarríki. Í þeim tilvikum ætti eftirlitsyfirvaldið að tilkynna forystueftirlitsyfirvaldinu um málið án tafar. Eftir að forystueftirlitsyfirvaldinu hefur verið tilkynnt um málið ætti það að ákveða hvort það muni afgreiða það samkvæmt ákvæðinu um samstarf milli forystueftirlitsyfirvaldsins og annarra hlutaðeigandi eftirlitsyfirvalda („afgreiðsla á einum stað“) eða hvort eftirlitsyfirvaldið, sem sendi því tilkynninguna, eigi að afgreiða málið á staðarvísu. Þegar forystueftirlitsyfirvaldið tekur ákvörðun um hvort það muni afgreiða málið ætti það að taka tillit til þess hvort ábyrgðaraðili eða vinnsluaðili er með starfsstöð í aðildarríki eftirlitsyfirvaldsins, sem tilkynnti um málið, til að tryggja skilvirka framfylgd ákvörðunar gagnvart ábyrgðaraðilanum eða vinnsluaðilanum. Ákveði forystueftirlitsyfirvaldið að taka sjálft að sér afgreiðslu málsins ætti eftirlitsyfirvaldið, sem tilkynnti um málið, að eiga kost á því að leggja fram drög

að ákvörðun sem forystueftirlitsyfirvaldinu ber að taka ítrasta tillit til þegar það útbýr drög sín að ákvörðun innan fyrirkomulagsins um afgreiðslu á einum stað.

128) Reglurnar um forystueftirlitsyfirvald og afgreiðslu á einum stað ættu ekki að gilda þegar opinber yfirvöld eða einkaaðilar annast vinnsluna í þágu almannahagsmuna. Í þeim tilvikum ætti eftirlitsyfirvald aðildarríkisins, þar sem opinbera yfirvaldið eða einkaaðilinn hefur staðfestu, að vera eina eftirlitsyfirvaldið sem er til þess bært að beita þeim valdheimildum sem því eru fengnar samkvæmt þessari reglugerð.

129) Til þess að tryggja samræmt eftirlit og framfylgd þessarar reglugerðar alls staðar í Sambandinu ættu eftirlitsyfirvöld að hafa í hverju aðildarríki á hendi sömu verkefni og skilvirkar valdheimildir, þ.m.t. heimildir til rannsókna, til að gera ráðstafanir til úrbóta og setja viðurlög og leyfisveitinga- og ráðgjafarheimildir, einkum þegar um er að ræða kvartanir frá einstaklingum og, án þess að það hafi áhrif á valdheimildir yfirvalda sem fara með ákæruvald samkvæmt lögum aðildarríkis, til að vekja athygli dómsyfirvalda á brotum gegn þessari reglugerð og fara með mál fyrir dóm. Á meðal slíkra valdheimilda ætti einnig að vera heimild til að taka upp tímabundna eða varanlega takmörkun á vinnslu, þ.m.t. bann. Aðildarríkin geta tilgreint önnur verkefni í tengslum við vernd persónuupplýsinga samkvæmt þessari reglugerð. Valdheimildum eftirlitsyfirvalda ætti að beita í samræmi við viðeigandi réttarfarsreglur sem settar eru fram í lögum Sambandsins og lögum aðildarríkis, af óhlutdrægni og sanngirni og innan hæfilegs tíma. Einkum ætti sérhver ráðstöfun að vera viðeigandi, nauðsynleg og hófleg til að tryggja að farið sé að þessari reglugerð, með hliðsjón af aðstæðum í hverju tilviki fyrir sig, virða rétt hvers aðila til að koma sjónarmiðum sínum á framfæri áður en gripið er til einhverrar þeirrar ráðstöfunar sem væri honum í óhag og þannig útfærð að komist sé hjá óhóflegum kostnaði og óþægindum fyrir viðkomandi einstaklinga. Rannsóknarheimildum að því er varðar aðgang að athafnasvæði ætti að beita í samræmi við sérstakar kröfur í réttarfarslögum aðildarríkisins, s.s. kröfuna um að afla fyrirframheimildar dómsmálayfirvalda. Sérhver lagalega bindandi ráðstöfun eftirlitsyfirvaldsins ætti að vera skrifleg, skýr og ótvíræð, í henni ætti að koma fram hvaða eftirlitsyfirvald gaf hana út, útgáfudagur, á henni ætti að vera undirskrift yfirmanns eða fulltrúa eftirlitsyfirvaldsins sem hann hefur veitt umboð sitt, þar skulu koma fram ástæður fyrir ráðstöfuninni og vísað til réttarins til skilvirks úrræðis til að leita réttar síns. Þetta útilokar ekki viðbótarkröfur samkvæmt réttarfarslögum aðildarríkis. Þegar tekin er lagalega bindandi ákvörðun getur það haft í för með sér endurskoðun dómstóla í aðildarríki eftirlitsyfirvaldsins sem samþykkti ákvörðunina.

130) Ef eftirlitsyfirvald, sem kvörtun er lögð fram hjá, er ekki forystueftirlitsyfirvald ætti forystueftirlitsyfirvaldið að starfa náið með eftirlitsyfirvaldinu, sem kvörtunin er lögð fram hjá, í samræmi við ákvæði þessarar reglugerðar um samstarf og samræmi. Í þeim tilvikum ætti forystueftirlitsyfirvaldið, þegar það gerir ráðstafanir sem ætlað er að hafa réttaráhrif, þ.m.t. þegar lagðar eru á stjórnsýslusektir, að taka ýtrasta tillit til sjónarmiða eftirlitsyfirvaldsins sem kvörtunin var lögð fram hjá og það yfirvald ætti áfram að vera til þess bært að annast hvers kyns rannsóknir á yfirráðasvæði eigin aðildarríkis í samráði við lögbæra eftirlitsyfirvaldið.

131) Þegar annað eftirlitsyfirvald ætti að fara með hlutverk forystueftirlitsyfirvalds vegna vinnslustarfsemi ábyrgðaraðila eða vinnsluaðila en efni kvörtunar eða hugsanlegt brot varðar einungis vinnslustarfsemi ábyrgðaraðila eða vinnsluaðila í aðildarríkinu þar sem kvörtunin var lögð fram eða hugsanlegt brot greindist og málið hefur ekki veruleg áhrif, né heldur er búist við að það muni hafa veruleg áhrif, á skráða einstaklinga í öðrum aðildarríkjum, ætti eftirlitsyfirvaldið, sem tekur við kvörtuninni eða sem kemst á snoðir um eða er látið vita á annan hátt af aðstæðum sem gætu haft í för með sér hugsanlegt brot á þessari reglugerð, að leitast við að ná góðri sátt við ábyrgðaraðilann og, ef það tekst ekki, beita valdheimildum sínum að fullu. Þetta ætti að ná til tiltekinnar vinnslu sem fram fer á yfirráðasvæði aðildarríkis eftirlitsyfirvaldsins eða, að því er varðar skráða einstaklinga á yfirráðasvæði þess aðildarríkis, vinnslu sem fram fer í tengslum við boð á vörum eða þjónustu sem beint er sérstaklega til skráðra einstaklinga á yfirráðasvæði aðildarríkis eftirlitsyfirvaldsins eða vinnslu sem þarf að meta með hliðsjón af viðeigandi lagaskyldum samkvæmt lögum aðildarríkis.

132) Starfsemi eftirlitsyfirvalda, sem miðar að vitundarvakningu og beint er að almenningi, ætti m.a. að fela í sér sérstakar ráðstafanir sem beint er að ábyrgðaraðilum og vinnsluaðilum, þ.m.t. örfyrirtækjum, litlum og meðalstórum fyrirtækjum, og einnig einstaklingum, einkum í fræðsluskyni.

133) Eftirlitsyfirvöld ættu að aðstoða hvert annað við framkvæmd verkefna sinna og láta í té gagnkvæma aðstoð til að tryggja samræmda beitingu og framkvæmd þessarar reglugerðar á innri markaðnum. Eftirlitsyfirvald, sem biður um gagnkvæma aðstoð, getur gripið til bráðabirgðaráðstöfunar ef því berst ekkert svar við beiðninni um gagnkvæma aðstoð innan mánaðar frá því að hinu eftirlitsyfirvaldinu barst beiðnin.

134) Sérhvert eftirlitsyfirvald ætti, eftir því sem við á, að taka þátt í sameiginlegum aðgerðum ásamt öðrum eftirlitsyfirvöldum. Eftirlitsyfirvaldi, sem berst beiðni, ætti að vera skylt að svara beiðninni innan tiltekins tíma.

135) Til þess að tryggja samræmda beitingu þessarar reglugerðar í öllu Sambandinu ætti að koma á fót samræmingarkerfi um samstarf milli eftirlitsyfirvalda. Einkum ætti að beita kerfinu þegar eftirlitsyfirvald hyggst gera ráðstöfun sem ætlað er að hafa réttaráhrif vegna vinnsluaðgerða sem hafa veigamikil áhrif á verulegan fjölda skráðra einstaklinga í nokkrum aðildarríkjum. Því ætti einnig að beita þegar eitthvert hlutaðeigandi eftirlitsyfirvalda eða framkvæmdastjórnin fer fram á að samræmingarkerfið annist meðferð slíks máls. Kerfið ætti ekki að hafa áhrif á neinar þær ráðstafanir sem framkvæmdastjórnin kann að grípa til þegar hún beitir valdheimildum sínum samkvæmt sáttmálunum.

136) Þegar samræmingarkerfið er notað ætti persónuverndarráðið, innan tiltekins tíma, að gefa út álit ef meirihluti fulltrúa þess ákveður það eða ef eitthvert hlutaðeigandi eftirlitsyfirvalda eða framkvæmdastjórnin fer fram á það. Persónuverndarráðið ætti einnig að hafa vald til að taka lagalega bindandi ákvarðanir þegar ágreiningur ríkir milli eftirlitsyfirvalda. Í því skyni ætti það að gefa út, að jafnaði með meirihluta sem nemur tveimur þriðju hlutum fulltrúa þess, lagalega bindandi ákvarðanir í skýrt skilgreindum málum þar sem eftirlitsyfirvöld greinir á um sjónarmið, sér í lagi innan samstarfskerfisins milli forystueftirlitsyfirvalds og hlutaðeigandi eftirlitsyfirvalda, um málavexti, einkum hvort um er að ræða brot á þessari reglugerð.

137) Skapast getur brýn þörf á aðgerðum til að vernda réttindi og frelsi skráðra einstaklinga, einkum þegar hætta gæti verið á verulegri hindrun á framfylgd réttinda skráðs einstaklings. Því ætti eftirlitsyfirvaldi að vera heimilt að grípa til, á yfirráðasvæði sínu, tilhlýðilega rökstuddra bráðabirgðaráðstafana með tilgreindan gildistíma sem ekki ætti að vera lengri en þrír mánuðir.

138) Beiting slíks kerfis ætti að vera skilyrði fyrir því að ráðstöfun eftirlitsyfirvalds, sem ætlað er að hafa réttaráhrif, teljist lögmæt í þeim tilvikum þar sem beiting þess er skyldubundin. Í öðrum tilvikum sem ná yfir landamæri ætti að beita samstarfskerfinu milli forystueftirlitsyfirvaldsins og hlutaðeigandi eftirlitsyfirvalda og beita mætti gagnkvæmri aðstoð og sameiginlegum aðgerðum milli hlutaðeigandi eftirlitsyfirvalda, tvíhliða eða marghliða, án þess að virkja samræmingarkerfið.

139) Til að ýta undir samræmda beitingu þessarar reglugerðar ætti að koma persónuverndarráðinu á fót sem sjálfstæðum aðila Sambandsins. Til að uppfylla markmið sín ætti persónuverndarráðið að hafa réttarstöðu lögaðila. Formaður persónuverndarráðsins kemur fram fyrir hönd þess. Það ætti að leysa af hólmi starfshópinn um vernd einstaklinga í tengslum við vinnslu persónuupplýsinga sem komið var á fót með tilskipun 95/46/EB. Í því ættu að eiga sæti yfirmenn eftirlitsyfirvalds hvers aðildarríkis og Evrópsku persónuverndarstofnunarinnar eða fulltrúar þeirra hvers um sig. Framkvæmdastjórnin ætti að taka þátt í starfsemi persónuverndarráðsins án atkvæðisréttar og Evrópska persónuverndarstofnunin ætti að hafa sérstakan atkvæðisrétt. Persónuverndarráðið ætti að stuðla að samræmdri beitingu þessarar reglugerðar í öllu Sambandinu, m.a. með ráðgjöf til framkvæmdastjórnarinnar, einkum um umfang verndar í þriðju löndum eða hjá alþjóðastofnunum og með því að ýta undir samstarf eftirlitsyfirvalda í Sambandinu. Persónuverndarráðið ætti að vera sjálfstætt í störfum sínum.

140) Persónuverndarráðið ætti að njóta aðstoðar skrifstofu sem Evrópska persónuverndarstofnunin sér því fyrir. Starfsfólk Evrópsku persónuverndarstofnunarinnar, sem kemur að framkvæmd þeirra verkefna sem persónuverndarráðinu eru falin með þessari reglugerð, ætti að vinna verkefni sín alfarið undir stjórn formanns persónuverndarráðsins og heyra undir hann.

141) Sérhver skráður einstaklingur ætti að eiga rétt á að leggja fram kvörtun hjá einu eftirlitsyfirvaldi, einkum í aðildarríkinu þar sem hann hefur fasta búsetu, og hafa rétt til skilvirks réttarúrræðis í samræmi við 47. gr. sáttmálans um

grundvallarréttindi ef hann telur að brotið sé á réttindum hans samkvæmt þessari reglugerð eða ef eftirlitsyfirvald sinnir ekki kvörtun, hafnar kvörtun að hluta til eða að öllu leyti eða vísar henni frá eða grípur ekki til aðgerða þar sem aðgerða er þörf til að vernda réttindi hans. Rannsókn á kvörtun ætti að fara fram, með fyrirvara um endurskoðun dómstóla, að því marki sem við á í hverju tilviki. Eftirlitsyfirvaldið ætti að tilkynna hinum skráða um framvindu og niðurstöðu kvörtunarinnar innan hæfilegs tíma. Ef þörf er á frekari rannsókn málsins eða samræmingu við annað eftirlitsyfirvald ætti að veita hinum skráða í millitíðinni upplýsingar um stöðu málsins. Til að auðvelda framlagningu kvartana ætti hvert eftirlitsyfirvald að gera ráðstafanir á borð við að bjóða upp á kvörtunareyðublað, sem einnig má fylla út rafrænt, án þess þó að útiloka aðra samskiptamöguleika.

142) Telji skráður einstaklingur að brotið hafi verið á réttindum hans samkvæmt þessari reglugerð ætti hann að hafa rétt til að veita stofnun, samtökum eða félagi, sem ekki eru rekin í hagnaðarskyni og sem stofnuð eru í samræmi við lög aðildarríkis, hafa lögboðin markmið og eru virk á sviði verndar persónuupplýsinga, umboð til að leggja fram kvörtun fyrir sína hönd hjá eftirlitsyfirvaldi, nýta réttinn til réttarúrræðis fyrir hönd skráðra einstaklinga eða, ef kveðið er á um það í lögum aðildarríkis, nýta réttinn til að taka við skaðabótum fyrir hönd skráðra einstaklinga. Aðildarríki er heimilt að mæla fyrir um að slík stofnun, samtök eða félag eigi rétt á að leggja fram kvörtun í því aðildarríki, óháð því hvort hinn skráði hefur veitt umboð til þess, og rétt til skilvirks réttarúrræðis hafi það ástæður til að ætla að réttindi skráðs einstaklings hafi verið brotin við vinnslu persónuupplýsinga sem brýtur gegn þessari reglugerð. Ekki má heimila stofnuninni, samtökunum eða félaginu að krefjast bóta fyrir hönd skráðs einstaklings án umboðs hans.

143) Einstaklingur eða lögaðili hefur rétt til þess að höfða mál til ógildingar ákvörðunum persónuverndarráðsins frammi fyrir Dómstólnum samkvæmt þeim skilyrðum sem kveðið er á um í 263. gr. sáttmálans um starfshætti Evrópusambandsins. Sem viðtakendur slíkra ákvarðana þurfa hlutaðeigandi eftirlitsyfirvöld, sem vilja vefengja þær, að höfða mál innan tveggja mánaða frá því að þeim er tilkynnt um þær, í samræmi við 263. gr. sáttmálans um starfshætti Evrópusambandsins. Þegar ákvarðanir persónuverndarráðsins varða beint sérstaka hagsmuni ábyrgðaraðila, vinnsluaðila eða kvartanda getur hann höfðað mál til ógildingar þessum ákvörðunum innan tveggja mánaða frá birtingu þeirra á vefsetri persónuverndarráðsins, í samræmi við 263. gr. sáttmálans um starfshætti Evrópusambandsins. Með fyrirvara um þennan rétt skv. 263. gr. sáttmálans um starfshætti Evrópusambandsins ætti sérhver einstaklingur eða lögaðili að hafa aðgang að skilvirku réttarúrræði fyrir lögbærum innlendum dómstóli að því er varðar ákvörðun eftirlitsyfirvalds sem hefur réttaráhrif gagnvart honum. Slík ákvörðun varðar einkum beitingu eftirlitsyfirvalds á rannsóknarheimildum, valdheimildum til að mæla fyrir um ráðstafanir til úrbóta og leyfisveitingarheimildum sínum eða frávísun eða höfnun kvartana. Þó nær réttur til skilvirks réttarúrræðis ekki til þeirra ráðstafana eftirlitsyfirvalda sem eru ekki lagalega bindandi, s.s. álitsgerða eða ráðgjafar eftirlitsyfirvaldsins. Höfða ætti mál gegn eftirlitsyfirvaldi fyrir dómstólum aðildarríkisins þar sem eftirlitsyfirvaldið hefur staðfestu og reka það í samræmi við réttarfarslög þess aðildarríkis. Þessir dómstólar ættu að fara með fulla lögsögu, m.a. til að rannsaka öll álitamál varðandi staðreyndir eða lög viðkomandi deiluefninu sem þeir hafa fengið til meðferðar.

Hafi eftirlitsyfirvald hafnað kröfu eða vísað henni frá getur sá sem lagði kvörtunina fram höfðað mál fyrir dómstólum í sama aðildarríki. Innan ramma réttarúrræða vegna beitingar þessarar reglugerðar geta innlendir dómstólar, sem telja að ákvörðun um álitaefnið sé nauðsynleg til að þeir geti kveðið upp úrskurð, farið fram á, eða verða að fara fram á í því tilviki sem um getur í 267. gr. sáttmálans um starfshætti Evrópusambandsins, að Dómstóllinn kveði upp forúrskurð um túlkun laga Sambandsins, m.a. þessarar reglugerðar. Þegar ákvörðun eftirlitsyfirvalds til framkvæmdar ákvörðun persónuverndarráðsins er vefengd fyrir innlendum dómstól og deilt er um gildi ákvörðunar persónuverndarráðsins hefur innlendi dómstóllinn ekki vald til að lýsa ákvörðun þess ógilda heldur verður hann að vísa álitaefninu um gildi hennar til Dómstólsins í samræmi við 267. gr. sáttmálans um starfshætti Evrópusambandsins, eins og Dómstóllinn túlkar hana, ef hann telur ákvörðunina ógilda. Hins vegar má innlendur dómstóll ekki vísa áfram álitamáli um gildi ákvörðunar persónuverndarráðsins að beiðni einstaklings eða lögaðila sem hafði haft tækifæri til að höfða mál til ógildingar þeirri ákvörðun, einkum ef ákvörðunin varðaði beint sérstaka hagsmuni hans, en gerði það ekki innan frestsins sem mælt er fyrir um í 263. gr. sáttmálans um starfshætti Evrópusambandsins.

144) Hafi dómstóll, sem mál er höfðað fyrir gegn ákvörðun eftirlitsyfirvalds, ástæðu til að ætla að höfðað hafi verið mál vegna sömu vinnslu fyrir lögbærum dómstóli í öðru aðildarríki, þar sem t.d. um er að ræða sama viðfangsefni að því er varðar vinnslu af hálfu sama ábyrgðaraðila eða vinnsluaðila eða sömu málsástæður, ætti hann að setja sig í samband við þann dómstól til að fá staðfest hvort um skyld mál sé að ræða. Ef skylt mál er til meðferðar hjá dómstóli í öðru aðildarríki getur hvaða dómstóll sem er, annar en sá sem málið var fyrst höfðað fyrir, frestað málsmeðferð sinni eða, að

beiðni eins málsaðilanna, vísað málinu frá dómi í þágu dómstólsins sem málið var fyrst höfðað fyrir ef sá dómstóll er bær til að fara með málið og lög, sem gilda við þann dómstól, heimila að skyld mál séu sótt sameiginlega. Með skyldum málum er átt við mál sem eru svo tengd innbyrðis að æskilegt er að fara með þau og úrskurða í þeim sameiginlega til að koma í veg fyrir að ósamrýmanlegir dómar verði kveðnir upp ef dæmt er í hverju þeirra sérstaklega.

145) Þegar um er að ræða mál á hendur ábyrgðaraðila eða vinnsluaðila ætti stefnandi að geta valið um það hvort hann höfðar málið fyrir dómstólum aðildarríkja þar sem ábyrgðaraðili eða vinnsluaðili hefur starfsstöð eða þar sem hinn skráði er búsettur nema ábyrgðaraðili sé opinbert yfirvald aðildarríkis sem fer með opinbert vald.

146) Ábyrgðaraðili eða vinnsluaðili ætti að bæta hvert það tjón sem aðili verður fyrir vegna vinnslu sem brýtur í bága við reglugerð þessa. Ábyrgðaraðili eða vinnsluaðili ætti að vera undanþeginn bótaábyrgð ef hann sannar að hann ber enga ábyrgð á tjóni. Hugtakið tjón ætti að túlka vítt í ljósi dómaframkvæmdar Dómstólsins á þann hátt að það endurspegli að fullu markmið þessarar reglugerðar. Þetta hefur ekki áhrif á neinar skaðabótakröfur vegna brota á öðrum reglum Sambandslaga eða laga aðildarríkis. Til vinnslu, sem brýtur í bága við þessa reglugerð, telst einnig vinnsla sem brýtur í bága við framseldar gerðir og framkvæmdargerðir sem samþykktar eru í samræmi við þessa reglugerð og þau lög aðildarríkis sem tilgreina nánar reglur þessarar reglugerðar. Skráðir einstaklingar ættu að fá fullar skaðabætur fyrir það tjón sem þeir verða fyrir. Þegar fleiri en einn ábyrgðaraðili eða vinnsluaðili koma að sömu vinnslu ætti hver ábyrgðaraðili eða vinnsluaðili að vera ábyrgur fyrir öllu tjóninu. Þegar þeir eiga hlut að sama dómsmáli, í samræmi við lög aðildarríkis, geta skaðabætur þó skipst niður á þá eftir þeirri ábyrgð sem hver ábyrgðaraðili eða vinnsluaðili bar á tjóninu sem vinnslan olli, að því tilskildu að skráði einstaklingurinn, sem varð fyrir tjóninu, fái fullar skaðabætur. Ábyrgðaraðili eða vinnsluaðili, sem hefur greitt fullar skaðabætur, getur í kjölfarið gert endurkröfu á aðra ábyrgðaraðila eða vinnsluaðila sem tóku þátt í sömu vinnslu.

147) Þar sem þessi reglugerð hefur að geyma sértækar reglur um lögsögu, einkum að því er varðar mál þar sem leitað er réttarúrræðis gegn ábyrgðaraðila eða vinnsluaðila, m.a. skaðabóta, ættu almennar lögsögureglur, eins og þær sem um getur í reglugerð Evrópuþingsins og ráðsins (ESB) nr. 1215/2012 ([1]), ekki að hafa áhrif á beitingu þessara sértæku reglna.

148) Til að efla framfylgd reglna þessarar reglugerðar ætti að leggja á viðurlög, þ.m.t. stjórnsýslusektir, við hvers konar brotum á þessari reglugerð, til viðbótar við eða í staðinn fyrir viðeigandi ráðstafanir sem eftirlitsyfirvald gerir samkvæmt þessari reglugerð. Veita má áminningu í stað sektar þegar um er að ræða minni háttar brot eða ef sektin, sem líklegt er að lögð verði á, yrði óhófleg byrði fyrir einstakling. Engu að síður ætti að taka tilhlýðilegt tillit til þess hvers eðlis brotið er, hversu alvarlegt það er og hversu lengi það hefur staðið yfir, hvort það var framið af ásetningi, til hvaða aðgerða var gripið til að draga úr tjóni, hversu mikil ábyrgðin var eða hvort um fyrri brot sem skipta máli er að ræða, hvernig eftirlitsyfirvaldið komst á snoðir um brotið, hvort ráðstöfunum sem settar voru gagnvart ábyrgðaraðila eða vinnsluaðila var fylgt, hvort hátternisreglum var fylgt ásamt öðrum mildandi eða íþyngjandi þáttum. Álagning viðurlaga, þ.m.t. stjórnsýslusekta, ætti að vera háð viðeigandi réttarfarsreglum í samræmi við almennar meginreglur laga Sambandsins og sáttmálans um grundvallarréttindi, m.a. um skilvirka réttarvernd og sanngjarna málsmeðferð.

149) Aðildarríkin ættu að geta sett reglur um refsiviðurlög vegna brota á þessari reglugerð, þ.m.t. vegna brota á innlendum reglum sem samþykktar eru samkvæmt henni og innan marka hennar. Slík refsiviðurlög geta einnig gert ráð fyrir að viðkomandi sé sviptur þeim ávinningi sem hann hafði af brotum á þessari reglugerð. Hins vegar ætti álagning refsiviðurlaga vegna brota á slíkum innlendum reglum og stjórnsýsluviðurlögum ekki að leiða til brots á meginreglunni um að verða ekki saksóttur eða refsað tvívegis fyrir sama brot (ne bis in idem), eins og Dómstóllinn hefur túlkað hana.

150) Til að efla og samræma stjórnsýsluviðurlög vegna brota á þessari reglugerð ætti sérhvert eftirlitsyfirvald að hafa heimild til að leggja á stjórnsýslusektir. Í reglugerðinni ætti að tilgreina brotin ásamt hámarki og viðmiðunum við álagningu

([1]) Reglugerð Evrópuþingsins og ráðsins (EB) nr. 1215/2012 frá 12. desember 2012 um dómsvald og viðurkenningu á og fullnustu dóma í einkamálum og viðskiptamálum (Stjtíð. ESB L 351, 20.12.2012, bls. 1).

tengdra stjórnsýslusekta, sem eftirlitsyfirvaldið ætti að ákveða í hverju tilviki fyrir sig með hliðsjón af öllum viðeigandi kringumstæðum í viðkomandi máli, einkum að teknu tilhlýðilegu tilliti til eðlis, alvarleika og lengdar brotsins og afleiðinga þess og ráðstafana sem gerðar hafa verið til að tryggja að skuldbindingar samkvæmt þessari reglugerð séu uppfylltar og til að koma í veg fyrir eða draga úr afleiðingum brotsins. Þegar stjórnsýslusektir eru lagðar á fyrirtæki er átt við fyrirtæki í samræmi við 101. og 102. gr. sáttmálans um starfshætti Evrópusambandsins. Þegar stjórnsýslusektir eru lagðar á aðila sem ekki eru fyrirtæki ætti eftirlitsyfirvaldið að taka tillit til almenns tekjustigs í aðildarríkinu og fjárhagsstöðu aðilans þegar viðeigandi sektarfjárhæð er ákveðin. Einnig má nota samræmingarkerfið til að stuðla að samræmdri beitingu stjórnsýslusekta. Það ætti að vera aðildarríkjanna að ákvarða hvort og að hvaða marki opinber yfirvöld ættu að sæta stjórnsýslusektum. Það að lögð sé á stjórnsýslusekt eða að gefin sé viðvörun hefur ekki áhrif á beitingu annarra valdheimilda eftirlitsyfirvalda eða á önnur viðurlög samkvæmt þessari reglugerð.

151) Réttarkerfi Danmerkur og Eistlands heimila ekki stjórnsýslusektir eins og þær sem settar eru fram í þessari reglugerð. Beita má reglunum um stjórnsýslusektir í Danmörku með þeim hætti að þar til bærir innlendir dómstólar leggi sektina á sem refsiviðurlög og í Eistlandi þannig að eftirlitsyfirvald leggi sektina á innan ramma málsmeðferðar vegna minni háttar brots, að því tilskildu að slík beiting reglnanna í þessum aðildarríkjum hafi jafngild áhrif og stjórnsýslusektir sem eftirlitsyfirvöld leggja á. Því ættu þar til bærir innlendir dómstólar að taka tillit til tilmæla eftirlitsyfirvaldsins sem hefur frumkvæðið að álagningu sektarinnar. Álagðar sektir ættu þó ætíð að vera skilvirkar, í réttu hlutfalli við brot og hafa varnaðaráhrif.

152) Þegar þessi reglugerð samræmir ekki stjórnsýsluviðurlög eða ef þörf er á í öðrum tilvikum, t.d. þegar um er að ræða alvarleg brot á þessari reglugerð, ættu aðildarríkin að innleiða kerfi sem kveður á um viðurlög sem eru skilvirk, í réttu hlutfalli við brot og hafa varnaðaráhrif. Það hvort slík viðurlög eigi að vera refsiviðurlög eða stjórnsýslulegs eðlis ætti að ákvarða í lögum aðildarríkjanna.

153) Í lögum aðildarríkjanna ætti að samræma reglur um tjáningar- og upplýsingafrelsi, þ.m.t. í fréttamennsku, fræðimennsku, listum eða bókmenntum, og réttinn til verndar persónuupplýsingum samkvæmt þessari reglugerð. Vinnsla persónuupplýsinga, sem fer einungis fram í þágu fréttamennsku eða fræðimennsku eða listrænnar eða bókmenntalegrar tjáningar, ætti að vera háð undanþágum eða frávikum frá tilteknum ákvæðum þessarar reglugerðar ef það er nauðsynlegt til að samræma réttinn til verndar persónuupplýsingum og réttinn til tjáningar- og upplýsingafrelsis sem er tryggður með 11. gr. sáttmálans um grundvallarréttindi. Þetta ætti einkum að gilda um vinnslu persónuupplýsinga á sviði hljóð- og myndmiðlunar og í gagna- og bókasöfnum fréttamiðla. Því ættu aðildarríkin að samþykkja löggjafarráðstafanir þar sem mælt er fyrir um nauðsynlegar undanþágur og frávik til að halda jafnvægi milli þessara grundvallarréttinda. Aðildarríkin ættu að samþykkja slíkar undanþágur og frávik varðandi almennar meginreglur, réttindi skráðra einstaklinga, ábyrgðaraðila og vinnsluaðila, miðlun persónuupplýsinga til þriðju landa eða alþjóðastofnana, sjálfstæð eftirlitsyfirvöld, samstarf og samræmi og gagnavinnslu við tilteknar aðstæður. Ef slíkar undanþágur og frávik eru mismunandi milli aðildarríkja gilda lög aðildarríkisins sem ábyrgðaraðili heyrir undir. Með tilliti til mikilvægis réttarins til tjáningarfrelsis í hverju lýðræðisþjóðfélagi er nauðsynlegt að túlka hugtök vítt í tengslum við það frelsi, s.s. fréttamennsku.

154) Reglugerð þessi heimilar að tekið sé mið af meginreglunni um aðgang almennings að opinberum skjölum við beitingu hennar. Telja má að aðgangur almennings að opinberum skjölum sé í þágu almannahagsmuna. Persónuupplýsingar í skjölum í vörslu opinbers yfirvalds eða opinberrar stofnunar ætti viðkomandi yfirvaldi eða aðila að vera heimilt að birta almenningi ef kveðið er á um birtinguna í lögum Sambandsins eða lögum aðildarríkis sem opinbera yfirvaldið eða opinbera stofnunin heyrir undir. Slík lög ættu að samræma aðgang almennings að opinberum skjölum og endurnotkun upplýsinga frá hinu opinbera annars vegar og réttinn til verndar persónuupplýsingum hins vegar og geta því kveðið á um nauðsynlega samræmingu við réttinn til verndar persónuupplýsingum samkvæmt þessari reglugerð. Tilvísunin til opinberra yfirvalda og stofnana ætti í því samhengi að taka til allra yfirvalda eða annarra stofnana sem heyra undir lög aðildarríkis um aðgang almennings að skjölum. Tilskipun Evrópuþingsins og ráðsins 2003/98/EB ([1]) skerðir ekki og hefur á engan hátt áhrif á umfang verndar einstaklinga með tilliti til vinnslu persónuupplýsinga samkvæmt ákvæðum

([1]) Tilskipun Evrópuþingsins og ráðsins 2003/98/EB frá 17. nóvember 2003 um endurnotkun upplýsinga frá hinu opinbera (Stjtíð. ESB L 345, 31.12.2003, bls. 90).

laga Sambandsins og laga aðildarríkis og einkum breytir hún ekki þeim skyldum og réttindum sem sett eru fram í þessari reglugerð. Einkum ætti sú tilskipun ekki að gilda um gögn, sem enginn eða takmarkaður aðgangur er að samkvæmt reglum um aðgangsrétt með vísan til verndar persónuupplýsinga, og um hluta úr skjölum, sem eru aðgengilegir samkvæmt slíkum reglum, þegar skjalshlutarnir innihalda persónuupplýsingar og kveðið hefur verið á um í lögum að endurnotkun þeirra sé ósamrýmanleg lögum um vernd einstaklinga að því er varðar vinnslu persónuupplýsinga.

155) Í lögum aðildarríkis eða í kjarasamningum, þ.m.t. „vinnustaðasamningum“, kann að vera kveðið á um sértækar reglur um vinnslu persónuupplýsinga starfsmanna í atvinnutengdu samhengi, einkum skilyrði fyrir því að vinna megi persónuupplýsingar í atvinnutengdu samhengi á grundvelli samþykkis starfsmannsins og í sambandi við ráðningar, framkvæmd ráðningarsamnings, m.a. uppfyllingu skuldbindinga sem mælt er fyrir um í lögum eða kjarasamningum, stjórnun, undirbúning og skipulagningu vinnunnar, jafnrétti og fjölbreytileika á vinnustað, heilbrigði og öryggi á vinnustað, nýtingu og notkun réttinda og fríðinda sem tengjast starfinu, jafnt einstaklingsbundinna og sameiginlegra, og í þeim tilgangi að ljúka ráðningarsambandi.

156) Vinnsla persónuupplýsinga vegna skjalavistunar í þágu almannahagsmuna, rannsókna á sviði vísinda eða sagnfræði eða í tölfræðilegum tilgangi ætti að vera með fyrirvara um viðeigandi verndarráðstafanir varðandi réttindi og frelsi skráðra einstaklinga samkvæmt þessari reglugerð. Þessar verndarráðstafanir ættu að tryggja að tæknilegar og skipulagslegar ráðstafanir séu gerðar, einkum til að sjá til þess að farið sé að meginreglunni um lágmörkun gagna. Frekari vinnsla persónuupplýsinga vegna skjalavistunar í þágu almannahagsmuna, rannsókna á sviði vísinda eða sagnfræði eða í tölfræðilegum tilgangi skal fara fram þegar ábyrgðaraðili hefur metið hvort framkvæmanlegt sé að ná þessum tilgangi með vinnslu gagna sem gera ekki kleift, eða gera ekki lengur kleift, að bera kennsl á skráða einstaklinga, að því tilskildu að viðeigandi verndarráðstafanir séu fyrir hendi (s.s. notkun gerviauðkenna fyrir upplýsingarnar). Aðildarríkin ættu að kveða á um viðeigandi verndarráðstafanir varðandi vinnslu persónuupplýsinga vegna skjalavistunar í þágu almannahagsmuna, rannsókna á sviði vísinda eða sagnfræði eða í tölfræðilegum tilgangi. Aðildarríkjunum ætti að vera heimilt, með tilteknum skilyrðum og með fyrirvara um viðeigandi verndarráðstafanir fyrir skráða einstaklinga, að setja fram nánari skilgreiningar og undanþágur að því er varðar kröfur um upplýsingar og réttinn til leiðréttingar, eyðingar, til að gleymast, til takmörkunar á vinnslu, til að flytja eigin gögn og til að andmæla vinnslu persónuupplýsinga vegna skjalavistunar í þágu almannahagsmuna, rannsókna á sviði vísinda eða sagnfræði eða í tölfræðilegum tilgangi. Viðkomandi skilyrði og verndarráðstafanir geta haft í för með sér að skráðir einstaklingar þurfi að fylgja tiltekinni málsmeðferð til að geta nýtt sér þessi réttindi, ef við á í ljósi þess tilgangs sem stefnt er að með þessari tilteknu vinnslu, auk tæknilegra og skipulagslegra ráðstafana sem miða að því að lágmarka vinnslu persónuupplýsinga í samræmi við meðalhófsregluna og nauðsynjarregluna. Vinnsla persónuupplýsinga í vísindaskyni ætti einnig að vera í samræmi við aðra viðeigandi löggjöf, s.s. um klínískar prófanir.

157) Með því að tengja saman upplýsingar úr mismunandi skrám geta vísindamenn öðlast nýja og afar verðmæta þekkingu á útbreiddu heilsufarsástandi á borð við hjarta- og æðasjúkdóma, krabbamein og þunglyndi. Með notkun skráa er hægt að efla rannsóknarniðurstöður, þar sem þær byggjast á stærra þýði. Í félagsvísindum gera rannsóknir a grundvelli skráa vísindamönnum kleift að öðlast mikilvæga þekkingu á langtímafylgni milli félagslegra aðstæðna af ýmsum toga, s.s. atvinnuleysis og menntunar, og annarra aðstæðna í lífi fólks. Rannsóknarniðurstöður, sem fást með notkun skráa, gefa trausta og vandaða þekkingu sem nota má til grundvallar við mótun og framkvæmd þekkingarstefnu, til að bæta lífsgæði margra og bæta skilvirkni félagslegrar þjónustu. Til að greiða fyrir vísindarannsóknum er heimilt að vinna persónuupplýsingar í þágu rannsókna á sviði vísinda að uppfylltum viðeigandi skilyrðum og verndarráðstöfunum í lögum Sambandsins eða lögum aðildarríkis.

158) Þessi reglugerð ætti einnig að gilda um vinnslu persónuupplýsinga vegna skjalavistunar en þó ætti að hafa í huga að reglugerðin á ekki við um látna einstaklinga. Opinber yfirvöld, opinberir aðilar eða einkaaðilar, sem halda skrár sem tengjast almannahagsmunum, ættu að vera þjónustuaðilar sem hafa samkvæmt lögum Sambandsins eða lögum aðildarríkis lagaskyldu til að afla, varðveita, meta, skipuleggja, lýsa, veita upplýsingar um, kynna, dreifa og veita aðgang að skrám sem hafa varanlegt gildi fyrir almannahagsmuni. Aðildarríkin ættu einnig að hafa heimild til að kveða á um frekari vinnslu persónuupplýsinga vegna skjalavistunar, t.d. í því skyni að veita sérstakar upplýsingar um stjórnmálahegðun í ríkjum þar sem áður ríkti einræði, um þjóðarmorð, glæpi gegn mannúð, einkum helförina, eða stríðsglæpi.

159) Þessi reglugerð ætti einnig að gilda um vinnslu persónuupplýsinga í þágu vísindarannsókna. Að því er þessa reglugerð varðar ber að túlka vinnslu persónuupplýsinga í þágu vísindarannsókna vítt þannig að undir hana falli t.d. tækniþróun og tilraunaverkefni, grunnrannsóknir, hagnýtar rannsóknir og rannsóknir sem einkaaðilar fjármagna. Auk þess ætti hún að taka tillit til þess markmiðs Sambandsins, skv. 1. mgr. 179. gr. sáttmálans um starfshætti Evrópusambandsins, að koma á evrópsku rannsóknasvæði. Rannsóknir í þágu almannahagsmuna á sviði lýðheilsu ættu einnig að teljast þjóna vísindalegum tilgangi Til að uppfylla þær sérstöku kröfur sem gerðar eru til vinnslu persónuupplýsinga í þágu vísindarannsókna ættu sérstök skilyrði að gilda, einkum að því er varðar útgáfu eða aðra birtingu persónuupplýsinga í þágu vísindarannsókna. Gefi niðurstöður vísindarannsóknar, einkum á heilbrigðissviði, ástæðu til að gera frekari ráðstafanir í þágu hins skráða ættu almennar reglur þessarar reglugerðar að gilda í ljósi þessara ráðstafana.

160) Þessi reglugerð ætti einnig að gilda um vinnslu persónuupplýsinga í þágu sagnfræðirannsókna. Þetta ætti auk þess að ná til sagnfræðirannsókna og rannsókna í erfðafræðilegum tilgangi en þó ætti að hafa í huga að reglugerðin ætti ekki að gilda um látna einstaklinga.

161) Að því er varðar veitingu samþykkis fyrir þátttöku í vísindalegri rannsóknastarfsemi í klínískum prófunum ættu viðeigandi ákvæði reglugerðar Evrópuþingsins og ráðsins (ESB) nr. 536/2014 ([1]) að gilda.

162) Þessi reglugerð ætti að gilda um vinnslu persónuupplýsinga í tölfræðilegum tilgangi. Í lögum Sambandsins eða lögum aðildarríkis ætti að ákvarða, innan marka þessarar reglugerðar, tölfræðilegt innihald, eftirlit með aðgangi, nákvæmar skilgreiningar á vinnslu persónuupplýsinga í tölfræðilegum tilgangi og viðeigandi ráðstafanir til að standa vörð um réttindi og frelsi skráðra einstaklinga og tryggja trúnað í tengslum við tölfræðilegar upplýsingar. Tölfræðilegur tilgangur telst vera hver sú aðgerð sem felst í söfnun og vinnslu persónuupplýsinga sem nauðsynlegar eru vegna tölfræðilegra kannana eða til að ná fram tölfræðilegum niðurstöðum. Þessar tölfræðilegu niðurstöður má nota frekar í ýmiss konar tilgangi, þ.m.t. til vísindarannsókna. Tölfræðilegur tilgangur þýðir að niðurstöður vinnslu í tölfræðilegum tilgangi eru ekki persónuupplýsingar heldur samantekin gögn og að þessar niðurstöður eða persónuupplýsingarnar eru ekki notaðar til stuðnings ráðstöfunum eða ákvörðunum viðvíkjandi tilteknum einstaklingi.

163) Vernda ætti trúnaðarupplýsingar sem hagskýrsluyfirvöld Sambandsins og hagskýrsluyfirvöld aðildarríkjanna safna til að gera opinberar hagskýrslur fyrir Evrópu og aðildarríkin. Þróa ætti og semja evrópskar hagskýrslur og miðla þeim í samræmi við meginreglur um hagskýrslur, eins og þær eru settar fram í 2. mgr. 338. gr. sáttmálans um starfshætti Evrópusambandsins, en jafnframt ættu innlendar hagskýrslur einnig að uppfylla lög aðildarríkis. Í reglugerð Evrópuþingsins og ráðsins (EB) nr. 223/2009 ([2]) er kveðið á um nánari skilgreiningar á trúnaðarskyldum við hagskýrslugerð að því er varðar evrópskar hagskýrslur.

164) Að því er varðar valdheimildir eftirlitsyfirvalda til að fá hjá ábyrgðaraðila eða vinnsluaðila aðgang að persónuupplýsingum og aðgang að athafnasvæðum þeirra mega aðildarríki samþykkja með lögum, innan marka þessarar reglugerðar, sértækar reglur til að standa vörð um þagnarskyldu eða aðrar samsvarandi trúnaðarskyldur, að því marki sem nauðsynlegt er til að samræma réttinn til verndar persónuupplýsingum og þagnarskyldu. Þetta hefur ekki áhrif á fyrirliggjandi skuldbindingar aðildarríkis um að samþykkja reglur um þagnarskyldu ef lög Sambandsins kveða á um það.

165) Þessi reglugerð virðir þá stöðu sem kirkjudeildir og trúarsamtök eða trúfélög hafa í aðildarríkjunum samkvæmt fyrirliggjandi stjórnskipunarlögum og dregur hana ekki í efa, eins og viðurkennt er í 17. gr. sáttmálans um starfshætti Evrópusambandsins.

166) Til að ná markmiðum þessarar reglugerðar, þ.e. að vernda grundvallarréttindi og frelsi einstaklinga og einkum rétt þeirra til verndar persónuupplýsingum og tryggja frjálsa miðlun persónuupplýsinga innan Sambandsins, ætti að framselja

([1]) Reglugerð Evrópuþingsins og ráðsins (ESB) nr. 536/2014 frá 16. apríl 2014 um klíniskar prófanir á mannalyfjum og niðurfellingu á tilskipun 2001/20/EB (Stjtíð. ESB L 158, 27.5.2014, bls. 1).

([2]) Reglugerð Evrópuþingsins og ráðsins (EB) nr. 223/2009 frá 11. mars 2009 um evrópskar hagskýrslur og niðurfellingu reglugerðar Evrópuþingsins og ráðsins (EB, KBE) nr. 1101/2008 um afhendingu gagna sem eru háð trúnaðarkvöðum í hagskýrslum til Hagstofu Evrópubandalaganna, reglugerðar ráðsins (EB) nr. 322/97 um hagskýrslur Bandalagsins og ákvörðunar ráðsins 89/382/EBE, KBE um að koma á fót hagskýrsluáætlunarnefnd Evrópubandalaganna (Stjtíð. ESB. L 87, 31.3.2009, bls. 164).

framkvæmdastjórninni vald til að samþykkja gerðir í samræmi við 290. gr. sáttmálans um starfshætti Evrópusambandsins. Einkum ætti að samþykkja framseldar gerðir um viðmiðanir og kröfur varðandi vottunarfyrirkomulag, upplýsingar sem veita ber með stöðluðum táknmyndum og aðferðir við að setja fram slíkar táknmyndir. Einkar mikilvægt er að framkvæmdastjórnin hafi viðeigandi samráð meðan á undirbúningsvinnu hennar stendur, þ.m.t. við sérfræðinga. Við undirbúning og samningu framseldra gerða ætti framkvæmdastjórnin að tryggja samhliða, tímanlega og viðeigandi afhendingu viðkomandi skjala til Evrópuþingsins og ráðsins.

167) Til að tryggja samræmd skilyrði vegna framkvæmdar þessarar reglugerðar ætti að fela framkvæmdastjórninni framkvæmdarvald þegar kveðið er á um það í þessari reglugerð. Þessu valdi ætti að beita í samræmi við reglugerð (ESB) nr. 182/2011. Í þessu sambandi ætti framkvæmdastjórnin að íhuga sértækar ráðstafanir fyrir örfyrirtæki, lítil og meðalstór fyrirtæki.

168) Beita ætti rannsóknarmálsmeðferðinni við samþykkt framkvæmdargerða um föst samningsákvæði milli ábyrgðaraðila og vinnsluaðila og milli vinnsluaðila, hátternisreglur, tæknistaðla og fyrirkomulag við vottun, fullnægjandi vernd sem þriðja land, yfirráðasvæði eða tilgreindur geiri innan þess þriðja lands eða alþjóðastofnun veitir, stöðluð verndarákvæði, snið og aðferðir við rafræn upplýsingaskipti milli ábyrgðaraðila, vinnsluaðila og eftirlitsyfirvalda að því er varðar bindandi fyrirtækjareglur, gagnkvæma aðstoð og fyrirkomulag við rafræn upplýsingaskipti milli eftirlitsyfirvalda og milli eftirlitsyfirvalda og persónuverndarráðsins.

169) Framkvæmdastjórnin ætti að samþykkja framkvæmdargerðir sem taka gildi þegar í stað ef fyrir liggja sannanir um að þriðja land, yfirráðasvæði eða tilgreindur geiri innan þess þriðja lands eða alþjóðastofnun tryggi ekki fullnægjandi öryggi og ef brýna nauðsyn ber til.

170) Þar eð aðildarríkin geta ekki fyllilega náð markmiði þessarar reglugerðar, þ.e. að tryggja einstaklingum í Sambandinu sambærilega vernd og frjálst flæði persónuupplýsinga í öllu Sambandinu, og því verður betur náð á vettvangi Sambandsins, vegna umfangs og áhrifa aðgerðarinnar, er Sambandinu heimilt að samþykkja ráðstafanir í samræmi við nálægðarregluna eins og kveðið er á um í 5. gr. sáttmálans um Evrópusambandið. Í samræmi við meðalhófsregluna, eins og hún er sett fram í þeirri grein, er ekki gengið lengra en nauðsyn krefur í þessari reglugerð til að ná því markmiði.

171) Þessi reglugerð ætti að fella úr gildi tilskipun 95/46/EB. Vinnslu, sem er þegar hafin á þeim degi er reglugerð þessi kemur til framkvæmda, ætti að færa til samræmis við reglugerð þessa innan tveggja ára frá gildistöku hennar. Þegar vinnsla er byggð á samþykki samkvæmt tilskipun 95/46/EB er ekki nauðsynlegt að skráður einstaklingur gefi samþykki sitt aftur, ef það var gefið með hætti sem samrýmist skilyrðum þessarar reglugerðar, til að ábyrgðaraðili geti haldið slíkri vinnslu áfram eftir þann dag sem reglugerð þessi kemur til framkvæmda. Ákvarðanir sem framkvæmdastjórnin hefur samþykkt og heimildir sem eftirlitsyfirvöld hafa veitt á grundvelli tilskipunar 95/46/EB eru áfram í gildi uns þeim er breytt, þau eru leyst af hólmi eða þau eru felld niður.

172) Haft var samráð við Evrópsku persónuverndarstofnunina í samræmi við 2. mgr. 28. gr. reglugerðar (EB) nr. 45/2001 og skilaði hún áliti 7. mars 2012 ([1]).

173) Reglugerð þessi ætti að gilda um öll mál er varða vernd grundvallarréttinda og mannfrelsis í tengslum við vinnslu persónuupplýsinga sem ekki heyra undir sérstakar skuldbindingar með sama markmiði sem settar eru fram í tilskipun Evrópuþingsins og ráðsins 2002/58/EB ([2]), þ. á m. skyldur ábyrgðaraðila og réttindi einstaklinga. Til þess að skýra tengslin milli þessarar reglugerðar og tilskipunar 2002/58/EB ætti að breyta þeirri tilskipun til samræmis við hana. Þegar reglugerð þessi hefur verið samþykkt ætti að endurskoða tilskipun 2002/58/EB í því skyni að tryggja samræmi hennar við þessa reglugerð.

([1]) Stjtíð. ESB C 192, 30.6.2012, bls. 7.

([2]) Tilskipun Evrópuþingsins og ráðsins 2002/58/EB frá 12. júlí 2002 um vinnslu persónuupplýsinga og um verndun einkalífs á sviði rafrænna fjarskipta (tilskipun um friðhelgi einkalífsins og rafræn fjarskipti) (Stjtíð. EB L 201, 31.7.2002, bls. 37).

SAMÞYKKT REGLUGERÐ ÞESSA:

I. KAFLI

Almenn ákvæði

1. gr.

Viðfangsefni og markmið

1. Í þessari reglugerð er mælt fyrir um reglur um vernd einstaklinga í tengslum við vinnslu persónuupplýsinga og um reglur er varða frjálsa miðlun persónuupplýsinga.

2. Þessi reglugerð verndar grundvallarréttindi og frelsi einstaklinga, einkum rétt þeirra til verndar persónuupplýsingum.

3. Hvorki skal takmarka né banna frjálsa miðlun persónuupplýsinga innan Sambandsins af ástæðum er varða vernd einstaklinga í tengslum við vinnslu persónuupplýsinga.

2. gr.

Efnislegt gildissvið

1. Þessi reglugerð gildir um vinnslu persónuupplýsinga sem er sjálfvirk að hluta eða í heild og um vinnslu með öðrum aðferðum en sjálfvirkum á persónuupplýsingum sem eru eða eiga að verða hluti af skráningarkerfi.

2. Þessi reglugerð gildir ekki um vinnslu persónuupplýsinga:

a) í starfsemi sem fellur utan gildissviðs laga Sambandsins,

b) af hálfu aðildarríkjanna vegna starfsemi sem fellur undir gildissvið 2. kafla V. bálks sáttmálans um Evrópusambandið,

c) af hálfu einstaklings ef vinnslan er hluti af starfsemi sem er einungis í þágu hans sjálfs eða fjölskyldu hans,

d) af hálfu lögbærra yfirvalda í tengslum við það að koma í veg fyrir, rannsaka, koma upp um eða saksækja fyrir refsiverð brot eða fullnægja refsiviðurlögum, þ.m.t. að vernda gegn og koma í veg fyrir ógnir við almannaöryggi.

3. Reglugerð (EB) nr. 45/2001 gildir um vinnslu stofnana, aðila, skrifstofa og sérstofnana Sambandsins á persónuupplýsingum. Laga skal reglugerð (EB) nr. 45/2001 og aðrar réttargerðir Sambandsins, sem gilda um slíka vinnslu persónuupplýsinga, að meginreglum og reglum þessarar reglugerðar í samræmi við 98. gr.

4. Þessi reglugerð hefur ekki áhrif á beitingu tilskipunar 2000/31/EB, einkum reglur í 12.–15. gr. hennar um bótaábyrgð þjónustuveitenda sem eru milliliðir.

3. gr.

Gildissvæði

1. Þessi reglugerð gildir um vinnslu persónuupplýsinga í tengslum við starfsemi starfsstöðvar ábyrgðaraðila eða vinnsluaðila í Sambandinu, óháð því hvort vinnslan sjálf fer fram í Sambandinu.

2. Þessi reglugerð gildir um vinnslu ábyrgðaraðila eða vinnsluaðila, sem ekki hefur staðfestu í Sambandinu, á persónuupplýsingum um skráða einstaklinga innan Sambandsins þegar vinnslustarfsemin tengist því að:

a) bjóða þessum skráðu einstaklingum í Sambandinu vöru eða þjónustu, án tillits til þess hvort það er gert gegn greiðslu, eða

b) hafa eftirlit með hegðun þeirra að svo miklu leyti sem hegðun þeirra á sér stað innan Sambandsins.

3. Þessi reglugerð gildir um vinnslu persónuupplýsinga af hálfu ábyrgðaraðila sem ekki hefur staðfestu innan Sambandsins en þó á stað þar sem lög aðildarríkis gilda samkvæmt þjóðarétti.

4. gr.

Skilgreiningar

Í reglugerð þessari er merking eftirfarandi hugtaka sem hér segir:

1) „persónuupplýsingar“: hvers kyns upplýsingar um persónugreindan eða persónugreinanlegan einstakling („skráðan einstakling“); einstaklingur telst persónugreinanlegur ef unnt er að persónugreina hann, beint eða óbeint, svo sem með tilvísun í auðkenni eins og nafn, kennitölu, staðsetningargögn, netauðkenni eða einn eða fleiri þætti sem einkenna hann í líkamlegu, lífeðlisfræðilegu, erfðafræðilegu, andlegu, efnalegu, menningarlegu eða félagslegu tilliti,

2) „vinnsla“: aðgerð eða röð aðgerða þar sem persónuupplýsingar eru unnar, hvort sem vinnslan er sjálfvirk eða ekki, s.s. söfnun, skráning, flokkun, kerfisbinding, varðveisla, aðlögun eða breyting, heimt, skoðun, notkun, miðlun með framsendingu, dreifing eða aðrar aðferðir til að gera upplýsingarnar tiltækar, samtenging eða samkeyrsla, aðgangstakmörkun, eyðing eða eyðilegging,

3) „takmörkun á vinnslu“: að auðkenna varðveittar persónuupplýsingar með það að markmiði að takmarka vinnslu þeirra í framtíðinni,

4) „gerð persónusniðs“: hvers kyns sjálfvirk vinnsla persónuupplýsinga sem felst í því að nota persónuupplýsingar til að meta ákveðna þætti er varða hagi einstaklings, einkum að greina eða spá fyrir um þætti er varða frammistöðu hans í starfi, fjárhagsstöðu, heilsu, smekk, áhugamál, áreiðanleika, hegðun, staðsetningu eða hreyfanleika,

5) „notkun gerviauðkenna“: þegar unnið er með persónuupplýsingar á þann hátt að ekki sé lengur hægt að rekja þær til tiltekins skráðs einstaklings án viðbótarupplýsinga, að því tilskildu að slíkum viðbótarupplýsingum sé haldið aðgreindum og að beitt sé tæknilegum og skipulagslegum ráðstöfunum til að tryggja að persónuupplýsingarnar sé ekki hægt að rekja til persónugreinds eða persónugreinanlegs einstaklings,

6) „skráningarkerfi“: sérhvert skipulegt safn persónuupplýsinga sem er aðgengilegt samkvæmt tilteknum viðmiðunum, hvort heldur það er miðlægt, dreift eða skipt upp eftir notkun eða staðsetningu,

7) „ábyrgðaraðili“: einstaklingur eða lögaðili, opinbert yfirvald, sérstofnun eða annar aðili sem ákvarðar, einn eða í samvinnu við aðra, tilgang og aðferðir við vinnslu persónuupplýsinga; ef tilgangur og aðferðir við slíka vinnslu eru ákveðin í lögum Sambandsins eða lögum aðildarríkis er heimilt að tilgreina ábyrgðaraðila eða sérstakar viðmiðanir fyrir tilnefningu hans í lögum Sambandsins eða lögum aðildarríkis,

8) „vinnsluaðili“: einstaklingur eða lögaðili, opinbert yfirvald, sérstofnun eða annar aðili sem vinnur persónuupplýsingar á vegum ábyrgðaraðila,

9) „viðtakandi“: einstaklingur eða lögaðili, opinbert yfirvald, sérstofnun eða annar aðili sem fær í hendur persónuupplýsingar, hvort sem hann er þriðji aðili eða ekki. Opinber yfirvöld, sem kunna að fá persónuupplýsingar sem svör við einstökum

fyrirspurnum í samræmi við lög Sambandsins eða lög aðildarríkis, skulu þó ekki teljast viðtakendur; vinnsla þessara opinberu yfirvalda á gögnunum skal samrýmast gildandi reglum um persónuvernd samkvæmt tilgangi vinnslunnar,

10) „þriðji aðili“: einstaklingur eða lögaðili, opinbert yfirvald, sérstofnun eða aðili annar en hinn skráði, ábyrgðaraðili, vinnsluaðili og einstaklingar eða lögaðilar sem hafa, undir beinni stjórn ábyrgðaraðila eða vinnsluaðila, heimild til að vinna persónuupplýsingar,

11) „samþykki“ skráðs einstaklings: óþvinguð, sértæk, upplýst og ótvíræð viljayfirlýsing hins skráða um að hann samþykki, með yfirlýsingu eða ótvíræðri staðfestingu, vinnslu persónuupplýsinga um hann sjálfan,

12) „öryggisbrestur við meðferð persónuupplýsinga“: brestur á öryggi sem leiðir til óviljandi eða ólögmætrar eyðingar persónuupplýsinga, sem eru sendar, varðveittar eða unnar á annan hátt, eða að þær glatist, breytist, verði birtar eða aðgangur veittur að þeim í leyfisleysi,

13) „erfðafræðilegar upplýsingar“: persónuupplýsingar sem varða arfgenga eða áunna erfðaeiginleika einstaklings sem gefa einkvæmar upplýsingar um lífeðlisfræði eða heilbrigði einstaklingsins og fást einkum með greiningu á líffræðilegu sýni frá viðkomandi einstaklingi,

14) „lífkennaupplýsingar“: persónuupplýsingar sem fást með sérstakri tæknivinnslu og tengjast líkamlegum, lífeðlisfræðilegum eða atferlisfræðilegum eiginleikum einstaklings og gera það kleift að greina eða staðfesta deili á einstaklingi með ótvíræðum hætti, s.s. andlitsmyndir eða gögn um fingraför,

15) „heilsufarsupplýsingar“: persónuupplýsingar sem varða líkamlegt eða andlegt heilbrigði einstaklings, þ.m.t. heilbrigðisþjónustu sem hann hefur fengið, og sem gefa upplýsingar um heilsufar hans,

16) „höfuðstöðvar“:

a) að því er varðar ábyrgðaraðila með starfsstöðvar í fleiri en einu aðildarríki, sá staður þar sem hann hefur yfirstjórn sína í Sambandinu nema ákvarðanir um tilgang og aðferðir við vinnslu persónuupplýsinga séu teknar í annarri starfsstöð ábyrgðaraðila í Sambandinu og síðarnefnda starfsstöðin sé sú sem hefur vald til að koma slíkum ákvörðunum til framkvæmda en í því tilviki skal starfsstöðin, sem tekið hefur slíkar ákvarðanir, teljast vera höfuðstöðvar,

b) að því er varðar vinnsluaðila með starfsstöðvar í fleiri en einu aðildarríki, sá staður þar sem hann hefur yfirstjórn sína í Sambandinu eða, hafi hann enga yfirstjórn í Sambandinu, starfsstöð vinnsluaðila í Sambandinu þar sem helsta vinnslustarfsemi innan ramma starfsemi starfsstöðvar vinnsluaðila fer fram, að því marki sem vinnsluaðili falli undir tilteknar skuldbindingar samkvæmt þessari reglugerð,

17) „fulltrúi“: einstaklingur eða lögaðili með staðfestu í Sambandinu, tilnefndur skriflega af ábyrgðaraðila eða vinnsluaðila skv. 27. gr., sem kemur fram sem fulltrúi ábyrgðaraðila eða vinnsluaðila að því er varðar skuldbindingar þeirra, hvors um sig, samkvæmt þessari reglugerð,

18) „fyrirtæki“: einstaklingur eða lögaðili sem stundar atvinnustarfsemi, óháð því hvert rekstrarform hans er að lögum, þ.m.t. sameignarfélög eða samtök sem stunda atvinnustarfsemi að staðaldri,

19) „fyrirtækjasamstæða“: ráðandi fyrirtæki og undirfyrirtæki þess,

20) „bindandi fyrirtækjareglur“: reglur um persónuvernd sem ábyrgðaraðili eða vinnsluaðili með staðfestu á yfirráðasvæði aðildarríkis fylgir varðandi miðlun eða endurtekna miðlun persónuupplýsinga til ábyrgðaraðila eða vinnsluaðila í einu eða fleiri þriðju löndum innan fyrirtækjasamstæðu eða hóps fyrirtækja sem stundar sameiginlega atvinnustarfsemi,

21) „eftirlitsyfirvald“: sjálfstætt opinbert yfirvald sem aðildarríki kemur á fót skv. 51. gr.,

22) „hlutaðeigandi eftirlitsyfirvald“: eftirlitsyfirvald sem vinnsla persónuupplýsinga varðar vegna þess að:

a) ábyrgðaraðili eða vinnsluaðili hefur staðfestu á yfirráðasvæði aðildarríkis þess eftirlitsyfirvalds,

b) skráðir einstaklingar, sem búa í aðildarríki þess eftirlitsyfirvalds, verða fyrir verulegum áhrifum eða líklegt er að þeir verði fyrir verulegum áhrifum af vinnslunni eða

c) kvörtun hefur verið lögð fram hjá því eftirlitsyfirvaldi,

23) „vinnsla yfir landamæri“: annaðhvort:

a) vinnsla persónuupplýsinga sem fram fer í tengslum við starfsemi starfsstöðva ábyrgðaraðila eða vinnsluaðila innan Sambandsins í fleiri en einu aðildarríki, þegar ábyrgðaraðili eða vinnsluaðili hefur staðfestu í fleiri en einu aðildarríki, eða

b) vinnsla persónuupplýsinga sem fram fer í tengslum við starfsemi einnar starfsstöðvar ábyrgðaraðila eða vinnsluaðila innan Sambandsins en hefur veruleg áhrif eða líklegt er að hafi veruleg áhrif á skráða einstaklinga í fleiri en einu aðildarríki,

24) „viðeigandi og rökstudd andmæli“: andmæli gegn drögum að ákvörðun varðandi það hvort brotið sé gegn þessari reglugerð eða hvort fyrirhuguð aðgerð í tengslum við ábyrgðaraðilann eða vinnsluaðilann samrýmist henni sem sýna greinilega fram á þá áhættu sem drögin að ákvörðuninni hafa í för með sér fyrir grundvallarréttindi og frelsi skráðra einstaklinga og, eftir því sem við á, frjálst flæði persónuupplýsinga innan Sambandsins,

25) „þjónusta í upplýsingasamfélaginu“: þjónusta eins og hún er skilgreind í b-lið 1. mgr. 1. gr. tilskipunar Evrópuþingsins og ráðsins (ESB) 2015/1535 ([1]),

26) „alþjóðastofnun“: stofnun og undirskipaðir aðilar hennar sem heyra undir þjóðarétt eða annar aðili sem komið er á fót með samningi milli tveggja eða fleiri landa eða á grundvelli hans.

II. KAFLI

Meginreglur

5. gr.

Meginreglur um vinnslu persónuupplýsinga

1. Persónuupplýsingar skulu vera:

a) unnar með lögmætum, sanngjörnum og gagnsæjum hætti gagnvart skráðum einstaklingi („lögmæti, sanngirni og gagnsæi“),

b) fengnar í tilgreindum, skýrum og lögmætum tilgangi og ekki unnar frekar á þann hátt að ósamrýmanlegt sé þeim tilgangi; frekari vinnsla persónuupplýsinga vegna skjalavistunar í þágu almannahagsmuna, rannsókna á sviði vísinda eða sagnfræði eða í tölfræðilegum tilgangi skal, í samræmi við 1. mgr. 89. gr., ekki teljast ósamrýmanleg upphaflegum tilgangi („takmörkun vegna tilgangs“),

c) nægilegar, viðeigandi og takmarkast við það sem nauðsynlegt er miðað við tilganginn með vinnslunni („lágmörkun gagna“),

d) áreiðanlegar og, ef nauðsyn krefur, uppfærðar; gera skal allar eðlilegar ráðstafanir til að tryggja að persónuupplýsingum, sem eru óáreiðanlegar, með hliðsjón af tilganginum með vinnslu þeirra, verði eytt eða þær leiðréttar án tafar („áreiðanleiki“),

([1]) Tilskipun Evrópuþingsins og ráðsins (ESB) 2015/1535 frá 9. september 2015 um tilhögun miðlunar upplýsinga um tæknilegar reglugerðir og reglur um þjónustu í upplýsingasamfélaginu (Stjtíð. ESB L 241, 17.9.2015, bls. 1).

e) varðveittar á því formi að ekki sé unnt að persónugreina skráða einstaklinga lengur en þörf er á miðað við tilganginn með vinnslu upplýsinganna; heimilt er að geyma persónuupplýsingar lengur að því tilskildu að vinnsla þeirra þjóni einungis skjalavistun í þágu almannahagsmuna, rannsóknum á sviði vísinda eða sagnfræði eða í tölfræðilegum tilgangi, í samræmi við 1. mgr. 89. gr., og sé með fyrirvara um að gerðar verði þær viðeigandi tæknilegu og skipulagslegu ráðstafanir til að vernda réttindi og frelsi hins skráða sem reglugerð þessi krefst („geymslutakmörkun“),

f) unnar með þeim hætti að viðeigandi öryggi persónuupplýsinganna sé tryggt, þ.m.t. vernd gegn óleyfilegri eða ólögmætri vinnslu og gegn glötun, eyðileggingu eða tjóni fyrir slysni, með viðeigandi tæknilegum og skipulagslegum ráðstöfunum („heilleiki og trúnaður“).

2. Ábyrgðaraðili skal vera ábyrgur fyrir því að farið sé að ákvæðum 1. mgr. og geta sýnt fram á það („ábyrgðarskylda“).

6. gr.

Lögmæti vinnslu

1. Vinnsla skal einungis teljast lögmæt ef og að því marki sem a.m.k. eitt af eftirfarandi atriðum á við:

a) skráður einstaklingur hefur gefið samþykki sitt fyrir vinnslu á persónuupplýsingum sínum í þágu eins eða fleiri tiltekinna markmiða,

b) vinnslan er nauðsynleg vegna framkvæmdar samnings sem skráður einstaklingur á aðild að eða til þess að gera ráðstafanir að beiðni hins skráða áður en samningur er gerður,

c) vinnslan er nauðsynleg til uppfylla lagaskyldu sem hvílir á ábyrgðaraðila,

d) vinnslan er nauðsynleg til að vernda brýna hagsmuni hins skráða eða annars einstaklings,

e) vinnslan er nauðsynleg vegna verkefnis sem unnið er í þágu almannahagsmuna eða við beitingu opinbers valds sem ábyrgðaraðili fer með,

f) vinnslan er nauðsynleg vegna lögmætra hagsmuna sem ábyrgðaraðili eða þriðji aðili gætir nema hagsmunir eða grundvallarréttindi og frelsi hins skráða, sem krefjast verndar persónuupplýsinga, vegi þyngra, einkum þegar hinn skráði er barn.

Ákvæði f-liðar fyrstu undirgreinar skulu ekki eiga við um vinnslu opinberra yfirvalda við störf sín.

2. Aðildarríkjunum er heimilt að viðhalda eða innleiða sértækari ákvæði til að aðlaga beitingu reglna þessarar reglugerðar að því er varðar vinnslu þannig að samrýmist c- og e-lið 1. mgr., með því að setja fram með ítarlegri hætti sértækar kröfur til vinnslunnar og aðrar ráðstafanir til að tryggja lögmæta og sanngjarna vinnslu, þ.m.t. varðandi aðrar sérstakar vinnsluaðstæður eins og kveðið er á um í IX. kafla.

3. Mæla skal fyrir um grundvöll vinnslunnar, sem um getur í c- og e-lið 1. mgr., í:

a) lögum Sambandsins eða

b) lögum aðildarríkis sem ábyrgðaraðili heyrir undir.

Tilgangur vinnslunnar skal ákvarðaður á þeim lagagrundvelli eða, að því er varðar vinnsluna sem um getur í e-lið 1. mgr., vera nauðsynlegur vegna framkvæmdar verkefnis sem unnið er í þágu almannahagsmuna eða við beitingu opinbers valds sem ábyrgðaraðili fer með. Lagagrundvöllurinn getur m.a. verið sértæk ákvæði til að aðlaga beitingu reglna þessarar reglugerðar, m.a. um: almenn skilyrði varðandi lögmæta vinnslu ábyrgðaraðilans, tegund gagna sem vinnslan varðar, hlutaðeigandi skráða einstaklinga, hvaða stofnanir mega fá persónuupplýsingarnar í hendur og í hvaða tilgangi, takmörkun vegna tilgangs, varðveislutímabil og vinnsluaðgerðir og verklag við vinnslu, þ.m.t. ráðstafanir til að tryggja að vinnsla fari fram á lögmætan og

sanngjarnan hátt, s.s. ráðstafanir varðandi aðrar sérstakar vinnsluaðstæður eins og kveðið er á um í IX. kafla. Lög Sambandsins eða lög aðildarríkis skulu þjóna hagsmunum almennings og hæfa því lögmæta markmiði sem stefnt er að.

4. Þegar vinnsla í öðrum tilgangi en þeim sem er að baki söfnun persónuupplýsinganna byggist ekki á samþykki hins skráða eða á lögum Sambandsins eða lögum aðildarríkis, sem teljast nauðsynleg og hófleg ráðstöfun í lýðræðisþjóðfélagi til að standa vörð um þau markmið sem getið er um í 1. mgr. 23. gr., skal ábyrgðaraðilinn, til þess að ganga úr skugga um hvort vinnsla í öðrum tilgangi samrýmist þeim tilgangi sem var forsenda söfnunar persónuupplýsinganna í upphafi, m.a. taka tillit til:

a) hvers kyns tengsla milli þess tilgangs sem er að baki söfnun persónuupplýsinganna og tilgangsins með fyrirhugaðri frekari vinnslu,

b) þess í hvaða samhengi persónuupplýsingunum var safnað, einkum að því er varðar tengsl milli skráðra einstaklinga og ábyrgðaraðilans,

c) eðlis persónuupplýsinganna, einkum þess hvort sérstakir flokkar persónuupplýsinga eru unnir, skv. 9. gr., eða hvort persónuupplýsingar er varða sakfellingar í refsimálum og refsiverð brot eru unnar, í samræmi við 10. gr.,

d) hugsanlegra afleiðinga fyrirhugaðrar frekari vinnslu upplýsinganna fyrir skráða einstaklinga,

e) þess hvort viðeigandi verndarráðstafanir hafi verið gerðar sem geta m.a. falist í dulkóðun eða notkun gerviauðkenna.

7. gr.

Skilyrði fyrir samþykki

1. Þegar vinnsla er byggð á samþykki skal ábyrgðaraðilinn geta sýnt fram á að skráður einstaklingur hafi samþykkt vinnslu persónuupplýsinga sinna.

2. Ef hinn skráði gefur samþykki sitt með skriflegri yfirlýsingu, sem einnig varðar önnur málefni, skal beiðnin um samþykki sett fram á þann hátt að hún sé auðgreinanleg frá hinum málefnunum, á skiljanlegu og aðgengilegu formi og skýru og einföldu máli. Ef einhver hluti slíkrar yfirlýsingar felur í sér brot á þessari reglugerð skal hann ekki vera bindandi.

3. Skráður einstaklingur á rétt á að draga samþykki sitt til baka hvenær sem er. Afturköllun samþykkis skal ekki hafa áhrif á lögmæti vinnslu á grundvelli samþykkisins fram að afturkölluninni. Hinum skráða skal tilkynnt um þetta áður en hann gefur samþykki sitt. Jafnauðvelt skal vera að draga samþykki sitt til baka og að veita það.

4. Þegar metið er hvort samþykki sé gefið af fúsum og frjálsum vilja skal taka ítrasta tillit til þess m.a. hvort það sé skilyrði fyrir framkvæmd samnings, þ. á m. veitingu þjónustu, að samþykki sé gefið fyrir vinnslu persónuupplýsinga sem ekki er nauðsynleg vegna framkvæmdar samningsins.

8. gr.

Skilyrði sem gilda um samþykki barns í tengslum við þjónustu í upplýsingasamfélaginu

1. Þegar a-liður 1. mgr. 6. gr. á við, í tengslum við það þegar barni er boðin þjónusta í upplýsingasamfélaginu með beinum hætti, skal vinnsla persónuupplýsinga barnsins teljast lögmæt ef það hefur náð a.m.k. 16 ára aldri. Hafi barn ekki náð 16 ára aldri skal vinnslan einungis teljast lögmæt ef, og að því marki sem, forsjáraðili barnsins gefur eða heimilar samþykkið.

Aðildarríkin geta í lögum kveðið á um lægri aldur að því er þetta varðar en þó ekki lægri en 13 ár.

2. Ábyrgðaraðili skal gera það sem sanngjarnt má telja til að sannreyna í slíkum tilvikum að samþykkið sé gefið eða heimilað af hálfu forsjáraðila barnsins, að teknu tilliti til þeirrar tækni sem fyrir hendi er.

3. Ákvæði 1. mgr. hafa ekki áhrif á almenn samningalög aðildarríkjanna, s.s. reglur um gildi, gerð eða áhrif samnings þegar um er að ræða barn.

9. gr.

Vinnsla sérstakra flokka persónuupplýsinga

1. Bannað er að vinna persónuupplýsingar er varða kynþátt eða þjóðernislegan uppruna, stjórnmálaskoðanir, trúarbrögð eða heimspekilega sannfæringu eða þátttöku í stéttarfélagi og að vinna erfðafræðilegar upplýsingar, lífkennaupplýsingar í því skyni að persónugreina einstakling með einkvæmum hætti, heilsufarsupplýsingar eða upplýsingar er varða kynlíf einstaklings eða kynhneigð.

2. Ákvæði 1. mgr. gilda ekki ef eitt af eftirfarandi á við:

a) skráður einstaklingur hefur veitt ótvírætt samþykki sitt fyrir vinnslu þessara persónuupplýsinga í þágu eins eða fleiri tiltekinna markmiða nema kveðið sé á um það í lögum Sambandsins eða lögum aðildarríkis að hinum skráða sé óheimilt að aflétta banninu sem um getur í 1. mgr.,

b) vinnslan er nauðsynleg til þess að ábyrgðaraðilinn eða hinn skráði geti staðið við skuldbindingar sínar og nýtt sér tiltekin réttindi samkvæmt vinnulöggjöf og löggjöf um almannatryggingar og félagslega vernd, að því marki sem vinnslan er heimil samkvæmt lögum Sambandsins eða lögum aðildarríkis eða kjarasamningi samkvæmt lögum aðildarríkis, þar sem kveðið er á um viðeigandi verndarráðstafanir í tengslum við grundvallarréttindi og hagsmuni hins skráða,

c) vinnslan er nauðsynleg til að vernda brýna hagsmuni hins skráða eða annars einstaklings ef hinn skráði er líkamlega eða í lagalegum skilningi ófær um að veita samþykki sitt,

d) vinnslan fer fram, með viðeigandi verndarráðstöfunum, sem liður í lögmætri starfsemi stofnunar, samtaka eða annars aðila sem starfar ekki í hagnaðarskyni og hefur stjórnmálaleg, heimspekileg, trúarleg eða stéttarfélagsleg markmið, enda nái vinnslan einungis til meðlima eða fyrrum meðlima viðkomandi aðila eða þeirra sem eru í reglulegu sambandi við hann í tengslum við tilgang hans, auk þess sem persónuupplýsingar séu ekki fengnar þriðja aðila í hendur án samþykkis hinna skráðu,

e) vinnslan tengist persónuupplýsingum sem hinn skráði hefur augljóslega gert opinberar,

f) vinnslan er nauðsynleg til að unnt sé að stofna, hafa uppi eða verja réttarkröfur eða þegar dómstólar fara með dómsvald sitt,

g) vinnslan er nauðsynleg, af ástæðum sem varða verulega almannahagsmuni, á grundvelli laga Sambandsins eða laga aðildarríkis sem skulu hæfa því markmiði sem stefnt er að, virða kjarna réttarins til persónuverndar og kveða á um viðeigandi og sértækar ráðstafanir til að vernda grundvallarréttindi og hagsmuni hins skráða,

h) vinnslan er nauðsynleg til að unnt sé að fyrirbyggja sjúkdóma eða vegna atvinnusjúkdómalækninga, til að meta vinnufærni starfsmanns, greina sjúkdóma, láta í té umönnun eða meðferð á sviði heilbrigðis- eða félagsþjónustu eða stjórna heilbrigðis- eða félagsþjónustu og -kerfum á grundvelli laga Sambandsins eða aðildarríkis eða samkvæmt samningi við heilbrigðisstarfsmann og með fyrirvara um skilyrðin og verndarráðstafanirnar sem um getur í 3. mgr.,

i) vinnslan er nauðsynleg af ástæðum er varða almannahagsmuni á sviði lýðheilsu, s.s. til að verjast alvarlegum heilsufarsógnum sem ná yfir landamæri eða tryggja að strangar kröfur séu gerðar um gæði og öryggi heilbrigðisþjónustu og lyfja eða lækningatækja, á grundvelli laga Sambandsins eða laga aðildarríkis sem kveða á um viðeigandi og sértækar ráðstafanir til að vernda réttindi og frelsi hins skráða, einkum þagnarskyldu,

j) vinnsla er nauðsynleg vegna skjalavistunar í þágu almannahagsmuna, rannsókna á sviði vísinda eða sagnfræði eða í tölfræðilegum tilgangi í samræmi við 1. mgr. 89. gr., á grundvelli laga Sambandsins eða laga aðildarríkis sem skulu hæfa því markmiði sem stefnt er að, virða kjarna réttarins til persónuverndar og kveða á um viðeigandi og sértækar ráðstafanir til að vernda grundvallarréttindi og hagsmuni hins skráða.

3. Vinnsla persónuupplýsinganna, sem um getur í 1. mgr., er heimil í þeim tilgangi sem um getur í h-lið 2. mgr. ef upplýsingarnar eru unnar af eða á ábyrgð fagmanns sem fellur undir þagnarskyldu samkvæmt lögum Sambandsins eða lögum aðildarríkis eða reglum, sem innlendir þar til bærir aðilar hafa sett, eða af öðrum aðila sem einnig er bundinn þagnarskyldu samkvæmt lögum Sambandsins eða lögum aðildarríkis eða reglum sem settar eru af innlendum þar til bærum aðilum.

4. Aðildarríkjunum er heimilt að viðhalda eða setja frekari skilyrði, þ.m.t. takmarkanir, með hliðsjón af vinnslu erfðafræðilegra upplýsinga, lífkennaupplýsinga eða heilsufarsupplýsinga.

10. gr.

Vinnsla persónuupplýsinga er varða sakfellingar í refsimálum og refsiverð brot

Vinnsla persónuupplýsinga, er varða sakfellingar í refsimálum og refsiverð brot eða tengdar öryggisráðstafanir á grundvelli 1. mgr. 6. gr., skal einungis fara fram undir eftirliti opinbers yfirvalds eða þegar vinnsla er heimiluð samkvæmt lögum Sambandsins eða lögum aðildarríkis þar sem kveðið er á um viðeigandi verndarráðstafanir í tengslum við réttindi og frelsi skráðra einstaklinga. Ítarlega skrá yfir refsidóma skal varðveita undir eftirliti opinbers yfirvalds.

11. gr.

Vinnsla sem ekki krefst persónugreiningar

1. Ef tilgangurinn með vinnslu ábyrgðaraðila á persónuupplýsingum krefst þess ekki, eða krefst þess ekki lengur, að ábyrgðaraðilinn geti persónugreint skráðan einstakling er ábyrgðaraðilanum ekki skylt að viðhalda, afla sér eða vinna viðbótarupplýsingar til að unnt sé að persónugreina hinn skráða í þeim tilgangi einum að uppfylla ákvæði þessarar reglugerðar.

2. Þegar ábyrgðaraðili, í tilvikum sem um getur í 1. mgr. þessarar greinar, getur sýnt fram á að hann sé ekki í aðstöðu til að persónugreina skráðan einstakling skal hann tilkynna hinum skráða um það ef mögulegt er. Í þeim tilvikum gilda 15.–20. gr. ekki nema hinn skráði veiti, í þeim tilgangi að neyta réttar síns samkvæmt þessum greinum, viðbótarupplýsingar sem gera kleift að persónugreina hann.

III. KAFLI

Réttindi skráðs einstaklings

1. þáttur

Gagnsæi og nánari reglur

12. gr.

Gagnsæi upplýsinga, tilkynninga og nánari reglur til að skráður einstaklingur geti neytt réttar síns

1. Ábyrgðaraðili skal gera viðeigandi ráðstafanir til að láta skráðum einstaklingi í té þær upplýsingar sem um getur í 13. og 14. gr. og tilkynningar skv. 15.–22. gr. og 34. gr. í tengslum við vinnslu á gagnorðu, gagnsæju, skiljanlegu og aðgengilegu formi og skýru og einföldu máli, einkum þegar um er að ræða upplýsingar sem beint er sérstaklega til barns. Upplýsingarnar skulu veittar skriflega eða á annan hátt, þ.m.t., eftir því sem við á, á rafrænu formi. Fari skráður einstaklingur fram á það má veita upplýsingarnar munnlega, að því tilskildu að hinn skráði sanni á sér deili með öðrum hætti.

2. Ábyrgðaraðili skal auðvelda skráðum einstaklingi að neyta réttar síns skv. 15.–22. gr. Í þeim tilvikum, sem um getur í 2. mgr. 11. gr., skal ábyrgðaraðilinn ekki neita að verða við beiðni hins skráða um að neyta réttar síns skv. 15.–22. gr. nema ábyrgðaraðilinn sýni fram á að hann sé ekki í aðstöðu til að staðfesta deili á hinum skráða.

3. Ábyrgðaraðilinn skal veita skráðum einstaklingi upplýsingar um aðgerðir, sem gripið er til vegna beiðni skv. 15.–22. gr., án ótilhlýðilegrar tafar og hvað sem öðru líður innan mánaðar frá viðtöku beiðninnar. Lengja má frestinn um tvo mánuði til viðbótar ef þörf er á, með hliðsjón af fjölda beiðna og því hversu flóknar þær eru. Ábyrgðaraðili skal tilkynna hinum skráða um slíkar framlengingar innan mánaðar frá viðtöku beiðninnar, ásamt ástæðunum fyrir töfinni. Leggi hinn skráði fram beiðnina rafrænt skulu upplýsingarnar látnar í té með rafrænum hætti þar sem kostur er nema hinn skráði fari fram á annað.

4. Verði ábyrgðaraðili ekki við beiðni skráðs einstaklings skal hann tilkynna honum, án tafar og í síðasta lagi innan mánaðar frá viðtöku beiðninnar, um ástæðurnar fyrir því að það var ekki gert og um möguleikann á að leggja fram kvörtun hjá eftirlitsyfirvaldi og leita réttarúrræðis.

5. Upplýsingar, sem veittar eru skv. 13. og 14. gr., og hvers konar tilkynningar og aðgerðir, sem gripið er til skv. 15.–22. gr. og 34. gr., skulu vera án endurgjalds. Séu beiðnir frá skráðum einstaklingi augljóslega tilefnislausar eða óhóflegar, einkum vegna endurtekningar, er ábyrgðaraðila heimilt að gera annaðhvort:

a) setja upp sanngjarnt gjald með tilliti til stjórnsýslukostnaðar við upplýsingagjöfina eða tilkynningarnar eða aðgerðirnar sem farið er fram á eða

b) neita að verða við beiðninni.

Það skal vera ábyrgðaraðilans að sýna fram á að beiðni sé tilefnislaus eða óhófleg.

6. Með fyrirvara um 11. gr. getur ábyrgðaraðili farið fram á að veittar séu nauðsynlegar viðbótarupplýsingar til að staðfesta deili á hinum skráða þyki honum leika verulegur vafi á því hver sá einstaklingur sé sem leggur fram beiðnina sem um getur í 15.–21. gr.

7. Hægt er að láta staðlaðar táknmyndir fylgja upplýsingunum, sem veita ber skráðum einstaklingum skv. 13. og 14. gr., til að veita marktækt yfirlit yfir fyrirhugaða vinnslu á auðsýnilegan, skiljanlegan og auðlæsilegan hátt. Táknmyndirnar skulu vera með tölvulesanlegu sniði þegar þær eru settar fram rafrænt.

8. Framkvæmdastjórninni skal falið vald til þess að samþykkja framseldar gerðir í samræmi við 92. gr. til að ákvarða hvaða upplýsingar setja má fram með táknmyndum og aðferðirnar við að setja fram staðlaðar táknmyndir.

2. þáttur

Upplýsingar og aðgangur að persónuupplýsingum

13. gr.

Upplýsingar sem ber að veita við öflun persónuupplýsinga hjá skráðum einstaklingi

1. Þegar persónuupplýsinga er aflað hjá skráðum einstaklingi um hann sjálfan skal ábyrgðaraðilinn, við söfnun persónuupplýsinganna, skýra hinum skráða frá öllum eftirfarandi atriðum:

a) heiti og samskiptaupplýsingum ábyrgðaraðilans og, eftir atvikum, fulltrúa hans,

b) samskiptaupplýsingum persónuverndarfulltrúa, ef við á,

c) tilganginum með fyrirhugaðri vinnslu persónuupplýsinganna og hver lagagrundvöllur hennar er,

d) þegar vinnslan byggist á f-lið 1. mgr. 6. gr., hvaða lögmætu hagsmunir það eru sem ábyrgðaraðili eða þriðji aðili gætir,

e) viðtakendum eða flokkum viðtakenda persónuupplýsinganna, ef einhverjir eru,

f) ef við á, því að ábyrgðaraðili hyggist miðla persónuupplýsingum til þriðja lands eða alþjóðastofnunar og hvort ákvörðun framkvæmdastjórnarinnar um það hvort vernd sé fullnægjandi liggi fyrir eða, í tilviki miðlunar sem um getur í 46. eða 47. gr. eða í annarri undirgrein 1. mgr. 49. gr., tilvísun til viðeigandi eða hæfilegra verndarráðstafana og leiða til að fá afrit af þeim eða upplýsingar um hvar þær hafa verið gerðar aðgengilegar.

2. Til viðbótar við þær upplýsingar, sem um getur í 1. mgr., skal ábyrgðaraðilinn, á þeim tíma þegar persónuupplýsingunum er safnað, veita hinum skráða eftirtaldar frekari upplýsingar sem nauðsynlegar eru til að tryggja sanngjarna og gagnsæja vinnslu:

a) hversu lengi persónuupplýsingarnar verða geymdar eða, sé það ekki mögulegt, þær viðmiðanir sem notaðar eru til að ákveða það,

b) að fyrir hendi sé réttur til að fara fram á það við ábyrgðaraðila að fá aðgang að persónuupplýsingum, láta leiðrétta þær, eyða þeim eða takmarka vinnslu þeirra hvað hinn skráða varðar eða til að andmæla vinnslu, auk réttarins til að flytja eigin gögn,

c) þegar vinnslan byggist á a-lið 1. mgr. 6. gr. eða a-lið 2. mgr. 9. gr., að fyrir hendi sé réttur til að draga samþykki sitt til baka hvenær sem er, án þess þó að það hafi áhrif á lögmæti vinnslu á grundvelli samþykkisins fram að afturkölluninni,

d) réttinn til að leggja fram kvörtun hjá eftirlitsyfirvaldi,

e) hvort það að veita persónuupplýsingar sé krafa samkvæmt lögum eða samkvæmt samningi eða krafa sem er forsenda þess að hægt sé að gera samning og einnig hvort skráðum einstaklingi sé skylt að láta persónuupplýsingarnar í té og mögulegar afleiðingar þess ef hann veitir ekki upplýsingarnar,

f) hvort fram fari sjálfvirk ákvarðanataka, þ.m.t. gerð persónusniðs, sem um getur í 1. og 4. mgr. 22. gr., og, a.m.k. í þeim tilvikum, marktækar upplýsingar um þau rök sem þar liggja að baki og einnig þýðingu og fyrirhugaðar afleiðingar slíkrar vinnslu fyrir hinn skráða.

3. Ef ábyrgðaraðilinn hyggst vinna persónuupplýsingarnar frekar í öðrum tilgangi en þeim sem lá að baki söfnun þeirra skal hann láta hinum skráða í té upplýsingar um þennan nýja tilgang áður en sú frekari vinnsla hefst, ásamt öðrum viðeigandi viðbótarupplýsingum eins og kveðið er á um í 2. mgr.

4. Ákvæði 1., 2. og 3. mgr. gilda ekki ef og að því marki sem hinn skráði hefur þegar fengið vitneskju um þessi atriði.

14. gr.

Upplýsingar sem ber að veita þegar persónuupplýsingar hafa ekki fengist hjá skráðum einstaklingi

1. Hafi persónuupplýsingar ekki fengist hjá skráðum einstaklingi skal ábyrgðaraðili skýra honum frá eftirfarandi atriðum:

a) heiti og samskiptaupplýsingum ábyrgðaraðilans og, eftir atvikum, fulltrúa hans,

b) samskiptaupplýsingum persónuverndarfulltrúa, ef við á,

c) tilganginum með fyrirhugaðri vinnslu persónuupplýsinganna og hver lagagrundvöllur hennar er,

d) flokkum viðkomandi persónuupplýsinga,

e) viðtakendum eða flokkum viðtakenda persónuupplýsinganna, ef einhverjir eru,

f) ef við á, að ábyrgðaraðili hyggist miðla persónuupplýsingum til viðtakanda í þriðja landi eða alþjóðastofnunar og hvort ákvörðun framkvæmdastjórnarinnar um það hvort vernd sé fullnægjandi liggi fyrir eða ekki eða, í tilviki miðlunar sem um getur í 46. eða 47. gr. eða í annarri undirgrein 1. mgr. 49. gr., tilvísun til viðeigandi eða hæfilegra verndarráðstafana og leiða til að fá afrit af þeim eða upplýsingar um hvar þær hafa verið gerðar aðgengilegar.

2. Til viðbótar við upplýsingarnar, sem um getur í 1. mgr., skal ábyrgðaraðilinn veita skráðum einstaklingi eftirfarandi upplýsingar sem nauðsynlegar eru til að tryggja sanngjarna og gagnsæja vinnslu gagnvart hinum skráða:

a) hversu lengi persónuupplýsingarnar verða geymdar eða, sé það ekki mögulegt, þær viðmiðanir sem notaðar eru til að ákveða það,

b) þegar vinnslan byggist á f-lið 1. mgr. 6. gr., hvaða lögmætu hagsmunir það eru sem ábyrgðaraðili eða þriðji aðili gætir,

c) að fyrir hendi sé réttur til að fara fram á það við ábyrgðaraðila að fá aðgang að persónuupplýsingum, láta leiðrétta þær, eyða þeim eða takmarka vinnslu þeirra hvað hinn skráða varðar og til að andmæla vinnslu, auk réttarins til að flytja eigin gögn,

d) þegar vinnslan byggist á a-lið 1. mgr. 6. gr. eða a-lið 2. mgr. 9. gr., að fyrir hendi sé réttur til að draga samþykki sitt til baka hvenær sem er, án þess þó að það hafi áhrif á lögmæti vinnslu á grundvelli samþykkisins fram að afturkölluninni,

e) réttinn til að leggja fram kvörtun hjá eftirlitsyfirvaldi,

f) hvaðan persónuupplýsingarnar eru fengnar og, ef við á, hvort um hafi verið ræða upplýsingar sem eru aðgengilegar almenningi,

g) hvort fram fari sjálfvirk ákvarðanataka, þ.m.t. gerð persónusniðs, sem um getur í 1. og 4. mgr. 22. gr. og, a.m.k. í þeim tilvikum, marktækar upplýsingar um þau rök sem þar liggja að baki og einnig þýðingu og fyrirhugaðar afleiðingar slíkrar vinnslu fyrir hinn skráða.

3. Ábyrgðaraðili skal veita upplýsingarnar, sem um getur í 1. og 2. mgr.:

a) innan hæfilegs tíma eftir að hafa fengið persónuupplýsingarnar, þó í síðasta lagi mánuði síðar, og hafa hliðsjón af þeim sérstöku kringumstæðum sem eiga við um vinnslu persónuupplýsinganna,

b) ef nota á persónuupplýsingarnar til samskipta við skráðan einstakling, í síðasta lagi þegar fyrst er haft samband við hann eða

c) ef fyrirhugað er að fá öðrum viðtakanda persónuupplýsingarnar í hendur, í síðasta lagi þegar það er gert í fyrsta sinn.

4. Ef ábyrgðaraðilinn hyggst vinna persónuupplýsingarnar frekar í öðrum tilgangi en lá að baki öflun þeirra skal hann láta hinum skráða í té upplýsingar um þennan nýja tilgang áður en sú frekari vinnsla hefst, ásamt öðrum viðeigandi viðbótar-upplýsingum eins og kveðið er á um í 2. mgr.

5. Ákvæði 1.–4. mgr. gilda ekki ef og að því marki sem:

a) hinn skráði hefur þegar fengið upplýsingarnar,

b) ekki er unnt að veita slíkar upplýsingar eða það kostar óhóflega fyrirhöfn, einkum þegar um er að ræða vinnslu vegna skjalavistunar í þágu almannahagsmuna, rannsókna á sviði vísinda eða sagnfræði eða í tölfræðilegum tilgangi, með fyrirvara um þau skilyrði og verndarráðstafanir sem um getur í 1. mgr. 89. gr., eða að því marki sem líklegt er að skyldan, sem um getur í 1. mgr. þessarar greinar, geri það ómögulegt eða hamli því verulega að markmið þeirrar vinnslu náist. Í þeim tilvikum skal ábyrgðaraðilinn gera viðeigandi ráðstafanir til að vernda réttindi, frelsi og lögmæta hagsmuni hins skráða, þ.m.t. með því að gera upplýsingarnar aðgengilegar almenningi,

c) skýrt er mælt fyrir um öflun eða miðlun upplýsinganna í lögum Sambandsins eða lögum aðildarríkis sem ábyrgðaraðili heyrir undir og sem kveða á um viðeigandi ráðstafanir til að vernda lögmæta hagsmuni hins skráða eða

d) þegar persónuupplýsingar eru bundnar trúnaði á grundvelli þagnarskyldu í samræmi við lög Sambandsins eða lög aðildarríkis, þ.m.t. lögbundinnar þagnarskyldu.

15. gr.

Réttur skráðs einstaklings til aðgangs

1. Skráður einstaklingur skal hafa rétt til að fá staðfestingu á því frá ábyrgðaraðila hvort unnar séu persónuupplýsingar er varða hann sjálfan og, ef svo er, rétt til aðgangs að persónuupplýsingunum og að upplýsingum um eftirfarandi atriði:

a) tilgang vinnslunnar,

b) viðkomandi flokka persónuupplýsinga,

c) viðtakendur eða flokka viðtakenda sem fengið hafa eða munu fá persónuupplýsingarnar í hendur, einkum viðtakendur í þriðju löndum eða alþjóðastofnanir,

d) ef mögulegt er, hversu lengi fyrirhugað er að varðveita persónuupplýsingarnar eða, ef það reynist ekki mögulegt, þær viðmiðanir sem notaðar eru til að ákveða það,

e) að fyrir liggi réttur til að fara fram á það við ábyrgðaraðila að láta leiðrétta persónuupplýsingar, eyða þeim eða takmarka vinnslu þeirra hvað hinn skráða varðar eða til að andmæla slíkri vinnslu,

f) réttinn til að leggja fram kvörtun hjá eftirlitsyfirvaldi,

g) ef persónuupplýsinganna er ekki aflað hjá hinum skráða, allar fyrirliggjandi upplýsingar um uppruna þeirra,

h) hvort fram fari sjálfvirk ákvarðanataka, þ.m.t. gerð persónusniðs, sem um getur í 1. og 4. mgr. 22. gr. og, a.m.k. í þeim tilvikum, marktækar upplýsingar um þau rök sem þar liggja að baki og einnig þýðingu og fyrirhugaðar afleiðingar slíkrar vinnslu fyrir hinn skráða.

2. Þegar persónuupplýsingum er miðlað til þriðja lands eða alþjóðastofnunar skal skráður einstaklingur eiga rétt á að fá upplýsingar um viðeigandi verndarráðstafanir skv. 46. gr. í tengslum við miðlunina.

3. Ábyrgðaraðili skal láta í té afrit af þeim persónuupplýsingum sem eru í vinnslu. Honum er heimilt að innheimta sanngjarnt gjald, byggt á umsýslukostnaði, fari skráði einstaklingurinn fram á fleiri eintök. Leggi hinn skráði beiðnina fram rafrænt skulu upplýsingarnar látnar í té með rafrænu sniði sem almennt er notað nema hann fari fram á annað.

4. Rétturinn til að fá afrit, sem um getur í 3. mgr., skal ekki skerða réttindi og frelsi annarra.

3. þáttur

Leiðrétting og eyðing

16. gr.

Réttur til leiðréttingar

Skráður einstaklingur á rétt á að fá óáreiðanlegar persónuupplýsingar er varða hann sjálfan leiðréttar af ábyrgðaraðila án ótilhlýðilegrar tafar. Að teknu tilliti til tilgangsins með vinnslunni skal hinn skráði eiga rétt á að láta fullgera ófullkomnar persónuupplýsingar, þ.m.t. með því að leggja fram yfirlýsingu til viðbótar.

17. gr.

Réttur til eyðingar („réttur til að gleymast“)

1. Skráður einstaklingur skal eiga rétt á að ábyrgðaraðilinn eyði persónuupplýsingum er hann varða án ótilhlýðilegrar tafar og skal ábyrgðaraðilanum skylt að eyða persónuupplýsingunum án ótilhlýðilegrar tafar ef ein eftirtalinna ástæðna á við:

a) persónuupplýsingarnar eru ekki lengur nauðsynlegar í þeim tilgangi sem lá að baki söfnun þeirra eða annarri vinnslu þeirra,

b) hinn skráði dregur til baka samþykkið sem vinnslan byggist á skv. a-lið 1. mgr. 6. gr. eða a-lið 2. mgr. 9. gr. og ekki er annar lagagrundvöllur fyrir vinnslunni,

c) hinn skráði andmælir vinnslunni skv. 1. mgr. 21. gr. og ekki eru fyrir hendi lögmætar ástæður fyrir vinnslunni sem ganga framar eða hann andmælir vinnslunni skv. 2. mgr. 21. gr.,

d) vinnsla persónuupplýsinganna var ólögmæt,

e) eyða þarf persónuupplýsingunum til að uppfylla lagaskyldu sem hvílir á ábyrgðaraðila samkvæmt lögum Sambandsins eða lögum aðildarríkis,

f) persónuupplýsingunum var safnað í tengslum við boð um þjónustu í upplýsingasamfélaginu sem um getur í 1. mgr. 8. gr.

2. Hafi ábyrgðaraðili gert persónuupplýsingar opinberar og honum er gert skylt skv. 1. mgr. að afmá þær skal hann, með hliðsjón af fyrirliggjandi tækni og kostnaði við framkvæmdina, gera eðlilegar ráðstafanir, þ.m.t. tæknilegar ráðstafanir, til að upplýsa ábyrgðaraðila, sem vinna persónuupplýsingarnar, um að hinn skráði hafi farið fram á að slíkir ábyrgðaraðilar afmái hvers kyns tengla í eða afrit eða eftirmyndir af þessum persónuupplýsingum.

3. Ákvæði 1. og 2. mgr. gilda ekki að því marki sem vinnsla er nauðsynleg:

a) til að neyta réttarins til tjáningar- og upplýsingafrelsis,

b) til að uppfylla lagaskyldu um vinnslu sem hvílir á ábyrgðaraðilanum samkvæmt lögum Sambandsins eða lögum aðildarríkis og krefst þess að unnið sé með persónuupplýsingar eða vegna verkefnis sem er unnið í þágu almannahagsmuna eða við beitingu opinbers valds sem ábyrgðaraðili fer með,

c) með skírskotun til almannahagsmuna á sviði lýðheilsu í samræmi við h- og i-lið 2. mgr. 9. gr. og 3. mgr. 9. gr.,

d) vegna skjalavistunar í þágu almannahagsmuna, rannsókna á sviði vísinda eða sagnfræði eða í tölfræðilegum tilgangi í samræmi við 1. mgr. 89. gr., að því marki sem líklegt er að rétturinn, sem um getur í 1. mgr., geri það ómögulegt eða hamli því verulega að markmið þeirrar vinnslu náist eða

e) til að stofna, hafa uppi eða verja réttarkröfur.

18. gr.

Réttur til takmörkunar á vinnslu

1. Skráður einstaklingur skal hafa rétt til þess að ábyrgðaraðili takmarki vinnslu þegar eitt af eftirfarandi á við:

a) hinn skráði vefengir að persónuupplýsingar séu réttar, þangað til ábyrgðaraðilinn hefur fengið tækifæri til að staðfesta að þær séu réttar,

b) vinnslan er ólögmæt og hinn skráði andmælir því að persónuupplýsingunum sé eytt og fer fram á takmarkaða notkun þeirra í staðinn,

c) ábyrgðaraðilinn þarf ekki lengur á persónuupplýsingunum að halda fyrir vinnsluna en skráði einstaklingurinn þarfnast þeirra til þess að stofna, hafa uppi eða verja réttarkröfur,

d) skráði einstaklingurinn hefur andmælt vinnslunni skv. 1. mgr. 21. gr. á meðan beðið er sannprófunar á því hvort hagsmunir ábyrgðaraðila gangi framar lögmætum hagsmunum hins skráða.

2. Þegar vinnsla hefur verið takmörkuð skv. 1. gr. skal einungis vinna slíkar persónuupplýsingar, að varðveislu undanskilinni, með samþykki hins skráða eða til að stofna, hafa uppi eða verja réttarkröfur eða til að vernda réttindi annars einstaklings eða lögaðila eða með skírskotun til brýnna almannahagsmuna Sambandsins eða aðildarríkis.

3. Ábyrgðaraðili skal tilkynna skráðum einstaklingi, sem fengið hefur fram takmörkun á vinnslu skv. 1. mgr., um það áður en takmörkuninni á vinnslunni er aflétt.

19. gr.

Tilkynningarskylda varðandi leiðréttingu eða eyðingu persónuupplýsinga eða takmörkun á vinnslu

Ábyrgðaraðili skal tilkynna sérhverjum viðtakanda, sem fengið hefur persónuupplýsingar í hendur, um hvers kyns leiðréttingu eða eyðingu persónuupplýsinga eða takmörkun á vinnslu sem á sér stað í samræmi við 16. gr., 17. gr. (1. mgr.) og 18. gr., nema það sé ekki unnt eða feli í sér óhóflega fyrirhöfn. Ábyrgðaraðilinn skal tilkynna hinum skráða um þessa viðtakendur fari hann fram á það.

20. gr.

Réttur til flytja eigin gögn

1. Skráður einstaklingur skal eiga rétt á að fá persónuupplýsingar er varða hann sjálfan, sem hann hefur látið ábyrgðaraðila í té, á skipulegu, algengu, tölvulesanlegu sniði og eiga rétt á að senda þessar upplýsingar til annars ábyrgðaraðila án þess að ábyrgðaraðilinn, sem veittar voru persónuupplýsingarnar, hindri það ef:

a) vinnslan byggist á samþykki skv. a-lið 1. mgr. 6. gr. eða a-lið 2. mgr. 9. gr. eða samningi skv. b-lið 1. mgr. 6. gr. og

b) vinnslan er sjálfvirk.

2. Þegar skráði einstaklingurinn neytir réttar síns til þess að flytja eigin gögn skv. 1. mgr. skal hann eiga rétt á að láta senda persónuupplýsingarnar beint frá einum ábyrgðaraðila til annars ef það er tæknilega framkvæmanlegt.

3. Það að neyta réttarins, sem um getur í 1. mgr. þessarar greinar, skal ekki hafa áhrif á 17. gr. Sá réttur skal ekki gilda um vinnslu sem er nauðsynleg vegna verkefnis sem unnið er í þágu almannahagsmuna eða við beitingu opinbers valds sem ábyrgðaraðili fer með.

4. Rétturinn, sem um getur í 1. mgr., skal ekki skerða réttindi og frelsi annarra.

4. þáttur

Andmælaréttur og sjálfvirk einstaklingsmiðuð ákvarðanataka

21. gr.

Andmælaréttur

1. Skráður einstaklingur skal eiga rétt á að andmæla hvenær sem er, vegna sérstakra aðstæðna sinna, vinnslu persónuupplýsinga er varða hann sjálfan og sem byggist á e- eða f-lið 1. mgr. 6. gr., þ.m.t. gerð persónusniðs á grundvelli þessara ákvæða. Ábyrgðaraðili skal ekki vinna persónuupplýsingarnar frekar nema hann geti sýnt fram á mikilvægar lögmætar ástæður fyrir vinnslunni sem ganga framar hagsmunum, réttindum og frelsi hins skráða eða því að stofna, hafa uppi eða verja réttarkröfur.

2. Þegar persónuupplýsingar eru unnar í þágu beinnar markaðssetningar skal skráði einstaklingurinn hvenær sem er eiga rétt á að andmæla vinnslu persónuupplýsinga sem varða hann sjálfan vegna slíkrar markaðssetningar, þ.m.t. gerð persónusniðs að því marki sem það tengist slíkri beinni markaðssetningu.

3. Ef hinn skráði andmælir vinnslu í þágu beinnar markaðssetningar skal ekki vinna persónuupplýsingarnar frekar í slíkum tilgangi.

4. Í síðasta lagi þegar fyrst er haft samband við hinn skráða skal honum sérstaklega gerð grein fyrir réttinum, sem um getur í 1. og 2. mgr., og skal hann settur skýrt fram og aðgreindur frá öðrum upplýsingum.

5. Með skírskotun til notkunar á þjónustu í upplýsingasamfélaginu og þrátt fyrir tilskipun 2002/58/EB er hinum skráða heimilt að neyta andmælaréttar síns rafrænt með notkun tækniforskrifta.

6. Þegar persónuupplýsingar eru unnar í þágu rannsókna á sviði vísinda eða sagnfræði eða í tölfræðilegum tilgangi í samræmi við 1. mgr. 89. gr. skal hinn skráði eiga rétt á, vegna sérstakra aðstæðna sinna, að andmæla vinnslu persónuupplýsinga er varða hann sjálfan nema vinnslan sé nauðsynleg vegna verkefnis sem unnið er í þágu almannahagsmuna.

22. gr.

Sjálfvirk einstaklingsmiðuð ákvarðanataka, þ.m.t. gerð persónusniðs

1. Skráður einstaklingur skal eiga rétt á því að ekki sé tekin ákvörðun eingöngu á grundvelli sjálfvirkrar gagnavinnslu, þ.m.t. gerðar persónusniðs, sem hefur réttaráhrif að því er hann sjálfan varðar eða snertir hann á sambærilegan hátt að verulegu leyti.

2. Ákvæði 1. mgr. gilda ekki ef ákvörðunin:

a) er forsenda þess að unnt sé að gera eða efna samning milli hins skráða og ábyrgðaraðila,

b) er heimiluð í lögum Sambandsins eða lögum aðildarríkis sem ábyrgðaraðili heyrir undir og þar sem einnig er kveðið á um viðeigandi ráðstafanir til að vernda réttindi og frelsi og lögmæta hagsmuni hins skráða eða

c) byggist á afdráttarlausu samþykki hins skráða.

3. Í þeim tilvikum, sem um getur í a- og c-lið 2. mgr., skal ábyrgðaraðili gagna gera viðeigandi ráðstafanir til að vernda réttindi og frelsi og lögmæta hagsmuni hins skráða, a.m.k. réttinn til mannlegrar íhlutunar af hálfu ábyrgðaraðilans, til að láta skoðun sína í ljós og til að vefengja ákvörðunina.

4. Ákvarðanir, sem um getur í 2. mgr., skulu ekki vera byggðar á sérstökum flokkum persónuupplýsinga, sem um getur í 1. mgr. 9. gr., nema a- eða g-liður 2. mgr. 9. gr. eigi við og fyrir hendi séu viðeigandi ráðstafanir til að vernda réttindi og frelsi og lögmæta hagsmuni hins skráða.

5. þáttur

Takmarkanir

23. gr.

Takmarkanir

1. Í Sambandslögum eða lögum aðildarríkis, sem ábyrgðaraðili eða vinnsluaðili gagna heyrir undir, er heimilt að takmarka með löggjafarráðstöfun gildissvið þeirra skyldna og réttinda, sem um getur í 12.–22. gr. og í 34. gr., og einnig í 5. gr. að því marki sem ákvæði hennar samsvara réttindum og skyldum sem kveðið er á um í 12.–22. gr., ef slík takmörkun virðir eðli grundvallarréttinda og mannfrelsis og telst nauðsynleg og hófleg ráðstöfun í lýðræðisþjóðfélagi með hliðsjón af:

a) þjóðaröryggi,

b) landvörnum,

c) almannaöryggi,

d) því að koma í veg fyrir, rannsaka, koma upp um eða saksækja fyrir refsiverð brot eða fullnægja refsiviðurlögum, þ.m.t. að vernda gegn og koma í veg fyrir ógnir við almannaöryggi,

e) öðrum mikilvægum markmiðum sem þjóna almannahagsmunum Sambandsins eða aðildarríkis, einkum mikilvægum efnahagslegum eða fjárhagslegum hagsmunum Sambandsins eða aðildarríkis, þ.m.t. gjaldeyrismálum, fjárlögum og skattamálum, lýðheilsu og almannatryggingum,

f) því að verja sjálfstæði dómskerfisins og dómsmeðferð,

g) forvörnum, rannsóknum, uppljóstrunum og lögsóknum vegna brota á siðareglum lögverndaðra starfsgreina,

h) eftirlits-, skoðunar- eða reglusetningarstörfum sem tengjast, þótt aðeins sé það endrum og eins, beitingu opinbers valds í þeim tilvikum sem um getur í a- til e-lið og í g-lið,

i) vernd skráðs einstaklings eða réttindum og frelsi annarra,

j) því að einkaréttarlegum kröfum sé fullnægt.

2. Í löggjafarráðstöfun, sem um getur í 1. mgr., skulu einkum vera a.m.k. sértæk ákvæði, ef við á, er varða:

a) tilgang vinnslunnar eða tegundir vinnslu,

b) tegundir persónuupplýsinga,

c) gildissvið þeirra takmarkana sem settar eru,

d) verndarráðstafanir til að koma í veg fyrir misnotkun eða ólögmætan aðgang eða miðlun,

e) tilgreiningu ábyrgðaraðila eða flokka ábyrgðaraðila,

f) varðveislutímabil og viðeigandi verndarráðstafanir með tilliti til eðlis, umfangs og tilgangs með vinnslu eða tegunda vinnslu,

g) áhættu fyrir réttindi og frelsi skráðra einstaklinga og

h) rétt skráðra einstaklinga til að fá upplýsingar um takmörkunina nema það kunni að skaða tilgang hennar.

IV. KAFLI

Ábyrgðaraðili og vinnsluaðili

1. þáttur

Almennar skyldur

24. gr.

Ábyrgð ábyrgðaraðila

1. Með hliðsjón af eðli, umfangi, samhengi og tilgangi vinnslunnar og áhættu, mislíklegri og misalvarlegri, fyrir réttindi og frelsi einstaklinga skal ábyrgðaraðilinn gera viðeigandi tæknilegar og skipulagslegar ráðstafanir til að tryggja og sýna fram á að vinnslan fari fram í samræmi við þessa reglugerð. Ráðstafanirnar skal endurskoða og uppfæra ef nauðsyn ber til.

2. Þar sem það samrýmist meðalhófi í tengslum við vinnslustarfsemina skulu ráðstafanirnar, sem um getur í 1. mgr., m.a. fela í sér að ábyrgðaraðili innleiði viðeigandi persónuverndarstefnur.

3. Sé samþykktum hátternisreglum fylgt, eins og um getur í 40. gr., eða samþykktu vottunarfyrirkomulagi, eins og um getur í 42. gr., má nota það til að sýna fram á að ábyrgðaraðili uppfylli skuldbindingar sínar.

25. gr.

Innbyggð og sjálfgefin persónuvernd

1. Með hliðsjón af nýjustu tækni, kostnaði við framkvæmd og eðli, umfangi, samhengi og tilgangi vinnslunnar og áhættu, mislíklegri og misalvarlegri, fyrir réttindi og frelsi einstaklinga skal ábyrgðaraðilinn, bæði þegar ákveðnar eru aðferðir við vinnsluna og þegar vinnslan sjálf fer fram, gera viðeigandi tæknilegar og skipulagslegar ráðstafanir, s.s. notkun gerviauðkenna, sem hannaðar eru til að framfylgja meginreglum um persónuvernd, s.s. lágmörkun gagna, með skilvirkum hætti og fella nauðsynlegar verndarráðstafanir inn í vinnsluna til að uppfylla kröfur þessarar reglugerðar og vernda réttindi skráðra einstaklinga.

2. Ábyrgðaraðilinn skal gera viðeigandi tæknilegar og skipulagslegar ráðstafanir til að tryggja að sjálfgefið sé að einungis þær persónuupplýsingar séu unnar sem nauðsynlegar eru vegna tilgangs vinnslunnar hverju sinni. Þessi skylda gildir um það hversu miklum persónuupplýsingum er safnað, að hvaða marki unnið er með þær, hversu lengi þær eru varðveittar og aðgang að þeim. Einkum skal tryggja með slíkum ráðstöfunum að það sé sjálfgefið að persónuupplýsingar verði ekki gerðar aðgengilegar ótakmörkuðum fjölda fólks án íhlutunar viðkomandi einstaklings.

3. Nota má samþykkt vottunarfyrirkomulag, skv. 42. gr., til að sýna fram á að kröfur 1. og 2. mgr. þessarar greinar séu uppfylltar.

26. gr.

Sameiginlegir ábyrgðaraðilar

1. Ef tveir eða fleiri ábyrgðaraðilar ákveða sameiginlega tilgang vinnslunnar og aðferðir við hana skulu þeir teljast vera sameiginlegir ábyrgðaraðilar. Þeir skulu, á gagnsæjan hátt, ákveða ábyrgð hvers um sig á því að skuldbindingar samkvæmt þessari reglugerð séu uppfylltar, einkum hvað snertir beitingu réttinda hinna skráðu og skyldur hvers um sig til að láta í té upplýsingarnar sem um getur í 13. og 14. gr., með samkomulagi sín á milli nema og að því marki sem ábyrgð hvers ábyrgðaraðila um sig er ákveðin í lögum Sambandsins eða lögum aðildarríkis sem ábyrgðaraðilarnir heyra undir. Í samkomulaginu má tilnefna tengilið fyrir skráða einstaklinga.

2. Samkomulagið, sem um getur í 1. mgr., skal endurspegla með tilhlýðilegum hætti hlutverk og tengsl hvers hinna sameiginlegu ábyrgðaraðila gagnvart skráðum einstaklingum. Megininntak samkomulagsins skal gert aðgengilegt skráðum einstaklingi.

3. Óháð skilmálum samkomulagsins, sem um getur í 1. mgr., er skráðum einstaklingi heimilt að neyta réttar síns samkvæmt þessari reglugerð að því er varðar og gagnvart hverjum ábyrgðaraðila um sig.

27. gr.

Fulltrúar ábyrgðaraðila eða vinnsluaðila sem ekki hafa staðfestu í Sambandinu

1. Þegar 2. mgr. 3. gr. á við skal ábyrgðaraðilinn eða vinnsluaðilinn tilnefna skriflega fulltrúa sinn innan Sambandsins.

2. Skyldan, sem mælt er fyrir um í 1. mgr., skal ekki eiga við um:

a) vinnslu sem fer fram endrum og eins, felur ekki í sér umfangsmikla meðferð sérstakra flokka upplýsinga, eins og um getur í 1. mgr. 9. gr., eða meðferð persónuupplýsinga í tengslum við sakfellingu í refsimálum og refsiverð brot, sem um getur í 10. gr., og sem ekki er líkleg til að leiða af sér áhættu að því er varðar réttindi og frelsi einstaklinga, að teknu tilliti til eðlis, samhengis, umfangs og tilgangs vinnslunnar eða

b) opinbert yfirvald eða stofnun.

3. Fulltrúinn skal hafa staðfestu í einu af aðildarríkjum þeirra skráðu einstaklinga sem persónuupplýsingar eru unnar um í tengslum við boð til þeirra á vörum eða þjónustu eða sem fylgst er með hegðun hjá.

4. Fulltrúinn skal hafa umboð ábyrgðaraðila eða vinnsluaðila til þess að vera sá aðili sem einkum og sér í lagi eftirlitsyfirvöld og skráðir einstaklingar geta snúið sér til, til viðbótar við eða í stað ábyrgðaraðilans eða vinnsluaðilans, með öll þau mál sem tengjast vinnslunni, í því skyni að tryggja að farið sé að þessari reglugerð.

5. Þó að ábyrgðaraðili eða vinnsluaðili tilnefni fulltrúa hefur það ekki áhrif á lögsóknir sem hefja mætti gegn ábyrgðaraðilanum eða vinnsluaðilanum sjálfum.

28. gr.

Vinnsluaðili

1. Þegar öðrum er falin vinnsla fyrir hönd ábyrgðaraðila skal ábyrgðaraðilinn einungis leita til vinnsluaðila sem veita nægilegar tryggingar fyrir því að þeir geri viðeigandi tæknilegar og skipulagslegar ráðstafanir til að vinnslan uppfylli kröfur þessarar reglugerðar og að vernd réttinda hins skráða sé tryggð.

2. Vinnsluaðili skal ekki ráða annan vinnsluaðila nema hafa til þess sértæka eða almenna skriflega heimild ábyrgðaraðila. Ef um er að ræða almenna skriflega heimild skal vinnsluaðilinn tilkynna ábyrgðaraðilanum um allar fyrirhugaðar breytingar sem fela í sér að bætt er við vinnsluaðilum eða þeim skipt út og gefa þannig ábyrgðaraðilanum tækifæri til að andmæla slíkum breytingum.

3. Vinnsla af hálfu vinnsluaðila skal falla undir samning eða aðra réttargerð samkvæmt lögum Sambandsins eða lögum aðildarríkis sem skuldbindur vinnsluaðila gagnvart ábyrgðaraðilanum og þar sem tilgreint er viðfangsefni og tímalengd vinnslunnar, eðli og tilgangur hennar, tegund persónuupplýsinga og flokkar skráðra einstaklinga og skyldur og réttindi ábyrgðaraðilans. Í samningi eða annarri réttargerð skal einkum mæla fyrir um að vinnsluaðili:

a) vinni einungis persónuupplýsingarnar samkvæmt skjalfestum fyrirmælum ábyrgðaraðila, þ.m.t. að því er varðar miðlun persónuupplýsinga til þriðja lands eða alþjóðastofnunar, nema honum sé það skylt samkvæmt lögum Sambandsins eða lögum aðildarríkis sem vinnsluaðilinn heyrir undir; í því tilviki skal vinnsluaðilinn upplýsa ábyrgðaraðila um það lagaskilyrði áður en vinnslan hefst nema lögin banni slíka upplýsingagjöf vegna mikilvægra almannahagsmuna,

b) tryggi að aðilar, sem hafa heimild til vinnslu persónuupplýsinga, hafi gengist undir trúnaðarskyldu eða heyri undir viðeigandi lögboðna trúnaðarskyldu,

c) geri allar ráðstafanir sem krafist er skv. 32. gr.,

d) virði skilyrði 2. og 4. mgr. varðandi ráðningu annars vinnsluaðila,

e) aðstoði, að teknu tilliti til eðlis vinnslunnar, ábyrgðaraðilann með viðeigandi tæknilegum og skipulagslegum ráðstöfunum, að því marki sem hægt er, við að uppfylla þá skyldu sína að svara beiðnum um að skráðir einstaklingar fái neytt réttar síns sem mælt er fyrir um í III. kafla,

f) aðstoði ábyrgðaraðila við að tryggja að skyldur skv. 32.–36. gr. séu uppfylltar, að teknu tilliti til eðlis vinnslunnar og upplýsinga sem vinnsluaðili hefur aðgang að,

g) eyði eða skili, að vali ábyrgðaraðila, öllum persónuupplýsingum til ábyrgðaraðilans eftir að veitingu þjónustunnar, sem tengist vinnslunni, lýkur og eyði öllum afritum nema þess sé krafist í lögum Sambandsins eða lögum aðildarríkis að persónuupplýsingar séu varðveittar,

h) geri ábyrgðaraðila aðgengilegar allar upplýsingar, sem nauðsynlegar eru til að sýna fram á að skuldbindingarnar, sem mælt er fyrir um í þessari grein, séu uppfylltar, gefi kost á úttektum, þ.m.t. eftirlitsskoðunum, sem ábyrgðaraðilinn eða annar úttektaraðili í umboði hans hafi með höndum, og leggi sitt af mörkum til þeirra.

Að því er varðar h-lið fyrstu undirgreinar skal vinnsluaðili þegar í stað láta ábyrgðaraðila vita ef fyrirmæli brjóta, að hans mati, í bága við þessa reglugerð eða önnur ákvæði Sambandsins eða aðildarríkis um persónuvernd.

4. Ráði vinnsluaðili annan vinnsluaðila til að inna af hendi tiltekna vinnslustarfsemi fyrir hönd ábyrgðaraðila leggjast sömu skyldur varðandi persónuvernd og settar eru fram í samningnum eða annarri réttargerð milli ábyrgðaraðila og vinnsluaðila, eins og um getur í 3. mgr., á þann vinnsluaðila með samningi eða annarri réttargerð samkvæmt lögum Sambandsins eða lögum aðildarríkis, þar sem einkum eru veittar nægar tryggingar fyrir því að gerðar séu viðeigandi tæknilegar og skipulagslegar ráðstafanir þannig að vinnslan uppfylli kröfur þessarar reglugerðar. Uppfylli þessi viðbótarvinnsluaðili ekki persónuverndarskyldur sínar skal upphaflegi vinnsluaðilinn áfram bera fulla ábyrgð gagnvart ábyrgðaraðila á því að hinn vinnsluaðilinn efni skuldbindingar sínar.

5. Fylgi vinnsluaðili samþykktum hátternisreglum, eins og um getur í 40. gr., eða samþykktu vottunarfyrirkomulagi, eins og um getur í 42. gr., má nota það til að sýna fram á nægilegar tryggingar eins og um getur í 1. og 4. mgr. þessarar greinar.

6. Án þess að það hafi áhrif á einstakan samning milli ábyrgðaraðila og vinnsluaðila getur samningurinn eða önnur réttargerð, sem um getur í 3. og 4. mgr. þessarar greinar, verið byggð, að öllu leyti eða að hluta til, á föstum samningsákvæðum sem um getur í 7. og 8. mgr. þessarar greinar, m.a. þegar þau eru hluti vottunar sem veitt er ábyrgðaraðila eða vinnsluaðila skv. 42. og 43. gr.

7. Framkvæmdastjórnin getur mælt fyrir um föst samningsákvæði um þau mál sem um getur í 3. og 4. mgr. þessarar greinar og í samræmi við rannsóknarmálsmeðferðina sem um getur í 2. mgr. 93. gr.

8. Eftirlitsyfirvald getur tekið upp föst samningsákvæði um þau mál sem um getur í 3. og 4. mgr. þessarar greinar og í samræmi við samræmingarkerfið sem um getur í 63. gr.

9. Samningurinn eða önnur réttargerð, sem um getur í 3. og 4. mgr., skal vera skrifleg, þ.m.t. á rafrænu formi.

10. Með fyrirvara um 82., 83. og 84. gr. skal vinnsluaðili, sem brýtur í bága við þessa reglugerð þegar hann ákveður tilgang og aðferðir við vinnsluna, teljast vera ábyrgðaraðili að því er varðar þá vinnslu.

29. gr.

Vinnsla í umboði ábyrgðaraðila eða vinnsluaðila

Vinnsluaðili og sérhver aðili, sem starfar í umboði ábyrgðaraðila eða vinnsluaðila og hefur aðgang að persónuupplýsingum, skal því aðeins vinna þessar upplýsingar að fyrir liggi fyrirmæli ábyrgðaraðila nema honum sé það skylt samkvæmt lögum Sambandsins eða lögum aðildarríkis.

30. gr.

Skrár yfir vinnslustarfsemi

1. Sérhver ábyrgðaraðili og, eftir atvikum, fulltrúi ábyrgðaraðila skal halda skrá yfir vinnslustarfsemi sem fram fer á ábyrgð hans. Í skránni skulu allar eftirfarandi upplýsingar koma fram:

a) heiti og samskiptaupplýsingar ábyrgðaraðila og, eftir atvikum, sameiginlegs ábyrgðaraðila, fulltrúa ábyrgðaraðila og persónuverndarfulltrúa,

b) tilgangur vinnslunnar,

c) lýsing á flokkum skráðra einstaklinga og flokkum persónuupplýsinga,

d) flokkar viðtakenda sem fengið hafa eða munu fá persónuupplýsingarnar í hendur, m.a. viðtakenda í þriðju löndum eða alþjóðastofnanir,

e) ef við á, miðlun persónuupplýsinga til þriðja lands eða alþjóðastofnunar, þ.m.t. um hvaða þriðja land eða alþjóðastofnun er að ræða, og, ef um er að ræða miðlun sem um getur í annarri undirgrein 1. mgr. 49. gr., gögn um viðeigandi verndarráðstafanir,

f) ef mögulegt er, fyrirhuguð tímamörk varðandi eyðingu mismunandi gagnaflokka,

g) ef mögulegt er, almenn lýsing á þeim tæknilegu og skipulagslegu öryggisráðstöfunum sem um getur í 1. mgr. 32. gr.

2. Sérhver vinnsluaðili og, eftir atvikum, fulltrúi vinnsluaðila skal halda skrá yfir alla flokka vinnslustarfsemi sem framkvæmd er fyrir hönd ábyrgðaraðila, en í henni skulu koma fram:

a) heiti og samskiptaupplýsingar vinnsluaðila, eins eða fleiri, og sérhvers ábyrgðaraðila sem vinnsluaðilinn starfar í umboði fyrir og, eftir atvikum, fulltrúa ábyrgðaraðila eða vinnsluaðila og persónuverndarfulltrúa,

b) flokkar vinnslu sem fram fer fyrir hönd hvers ábyrgðaraðila,

c) ef við á, miðlun persónuupplýsinga til þriðja lands eða alþjóðastofnunar, þ.m.t. um hvaða þriðja land eða alþjóðastofnun er að ræða, og, ef um er að ræða miðlun sem um getur í annarri undirgrein 1. mgr. 49. gr., gögn um viðeigandi verndarráðstafanir,

d) ef mögulegt er, almenn lýsing á þeim tæknilegu og skipulagslegu öryggisráðstöfunum sem um getur í 1. mgr. 32. gr.

3. Skrárnar, sem um getur í 1. og 2. mgr., skulu vera skriflegar, þ.m.t. á rafrænu formi.

4. Ábyrgðaraðili eða vinnsluaðili og, eftir atvikum, fulltrúi ábyrgðaraðilans eða vinnsluaðilans skulu gera skrána aðgengilega eftirlitsyfirvaldinu að beiðni þess.

5. Skyldurnar, sem um getur í 1. og 2. mgr., skulu ekki eiga við um fyrirtæki eða stofnun sem hefur færri en 250 starfsmenn nema vinnslan, sem innt er þar af hendi, sé líkleg til að leiða af sér áhættu fyrir réttindi og frelsi skráðra einstaklinga, vinnslan sé ekki tilfallandi eða taki til sérstakra flokka upplýsinga, eins og um getur í 1. mgr. 9. gr., eða persónuupplýsinga er varða sakfellingar í refsimálum og refsiverð brot sem um getur í 10. gr.

31. gr.

Samvinna við eftirlitsyfirvald

Ábyrgðaraðili og vinnsluaðili og, eftir atvikum, fulltrúar þeirra skulu, að fenginni beiðni, hafa samvinnu við eftirlitsyfirvaldið við framkvæmd verkefna þess.

2. þáttur

Öryggi persónuupplýsinga

32. gr.

Öryggi við vinnslu

1. Með hliðsjón af nýjustu tækni, kostnaði við framkvæmd og eðli, umfangi, samhengi og tilgangi vinnslunnar og áhættu, mislíklegri og misalvarlegri, fyrir réttindi og frelsi einstaklinga skulu ábyrgðaraðili og vinnsluaðili gera viðeigandi tæknilegar og skipulagslegar ráðstafanir til að tryggja viðunandi öryggi miðað við áhættuna, m.a. eftir því sem við á:

a) nota gerviauðkenni og dulkóða persónuupplýsingar,

b) geta tryggt viðvarandi trúnað, samfellu, tiltækileika og álagsþol vinnslukerfa og -þjónustu,

c) geta gert persónuupplýsingar tiltækar og endurheimt aðgang að þeim tímanlega ef til efnislegs eða tæknilegs atviks kemur,

d) taka upp ferli til að prófa og meta reglulega skilvirkni tæknilegra og skipulagslegra ráðstafana til að tryggja öryggi vinnslunnar.

2. Þegar viðunandi öryggi er metið skal einkum hafa hliðsjón af þeirri áhættu sem vinnslan hefur í för með sér, einkum að því er varðar óviljandi eða ólögmæta eyðingu persónuupplýsinga, sem eru sendar, geymdar eða unnar á annan hátt, eða að þær glatist, breytist, verði birtar eða veittur aðgangur að þeim í leyfisleysi.

3. Sé samþykktum hátternisreglum fylgt, eins og um getur í 40. gr., eða samþykktu vottunarfyrirkomulagi, eins og um getur í 42. gr., má nota það til að sýna fram á að kröfur 1. mgr. þessarar greinar séu uppfylltar.

4. Ábyrgðaraðili og vinnsluaðili skulu gera ráðstafanir til að tryggja að sérhver einstaklingur, sem starfar í umboði ábyrgðaraðila eða vinnsluaðila og hefur aðgang að persónuupplýsingum, vinni þessar upplýsingar því aðeins að fyrir liggi fyrirmæli ábyrgðaraðila nema honum sé það skylt samkvæmt lögum Sambandsins eða lögum aðildarríkis.

33. gr.

Tilkynning til eftirlitsyfirvalds um öryggisbrest við meðferð persónuupplýsinga

1. Ef um öryggisbrest við meðferð persónuupplýsinga er að ræða skal ábyrgðaraðili, án ótilhlýðilegrar tafar, og, ef mögulegt er, eigi síðar en 72 klst. eftir að hann verður brestsins var, tilkynna eftirlitsyfirvaldinu, sem er lögbært skv. 55. gr., um hann nema ólíklegt þyki að bresturinn leiði til áhættu fyrir réttindi og frelsi einstaklinga. Sé eftirlitsyfirvaldinu ekki tilkynnt um brestinn innan 72 klst. skulu ástæður fyrir töfinni fylgja tilkynningunni.

2. Vinnsluaðili skal tilkynna ábyrgðaraðila um það án ótilhlýðilegrar tafar ef hann verður var við öryggisbrest við meðferð persónuupplýsinga.

3. Í tilkynningunni, sem um getur í 1. mgr., skal a.m.k.:

a) lýsa eðli öryggisbrests við meðferð persónuupplýsinga, þ.m.t., ef hægt er, þeim flokkum og áætluðum fjölda skráðra einstaklinga sem hann varðar og flokkum og áætluðum fjölda skráa með persónuupplýsingum sem um er að ræða,

b) gefa upp nafn og samskiptaupplýsingar persónuverndarfulltrúa eða annars tengiliðar þar sem hægt er að fá frekari upplýsingar,

c) lýsa líklegum afleiðingum öryggisbrests við meðferð persónuupplýsinga,

d) lýsa þeim ráðstöfunum sem ábyrgðaraðili hefur gert eða fyrirhugar að gera vegna öryggisbrests við meðferð persónuupplýsinga, þ.m.t., eftir því sem við á, ráðstöfunum til að milda hugsanleg skaðleg áhrif hans.

4. Ef, og að því marki sem, ekki er mögulegt að láta upplýsingarnar í té á sama tíma er heimilt að veita þær í áföngum án ástæðulausrar frekari tafar.

5. Ábyrgðaraðili skal skrá niður hvers kyns öryggisbresti við meðferð persónuupplýsinga og tilgreina málsatvik í tengslum við viðkomandi brest, áhrif hans og aðgerðir til úrbóta sem gripið var til. Þessi skráning skal gera eftirlitsyfirvaldinu kleift að sannreyna að farið sé að ákvæðum þessarar greinar.

34. gr.

Skráðum einstaklingi gert viðvart um öryggisbrest við meðferð persónuupplýsinga

1. Ef líklegt er að öryggisbrestur við meðferð persónuupplýsinga leiði af sér mikla áhættu fyrir réttindi og frelsi einstaklinga skal ábyrgðaraðili tilkynna skráðum einstaklingi um brestinn án ótilhlýðilegrar tafar.

2. Í tilkynningunni til hins skráða, sem um getur í 1. mgr. þessarar greinar, skal lýsa á skýru og einföldu máli eðli öryggisbrests við meðferð persónuupplýsinga og skal hún a.m.k. innihalda þær upplýsingar og ráðstafanir sem um getur í b-, c- og d-lið 3. mgr. 33. gr.

3. Þess skal ekki krafist að skráðum einstaklingi sé gert viðvart ef eitthvert eftirtalinna skilyrða er uppfyllt:

a) ábyrgðaraðilinn hefur gert viðeigandi tæknilegar og skipulagslegar verndarráðstafanir og þessar ráðstafanir voru gerðar varðandi þær persónuupplýsingar sem öryggisbrestur við meðferð persónuupplýsinga hafði áhrif á, einkum ráðstafanir til að gera persónuupplýsingar ólæsilegar hverjum þeim sem ekki hefur aðgangsheimild að þeim, s.s. með dulkóðun,

b) ábyrgðaraðilinn hefur gert ráðstafanir í kjölfarið sem tryggja að ólíklegt sé að það komi til jafnmikillar áhættu fyrir réttindi og frelsi skráðra einstaklinga og um getur í 1. mgr.,

c) það myndi hafa í för með sér óhóflega fyrirhöfn. Í því tilviki skal í staðinn birta almenna tilkynningu eða grípa til svipaðrar ráðstöfunar þar sem hinum skráðu er gert viðvart með jafnáhrifaríkum hætti.

4. Hafi ábyrgðaraðili ekki þegar látið hinn skráða vita af öryggisbresti við meðferð persónuupplýsinga getur eftirlitsyfirvaldið, eftir að hafa metið líkur á því að bresturinn leiði af sér mikla áhættu, annaðhvort krafist þess að hann geri það eða ákveðið að einhver þeirra skilyrða, sem um getur í 3. mgr., séu uppfyllt.

3. þáttur

Mat á áhrifum á persónuvernd og fyrirframsamráð

35. gr.

Mat á áhrifum á persónuvernd

1. Ef líklegt er að tiltekin tegund vinnslu geti haft í för með sér mikla áhættu fyrir réttindi og frelsi einstaklinga, einkum þar sem beitt er nýrri tækni og með hliðsjón af eðli, umfangi, samhengi og tilgangi vinnslunnar, skal ábyrgðaraðilinn láta fara fram mat á áhrifum fyrirhugaðra vinnsluaðgerða á vernd persónuupplýsinga áður en vinnslan hefst. Eitt og sama mat getur tekið til nokkurra svipaðra vinnsluaðgerða sem geta haft í för með sér svipaða áhættuþætti.

2. Ábyrgðaraðilinn skal leita ráða hjá persónuverndarfulltrúa, hafi slíkur fulltrúi verið tilnefndur, þegar hann framkvæmir mat á áhrifum á persónuvernd.

3. Þess skal einkum krafist að fram fari mat á áhrifum á persónuvernd, sem um getur í 1. mgr., þegar um er að ræða:

a) kerfisbundið og umfangsmikið mat á persónulegum þáttum, sem tengjast einstaklingum, sem byggist á sjálfvirkri vinnslu, þ.m.t. gerð persónusniðs, og sem leiðir til töku ákvarðana sem hafa réttaráhrif fyrir einstaklinginn eða snerta hann verulega með svipuðum hætti,

b) umfangsmikla vinnslu sérstakra flokka upplýsinga sem um getur í 1. mgr. 9. gr. eða persónuupplýsinga er varða sakfellingar í refsimálum og refsiverð brot sem um getur í 10. gr. eða

c) kerfisbundið og umfangsmikið eftirlit með svæði sem er aðgengilegt almenningi.

4. Eftirlitsyfirvaldið skal koma á fót og birta skrá yfir þær tegundir vinnsluaðgerða þar sem krafist er mats á áhrifum á persónuvernd skv. 1. mgr. Eftirlitsyfirvaldið skal senda persónuverndarráðinu, sem um getur í 68. gr., þessar skrár.

5. Eftirlitsyfirvaldinu er einnig heimilt að koma á fót og birta skrá yfir þær tegundir vinnsluaðgerða þar sem ekki er krafist mats á áhrifum á persónuvernd. Eftirlitsyfirvaldið skal senda persónuverndarráðinu þessar skrár.

6. Ef í skránum, sem um getur í 4. og 5. mgr., er greint frá vinnslustarfsemi, sem tengist því að bjóða skráðum einstaklingum vörur eða þjónustu eða hafa eftirlit með hegðun þeirra í fleiri en einu aðildarríki eða sem gæti haft veruleg áhrif á frjálsa miðlun persónuupplýsinga innan Sambandsins, skal lögbært eftirlitsyfirvald beita samræmingarkerfinu, sem um getur í 63. gr., áður en þessar skrár eru samþykktar.

7. Þegar þessar upplýsingar eru birtar skal a.m.k. eftirfarandi koma fram:

a) kerfisbundin lýsing á fyrirhuguðum vinnsluaðgerðum og tilganginum með vinnslunni, þ.m.t., eftir atvikum, lögmætum hagsmunum ábyrgðaraðilans,

b) mat á því hvort vinnsluaðgerðirnar eru nauðsynlegar og hóflegar miðað við tilganginn með þeim,

c) mat á áhættu fyrir réttindi og frelsi skráðra einstaklinga sem um getur í 1. mgr. og

d) ráðstafanir sem fyrirhugað er að grípa til gegn slíkri áhættu, þ.m.t. verndarráðstafanir, öryggisráðstafanir og fyrirkomulag við að tryggja vernd persónuupplýsinga og sýna fram á að farið sé að þessari reglugerð, að teknu tilliti til réttinda og lögmætra hagsmuna skráðra einstaklinga og annarra einstaklinga sem í hlut eiga.

8. Taka skal tilhlýðilegt tillit til þess hvort hlutaðeigandi ábyrgðaraðilar eða vinnsluaðilar fylgja samþykktum hátternisreglum, sem um getur í 40. gr., þegar áhrif vinnsluaðgerða téðra ábyrgðaraðila eða vinnsluaðila eru metin, einkum að því er varðar mat á áhrifum á persónuvernd.

9. Þegar við á skal ábyrgðaraðili leita álits skráðra einstaklinga eða fulltrúa þeirra á fyrirhugaðri vinnslu, án þess að það hafi áhrif á vernd viðskiptahagsmuna eða almannahagsmuna eða öryggi vinnsluaðgerða.

10. Ef vinnsla skv. c- eða e-lið 1. mgr. 6. gr. á sér lagagrundvöll í lögum Sambandsins eða lögum aðildarríkis, sem ábyrgðaraðili heyrir undir, og þau lög gilda um þá tilteknu vinnsluaðgerð eða -aðgerðir sem um er að ræða og mat á áhrifum á persónuvernd hefur þegar farið fram, sem hluti af almennu áhrifamati í tengslum við samþykkt þess lagagrundvallar, gilda 1.–7. mgr. ekki nema aðildarríkin telji nauðsynlegt að láta slíkt mat fara fram áður en vinnslustarfsemin hefst.

11. Ef nauðsyn krefur skal ábyrgðaraðilinn láta fara fram endurskoðun til að meta hvort vinnslan fari fram í samræmi við matið á áhrifum á persónuvernd, a.m.k. þegar breyting verður á þeirri áhættu sem fylgir vinnsluaðgerðunum.

36. gr.

Fyrirframsamráð

1. Ef mat á áhrifum á persónuvernd skv. 35. gr. gefur til kynna að vinnslan myndi hafa mikla áhættu í för með sér, nema ábyrgðaraðilinn grípi til ráðstafana til að draga úr henni, skal ábyrgðaraðilinn hafa samráð við eftirlitsyfirvaldið áður en vinnsla hefst.

2. Telji eftirlitsyfirvaldið að fyrirhuguð vinnsla, sem um getur í 1. mgr., myndi brjóta í bága við þessa reglugerð, einkum ef ábyrgðaraðili hefur ekki greint eða dregið úr áhættunni með fullnægjandi hætti, skal eftirlitsyfirvaldið, innan átta vikna frá að því berst beiðni um samráð, veita ábyrgðaraðila og, eftir atvikum, vinnsluaðila skriflega ráðgjöf og getur notað til þess allar þær valdheimildir sínar sem um getur í 58. gr. Lengja má frestinn um sex vikur með hliðsjón af því hversu flókin fyrirhuguð vinnsla er. Eftirlitsyfirvaldið skal tilkynna ábyrgðaraðila og, eftir atvikum, vinnsluaðila um slíkar framlengingar innan mánaðar frá viðtöku beiðni um samráð, ásamt ástæðunum fyrir töfinni. Þessa fresti má framlengja þar til eftirlitsyfirvaldið hefur fengið þær upplýsingar sem það óskar eftir vegna samráðsins.

3. Þegar ábyrgðaraðili hefur samráð við eftirlitsyfirvaldið skv. 1. mgr. skal hann gefa því upp:

a) eftir atvikum, ábyrgðarsvið ábyrgðaraðila, sameiginlegra ábyrgðaraðila og vinnsluaðila, sem koma að vinnslunni, hvers um sig, einkum þegar um er að ræða vinnslu innan fyrirtækjasamstæðu,

b) tilgang fyrirhugaðrar vinnslu og aðferðir við hana,

c) ráðstafanir og verndarráðstafanir sem gerðar eru til að vernda réttindi og frelsi skráðra einstaklinga samkvæmt þessari reglugerð,

d) ef við á, samskiptaupplýsingar persónuverndarfulltrúa,

e) mat á áhrifum á persónuvernd sem kveðið er á um í 35. gr. og

f) hverjar þær upplýsingar aðrar sem eftirlitsyfirvaldið fer fram á.

4. Aðildarríkin skulu hafa samráð við eftirlitsyfirvaldið við undirbúning tillögu að löggjafarráðstöfun, sem tengist vinnslu og þjóðþing skal samþykkja, eða stjórnvaldsráðstöfun sem byggir á slíkri löggjafarráðstöfun.

5. Þrátt fyrir 1. mgr. má krefjast þess í lögum aðildarríkis að ábyrgðaraðilar hafi samráð við og fái fyrirframleyfi eftirlitsyfirvalds í tengslum við vinnslu ábyrgðaraðila sem annast framkvæmd verkefnis í þágu almannahagsmuna, þ.m.t. vinnslu sem tengist félagslegri vernd og lýðheilsu.

4. þáttur

Persónuverndarfulltrúi

37. gr.

Tilnefning persónuverndarfulltrúa

1. Ábyrgðaraðili og vinnsluaðili skulu tilnefna persónuverndarfulltrúa í sérhverju tilviki þar sem:

a) vinnsla er í höndum opinbers yfirvalds eða stofnunar, að undanskildum dómstólum þegar þeir fara með dómsvald sitt,

b) meginstarfsemi ábyrgðaraðila eða vinnsluaðila felst í vinnsluaðgerðum sem krefjast, sakir eðlis síns, umfangs og/eða tilgangs, umfangsmikils, reglubundins og kerfisbundins eftirlits með skráðum einstaklingum eða

c) meginstarfsemi ábyrgðaraðila eða vinnsluaðila felst í umfangsmikilli vinnslu sérstakra flokka upplýsinga skv. 9. gr. eða persónuupplýsinga er varða sakfellingar í refsimálum og refsiverð brot sem um getur í 10. gr.

2. Fyrirtækjasamstæðu er heimilt að skipa einn persónuverndarfulltrúa að því tilskildu að sérhver starfsstöð hafi greiðan aðgang að honum.

3. Ef ábyrgðaraðili eða vinnsluaðili er opinbert yfirvald eða stofnun er heimilt að tilnefna einn persónuverndarfulltrúa fyrir fleiri en eitt slíkt yfirvald eða stofnun, að teknu tilliti til stjórnskipulags þeirra og stærðar.

4. Í öðrum tilvikum en þeim sem um getur í 1. mgr. er ábyrgðaraðila eða vinnsluaðila eða samtökum og öðrum aðilum, sem eru fulltrúar flokka ábyrgðaraðila eða vinnsluaðila, heimilt eða jafnvel skylt, sé þess krafist í lögum Sambandsins eða lögum aðildarríkis, að tilnefna persónuverndarfulltrúa. Persónuverndarfulltrúinn getur komið fram fyrir hönd slíkra samtaka og annarra aðila sem eru fulltrúar ábyrgðaraðila eða vinnsluaðila.

5. Persónuverndarfulltrúinn skal tilnefndur á grundvelli faglegrar hæfni sinnar og einkum sérþekkingar á lögum og lagaframkvæmd á sviði persónuverndar og getu sinnar til að vinna þau verkefni sem um getur í 39. gr.

6. Persónuverndarfulltrúinn getur verið starfsmaður ábyrgðaraðila eða vinnsluaðila eða sinnt verkefnum á grundvelli þjónustusamnings.

7. Ábyrgðaraðili eða vinnsluaðili skal birta samskiptaupplýsingar persónuverndarfulltrúans og senda eftirlitsyfirvaldinu þær.

38. gr.

Staða persónuverndarfulltrúa

1. Ábyrgðaraðili og vinnsluaðili skulu tryggja að persónuverndarfulltrúi komi, með viðeigandi hætti og tímanlega, að öllum málum sem tengjast vernd persónuupplýsinga.

2. Ábyrgðaraðili og vinnsluaðili skulu styðja persónuverndarfulltrúann við framkvæmd þeirra verkefna sem um getur í 39. gr. 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.

3. Ábyrgðaraðili og vinnsluaðili skulu tryggja að persónuverndarfulltrúi fái engin fyrirmæli varðandi framkvæmd þessara verkefna. Ábyrgðaraðili eða vinnsluaðili skal hvorki víkja honum úr starfi né refsa honum fyrir framkvæmd verkefna sinna. Persónuverndarfulltrúi skal heyra beint undir æðsta stjórnunarstig hjá ábyrgðaraðila eða vinnsluaðila.

4. Skráðir einstaklingar geta haft samband við persónuverndarfulltrúann með öll mál sem tengjast vinnslu á persónuupplýsingum þeirra og því hvernig þeir geta neytt réttar síns samkvæmt þessari reglugerð.

5. Persónuverndarfulltrúi skal bundinn þagnarskyldu eða trúnaði um framkvæmd verkefna sinna í samræmi við lög Sambandsins eða lög aðildarríkis.

6. Persónuverndarfulltrúi má sinna öðrum verkefnum og skyldustörfum. Ábyrgðaraðili eða vinnsluaðili skal tryggja að slík verkefni og skyldustörf leiði ekki til hagsmunaárekstra.

39. gr.

Verkefni persónuverndarfulltrúa

1. Persónuverndarfulltrúi skal sinna a.m.k. eftirfarandi verkefnum:

a) upplýsa ábyrgðaraðila eða vinnsluaðila og starfsmenn, sem annast vinnslu, um skyldur sínar samkvæmt þessari reglugerð og öðrum ákvæðum Sambandsins eða aðildarríkis um persónuvernd og veita þeim ráðgjöf þar að lútandi,

b) fylgjast með því að farið sé að ákvæðum þessarar reglugerðar, öðrum ákvæðum Sambandsins eða aðildarríkis um persónuvernd og stefnum ábyrgðaraðila eða vinnsluaðila varðandi vernd persónuupplýsinga, þ.m.t. úthlutun ábyrgðar, vitundarvakning og þjálfun starfsfólks sem tekur þátt í vinnslustarfsemi og tilheyrandi úttektir,

c) veita ráðgjöf, sé farið fram á það, varðandi mat á áhrifum á persónuvernd og fylgjast með framkvæmd þess skv. 35. gr.,

d) vinna með eftirlitsyfirvaldinu,

e) vera tengiliður fyrir eftirlitsyfirvaldið varðandi mál sem tengjast vinnslu, þ.m.t. fyrirframsamráðið sem um getur í 36. gr., og leita ráða, eftir því sem við á, varðandi önnur málefni.

2. Persónuverndarfulltrúi skal við framkvæmd verkefna sinna taka tilhlýðilegt tillit til þeirrar áhættu sem fylgir vinnslustarfseminni, með hliðsjón af eðli, umfangi, samhengi og tilgangi vinnslunnar.

5. þáttur

Hátternisreglur og vottun

40. gr.

Hátternisreglur

1. Aðildarríkin, eftirlitsyfirvöld, persónuverndarráðið og framkvæmdastjórnin skulu hvetja til þess að samdar verði hátternisreglur, sem eiga að stuðla að réttri beitingu þessarar reglugerðar, með tilliti til sérkenna hinna ýmsu vinnslusviða og sérstakra þarfa örfyrirtækja, lítilla og meðalstórra fyrirtækja.

2. Samtökum og öðrum aðilum, sem eru fulltrúar flokka ábyrgðaraðila eða vinnsluaðila, er heimilt að semja hátternisreglur, eða breyta slíkum reglum eða rýmka þær, í því skyni að kveða nánar á um beitingu þessarar reglugerðar, t.d. að því er varðar:

a) sanngjarna og gagnsæja vinnslu,

b) lögmæta hagsmuni ábyrgðaraðila í tilteknu samhengi,

c) söfnun persónuupplýsinga,

d) notkun gerviauðkenna við vinnslu persónuupplýsinga,

e) upplýsingar sem veittar eru almenningi og skráðum einstaklingum,

f) það að skráðir einstaklingar geti neytt réttar síns,

g) upplýsingar sem veittar eru börnum og þeim til verndar og það hvernig afla beri samþykkis forsjáraðila,

h) þær ráðstafanir og aðferðir sem um getur í 24. og 25. gr. og ráðstafanir til að tryggja öryggi vinnslu sem um getur í 32. gr.,

i) tilkynningar til eftirlitsyfirvalda um öryggisbresti við meðferð persónuupplýsinga og það að skráðum einstaklingum sé gert viðvart um slíka bresti,

j) miðlun persónuupplýsinga til þriðju landa eða alþjóðastofnana eða

k) málsmeðferð utan dómstóla og aðra málsmeðferð við lausn deilumála til að leysa deilur er varða vinnslu milli ábyrgðaraðila og skráðra einstaklinga, sbr. þó réttindi hinna skráðu skv. 77. og 79. gr.

3. Auk þess að ábyrgðaraðilar eða vinnsluaðilar, sem heyra undir þessa reglugerð, beiti hátternisreglum, sem samþykktar eru skv. 5. mgr. þessarar greinar og hafa almennt gildi skv. 9. mgr. þessarar greinar, geta ábyrgðaraðilar eða vinnsluaðilar, sem ekki heyra undir þessa reglugerð skv. 3. gr., einnig gert það til að tryggja að viðeigandi verndarráðstafanir séu fyrir hendi innan ramma miðlunar persónuupplýsinga til þriðju landa eða alþjóðastofnana samkvæmt þeim skilmálum sem um getur í e-lið 2. mgr. 46. gr. Slíkir ábyrgðaraðilar eða vinnsluaðilar skulu skuldbinda sig, með bindandi og framfylgjanlegum hætti, til að beita þessum viðeigandi verndarráðstöfunum, m.a. að því er varðar réttindi skráðra einstaklinga, með samningi eða öðrum lagalega bindandi gerningum.

4. Hátternisreglur, sem um getur í 2. mgr. þessarar greinar, skulu fela í sér fyrirkomulag sem gerir aðilanum, sem um getur í 1. mgr. 41. gr., kleift að annast skyldubundið eftirlit með því að ábyrgðaraðilar eða vinnsluaðilar, sem skuldbinda sig til að beita þeim, fylgi ákvæðum þeirra, án þess þó að það hafi áhrif á verkefni og valdheimildir eftirlitsyfirvalda sem lögbær eru skv. 55. eða 56. gr.

5. Samtök og aðrir aðilar, sem um getur í 2. mgr. þessarar greinar, sem hafa í hyggju að semja hátternisreglur eða breyta reglum eða rýmka reglur sem fyrir eru, skulu leggja drög að reglum, breytingu eða rýmkun fyrir það eftirlitsyfirvald sem lögbært er skv. 55. gr. Eftirlitsyfirvaldið skal gefa álit sitt á því hvort drögin að hátternisreglum, breytingin eða rýmkunin samrýmist þessari reglugerð og samþykkja drögin, breytinguna eða rýmkunina ef það telur að með þeim séu tryggðar nægilegar og viðeigandi verndarráðstafanir.

6. Ef drögin að hátternisreglum, breytingin eða rýmkunin er samþykkt í samræmi við 5. mgr. og ef viðkomandi hátternisreglur varða ekki vinnslustarfsemi í fleiri en einu aðildarríki skal eftirlitsyfirvaldið skrá reglurnar og birta þær.

7. Varði drögin að hátternisreglum vinnslustarfsemi í fleiri en einu aðildarríki skal eftirlitsyfirvaldið, sem lögbært er skv. 55. gr., áður en það samþykkir drögin, breytinguna eða rýmkunina, leggja þau fyrir persónuverndarráðið samkvæmt þeirri málsmeðferð sem um getur í 63. gr. og skal ráðið gefa álit sitt á því hvort drögin að reglunum, breytingin eða rýmkunin samrýmist þessari reglugerð eða, í þeim aðstæðum sem um getur í 3. mgr. þessarar greinar, tryggi viðeigandi verndarráðstafanir.

8. Staðfesti álitið, sem um getur í 7. mgr., að drögin að hátternisreglum, breytingin eða rýmkunin samrýmist þessari reglugerð eða, í þeim aðstæðum sem um getur í 3. mgr., tryggi viðeigandi verndarráðstafanir, skal persónuverndarráðið leggja álit sitt fyrir framkvæmdastjórnina.

9. Framkvæmdastjórninni er heimilt að ákveða, með framkvæmdargerðum, að hátternisreglurnar, breytingin eða rýmkunin, sem hlotið hafa samþykki og hún fær til umfjöllunar skv. 8. mgr. þessarar greinar, hafi almennt gildi innan Sambandsins. Þessar framkvæmdargerðir skulu samþykktar í samræmi við rannsóknarmálsmeðferðina sem um getur í 2. mgr. 93. gr.

10. Framkvæmdastjórnin skal sjá til þess að samþykktar reglur, sem ákveðið hefur verið að hafi almennt gildi í samræmi við 9. mgr., fái viðeigandi kynningu.

11. Persónuverndarráðið skal safna saman öllum samþykktum hátternisreglum, breytingum og rýmkunum í skrá og gera þær aðgengilegar almenningi með viðeigandi hætti.

41. gr.

Eftirlit með samþykktum hátternisreglum

1. Með fyrirvara um verkefni og valdheimildir lögbærs eftirlitsyfirvalds skv. 57. og 58. gr. má eftirlit með því að hátternisreglum skv. 40. gr. sé fylgt vera í höndum aðila sem ræður yfir viðeigandi sérþekkingu á viðfangsefni reglnanna og hefur fengið faggildingu í þeim tilgangi frá lögbæru eftirlitsyfirvaldi.

2. Aðili skv. 1. mgr. getur fengið faggildingu til að hafa eftirlit með því að hátternisreglum sé fylgt ef hann hefur:

a) sýnt fram á sjálfstæði sitt og sérþekkingu á viðfangsefni reglnanna með hætti sem lögbæru eftirlitsyfirvaldi þykir fullnægjandi,

b) komið á verklagi sem gerir honum kleift að meta hæfi hlutaðeigandi ábyrgðaraðila og vinnsluaðila til að beita hátternisreglunum, hafa eftirlit með því að þeir fari að ákvæðum þeirra og endurskoða starfsemi þeirra með reglubundnum hætti,

c) komið á verklagi og kerfum til að annast meðferð kvartana um brot á reglunum eða á því hvernig ábyrgðaraðili eða vinnsluaðili framkvæmir, eða hefur framkvæmt, reglurnar og til að gera þetta verklag og þessi kerfi gagnsæ fyrir skráða einstaklinga og almenning og

d) sýnt fram á, með fullnægjandi hætti að mati lögbærs eftirlitsyfirvalds, að verkefni hans og skyldustörf leiði ekki til hagsmunaáreksturs.

3. Lögbæra eftirlitsyfirvaldið skal leggja fyrir persónuverndarráðið drög að kröfum varðandi faggildingu aðila, eins og um getur í 1. mgr. þessarar greinar, samkvæmt samræmingarkerfinu sem um getur í 63. gr.

4. Með fyrirvara um verkefni og valdheimildir lögbæra eftirlitsyfirvaldsins og ákvæði VIII. kafla skal aðili, eins og um getur í 1. mgr. þessarar greinar, með fyrirvara um viðeigandi verndarráðstafanir, grípa til viðeigandi aðgerða ef ábyrgðaraðili eða vinnsluaðili brýtur gegn reglunum, þ.m.t. tímabundinnar eða varanlegrar útilokunar ábyrgðaraðilans eða vinnsluaðilans frá reglunum. Hann skal tilkynna lögbæru eftirlitsyfirvaldi um slíkar aðgerðir og ástæðurnar fyrir þeim.

5. Lögbæra eftirlitsyfirvaldið skal afturkalla faggildingu aðila, eins og um getur í 1. mgr., ef kröfurnar varðandi faggildingu eru ekki, eða eru ekki lengur, uppfylltar eða ef aðgerðir aðilans brjóta í bága við þessa reglugerð.

6. Þessi grein gildir ekki um vinnslu af hálfu opinberra yfirvalda og stofnana.

42. gr.

Vottun

1. Aðildarríkin, eftirlitsyfirvöldin, persónuverndarráðið og framkvæmdastjórnin skulu hvetja til þess, einkum á vettvangi Sambandsins, að komið verði á fót vottunarfyrirkomulagi vegna persónuverndar ásamt persónuverndarinnsiglum og -merkjum til að sýna fram á að vinnsla ábyrgðaraðila og vinnsluaðila uppfylli ákvæði þessarar reglugerðar. Taka skal tillit til sérstakra þarfa örfyrirtækja, lítilla og meðalstórra fyrirtækja.

2. Auk þess að ábyrgðaraðilar eða vinnsluaðilar, sem heyra undir þessa reglugerð, komi á fót vottunarfyrirkomulagi vegna persónuverndar ásamt persónuverndarinnsiglum eða -merkjum skv. 5. mgr. þessarar greinar geta ábyrgðaraðilar og vinnsluaðilar, sem heyra ekki undir þessa reglugerð skv. 3. gr., komið slíku á til að sýna fram á að fyrir hendi séu viðeigandi verndarráðstafanir innan ramma miðlunar persónuupplýsinga til þriðju landa eða alþjóðastofnana samkvæmt þeim skilmálum sem um getur í e-lið 2. mgr. 46. gr. Slíkir ábyrgðaraðilar eða vinnsluaðilar skulu skuldbinda sig, með bindandi og framfylgjanlegum hætti, til að beita þessum viðeigandi verndarráðstöfunum, m.a. að því er varðar réttindi skráðra einstaklinga, með samningi eða öðrum lagalega bindandi gerningum.

3. Vottunin skal vera valfrjáls og aðgengileg í gagnsæju ferli.

4. Vottun samkvæmt þessari grein dregur ekki úr þeirri skyldu ábyrgðaraðila eða vinnsluaðila að fara að ákvæðum þessarar reglugerðar og hún hefur ekki áhrif á verkefni og valdheimildir eftirlitsyfirvalda sem eru lögbær skv. 55. eða 56. gr.

5. Vottunaraðilarnir, sem um getur í 43. gr., eða lögbært eftirlitsyfirvald skulu gefa út vottun samkvæmt þessari grein, á grundvelli viðmiðana sem lögbæra eftirlitsyfirvaldið samþykkir skv. 3. mgr. 58. gr. eða persónuverndarráðið skv. 63. gr. Samþykki persónuverndarráðið viðmiðanirnar getur það leitt til almennrar vottunar, Evrópska persónuverndarmerkisins.

6. Ábyrgðaraðili eða vinnsluaðili, sem óskar eftir vottun á vinnslu sinni samkvæmt vottunarkerfinu, skal láta vottunaraðilanum, sem um getur í 43. gr., eða, þar sem við á, lögbæra eftirlitsyfirvaldinu í té allar upplýsingar sem nauðsynlegar eru og þann aðgang að vinnslustarfsemi sinni sem nauðsynlegur er til að leiða vottunarferlið til lykta.

7. Vottunin skal gefin út til handa ábyrgðaraðila eða vinnsluaðila til þriggja ára að hámarki og hana má endurnýja, með sömu skilyrðum, að því tilskildu að viðeigandi viðmiðanir séu áfram uppfylltar. Séu viðmiðanirnar um vottunina ekki, eða ekki lengur, uppfylltar skulu vottunaraðilarnir, sem um getur í 43. gr., eða lögbæra eftirlitsyfirvaldið, eftir því sem við á, afturkalla vottunina.

8. Persónuverndarráðið skal safna öllu vottunarfyrirkomulagi og persónuverndarinnsiglum og -merkjum saman í skrá og gera aðgengilegt almenningi með viðeigandi hætti.

43. gr.

Vottunaraðilar

1. Með fyrirvara um verkefni og valdheimildir lögbæra eftirlitsyfirvaldsins skv. 57. og 58. gr. skulu vottunaraðilar með viðeigandi sérþekkingu á persónuvernd annast, ef nauðsyn krefur, útgáfu og endurnýjun vottunar, eftir að hafa tilkynnt það eftirlitsyfirvaldinu til að gera því kleift að beita valdheimildum sínum skv. h-lið 2. mgr. 58. gr. Aðildarríkin skulu tryggja að þessir vottunaraðilar séu faggiltir af öðrum eða báðum eftirtalinna aðila:

a) eftirlitsyfirvaldinu sem lögbært er skv. 55. eða 56. gr.,

b) faggildingarstofu í aðildarríki sem tilgreind er í samræmi við reglugerð Evrópuþingsins og ráðsins (EB) nr. 765/2008 ([1]) í samræmi við Evrópustaðal EN-ISO/IEC 17065/2012 og viðbótarkröfur sem settar eru af eftirlitsyfirvaldinu sem lögbært er skv. 55. eða 56. gr.

2. Vottunaraðilar, sem um getur í 1. mgr., skulu aðeins hljóta faggildingu í samræmi við þá málsgrein ef þeir hafa:

a) sýnt fram á sjálfstæði sitt og sérþekkingu á viðfangsefni vottunarinnar með hætti sem lögbæru eftirlitsyfirvaldi þykir fullnægjandi,

([1]) Reglugerð Evrópuþingsins og ráðsins (EB) nr. 765/2008 frá 9. júlí 2008 um kröfur varðandi faggildingu og markaðseftirlit í tengslum við markaðssetningu á vörum og um niðurfellingu reglugerðar (EBE) nr. 339/93 (Stjtíð. ESB L 218, 13.8.2008, bls. 30).

b) skuldbundið sig til að virða viðmiðanirnar sem um getur í 5. mgr. 42. gr. og samþykktar eru af eftirlitsyfirvaldinu sem er lögbært skv. 55. eða 56. gr. eða af persónuverndarráðinu skv. 63. gr.,

c) komið á verklagi hvað varðar útgáfu, reglubundna endurskoðun og afturköllun persónuverndarvottunar, persónuverndarinnsigla eða -merkja,

d) komið á fót verklagi og kerfum til að annast meðferð kvartana um brot gegn ákvæðum vottunarinnar eða á því hvernig ábyrgðaraðili eða vinnsluaðili framkvæmir eða hefur framkvæmt vottunina og til að gera þetta verklag og þessi kerfi gagnsæ fyrir skráða einstaklinga og almenning og

e) sýnt fram á, með hætti sem lögbæru eftirlitsyfirvaldi þykir fullnægjandi, að verkefni þeirra og skyldustörf leiði ekki til hagsmunaáreksturs.

3. Faggilding vottunaraðila, eins og um getur í 1. og 2. mgr. þessarar greinar, skal fara fram á grundvelli krafna sem samþykktar eru af eftirlitsyfirvaldinu sem er lögbært skv. 55. eða 56. gr. eða persónuverndarráðinu skv. 63. gr. Ef um er að ræða faggildingu skv. b-lið 1. mgr. þessarar greinar skulu þessar kröfur koma til viðbótar þeim sem gert er ráð fyrir í reglugerð (EB) nr. 765/2008 og tæknireglunum sem lýsa aðferðum og verklagsreglum vottunaraðilanna.

4. Vottunaraðilarnir, sem um getur í 1. mgr., skulu bera ábyrgð á réttu mati, sem leiðir til vottunar eða afturköllunar á vottun, með fyrirvara um ábyrgð ábyrgðaraðila eða vinnsluaðila á því að farið sé að þessari reglugerð. Gefa skal faggildinguna út til fimm ára að hámarki og hana má endurnýja með sömu skilyrðum, að því tilskildu að vottunaraðili uppfylli kröfur þessarar greinar.

5. Vottunaraðilarnir, sem um getur í 1. mgr., skulu láta lögbærum eftirlitsyfirvöldum í té rökstuðning fyrir því að veita eða afturkalla umbeðna vottun.

6. Eftirlitsyfirvaldið skal birta kröfurnar sem um getur í 3. mgr. þessarar greinar og viðmiðanirnar sem um getur í 5. mgr. 42. gr. á aðgengilegu formi. Eftirlitsyfirvöldin skulu einnig senda persónuverndarráðinu þessar kröfur og viðmiðanir.

7. Með fyrirvara um VIII. kafla skal lögbæra eftirlitsyfirvaldið eða faggildingarstofan í aðildarríki afturkalla faggildingu vottunaraðila skv. 1. mgr. þessarar greinar ef skilyrðin fyrir faggildingunni eru ekki, eða eru ekki lengur, uppfyllt eða ef aðgerðir vottunaraðilans brjóta í bága við þessa reglugerð.

8. Framkvæmdastjórninni skal falið vald til þess að samþykkja framseldar gerðir í samræmi við 92. gr. í þeim tilgangi að tilgreina þær kröfur sem taka þarf tillit til í vottunarfyrirkomulagi vegna persónuverndar sem um getur í 1. mgr. 42. gr.

9. Framkvæmdastjórnin getur samþykkt framkvæmdargerðir þar sem mælt er fyrir um tæknistaðla fyrir vottunarfyrirkomulag og persónuverndarinnsigli og -merki og fyrirkomulag við að kynna og viðurkenna slíkt vottunarfyrirkomulag, innsigli og merki. Þessar framkvæmdargerðir skulu samþykktar í samræmi við rannsóknarmálsmeðferðina sem um getur í 2. mgr. 93. gr.

V. KAFLI

Miðlun persónuupplýsinga til þriðju landa eða alþjóðastofnana

44. gr.

Almennar meginreglur um miðlun upplýsinga

Með fyrirvara um önnur ákvæði þessarar reglugerðar skal aðeins miðla persónuupplýsingum, sem eru í vinnslu eða eru ætlaðar til vinnslu að lokinni miðlun þeirra til þriðja lands eða til alþjóðastofnunar, ef ábyrgðaraðilinn og vinnsluaðilinn uppfylla skilyrðin sem mælt er fyrir um í þessum kafla, þ.m.t. til framsendingar persónuupplýsinga frá þriðja landi eða alþjóðastofnun til annars þriðja lands eða annarrar alþjóðastofnunar. Beita skal öllum ákvæðum í þessum kafla þannig að tryggja megi að ekki sé grafið undan vernd einstaklinga sem tryggð er með þessari reglugerð.

45. gr.

Miðlun á grundvelli ákvörðunar um hvort vernd sé fullnægjandi

1. Miðlun persónuupplýsinga til þriðja lands eða til alþjóðastofnunar er heimil ef framkvæmdastjórnin hefur ákveðið að þriðja landið, yfirráðasvæði eða einn eða fleiri tilgreindir geirar innan viðkomandi þriðja lands eða umrædd alþjóðastofnun tryggi fullnægjandi vernd. Slík miðlun þarfnast ekki sérstakrar heimildar.

2. Þegar framkvæmdastjórnin metur hvort vernd sé fullnægjandi skal hún einkum taka mið af eftirfarandi þáttum:

a) grunnreglum réttarríkisins, virðingu fyrir mannréttindum og mannfrelsi, viðeigandi löggjöf, jafnt almennri löggjöf sem sérlöggjöf, þ. á m. varðandi almannaöryggi, landvarnir, þjóðaröryggi og refsirétt og aðgang opinberra yfirvalda að persónuupplýsingum, ásamt framkvæmd umræddrar löggjafar, reglum um persónuvernd, starfsreglum og öryggisráðstöfunum, þ.m.t. reglum um miðlun persónuupplýsinga til annars þriðja lands eða alþjóðastofnunar sem fylgt er í umræddu landi eða hjá alþjóðastofnun, dómaframkvæmd, sem og skilvirkum og fullnustuhæfum réttindum skráðra einstaklinga og skilvirkri stjórnsýslu- og dómsmeðferð fyrir skráða einstaklinga hvað varðar miðlun persónuupplýsinga um þá,

b) hvort fyrir hendi er sjálfstætt og skilvirkt eftirlitsyfirvald, eitt eða fleiri, í þriðja landinu eða sem alþjóðastofnun fellur undir, sem ber ábyrgð á að tryggja og framfylgja því að farið sé að reglum um persónuvernd, þ. á m. með fullnægjandi valdheimildum til að framfylgja þeim, á að veita skráðum einstaklingum aðstoð og ráðleggingar þegar þeir nýta sér réttindi sín og á samvinnu við eftirlitsyfirvöld í aðildarríkjunum og

c) alþjóðlegum skuldbindingum sem þriðja landið eða alþjóðastofnunin hefur tekist á hendur eða öðrum skyldum samkvæmt lagalega bindandi samningum eða gerningum, sem og þátttöku í marghliða eða svæðisbundnum kerfum, einkum í tengslum við vernd persónuupplýsinga.

3. Framkvæmdastjórnin getur, eftir að hún hefur metið hvort umfang verndar er fullnægjandi, ákveðið á grundvelli framkvæmdargerðar, að þriðja land, yfirráðasvæði eða einn eða fleiri tilgreindur geiri innan þriðja lands, eða alþjóðastofnun, tryggi fullnægjandi vernd í skilningi 2. mgr. þessarar greinar. Í framkvæmdargerðinni skal kveða á um fyrirkomulag reglubundinnar endurskoðunar, a.m.k. á fjögurra ára fresti, þar sem tekið skal tillit til viðeigandi þróunar í þriðja landinu eða hjá alþjóðastofnuninni. Í framkvæmdargerðinni skal tilgreina svæðis- og geirabundið gildissvið og, eftir atvikum, tilgreina eftirlitsyfirvald eða -yfirvöld sem um getur í b-lið 2. mgr. þessarar greinar. Framkvæmdargerðin skal samþykkt í samræmi við rannsóknarmálsmeðferðina sem um getur í 2. mgr. 93. gr.

4. Framkvæmdastjórnin skal fylgjast jafnt og þétt með þróun mála í þriðju löndum og hjá alþjóðastofnunum sem gætu haft áhrif á framkvæmd ákvarðana sem samþykktar eru skv. 3. mgr. þessarar greinar og 6. mgr. 25. gr. tilskipunar 95/46/EB.

5. Framkvæmdastjórnin skal, að því marki sem nauðsynlegt telst, afturkalla, breyta eða fella tímabundið úr gildi ákvörðunina, sem um getur í 3. mgr. þessarar greinar, á grundvelli framkvæmdargerða, án afturvirkni, ef fyrirliggjandi upplýsingar leiða í ljós, einkum í kjölfar endurskoðunarinnar sem um getur í 3. mgr. þessarar greinar, að þriðja land, yfirráðasvæði eða einn eða fleiri tilgreindur geiri innan þriðja lands eða alþjóðastofnun tryggi ekki lengur fullnægjandi vernd í skilningi 2. mgr. þessarar greinar. Þessar framkvæmdargerðir skulu samþykktar í samræmi við rannsóknarmálsmeðferðina sem um getur í 2. mgr. 93. gr.

Þegar brýna nauðsyn ber til í tilhlýðilega rökstuddum tilvikum skal framkvæmdastjórnin samþykkja framkvæmdargerðir sem öðlast gildi án tafar í samræmi við málsmeðferðina sem um getur í 3. mgr. 93. gr.

6. Framkvæmdastjórnin skal hefja viðræður við þriðja landið eða alþjóðastofnunina með það fyrir augum að ráða bót á ástandinu sem varð til þess að ákvörðunin var tekin skv. 5. mgr.

7. Ákvörðun skv. 5. mgr. þessarar greinar hefur ekki áhrif á miðlun persónuupplýsinga til þriðja lands, yfirráðasvæðis eða eins eða fleiri tilgreindra geira innan þessa þriðja lands eða viðkomandi alþjóðastofnunar skv. 46.–49. gr.

8. Framkvæmdastjórnin skal birta í *Stjórnartíðindum Evrópusambandsins* og á vefsetri sínu skrá yfir þau þriðju lönd, yfirráðasvæði og tilgreindu geira innan þriðja lands og alþjóðastofnanir sem hún hefur ákveðið að veiti ekki, eða ekki lengur, fullnægjandi vernd.

9. Ákvarðanir sem framkvæmdastjórnin hefur samþykkt á grundvelli 6. mgr. 25. gr. tilskipunar 95/46/EB gilda áfram uns þeim er breytt, þær eru leystar af hólmi eða þær eru felldar niður með ákvörðun framkvæmdastjórnarinnar sem er samþykkt í samræmi við 3. eða 5. mgr. þessarar greinar.

46. gr.

Miðlun sem fellur undir viðeigandi verndarráðstafanir

1. Ef ekki er tekin ákvörðun skv. 3. mgr. 45. gr. getur ábyrgðaraðili eða vinnsluaðili því aðeins miðlað persónuupplýsingum til þriðja lands eða alþjóðastofnunar að hann hafi gert viðeigandi verndarráðstafanir og með því skilyrði að fyrir hendi séu framfylgjanleg réttindi og skilvirk lagaleg úrræði fyrir skráða einstaklinga.

2. Viðeigandi verndarráðstafanir, sem um getur í 1. mgr., geta, án þess að krafist sé sérstakrar heimildar frá eftirlitsyfirvaldi, falist í eftirfarandi:

a) lagalega bindandi og framfylgjanlegum gerningi milli opinberra yfirvalda eða stofnana,

b) bindandi fyrirtækjareglum í samræmi við 47. gr.,

c) stöðluðum ákvæðum um persónuvernd sem framkvæmdastjórnin hefur samþykkt í samræmi við rannsóknarmálsmeðferðina sem um getur í 2. mgr. 93. gr.,

d) stöðluðum ákvæðum um persónuvernd sem eftirlitsyfirvald hefur samþykkt og framkvæmdastjórnin viðurkennt í samræmi við rannsóknarmálsmeðferðina sem um getur í 2. mgr. 93. gr.,

e) viðurkenndum hátternisreglum skv. 40. gr., ásamt bindandi og framfylgjanlegum skuldbindingum ábyrgðaraðilans eða vinnsluaðilans í þriðja landinu um að beita viðeigandi verndarráðstöfunum, einnig að því er varðar réttindi skráðra einstaklinga, eða

f) viðurkenndu vottunarkerfi skv. 42. gr., ásamt bindandi og framfylgjanlegum skuldbindingum ábyrgðaraðilans eða vinnsluaðilans í þriðja landinu um að beita viðeigandi verndarráðstöfunum, einnig að því er varðar réttindi hinna skráðu.

3. Með fyrirvara um heimild frá lögbæru eftirlitsyfirvaldi geta viðeigandi verndarráðstafanir, sem um getur í 1. mgr., einnig falist í einkum eftirfarandi:

a) samningsákvæðum milli ábyrgðaraðilans eða vinnsluaðilans og ábyrgðaraðila, vinnsluaðila eða viðtakanda persónuupplýsinganna í þriðja landinu eða hjá alþjóðastofnuninni eða

b) ákvæðum sem felld eru inn í stjórnvaldsráðstafanir milli opinberra yfirvalda eða stofnana sem ná yfir framfylgjanleg og skilvirk réttindi skráðra einstaklinga.

4. Eftirlitsyfirvaldið skal beita samræmingarkerfinu sem um getur í 63. gr. í þeim tilvikum sem um getur í 3. mgr. þessarar greinar.

5. Heimildir, sem aðildarríki eða eftirlitsyfirvald veitir á grundvelli 2. mgr. 26. gr. tilskipunar 95/46/EB, gilda áfram þar til eftirlitsyfirvaldið breytir þeim, leysir þær af hólmi eða fellir þær niður, ef nauðsyn krefur. Ákvarðanir, sem framkvæmdastjórnin hefur samþykkt á grundvelli tilskipunar 95/46/EB, gilda áfram þar til þeim er breytt, þær eru leystar af hólmi eða þær eru felldar niður, ef nauðsyn krefur, með ákvörðun framkvæmdastjórnarinnar sem er samþykkt í samræmi við 2. mgr. þessarar greinar.

47. gr.

Bindandi fyrirtækjareglur

1. Lögbær eftirlitsyfirvöld skulu samþykkja bindandi fyrirtækjareglur í samræmi við samræmingarkerfið sem tilgreint er í 63. gr., að því tilskildu að þær:

a) séu lagalega bindandi og að þær gildi um og þeim sé framfylgt af sérhverjum hlutaðeigandi aðila að fyrirtækjasamstæðu eða hópi fyrirtækja sem stunda sameiginlega atvinnustarfsemi, þ.m.t. starfsmönnum þeirra,

b) veiti skráðum einstaklingum framfylgjanleg réttindi með ótvíræðum hætti með hliðsjón af vinnslu persónuupplýsinga um þá og

c) uppfylli kröfurnar sem mælt er fyrir um í 2. gr.

2. Í bindandi fyrirtækjareglum, sem um getur í 1. mgr., skal tilgreina a.m.k.:

a) skipulag og samskiptaupplýsingar viðkomandi fyrirtækjasamstæðu eða hóps fyrirtækja sem stunda sameiginlega atvinnustarfsemi og sérhvers aðila samstæðunnar eða hópsins,

b) miðlun eða endurtekna miðlun upplýsinga, þ.m.t. hvaða flokka persónuupplýsinga er um að ræða, tegund og tilgang vinnslu, hvaða hópur skráðra einstaklinga verður fyrir áhrifum af henni og hvaða þriðja land eða þriðju lönd er um að ræða,

c) lagalega bindandi eðli þeirra, jafnt inn á við sem út á við,

d) beitingu almennra meginreglna um persónuvernd, einkum um takmörkun vegna tilgangs, lágmörkun gagna, takmörkun á varðveislutímabili, gæði gagna, innbyggða og sjálfgefna persónuvernd, lagagrundvöll vinnslu, vinnslu sérstakra flokka persónuupplýsinga, ráðstafanir til að tryggja persónuvernd og kröfur sem lúta að framsendingu til aðila sem eru ekki háðir bindandi fyrirtækjareglum,

e) réttindi skráðra einstaklinga að því er varðar vinnslu og leiðir til að neyta þeirra réttinda, þ.m.t. réttinn til að falla ekki undir ákvarðanir sem byggjast eingöngu á sjálfvirkri vinnslu, m.a. gerð persónusniðs í samræmi við 22. gr., til að leggja fram kvörtun hjá lögbæru eftirlitsyfirvaldi og hjá lögbærum dómstólum aðildarríkjanna í samræmi við 79. gr. og til að rétta hlut sinn og, eftir því sem við á, til bóta vegna brots á bindandi fyrirtækjareglum,

f) viðurkenningu ábyrgðaraðila eða vinnsluaðila, sem hafa staðfestu á yfirráðasvæði aðildarríkis, á ábyrgð vegna hvers kyns brota gegn bindandi fyrirtækjareglum af hálfu hlutaðeigandi aðila sem hafa ekki staðfestu í Sambandinu; ábyrgðaraðilinn eða vinnsluaðilinn skal því aðeins vera undanþeginn bótaábyrgð, að fullu eða að hluta, að hann færi sönnur á að viðkomandi aðili sé ekki ábyrgur fyrir tilvikinu sem leiddi til tjónsins,

g) hvernig skráðum einstaklingum eru veittar upplýsingar um bindandi fyrirtækjareglur, einkum ákvæðin sem um getur í d-, e- og f-lið þessarar málsgreinar, auk 13. og 14. gr.,

h) verkefni persónuverndarfulltrúa sem eru tilnefndir í samræmi við 37. gr. eða annars aðila eða stofnunar sem hefur með höndum eftirlit með því að bindandi fyrirtækjareglum sé fylgt innan fyrirtækjasamstæðu eða hóps fyrirtækja sem stunda sameiginlega atvinnustarfsemi, ásamt eftirliti með starfsþjálfun og meðferð kvörtunarmála,

i) málsmeðferð vegna kvörtunarmála,

j) fyrirkomulag innan fyrirtækjasamstæðunnar eða hóps fyrirtækja, sem stunda sameiginlega atvinnustarfsemi, til að tryggja sannprófun á því að farið sé að bindandi fyrirtækjareglum. Þetta fyrirkomulag skal fela í sér úttektir á persónuvernd og aðferðir við að tryggja að gripið sé til aðgerða til úrbóta til að vernda réttindi hins skráða. Tilkynna ætti þeim aðila eða stofnun, sem um getur í h-lið, og stjórn fyrirtækisins, sem er ráðandi í fyrirtækjasamstæðu eða hópi fyrirtækja sem stunda sameiginlega atvinnustarfsemi, um niðurstöður sannprófunarinnar og þær ættu að vera aðgengilegar lögbærum eftirlitsyfirvöldum fari þau fram á það,

k) fyrirkomulag skýrslugjafar og skráningar á breytingum á reglunum og skýrslugjafar um breytingarnar til eftirlits-yfirvaldsins,

l) fyrirkomulag samvinnu við eftirlitsyfirvaldið til að tryggja reglufylgni aðila að fyrirtækjasamstæðunni eða hópi fyrirtækja sem stunda sameiginlega atvinnustarfsemi, einkum með því að sjá til þess að eftirlitsyfirvaldið fái aðgang að niðurstöðum sannprófunar á þeim ráðstöfunum sem um getur í j-lið,

m) fyrirkomulag vegna skýrslugjafar til lögbærs eftirlitsyfirvalds um þau lagaskilyrði sem aðili að fyrirtækjasamstæðu eða hópi fyrirtækja, sem stunda sameiginlega atvinnustarfsemi, þarf að hlíta í þriðja landi sem líklegt er að hafi umtalsverð neikvæð áhrif á þær tryggingar sem felast í bindandi fyrirtækjareglum og

n) viðeigandi þjálfun starfsmanna, sem hafa stöðugan eða reglulegan aðgang að persónuupplýsingum, á sviði persónuverndar.

3. Framkvæmdastjórnin getur tilgreint nánar snið og aðferðir við upplýsingaskipti milli ábyrgðaraðila, vinnsluaðila og eftirlitsyfirvalda að því er varðar bindandi fyrirtækjareglur í skilningi þessarar greinar. Þessar framkvæmdargerðir skulu samþykktar í samræmi við rannsóknarmálsmeðferðina sem um getur í 2. mgr. 93. gr.

48. gr.

Miðlun eða birting sem ekki er heimiluð samkvæmt lögum Sambandsins

Dóma, sem dómstólar kveða upp, og ákvarðanir stjórnsýsluyfirvalds í þriðja landi, sem krefjast þess að ábyrgðaraðili eða vinnsluaðili miðli persónuupplýsingum eða birti þær, má því aðeins viðurkenna eða framfylgja með einhverjum hætti að slíkt byggist á alþjóðasamningi, s.s. samningi um gagnkvæma dómsmálaaðstoð, sem er í gildi milli þriðja landsins sem leggur fram beiðni og Sambandsins eða aðildarríkis, án þess að það hafi áhrif á aðrar ástæður til miðlunar samkvæmt þessum kafla.

49. gr.

Undanþágur vegna sérstakra aðstæðna

1. Ef ekki liggur fyrir ákvörðun um að vernd sé fullnægjandi skv. 3. mgr. 45. gr. eða ekki hafa verið gerðar viðeigandi verndarráðstafanir skv. 46. gr., þ.m.t. bindandi fyrirtækjareglur, skal miðlun eða endurtekin miðlun persónuupplýsinga til þriðja lands eða alþjóðastofnunar aðeins fara fram að uppfylltu einu af eftirfarandi skilyrðum:

a) hinn skráði hefur veitt ótvírætt samþykki sitt fyrir fyrirhugaðri miðlun eftir að honum hefur verið tilkynnt um mögulega áhættu sem miðlunin kann að hafa í för með sér fyrir hann vegna þess að ekki liggur fyrir ákvörðun um að vernd sé fullnægjandi og viðeigandi verndarráðstafanir hafa ekki verið gerðar,

b) miðlunin er nauðsynleg vegna framkvæmdar samnings milli hins skráða og ábyrgðaraðilans eða ráðstafana sem gerðar eru að beiðni hins skráða áður en til gerðar samnings kemur,

c) miðlunin er nauðsynleg fyrir gerð eða framkvæmd samnings í þágu hins skráða, sem ábyrgðaraðilinn og annar einstaklingur eða lögaðili gera sín í milli,

d) miðlunin er nauðsynleg vegna mikilvægra almannahagsmuna,

e) miðlunin er nauðsynleg til að stofna, hafa uppi eða verja réttarkröfur,

f) miðlunin er nauðsynleg til að vernda brýna hagsmuni hins skráða eða annarra aðila ef hinn skráði er líkamlega eða í lagalegum skilningi ófær um að gefa samþykki sitt,

g) upplýsingum er miðlað úr skrá sem er samkvæmt lögum Sambandsins eða lögum aðildarríkis ætlað að veita almenningi upplýsingar og er aðgengileg annaðhvort öllum almenningi eða hverjum þeim sem getur sýnt fram á að hann hafi lögmætra hagsmuna að gæta, en aðeins að svo miklu leyti sem skilyrði fyrir aðgangi, sem mælt er fyrir um í lögum Sambandsins eða lögum aðildarríkis, séu uppfyllt í því tilviki.

Ef ekki er hægt að byggja miðlun á ákvæði í 45. eða 46. gr., þ.m.t. ákvæðum um bindandi fyrirtækjareglur, og engin af undanþágunum vegna sérstakra aðstæðna, sem um getur í fyrstu undirgrein þessarar málsgreinar, á við, er aðeins heimilt að miðla persónuupplýsingum til þriðja lands eða til alþjóðastofnunar ef miðlunin er ekki endurtekin, varðar aðeins takmarkaðan fjölda skráðra einstaklinga, er nauðsynleg vegna mikilvægra lögmætra hagsmuna sem ábyrgðaraðili gætir þegar hagsmunir eða réttindi og frelsi hins skráða vega ekki þyngra og ef ábyrgðaraðilinn hefur kannað allar aðstæður er varða miðlun upplýsinganna og hefur, á grundvelli þess mats, gert viðeigandi verndarráðstafanir að því er varðar vernd persónuupplýsinga. Ábyrgðaraðilinn skal upplýsa eftirlitsyfirvaldið um miðlunina. Auk þess að láta í té þær upplýsingar, sem um getur í 13. og 14. gr., skal ábyrgðaraðilinn upplýsa hinn skráða um miðlunina og þá mikilvægu, lögmætu hagsmuni sem gætt er.

2. Miðlun skv. g-lið fyrstu undirgreinar 1. mgr. skal ekki taka til persónuupplýsinganna í heild sinni eða heilla flokka persónuupplýsinga í skránni. Ef skráin er ætluð til skoðunar fyrir þá sem hafa lögmætra hagsmuna að gæta skal miðlun aðeins fara fram að beiðni þessara aðila eða ef þeir eiga að vera viðtakendur upplýsinganna.

3. Ákvæði a-, b- og c-liðar fyrstu undirgreinar 1. mgr. og annarrar undirgreinar hennar gilda ekki um starfsemi opinberra yfirvalda við beitingu þeirra á opinberu valdi.

4. Viðurkenna skal þá almannahagsmuni, sem um getur í d-lið fyrstu undirgreinar 1. mgr., í lögum Sambandsins eða í lögum þess aðildarríkis sem ábyrgðaraðilinn heyrir undir.

5. Þegar ekki hefur verið tekin ákvörðun um hvort fullnægjandi vernd er fyrir hendi geta lög Sambandsins eða lög aðildarríkis takmarkað með ótvíræðum hætti miðlun sérstakra flokka persónuupplýsinga til þriðja lands eða alþjóðastofnunar á grundvelli mikilvægra almannahagsmuna. Aðildarríkin skulu tilkynna framkvæmdastjórninni um slík ákvæði.

6. Ábyrgðaraðilinn eða vinnsluaðilinn skal staðfesta matið og viðeigandi verndarráðstafanir, sem um getur í annarri undirgrein 1. mgr. þessarar greinar, í skránum sem um getur í 30. gr.

50. gr.

Alþjóðleg samvinna um vernd persónuupplýsinga

Þegar um er að ræða þriðju lönd eða alþjóðastofnanir skulu framkvæmdastjórnin og eftirlitsyfirvöld gera viðeigandi ráðstafanir til að:

a) þróa fyrirkomulag alþjóðlegrar samvinnu til að greiða fyrir skilvirkri framkvæmd löggjafar um vernd persónuupplýsinga,

b) veita gagnkvæma alþjóðlega aðstoð við framfylgd löggjafar um vernd persónuupplýsinga, m.a. með tilkynningum, framsendingu kvörtunarmála, aðstoð við rannsóknir og upplýsingaskiptum, með fyrirvara um viðeigandi verndarráðstafanir til verndar persónuupplýsingum og öðrum grundvallarréttindum og mannfrelsi,

c) fá viðkomandi hagsmunaaðila til að taka þátt í umfjöllun og starfi sem miðar að því að efla alþjóðlega samvinnu við framfylgd löggjafar um vernd persónuupplýsinga,

d) stuðla að skiptum á og skjalahaldi um löggjöf og starfsvenjur á sviði verndar persónuupplýsinga, einkum um ágreining við þriðju lönd um lögsögu.

VI. KAFLI

Sjálfstæð eftirlitsyfirvöld

1. þáttur

Sjálfstæði

51. gr.

Eftirlitsyfirvald

1. Sérhvert aðildarríki skal sjá til þess að eitt eða fleiri sjálfstæð opinber yfirvöld beri ábyrgð á að fylgjast með beitingu þessarar reglugerðar til þess að vernda grundvallarréttindi og frelsi einstaklinga í tengslum við vinnslu persónuupplýsinga og til að greiða fyrir frjálsu flæði persónuupplýsinga innan Sambandsins („eftirlitsyfirvald“).

2. Sérhvert eftirlitsyfirvald skal stuðla að samræmdri beitingu þessarar reglugerðar í öllu Sambandinu. Í þessum tilgangi skulu eftirlitsyfirvöldin eiga samstarf sín í milli og við framkvæmdastjórnina í samræmi við VII. kafla.

3. Ef fleiri en einu eftirlitsyfirvaldi er komið á fót í aðildarríki skal aðildarríkið tilnefna það eftirlitsyfirvald sem á að koma fram fyrir hönd þessara yfirvalda í persónuverndarráðinu og skal koma á kerfi til að tryggja að hin yfirvöldin fari að þeim reglum sem varða samræmingarkerfið sem um getur í 63. gr.

4. Sérhvert aðildarríki skal tilkynna framkvæmdastjórninni eigi síðar en 25. maí 2018 um ákvæði landslaga sem þau hafa samþykkt samkvæmt þessum kafla og skulu án tafar tilkynna um síðari breytingar sem hafa áhrif á þau.

52. gr.

Sjálfstæði

1. Sérhvert eftirlitsyfirvald skal vera algerlega sjálfstætt í störfum sínum og þegar það beitir valdheimildum sínum í samræmi við þessa reglugerð.

2. Fulltrúi eða fulltrúar hvers eftirlitsyfirvalds skulu, í störfum sínum og þegar þeir beita valdheimildum sínum í samræmi við þessa reglugerð, vera lausir við utanaðkomandi áhrif, jafnt bein sem óbein, og skulu hvorki leita eftir né taka við fyrirmælum frá öðrum aðilum.

3. Fulltrúi eða fulltrúar hvers eftirlitsyfirvalds skulu ekki aðhafast neitt það sem er ósamrýmanlegt skyldum þeirra og skulu ekki stunda önnur ósamrýmanleg störf á skipunartíma sínum, hvorki launuð né ólaunuð.

4. Sérhvert aðildarríki skal tryggja að hvert eftirlitsyfirvald hafi yfir að ráða þeim mannauði, tækniúrræðum og fjármagni, húsakosti og innviðum sem nauðsynleg eru til að það geti unnið störf sín og beitt valdheimildum sínum með skilvirkum hætti, þ. á m. í tengslum við gagnkvæma aðstoð, samvinnu og þátttöku í starfi persónuverndarráðsins.

5. Sérhvert aðildarríki skal sjá til þess að hvert eftirlitsyfirvald velji og hafi eigið starfslið og ætti það eingöngu að lúta stjórn fulltrúa hlutaðeigandi eftirlitsyfirvalds.

6. Sérhvert aðildarríki skal sjá til þess að hvert eftirlitsyfirvald sæti eftirliti með fjárreiðum, sem hefur ekki áhrif á sjálfstæði þess, og að það hafi sérstaka opinbera, árlega fjárhagsáætlun sem getur verið hluti af heildarfjárlögum fylkisins eða ríkisins.

53. gr.

Almenn skilyrði varðandi fulltrúa eftirlitsyfirvaldsins

1. Aðildarríkin skulu kveða á um að sérhver fulltrúi eftirlitsyfirvalda þeirra sé skipaður samkvæmt gagnsærri málsmeðferð af:

— þingi þeirra,

— ríkisstjórn þeirra,

— þjóðhöfðingja þeirra eða

— óháðri stofnun sem falin er skipunin samkvæmt lögum aðildarríkisins.

2. Sérhver fulltrúi skal búa yfir menntun og hæfi, reynslu og færni, einkum á sviði verndar persónuupplýsinga, sem honum er nauðsynleg til að hann geti sinnt skyldustörfum sínum og beitt valdheimildum sínum.

3. Skyldustörfum fulltrúa skal ljúka þegar skipunartími hans rennur út, hann segir starfinu lausu eða lætur af störfum fyrir aldurs sakir, í samræmi við lög hlutaðeigandi aðildarríkis.

4. Aðeins skal víkja fulltrúa brott ef um alvarlegt misferli er að ræða eða ef hann fullnægir ekki lengur þeim skilyrðum sem krafist er vegna skyldustarfa hans.

54. gr.

Reglur um stofnun eftirlitsyfirvalds

1. Sérhvert aðildarríki skal kveða á um öll eftirfarandi atriði í lögum:

a) stofnun sérhvers eftirlitsyfirvalds,

b) menntun og hæfisskilyrði sem krafist er vegna skipunar fulltrúa sérhvers eftirlitsyfirvalds,

c) reglur og verklagsreglur að því er varðar skipun fulltrúa sérhvers eftirlitsyfirvalds,

d) skipunartíma fulltrúa sérhvers eftirlitsyfirvalds sem ekki skal vera skemmri en fjögur ár, að undanskilinni fyrstu skipun eftir 24. maí 2016, sem getur verið til skemmri tíma ef það er nauðsynlegt til að standa vörð um sjálfstæði eftirlitsyfirvaldsins með því að nota áfangabundið skipunarferli,

e) hvort og þá hversu oft heimilt er að endurnýja skipun fulltrúa sérhvers eftirlitsyfirvalds,

f) skilyrði varðandi skyldur fulltrúa sérhvers eftirlitsyfirvalds og starfsmanna þess, bann við aðgerðum, störfum og fríðindum sem eru ósamrýmanleg þeim á starfstímanum og að honum loknum og reglur um starfslok.

2. Fulltrúi eða fulltrúar sérhvers eftirlitsyfirvalds og starfsmenn þess skulu, í samræmi við lög Sambandsins eða lög aðildarríkis, vera bundnir þagnarskyldu, bæði á starfstímanum og að honum loknum, með tilliti til trúnaðarupplýsinga sem þeir hafa fengið við skyldustörf sín eða við beitingu valdheimilda sinna. Meðan starfstími þeirra varir skal þagnarskylda þeirra einkum gilda um tilkynningar einstaklinga um brot gegn þessari reglugerð.

2. þáttur

Valdsvið, verkefni og valdheimildir

55. gr.

Valdsvið

1. Sérhvert eftirlitsyfirvald skal vera til þess bært að sinna þeim verkefnum sem því eru falin og beita þeim valdheimildum sem því hafa verið veittar í samræmi við þessa reglugerð á yfirráðasvæði eigin aðildarríkis.

2. Þegar vinnsla er í höndum opinberra yfirvalda eða einkaaðila, sem starfa á grundvelli c- eða e-liðar 1. mgr. 6. gr., skal eftirlitsyfirvald hlutaðeigandi aðildarríkis teljast lögbært. Í þeim tilvikum á 56. gr. ekki við.

3. Eftirlitsyfirvöld skulu ekki vera til þess bær að hafa eftirlit með vinnsluaðgerðum dómstóla þegar þeir fara með dómsvald sitt.

56. gr.

Valdsvið forystueftirlitsyfirvalds

1. Með fyrirvara um 55. gr. skal eftirlitsyfirvald yfir höfuðstöðvum eða hinni einu starfsstöð ábyrgðaraðilans eða vinnsluaðilans teljast til þess bært að koma fram sem forystueftirlitsyfirvald vegna vinnslu yfir landamæri sem sá ábyrgðaraðili eða vinnsluaðili annast í samræmi við málsmeðferðina sem kveðið er á um í 60. gr.

2. Þrátt fyrir 1. mgr. skal sérhvert eftirlitsyfirvald teljast til þess bært að fjalla um kvörtun sem lögð er fyrir það eða mögulegt brot gegn þessari reglugerð ef viðfangsefnið tengist eingöngu starfsstöð í aðildarríki þess eða hefur eingöngu veruleg áhrif á skráða einstaklinga í aðildarríki þess.

3. Í þeim tilvikum sem um getur í 2. mgr. þessarar greinar skal eftirlitsyfirvaldið tilkynna forystueftirlitsyfirvaldinu um málavöxtu án tafar. Forystueftirlitsyfirvaldið skal, innan þriggja vikna frá því að tilkynningin berst, ákveða hvort það muni fjalla um málið í samræmi við málsmeðferðina sem kveðið er á um í 60. gr., að teknu tilliti til þess hvort ábyrgðaraðilinn eða vinnsluaðilinn hefur staðfestu í aðildarríki eftirlitsyfirvaldsins sem tilkynnti um það.

4. Ef forystueftirlitsyfirvaldið ákveður að fjalla um málið gildir málsmeðferðin sem kveðið er á um í 60. gr. Eftirlitsyfirvaldið, sem sendi tilkynninguna til forystueftirlitsyfirvaldsins, getur sent því drög að ákvörðun. Forystu-eftirlitsyfirvaldið skal taka ýtrasta tillit til umræddra draga þegar það semur drög að ákvörðuninni sem um getur í 3. mgr. 60. gr.

5. Ef forystueftirlitsyfirvaldið ákveður að fjalla ekki um málið skal eftirlitsyfirvaldið, sem tilkynnti forystueftirlitsyfirvaldinu um það, fjalla um málið skv. 61. og 62. gr.

6. Forystueftirlitsyfirvaldið skal vera eini tengiliður ábyrgðaraðilans eða vinnsluaðilans vegna vinnslu hans yfir landamæri.

57. gr.

Verkefni

1. Með fyrirvara um önnur verkefni, sem sett eru fram í þessari reglugerð, skal sérhvert eftirlitsyfirvald, á eigin yfirráðasvæði:

a) fylgjast með og framfylgja beitingu þessarar reglugerðar,

b) efla vitund og skilning almennings á áhættu, reglum, verndarráðstöfunum og réttindum í tengslum við vinnslu. Gefa skal starfsemi sem beinist einkum að börnum sérstakan gaum,

c) veita þjóðþingi, ríkisstjórn og öðrum stofnunum og aðilum ráðgjöf, í samræmi við landslög aðildarríkis, um ráðstafanir á sviði lagasetningar og stjórnsýslu sem tengist vernd réttinda og frelsis einstaklinga að því er varðar vinnslu,

d) efla vitund ábyrgðaraðila og vinnsluaðila um skyldur sínar samkvæmt þessari reglugerð,

e) veita, að fenginni beiðni, skráðum einstaklingi upplýsingar um það hvernig hann getur neytt réttinda sinna samkvæmt þessari reglugerð og, ef við á, starfa með eftirlitsyfirvöldum í öðrum aðildarríkjum í því skyni,

f) fjalla um kvartanir sem skráður einstaklingur eða stofnun, samtök eða félag leggja fram í samræmi við 80. gr. og rannsaka, að því marki sem við á, efni kvörtunarinnar og upplýsa kvartandann um framvindu og niðurstöður rannsóknarinnar innan hæfilegs tíma, einkum ef nauðsyn er á frekari rannsóknum eða samræmingu við annað eftirlitsyfirvald,

g) eiga samstarf við önnur eftirlitsyfirvöld, þ.m.t. með því að skiptast á upplýsingum, og veita gagnkvæma aðstoð, með það fyrir augum að tryggja samkvæmni í beitingu og framfylgd þessarar reglugerðar,

h) gera rannsókn á beitingu þessarar reglugerðar, m.a. á grundvelli upplýsinga frá öðru eftirlitsyfirvaldi eða öðru opinberu yfirvaldi,

i) fylgjast með þróun sem skiptir máli, að svo miklu leyti sem hún hefur áhrif á vernd persónuupplýsinga, einkum þróun upplýsinga- og fjarskiptatækni og viðskiptahátta,

j) samþykkja föst samningsákvæði sem um getur í 8. mgr. 28. gr. og d-lið 2. mgr. 46. gr.,

k) útbúa og viðhalda skrá í tengslum við kröfu um mat á áhrifum á persónuvernd skv. 4. mgr. 35. gr.,

l) veita ráðgjöf um vinnsluaðgerðir sem um getur í 2. mgr. 36. gr.,

m) hvetja til þess að samdar verði hátternisreglur skv. 1. mgr. 40. gr. og gefa álit á og samþykkja hátternisreglur sem tryggja fullnægjandi verndarráðstafanir skv. 5. mgr. 40. gr.,

n) hvetja til þess að vottunarfyrirkomulagi vegna persónuverndar og persónuverndarinnsiglum og -merkjum verði komið á skv. 1. mgr. 42. gr. og samþykkja viðmiðanir vegna vottunar skv. 5. mgr. 42. gr.,

o) eftir atvikum, láta fara fram reglubundna endurskoðun á vottunum sem eru gefnar út í samræmi við 7. mgr. 42. gr.,

p) semja og birta drög að kröfum varðandi faggildingu aðila sem hefur eftirlit með hátternisreglum skv. 41. gr. og vottunaraðila skv. 43. gr.,

q) annast faggildingu aðila vegna eftirlits með hátternisreglum skv. 41. gr. og vottunaraðila skv. 43. gr.,

r) heimila samningsákvæði og ákvæði sem um getur í 3. mgr. 46. gr.,

s) samþykkja bindandi fyrirtækjareglur skv. 47. gr.,

t) taka þátt í starfsemi persónuverndarráðsins,

u) halda innri skrár yfir brot á þessari reglugerð og ráðstafanir sem gerðar eru í samræmi við 2. mgr. 58. gr. og

v) sinna öðrum störfum sem tengjast vernd persónuupplýsinga.

2. Sérhvert eftirlitsyfirvald skal auðvelda framlagningu kvartana, sem um getur í f-lið 1. mgr., með því að gera ráðstafanir á borð við kvörtunareyðublað, sem einnig má fylla út rafrænt, án þess þó að aðrir samskiptamöguleikar séu útilokaðir.

3. Sérhvert eftirlitsyfirvald skal sinna störfum sínum, skráðum einstaklingum og, eftir atvikum, persónuverndarfulltrúanum að kostnaðarlausu.

4. Þegar beiðnir eru augljóslega tilefnislausar eða óhóflegar, einkum vegna þess að þær eru endurteknar, er eftirlitsyfirvaldinu heimilt að setja upp sanngjarnt gjald, á grundvelli umsýslukostnaðar, eða neita að fjalla um beiðnina. Það skal vera eftirlitsyfirvaldsins að sýna fram á að beiðni sé tilefnislaus eða óhófleg.

58. gr.

Valdheimildir

1. Sérhvert eftirlitsyfirvald skal hafa allar eftirfarandi rannsóknarheimildir:

a) heimild til að fyrirskipa að ábyrgðaraðilinn og vinnsluaðilinn og, eftir atvikum, fulltrúi ábyrgðaraðilans eða vinnsluaðilans veiti hvers kyns upplýsingar sem það þarfnast vegna skyldustarfa sinna,

b) heimild til að láta fara fram rannsóknir í formi úttekta á persónuvernd,

c) heimild til að láta fara fram endurskoðun á vottunum sem eru gefnar út skv. 7. mgr. 42. gr.,

d) heimild til að tilkynna ábyrgðaraðila eða vinnsluaðila um meint brot á þessari reglugerð,

e) heimild til að fá hjá ábyrgðaraðila og vinnsluaðila aðgang að öllum persónuupplýsingum og öllum upplýsingum sem nauðsynlegar eru vegna verkefna þess,

f) heimild til að fá aðgang að húsnæði ábyrgðaraðila og vinnsluaðila, þ.m.t. hvers kyns gagnavinnslubúnaði og -aðferðum, í samræmi við réttarfarslög Sambandsins eða aðildarríkis.

2. Sérhvert eftirlitsyfirvald skal hafa allar eftirfarandi valdheimildir til að gera ráðstafanir til úrbóta:

a) heimild til að veita ábyrgðaraðila eða vinnsluaðila viðvörun um að líklegt sé að fyrirhugaðar vinnsluaðgerðir brjóti í bága við ákvæði þessarar reglugerðar,

b) heimild til að veita ábyrgðaraðila eða vinnsluaðila áminningu ef vinnsluaðgerðir hafa brotið í bága við þessa reglugerð,

c) heimild til að fyrirskipa að ábyrgðaraðili eða vinnsluaðili fari að beiðnum hins skráða um að fá að neyta réttinda sinna samkvæmt þessari reglugerð,

d) heimild til að fyrirskipa að ábyrgðaraðili eða vinnsluaðili færi vinnsluaðgerðir til samræmis við ákvæði þessarar reglugerðar, eftir því sem við á, með tilteknum hætti og innan tiltekins tíma,

e) heimild til að fyrirskipa að ábyrgðaraðili tilkynni hinum skráða um öryggisbrest við meðferð persónuupplýsinga,

f) heimild til að setja tímabundna eða varanlega takmörkun á vinnslu, þ.m.t. bann,

g) heimild til að fyrirskipa leiðréttingu eða eyðingu persónuupplýsinga eða takmörkun á vinnslu þeirra skv. 16., 17. og 18. gr. og að slíkar aðgerðir verði tilkynntar viðtakendum sem fengið hafa persónuupplýsingarnar í hendur skv. 2. mgr. 17. gr. og 19. gr.,

h) heimild til að afturkalla vottun eða fyrirskipa að vottunaraðilinn afturkalli vottun sem gefin var út skv. 42. og 43. gr. eða fyrirskipa að vottunaraðilinn gefi ekki út vottun ef kröfum vegna vottunarinnar er ekki, eða er ekki lengur, fullnægt,

i) heimild til að leggja á stjórnsýslusekt skv. 83. gr., til viðbótar við eða í stað ráðstafana sem um getur í þessari málsgrein, allt eftir aðstæðum í hverju einstöku máli,

j) heimild til að fyrirskipa tímabundna stöðvun gagnaflæðis til viðtakanda í þriðja landi eða til alþjóðastofnunar.

3. Sérhvert eftirlitsyfirvald skal hafa allar eftirfarandi leyfisveitinga- og ráðgjafarheimildir:

a) heimild til að veita ábyrgðaraðila ráðgjöf í samræmi við fyrirframsamráðsferlið sem um getur í 36. gr.,

b) heimild til að leggja, að eigin frumkvæði eða samkvæmt beiðni, álitsgerðir fyrir þjóðþing eða ríkisstjórn aðildarríkisins eða, í samræmi við lög aðildarríkisins, aðrar stofnanir og aðila, sem og almenning, um hvert það málefni sem tengist vernd persónuupplýsinga,

c) heimild til að leyfa vinnslu sem um getur í 5. mgr. 36. gr., sé slíkrar fyrirframheimildar krafist samkvæmt lögum aðildarríkisins,

d) heimild til að gefa út álit og samþykkja drög að hátternisreglum skv. 5. mgr. 40. gr.,

e) heimild til að faggilda vottunaraðila skv. 43. gr.,

f) heimild til að gefa út vottanir og samþykkja viðmiðanir fyrir vottun í samræmi við 5. mgr. 42. gr.,

g) heimild til að samþykkja stöðluð ákvæði um persónuvernd sem um getur í 8. mgr. 28. gr. og d-lið 2. mgr. 46. gr.,

h) heimild til að leyfa samningsákvæði sem um getur í a-lið 3. mgr. 46. gr.,

i) heimild til að leyfa stjórnvaldsráðstafanir sem um getur í b-lið 3. mgr. 46. gr.,

j) heimild til að samþykkja bindandi fyrirtækjareglur skv. 47. gr.

4. Beiting þeirra valdheimilda, sem eftirlitsyfirvaldinu eru veittar samkvæmt þessari grein, skal vera með fyrirvara um viðeigandi verndarráðstafanir, þ. á m. skilvirk réttarúrræði og sanngjarna málsmeðferð sem sett er fram í lögum Sambandsins og lögum aðildarríkis í samræmi við sáttmálann um grundvallarréttindi.

5. Sérhvert aðildarríki skal kveða á um í lögum að eftirlitsyfirvald þess hafi heimild til að vekja athygli dómsyfirvalda á brotum gegn þessari reglugerð og, eftir því sem við á, hefja eða taka þátt í málarekstri til þess að framfylgja ákvæðum hennar.

6. Sérhvert aðildarríki getur kveðið á um í lögum að eftirlitsyfirvald þess hafi valdheimildir til viðbótar þeim sem um getur í 1., 2. og 3. mgr. Beiting þessara valdheimilda skal ekki draga úr skilvirkri framkvæmd VII. kafla.

59. gr.

Skýrslur um starfsemi

Sérhvert eftirlitsyfirvald skal semja ársskýrslu um starfsemi sína sem má m.a. innihalda skrá yfir tegundir brota sem hafa verið tilkynnt og tegundir ráðstafana sem gerðar hafa verið í samræmi við 2. mgr. 58. gr. Þessar skýrslur skal senda þjóðþingi, ríkisstjórn og öðrum yfirvöldum eins og tilgreint er í lögum aðildarríkisins. Þær skulu gerðar aðgengilegar almenningi, framkvæmdastjórninni og persónuverndarráðinu.

VII. KAFLI

Samstarf og samræming

1. þáttur

Samstarf

60. gr.

Samstarf milli forystueftirlitsyfirvaldsins og annarra hlutaðeigandi eftirlitsyfirvalda

1. Forystueftirlitsyfirvaldið skal starfa með öðrum hlutaðeigandi eftirlitsyfirvöldum í samræmi við þessa grein með það fyrir augum að ná samstöðu. Forystueftirlitsyfirvaldið og hlutaðeigandi eftirlitsyfirvöld skulu skiptast á öllum viðeigandi upplýsingum.

2. Forystueftirlitsyfirvaldið getur hvenær sem er óskað eftir því að önnur hlutaðeigandi eftirlitsyfirvöld veiti gagnkvæma aðstoð skv. 61. gr. og getur framkvæmt sameiginlegar aðgerðir skv. 62. gr., einkum við rannsóknir eða þegar fylgst er með framkvæmd ráðstöfunar sem varðar ábyrgðaraðila eða vinnsluaðila með staðfestu í öðru aðildarríki.

3. Forystueftirlitsyfirvaldið skal án tafar senda viðeigandi upplýsingar um málið til hinna eftirlitsyfirvaldanna sem í hlut eiga. Það skal án tafar senda drög að ákvörðun til hinna eftirlitsyfirvaldanna sem í hlut eiga til að fá álit þeirra og taka tilhlýðilegt tillit til sjónarmiða þeirra.

4. Ef eitthvert hinna eftirlitsyfirvaldanna sem í hlut eiga leggur fram viðeigandi og rökstudd andmæli gegn drögum að ákvörðuninni innan fjögurra vikna frá því að samráð fer fram í samræmi við 3. mgr. þessarar greinar skal forystu-eftirlitsyfirvaldið vísa málinu til samræmingarkerfisins sem um getur í 63. gr. sé það ekki fylgjandi þessum viðeigandi og rökstuddu andmælum eða telji það að andmælin séu ekki viðeigandi eða rökstudd.

5. Ef forystueftirlitsyfirvaldið hyggst fylgja þeim viðeigandi og rökstuddu andmælum sem lögð voru fram skal það senda hinum eftirlitsyfirvöldunum sem í hlut eiga endurskoðuð drög að ákvörðun til að fá álit þeirra. Taka skal endurskoðuð drög að ákvörðuninni til umfjöllunar samkvæmt málsmeðferðinni, sem um getur í 4. mgr., innan tveggja vikna.

6. Ef ekkert hinna eftirlitsyfirvaldanna sem í hlut eiga hefur andmælt drögum að ákvörðuninni, sem forystueftirlitsyfirvaldið lagði fyrir þau, innan frestsins sem um getur í 4. og 5. mgr., skal líta svo á að forystueftirlitsyfirvaldið og hlutaðeigandi eftirlitsyfirvöld séu sammála um umrædd drög að ákvörðun og skulu þau bundin af þeim.

7. Forystueftirlitsyfirvaldið skal samþykkja ákvörðunina og tilkynna hana höfuðstöðvum eða hinni einu starfsstöð ábyrgðaraðilans eða vinnsluaðilans, eftir atvikum, og veita hinum eftirlitsyfirvöldunum sem í hlut eiga og persónuverndarráðinu upplýsingar um viðkomandi ákvörðun, þ.m.t. samantekt um þær staðreyndir og ástæður sem máli skipta. Eftirlitsyfirvaldið, sem kvörtun hefur verið lögð fram hjá, skal tilkynna kvartandanum um ákvörðunina.

8. Ef kvörtun er vísað frá eða henni hafnað skal eftirlitsyfirvaldið, sem kvörtun hefur verið lögð fram hjá, samþykkja ákvörðunina, þrátt fyrir 7. mgr., og tilkynna það kvartandanum og upplýsa ábyrgðaraðilann um það.

9. Ef forystueftirlitsyfirvaldið og hlutaðeigandi eftirlitsyfirvöld eru sammála um að vísa frá eða hafna hluta af kvörtun og fjalla um aðra hluta hennar skal samþykkja sérstaka ákvörðun fyrir hvern þessara hluta kvörtunarefnisins. Forystu-eftirlitsyfirvaldið skal samþykkja ákvörðunina um þann hluta sem varðar aðgerðir í tengslum við ábyrgðaraðilann, tilkynna það höfuðstöðvum eða hinni einu starfsstöð ábyrgðaraðilans eða vinnsluaðilans á yfirráðasvæði aðildarríkis síns og upplýsa kvartandann um það, en eftirlitsyfirvald kvartandans skal samþykkja ákvörðunina um þann hluta sem varðar frávísun eða höfnun umræddrar kvörtunar og tilkynna þá ákvörðun kvartandanum og upplýsa ábyrgðaraðilann eða vinnsluaðilann þar um.

10. Ábyrgðaraðili eða vinnsluaðili skal, eftir að honum hefur borist tilkynning um ákvörðunina skv. 7. og 9. mgr., gera nauðsynlegar ráðstafanir til að tryggja að ákvörðuninni verði fylgt að því er varðar vinnsluaðgerðir sem tengjast öllum starfsstöðvum hans í Sambandinu. Ábyrgðaraðilinn eða vinnsluaðilinn skal tilkynna forystueftirlitsyfirvaldinu um þær ráðstafanir sem hafa verið gerðar til að framfylgja ákvörðuninni og skal það upplýsa önnur hlutaðeigandi eftirlitsyfirvöld um það.

11. Ef hlutaðeigandi eftirlitsyfirvald hefur ástæðu til að ætla, í undantekningartilvikum, að brýn nauðsyn sé á að grípa til aðgerða til að vernda hagsmuni skráðra einstaklinga gildir flýtimeðferðin sem um getur í 66. gr.

12. Forystueftirlitsyfirvaldið og önnur hlutaðeigandi eftirlitsyfirvöld skulu senda hvert öðru upplýsingarnar, sem krafist er samkvæmt þessari grein, með rafrænum hætti og nota til þess staðlað snið.

61. gr.

Gagnkvæm aðstoð

1. Eftirlitsyfirvöld skulu veita hvert öðru viðeigandi upplýsingar og gagnkvæma aðstoð til þess að framkvæma og beita þessari reglugerð með samræmdum hætti og skulu gera ráðstafanir til að starfa saman á árangursríkan hátt. Gagnkvæm aðstoð skal einkum ná yfir óskir um upplýsingar og eftirlitsráðstafanir, s.s. beiðnir um fyrirframleyfisveitingar og samráð, skoðanir og rannsóknir.

2. Sérhvert eftirlitsyfirvald skal gera allar viðeigandi ráðstafanir sem nauðsynlegar eru til að bregðast við beiðni annars eftirlitsyfirvalds án ástæðulausrar tafar og eigi síðar en einum mánuði eftir að beiðnin berst. Slíkar ráðstafanir geta einkum falið í sér að senda viðeigandi upplýsingar um framkvæmd rannsóknar.

3. Beiðni um aðstoð skal innihalda allar nauðsynlegar upplýsingar, þ.m.t. um tilgang og ástæður beiðninnar. Upplýsingar sem miðlað er má aðeins nota í þeim tilgangi sem lá að baki beiðninni.

4. Eftirlitsyfirvaldið, sem beiðninni er beint til, skal ekki neita að verða við beiðninni nema:

a) viðfangsefni beiðninnar eða þær ráðstafanir, sem óskað er eftir að yfirvaldið grípi til, falli ekki undir heimildir þess eða

b) það að verða við beiðninni myndi brjóta í bága við þessa reglugerð eða lög Sambandsins eða lög aðildarríkis sem eftirlitsyfirvaldið, sem beiðninni er beint til, heyrir undir.

5. Eftirlitsyfirvaldið, sem beiðninni er beint til, skal tilkynna eftirlitsyfirvaldinu, sem lagði fram beiðnina, um niðurstöðurnar eða, eftir því sem við á, framvindu þeirra ráðstafana sem gerðar voru til að bregðast við beiðninni. Neiti eftirlitsyfirvaldið, sem beiðninni er beint til, að verða við beiðni skv. 4. mgr. skal það gefa upp ástæður þess.

6. Eftirlitsyfirvöld, sem beiðninni er beint til, skulu að jafnaði veita upplýsingar sem önnur eftirlitsyfirvöld biðja um með rafrænum hætti og nota til þess staðlað snið.

7. Eftirlitsyfirvöld, sem beiðninni er beint til, skulu ekki krefjast gjalds fyrir aðgerðir sem þau grípa til samkvæmt beiðni um gagnkvæma aðstoð. Eftirlitsyfirvöld geta komið sér saman um reglur til að bæta hvert öðru skaða vegna sérstakra útgjalda sem hljótast af því þegar gagnkvæm aðstoð er veitt í undantekningartilvikum.

8. Ef eftirlitsyfirvald veitir ekki upplýsingarnar, sem um getur í 5. mgr. þessarar greinar, innan eins mánaðar frá því að beiðni berst frá öðru eftirlitsyfirvaldi getur eftirlitsyfirvaldið, sem leggur fram beiðnina, samþykkt bráðabirgðaráðstöfun á yfirráðasvæði eigin aðildarríkis í samræmi við 1. mgr. 55. gr. Í því tilviki skal líta svo á að brýnni þörf á að grípa til aðgerða skv. 1. mgr. 66. gr. hafi verið fullnægt og að hún krefjist skjótrar bindandi ákvörðunar persónuverndarráðsins skv. 2. mgr. 66. gr.

9. Framkvæmdastjórnin getur, með framkvæmdargerðum, ákvarðað snið og tilhögun gagnkvæmrar aðstoðar, sem um getur í þessari grein, og fyrirkomulag við upplýsingaskipti með rafrænum hætti milli eftirlitsyfirvalda og milli eftirlitsyfirvalda og persónuverndarráðsins, einkum staðlaða sniðið sem um getur í 6. mgr. þessarar greinar. Þessar framkvæmdargerðir skulu samþykktar í samræmi við rannsóknarmálsmeðferðina sem um getur í 2. mgr. 93. gr.

62. gr.

Sameiginlegar aðgerðir eftirlitsyfirvalda

1. Eftirlitsyfirvöldin skulu, eftir því sem við á, grípa til sameiginlegra aðgerða, þ.m.t. sameiginlegra rannsókna og sameiginlegra framfylgdarráðstafana, sem fulltrúar eða starfsmenn eftirlitsyfirvalda annarra aðildarríkja taka þátt í.

2. Ef ábyrgðaraðilinn eða vinnsluaðilinn hefur starfsstöðvar í fleiri en einu aðildarríki eða ef búast má við að vinnsluaðgerðir hafi umtalsverð áhrif á verulegan fjölda skráðra einstaklinga í fleiri en einu aðildarríki hefur eftirlitsyfirvald hvers þessara aðildarríkja rétt til að taka þátt í sameiginlegum aðgerðum. Eftirlitsyfirvaldið, sem er lögbært skv. 1. eða 4. mgr. 56. gr., skal bjóða eftirlitsyfirvaldi frá sérhverju þessara aðildarríkja að taka þátt í sameiginlegum aðgerðum og skal án tafar bregðast við beiðni eftirlitsyfirvalds um þátttöku.

3. Eftirlitsyfirvald getur, í samræmi við lög aðildarríkis og að fenginni heimild sendieftirlitsyfirvaldsins, veitt fulltrúum eða starfsfólki sendieftirlitsyfirvaldsins, sem tekur þátt í sameiginlegum aðgerðum, valdheimildir, þ.m.t. rannsóknarheimildir, eða, að svo miklu leyti sem heimilt er samkvæmt lögum aðildarríkis gistieftirlitsyfirvaldsins, leyft fulltrúum eða starfsfólki sendieftirlitsyfirvaldsins að beita rannsóknarheimildum sínum í samræmi við lög aðildarríkis sendieftirlitsyfirvaldsins. Aðeins er heimilt að beita slíkum rannsóknarheimildum undir leiðsögn fulltrúa eða starfsfólks gistieftirlitsyfirvaldsins og í þeirra viðurvist. Fulltrúar eða starfsfólk sendieftirlitsyfirvaldsins skal falla undir lög aðildarríkis gistieftirlitsyfirvaldsins.

4. Þegar starfsmenn sendieftirlitsyfirvalds eru að störfum í öðru aðildarríki, í samræmi við 1. mgr., skal aðildarríki gistieftirlitsyfirvaldsins bera ábyrgð á störfum þeirra, þ.m.t. bótaábyrgð, vegna hvers þess tjóns sem þeir valda með aðgerðum sínum í samræmi við löggjöf þess aðildarríkis þar sem þeir eru að störfum.

5. Aðildarríkið þar sem tjónið varð skal bæta tjónið með sömu skilyrðum og eiga við um tjón sem þess eigin starfsmenn valda. Ef starfsmenn sendieftirlitsyfirvaldsins hafa valdið aðila tjóni á yfirráðasvæði annars aðildarríkis skal aðildarríki sendieftirlitsyfirvaldsins endurgreiða hinu aðildarríkinu að fullu þær fjárhæðir sem það hefur greitt þeim sem eiga rétt á bótum fyrir þeirra hönd.

6. Með fyrirvara um réttindi gagnvart þriðju aðilum og að undanskilinni 5. mgr. skal hvert aðildarríki, í því tilviki sem kveðið er á um í 1. mgr., forðast að krefja annað aðildarríki um endurgreiðslu skaðabóta vegna tjóns sem um getur í 4. mgr.

7. Ef sameiginleg aðgerð er fyrirhuguð og eftirlitsyfirvald fullnægir ekki skuldbindingunni, sem mælt er fyrir um í öðrum málslið 2. mgr. þessarar greinar, innan eins mánaðar, er hinum eftirlitsyfirvöldunum heimilt að samþykkja bráðabirgðaráðstöfun sem gildir á yfirráðasvæði þess í samræmi við 55. gr. Í því tilviki skal líta svo á að brýnni þörf á að grípa til aðgerða skv. 1. mgr. 66. gr. hafi verið fullnægt og krefjast álits eða skjótrar bindandi ákvörðunar persónuverndarráðsins skv. 2. mgr. 66. gr.

2. þáttur

Samræmi

63. gr.

Samræmingarkerfi

Til að stuðla að samræmdri beitingu þessarar reglugerðar í öllu Sambandinu skulu eftirlitsyfirvöldin eiga samstarf sín í milli og, ef við á, við framkvæmdastjórnina með hjálp samræmingarkerfisins, eins og fram kemur í þessum þætti.

64. gr.

Álit persónuverndarráðsins

1. Persónuverndarráðið skal gefa út álit ef lögbært eftirlitsyfirvald hyggst samþykkja einhverja af neðangreindum ráðstöfunum. Lögbæra eftirlitsyfirvaldið skal í því skyni senda persónuverndarráðinu drög að ákvörðuninni ef hún:

a) miðar að samþykkt skrár yfir vinnsluaðgerðir sem falla undir kröfu um mat á áhrifum á persónuvernd skv. 4. mgr. 35. gr.,

b) varðar málefni skv. 7. mgr. 40. gr. um það hvort drög að hátternisreglum, eða breytingar eða útvíkkun hátternisreglna, samrýmast þessari reglugerð,

c) miðar að samþykkt krafna varðandi faggildingu aðila skv. 3. mgr. 41. gr., vottunaraðila skv. 3. mgr. 43. gr. eða viðmiðana um faggildingu sem um getur í 5. mgr. 42. gr.,

d) miðar að ákvörðun staðlaðra ákvæða um persónuvernd sem um getur í d-lið 2. mgr. 46. gr. og 8. mgr. 28. gr.,

e) miðar að því að heimila samningsákvæði sem um getur í a-lið 3. mgr. 46. gr. eða

f) miðar að samþykkt bindandi fyrirtækjareglna í skilningi 47. gr.

2. Eftirlitsyfirvald, formaður persónuverndarráðsins eða framkvæmdastjórnin getur óskað eftir því að persónuverndarráðið rannsaki málefni, sem hafa almenna skírskotun eða afleiðingar í fleiri en einu aðildarríki, með það fyrir augum að fá álit þess, einkum ef lögbært eftirlitsyfirvald fer ekki að skyldum um gagnkvæma aðstoð í samræmi við 61. gr. eða sameiginlegar aðgerðir í samræmi við 62. gr.

3. Í þeim tilvikum, sem um getur í 1. og 2. mgr., skal persónuverndarráðið gefa út álit sitt varðandi það mál sem var vísað til þess að því tilskildu að það hafi ekki þegar gefið út álit um sama efni. Fulltrúar í persónuverndarráðinu skulu samþykkja álitið með einföldum meirihluta innan átta vikna. Lengja má frestinn um sex vikur til viðbótar með hliðsjón af því hversu flókið málið er. Að því er varðar drög að ákvörðuninni, sem um getur í 1. mgr., sem er dreift til fulltrúa í persónuverndarráðinu í samræmi við 5. mgr. skal líta svo á að fulltrúi sé samþykkur drögunum ef hann hefur ekki hreyft andmælum innan hæfilegs frests sem formaður tilgreinir.

4. Eftirlitsyfirvöld og framkvæmdastjórnin skulu, án ástæðulausrar tafar, senda persónuverndarráðinu hvers kyns viðeigandi upplýsingar með rafrænum hætti og á stöðluðu sniði, m.a., eftir atvikum, samantekt um staðreyndir málsins, drög að ákvörðuninni, ástæður þess að nauðsynlegt er talið að kveða á um slíka ráðstöfun og sjónarmið annarra hlutaðeigandi eftirlitsyfirvalda.

5. Formaður persónuverndarráðsins skal tilkynna með rafrænum hætti, án ástæðulausrar tafar:

a) fulltrúum í persónuverndarráðinu og framkvæmdastjórninni um allar viðeigandi upplýsingar sem því hafa verið sendar á stöðluðu sniði. Skrifstofa persónuverndarráðsins skal, ef nauðsyn krefur, láta þýða viðeigandi upplýsingar, og

b) eftirlitsyfirvaldinu, sem um getur í 1. og 2. mgr., eftir því sem við á, og framkvæmdastjórninni um álitið og birta það.

6. Lögbæra eftirlitsyfirvaldið, sem um getur í 1. mgr., skal ekki samþykkja drög sín að ákvörðuninni sem um getur í 1. mgr. innan þeirra tímamarka sem um getur í 3. mgr.

7. Lögbæra eftirlitsyfirvaldið, sem um getur í 1. mgr., skal taka ýtrasta tillit til álits persónuverndarráðsins og skal, innan tveggja vikna frá því að álitið berst, senda formanni persónuverndarráðsins tilkynningu með rafrænum hætti um hvort það muni standa við drögin að ákvörðuninni eða gera breytingar á þeim og, ef svo er, hin breyttu drög að ákvörðuninni á stöðluðu sniði.

8. Ef lögbæra eftirlitsyfirvaldið, sem um getur í 1. mgr., upplýsir formann persónuverndarráðsins innan frestsins, sem um getur í 7. mgr. þessarar greinar, um að það hyggist ekki fara að áliti persónuverndarráðsins, í heild eða að hluta, og færir rök fyrir því, gildir 1. mgr. 65. gr.

65. gr.

Lausn deilumála með hjálp persónuverndarráðsins

1. Til þess að tryggja rétta og samræmda beitingu þessarar reglugerðar í hverju einstöku tilviki skal persónuverndarráðið samþykkja bindandi ákvörðun í eftirfarandi tilvikum:

a) ef hlutaðeigandi eftirlitsyfirvald hefur, í því tilviki sem um getur í 4. mgr. 60. gr., haft uppi viðeigandi og rökstudd andmæli gegn drögum að ákvörðun forystueftirlitsyfirvaldsins og forystueftirlitsyfirvaldið hefur ekki fylgt andmælunum eða hefur hafnað slíkum andmælum þar sem þau séu ekki viðeigandi eða rökstudd. Þessi bindandi ákvörðun skal ná yfir öll málefni sem fjallað er um í þessum viðeigandi og rökstuddu andmælum, einkum hvort um er að ræða brot gegn þessari reglugerð,

b) ef ágreiningur er uppi um hvert af hlutaðeigandi eftirlitsyfirvöldum telst vera lögbært að því er varðar höfuðstöðvarnar,

c) ef lögbært eftirlitsyfirvald óskar ekki eftir áliti persónuverndarráðsins í tilvikum sem um getur í 1. mgr. 64. gr. eða fylgir ekki áliti sem persónuverndarráðið hefur gefið út skv. 64. gr. Í því tilviki getur hlutaðeigandi eftirlitsyfirvald eða framkvæmdastjórnin vísað málinu til persónuverndarráðsins.

2. Persónuverndarráðið skal samþykkja ákvörðunina, sem um getur í 1. mgr., með tveimur þriðju hlutum atkvæða fulltrúa í ráðinu innan eins mánaðar frá því að málið var lagt fyrir það. Lengja má frestinn um einn mánuð til viðbótar með hliðsjón af því hversu flókið málið er. Ákvörðunin, sem um getur í 1. mgr., skal vera rökstudd og henni skal beint til forystu-eftirlitsyfirvaldsins og allra hlutaðeigandi eftirlitsyfirvalda og vera bindandi fyrir þau.

3. Ef persónuverndarráðið hefur ekki getað tekið ákvörðun innan þeirra tímamarka, sem um getur í 2. mgr., skal það samþykkja ákvörðunina, innan tveggja vikna frá lokum annars mánaðarins sem um getur í 2. mgr., með einföldum meirihluta atkvæða fulltrúa í ráðinu. Ef atkvæði fulltrúa í persónuverndarráðinu falla að jöfnu skal ákvörðunin samþykkt með atkvæði formannsins.

4. Hlutaðeigandi eftirlitsyfirvöld skulu ekki samþykkja ákvörðun um það mál sem vísað er til persónuverndarráðsins skv. 1. mgr. á þeim tímabilum sem um getur í 2. og 3. mgr.

5. Formaður persónuverndarráðsins skal tilkynna, án ótilhlýðilegrar tafar, hlutaðeigandi eftirlitsyfirvöldum um ákvörðunina sem um getur í 1. mgr. Hann skal tilkynna framkvæmdastjórninni um það. Birta skal ákvörðunina á vefsetri persónuverndar-ráðsins án tafar eftir að eftirlitsyfirvaldið hefur tilkynnt um endanlega ákvörðun sem um getur í 6. mgr.

6. Forystueftirlitsyfirvaldið eða, eftir atvikum, eftirlitsyfirvaldið sem kvörtunin var lögð fram hjá skal samþykkja endanlega ákvörðun sína á grundvelli ákvörðunarinnar, sem um getur í 1. mgr. þessarar greinar, án ótilhlýðilegrar tafar og eigi síðar en einum mánuði eftir að persónuverndarráðið tilkynnir um ákvörðun sína. Forystueftirlitsyfirvaldið eða, eftir atvikum, eftirlitsyfirvaldið, sem kvörtunin var lögð fram hjá, skal upplýsa persónuverndarráðið um hvaða dag endanleg ákvörðun þess er tilkynnt annars vegar ábyrgðaraðilanum eða vinnsluaðilanum og hins vegar hinum skráða. Endanleg ákvörðun hlutaðeigandi eftirlitsyfirvalda skal samþykkt samkvæmt skilmálunum í 7., 8. og 9. mgr. 60. gr. Í endanlegri ákvörðun skal vísa í ákvörðunina, sem um getur í 1. mgr. þessarar greinar, og tilgreina að ákvörðunin, sem um getur í þeirri málsgrein, verði birt á vefsetri persónuverndarráðsins í samræmi við 5. mgr. þessarar greinar. Ákvörðunin, sem um getur í 1. mgr. þessarar greinar, skal fylgja endanlegu ákvörðuninni.

66. gr.

Flýtimeðferð

1. Í undantekningartilvikum er hlutaðeigandi eftirlitsyfirvaldi heimilt, þegar það telur brýna nauðsyn á að grípa til aðgerða til verndar réttindum og frelsi skráðra einstaklinga, með undanþágu frá samræmingarkerfinu sem um getur í 63., 64. og 65. gr. eða málsmeðferðinni sem um getur í 60. gr., að samþykkja tafarlaust bráðabirgðaráðstafanir sem er ætlað að hafa réttaráhrif á yfirráðasvæði þess og hafa tiltekinn gildistíma sem skal ekki vera lengri en þrír mánuðir. Eftirlitsyfirvaldið skal án tafar tilkynna öðrum hlutaðeigandi eftirlitsyfirvöldum, persónuverndarráðinu og framkvæmdastjórninni um þessar ráðstafanir og ástæðurnar fyrir samþykkt þeirra.

2. Ef eftirlitsyfirvald hefur gert ráðstöfun skv. 1. mgr. og telur brýnt að samþykkja endanlegar ráðstafanir getur það óskað eftir flýtiáliti eða bindandi flýtiákvörðun persónuverndarráðsins og tilgreint ástæður fyrir beiðni um slíkt álit eða ákvörðun.

3. Sérhvert eftirlitsyfirvald getur óskað eftir flýtiáliti eða bindandi flýtiákvörðun persónuverndarráðsins, eftir því sem við á, ef lögbært eftirlitsyfirvald hefur ekki gert viðeigandi ráðstafanir við aðstæður sem kalla á að brugðist verði við með skjótum hætti til að vernda réttindi og frelsi skráðra einstaklinga, og gefið upp ástæður fyrir beiðni um slíkt álit eða ákvörðun, m.a. hvers vegna brýnt er að grípa til aðgerða.

4. Þrátt fyrir 3. mgr. 64. gr. og 2. mgr. 65. gr. skal samþykkja flýtiálit eða bindandi flýtiákvörðun, sem um getur í 2. og 3. mgr. þessarar greinar, innan tveggja vikna með einföldum meirihluta atkvæða fulltrúa í persónuverndarráðinu.

67. gr.

Upplýsingaskipti

Framkvæmdastjórnin getur samþykkt almennar framkvæmdargerðir til þess að tilgreina nánar fyrirkomulag við upplýsingaskipti með rafrænum hætti milli eftirlitsyfirvalda og milli eftirlitsyfirvalda og persónuverndarráðsins, einkum staðlaða sniðið sem um getur í 64. gr.

Þessar framkvæmdargerðir skulu samþykktar í samræmi við rannsóknarmálsmeðferðina sem um getur í 2. mgr. 93. gr.

3. þáttur

Evrópska persónuverndarráðið

68. gr.

Evrópska persónuverndarráðið

1. Evrópska persónuverndarráðinu („persónuverndarráðið“) er hér með komið á fót sem stofnun á vegum Sambandsins og skal það hafa réttarstöðu lögaðila.

2. Formaður persónuverndarráðsins kemur fram fyrir hönd þess.

3. Í því skulu eiga sæti yfirmaður eins eftirlitsyfirvalds hvers aðildarríkis og Evrópsku persónuverndarstofnunarinnar eða fulltrúar þeirra hvers um sig.

4. Ef fleiri en eitt eftirlitsyfirvald í aðildarríki bera ábyrgð á að fylgjast með beitingu ákvæða samkvæmt þessari reglugerð skal skipa sameiginlegan fulltrúa í samræmi við löggjöf þess aðildarríkis.

5. Framkvæmdastjórnin hefur rétt til að taka þátt í starfsemi og fundum persónuverndarráðsins án atkvæðisréttar. Framkvæmdastjórnin skal tilnefna fulltrúa sinn. Formaður persónuverndarráðsins skal upplýsa framkvæmdastjórnina um störf sín.

6. Í þeim tilvikum, sem um getur í 65. gr., skal Evrópska persónuverndarstofnunin aðeins hafa atkvæðisrétt um ákvarðanir er varða meginreglur og reglur sem eiga við um stofnanir, aðila, skrifstofur og sérstofnanir Sambandsins sem svara efnislega til meginreglna og reglna þessarar reglugerðar.

69. gr.

Sjálfstæði

1. Persónuverndarráðið skal vera sjálfstætt í störfum sínum og þegar það beitir valdheimildum sínum skv. 70. og 71. gr.

2. Persónuverndarráðið skal í störfum sínum og þegar það beitir valdheimildum sínum hvorki leita eftir né taka við fyrirmælum frá öðrum aðilum, með fyrirvara um beiðnir framkvæmdastjórnarinnar sem um getur í 1. og 2. mgr. 70. gr.

70. gr.

Verkefni persónuverndarráðsins

1. Persónuverndarráðið skal tryggja samræmi í beitingu þessarar reglugerðar. Í því skyni skal persónuverndarráðið, annaðhvort að eigin frumkvæði eða, ef við á, að beiðni framkvæmdastjórnarinnar, einkum:

a) fylgjast með og tryggja rétta beitingu þessarar reglugerðar í tilvikum sem kveðið er á um í 64. og 65. gr., án þess að það hafi áhrif á verkefni landsbundinna eftirlitsyfirvalda,

b) veita framkvæmdastjórninni ráðgjöf um hvers kyns mál er tengjast vernd persónuupplýsinga í Sambandinu, m.a. varðandi tillögur að breytingum á þessari reglugerð,

c) veita framkvæmdastjórninni ráðgjöf um snið og aðferðir við upplýsingaskipti milli ábyrgðaraðila, vinnsluaðila og eftirlitsyfirvalda að því er varðar bindandi fyrirtækjareglur,

d) gefa út viðmiðunarreglur, tilmæli og bestu starfsvenjur í tengslum við verklag við að afmá tengla, afrit eða eftirmyndir af persónuupplýsingum hjá fjarskiptaþjónustu sem er aðgengileg almenningi, eins og um getur í 2. mgr. 17. gr.,

e) kanna, að eigin frumkvæði, að beiðni fulltrúa síns eða framkvæmdastjórnarinnar, hvers kyns álitaefni sem varða beitingu þessarar reglugerðar og gefa út viðmiðunarreglur, tilmæli og bestu starfsvenjur til þess að hvetja til samræmdrar beitingar hennar,

f) gefa út viðmiðunarreglur, tilmæli og bestu starfsvenjur í samræmi við e-lið þessarar málsgreinar til að tilgreina nánar viðmiðanir og skilyrði fyrir ákvörðunum sem byggðar eru á gerð persónusniðs skv. 2. mgr. 22. gr.,

g) gefa út viðmiðunarreglur, tilmæli og bestu starfsvenjur í samræmi við e-lið þessarar málsgreinar að því er varðar staðfestingu á öryggisbresti við meðferð persónuupplýsinga og ákvörðun ótilhlýðilegrar tafar sem um getur í 1. og 2. mgr. 33. gr. og þær tilteknu aðstæður þegar ábyrgðaraðili eða vinnsluaðili verður að tilkynna um slíkan öryggisbrest við meðferð persónuupplýsinga,

h) gefa út viðmiðunarreglur, tilmæli og bestu starfsvenjur í samræmi við e-lið þessarar málsgreinar að því er varðar aðstæður þegar líklegt er að öryggisbrestur við meðferð persónuupplýsinga leiði af sér mikla áhættu fyrir réttindi og frelsi þeirra einstaklinga sem um getur í 1. mgr. 34. gr.,

i) gefa út viðmiðunarreglur, tilmæli og bestu starfsvenjur í samræmi við e-lið þessarar málsgreinar að því er varðar nánari tilgreiningu á viðmiðunum og kröfum varðandi miðlun persónuupplýsinga á grundvelli bindandi fyrirtækjareglna sem ábyrgðaraðilar hlíta og bindandi fyrirtækjareglna sem vinnsluaðilar hlíta og frekari kröfum sem nauðsynlegar eru til að tryggja vernd persónuupplýsinga þeirra hlutaðeigandi skráðu einstaklinga sem um getur í 47. gr.,

j) gefa út viðmiðunarreglur, tilmæli og bestu starfsvenjur í samræmi við e-lið þessarar málsgreinar í þeim tilgangi að tilgreina nánar viðmiðanir og skilyrði varðandi miðlun persónuupplýsinga skv. 1. mgr. 49. gr.,

k) semja viðmiðunarreglur fyrir eftirlitsyfirvöld um beitingu þeirra ráðstafana sem um getur í 1., 2. og 3. mgr. 58. gr. og álagningu stjórnsýslusekta skv. 83. gr.,

l) endurskoða beitingu viðmiðunarreglna, tilmæla og bestu starfsvenja,

m) gefa út viðmiðunarreglur, tilmæli og bestu starfsvenjur í samræmi við e-lið þessarar málsgreinar til að koma á sameiginlegri málsmeðferð að því er varðar tilkynningar einstaklinga um brot gegn ákvæðum þessarar reglugerðar skv. 2. mgr. 54. gr.,

n) hvetja til þess að samdar verði hátternisreglur og að komið verði á vottunarfyrirkomulagi vegna persónuverndar og persónuverndarinnsigla og -merkja skv. 40. og 42. gr.,

o) samþykkja viðmiðanir vegna vottunar skv. 5. mgr. 42. gr. og halda opinbera skrá yfir vottunarfyrirkomulag og persónuverndar-innsigli og -merki skv. 8. mgr. 42. gr. og vottaða ábyrgðaraðila eða vinnsluaðila með staðfestu í þriðju löndum skv. 7. mgr. 42. gr.,

p) samþykkja kröfurnar, sem um getur í 3. mgr. 43. gr., að því er varðar faggildingu vottunaraðila sem um getur í 43. gr.,

q) láta framkvæmdastjórninni í té álitsgerð um vottunarkröfurnar sem um getur í 8. mgr. 43. gr.,

r) láta framkvæmdastjórninni í té álitsgerð um táknmyndirnar sem um getur í 7. mgr. 12. gr.,

s) láta framkvæmdastjórninni í té álitsgerð vegna mats á því hvort vernd sé fullnægjandi í þriðja landi eða hjá alþjóðastofnun, einnig vegna mats á því hvort þriðja land, yfirráðasvæði eða einn eða fleiri tilgreindir geirar innan umrædds þriðja lands eða alþjóðastofnun tryggi ekki lengur fullnægjandi vernd. Í því skyni skal framkvæmdastjórnin láta persónuverndarráðinu í té öll nauðsynleg gögn, þ.m.t. bréfaskipti við ríkisstjórn þriðja landsins að því er varðar umrætt þriðja land, yfirráðasvæði eða tilgreindan geira, eða við alþjóðastofnunina,

t) leggja fram álit varðandi drög að ákvörðunum eftirlitsyfirvalda samkvæmt samræmingarkerfinu sem um getur í 1. mgr. 64. gr., málefni, sem lögð eru fram skv. 2. mgr. 64. gr., og gefa út bindandi ákvarðanir skv. 65. gr., m.a. í þeim tilvikum sem um getur í 66. gr.,

u) stuðla að samvinnu og skilvirkum tvíhliða og marghliða skiptum á upplýsingum og bestu starfsvenjum milli eftirlitsyfirvaldanna,

v) stuðla að sameiginlegum þjálfunaráætlunum og greiða fyrir starfsmannaskiptum milli eftirlitsyfirvalda og, ef við á, gagnvart eftirlitsyfirvöldum þriðju landa eða alþjóðastofnunum,

w) stuðla að skiptum á þekkingu og gögnum um persónuverndarlöggjöf og starfsvenjur við eftirlitsyfirvöld á sviði persónuverndar um heim allan,

x) gefa út álit um hátternisreglur sem eru samdar á vettvangi Sambandsins skv. 9. mgr. 40. gr. og

y) halda rafræna skrá, sem er aðgengileg almenningi, yfir ákvarðanir sem eftirlitsyfirvöld og dómstólar taka um mál sem tekin eru til meðferðar í samræmingarkerfinu.

2. Þegar framkvæmdastjórnin óskar eftir ráðgjöf persónuverndarráðsins getur hún tilgreint frest með hliðsjón af því hversu brýnt málið er.

3. Persónuverndarráðið skal framsenda álit sitt, viðmiðunarreglur, tilmæli og bestu starfsvenjur til framkvæmdastjórnarinnar og til nefndarinnar sem um getur í 93. gr. og birta opinberlega.

4. Persónuverndarráðið skal, eftir því sem við á, hafa samráð við hagsmunaaðila og gefa þeim tækifæri til að leggja fram athugasemdir innan hæfilegs tíma. Persónuverndarráðið skal, með fyrirvara um 76. gr., gera niðurstöður samráðsferlisins aðgengilegar almenningi.

71. gr.

Skýrslur

1. Persónuverndarráðið skal semja ársskýrslu um vernd einstaklinga í tengslum við vinnslu í Sambandinu og, ef við á, þriðju löndum og hjá alþjóðastofnunum. Skýrslan skal birt opinberlega og send til Evrópuþingsins, ráðsins og framkvæmdastjórnarinnar.

2. Í skýrslunni skal m.a. koma fram endurskoðun á því hvernig viðmiðunarreglum, tilmælum og bestu starfsvenjum, sem um getur í l-lið 1. mgr. 70. gr., er beitt í reynd, sem og bindandi ákvörðunum sem um getur í 65. gr.

72. gr.

Málsmeðferð

1. Persónuverndarráðið skal taka ákvarðanir með einföldum meirihluta fulltrúa sinna nema kveðið sé á um annað í þessari reglugerð.

2. Persónuverndarráðið skal setja sér starfsreglur með tveimur þriðju hlutum atkvæða fulltrúa sinna og skipuleggja starfsfyrirkomulag sitt.

73. gr.

Formaður

1. Persónuverndarráðið skal kjósa formann og tvo varaformenn úr röðum fulltrúa sinna með einföldum meirihluta.

2. Skipunartími formanns og varaformanna er fimm ár og má endurnýja hann einu sinni.

74. gr.

Verkefni formanns

1. Formaðurinn skal sinna eftirfarandi verkefnum:

a) boða til funda í persónuverndarráðinu og undirbúa fundardagskrá,

b) tilkynna forystueftirlitsyfirvaldinu og hlutaðeigandi eftirlitsyfirvöldum um ákvarðanir sem persónuverndarráðið samþykkir skv. 65. gr.,

c) tryggja tímanlega framkvæmd verkefna persónuverndarráðsins, einkum að því er varðar samræmingarkerfið sem um getur í 63. gr.

2. Persónuverndarráðið skal mæla fyrir um skiptingu verkefna milli formanns og varaformanna í starfsreglum sínum.

75. gr.

Skrifstofa

1. Persónuverndarráðið skal hafa skrifstofu sem Evrópska persónuverndarstofnunin sér því fyrir.

2. Skrifstofan vinnur verkefni sín alfarið samkvæmt fyrirmælum formanns persónuverndarráðsins.

3. Starfsfólk Evrópsku persónuverndarstofnunarinnar, sem tekur þátt í framkvæmd verkefna sem persónuverndarráðinu eru falin með þessari reglugerð, skal fylgja öðrum boðleiðum en það starfsfólk sem tekur þátt í framkvæmd verkefna sem Evrópsku persónuverndarstofnuninni eru falin.

4. Persónuverndarráðið og Evrópska persónuverndarstofnunin skulu, eftir því sem við á, setja fram og birta viljayfirlýsingu til framkvæmdar þessari grein, þar sem skilmálar samstarfs þeirra eru ákvarðaðir og sem á við um starfsfólk Evrópsku persónuverndarstofnunarinnar sem tekur þátt í framkvæmd verkefna sem persónuverndarráðinu eru falin með þessari reglugerð.

5. Skrifstofan skal veita persónuverndarráðinu stuðning á sviði greiningar, stjórnunar og skipulags.

6. Skrifstofan ber einkum ábyrgð á:

a) daglegum rekstri persónuverndarráðsins,

b) samskiptum milli fulltrúa í persónuverndarráðinu, formanns þess og framkvæmdastjórnarinnar,

c) samskiptum við aðrar stofnanir og við almenning,

d) notkun rafrænna miðla fyrir innri og ytri samskipti,

e) þýðingum á viðeigandi upplýsingum,

f) undirbúningi fyrir fundi persónuverndarráðsins og eftirfylgni í kjölfar þeirra,

g) undirbúningi, gerð og birtingu álitsgerða, ákvarðana um lausn deilumála milli eftirlitsyfirvalda og annars texta sem persónuverndarráðið samþykkir.

76. gr.

Trúnaðarskyldur

1. Trúnaður skal ríkja um umfjöllun persónuverndarráðsins ef það telur slíkt nauðsynlegt, eins og kveðið er á um í starfsreglum þess.

2. Um aðgang að skjölum, sem send eru fulltrúum í persónuverndarráðinu, sérfræðingum og fulltrúum þriðju aðila, fer samkvæmt reglugerð Evrópuþingsins og ráðsins (EB) nr. 1049/2001 ([1]).

VIII. KAFLI

Úrræði, bótaábyrgð og viðurlög

77. gr.

Réttur til að leggja fram kvörtun hjá eftirlitsyfirvaldi

1. Sérhver skráður einstaklingur skal, án þess að það hafi áhrif á önnur stjórnsýslu- eða réttarúrræði, hafa rétt til að leggja fram kvörtun hjá eftirlitsyfirvaldi, einkum í því aðildarríki þar sem hann hefur fasta búsetu, vinnur eða þar sem meint brot átti sér stað ef hann telur að vinnsla persónuupplýsinga um sig brjóti í bága við þessa reglugerð.

2. Eftirlitsyfirvaldið, sem kvörtunin var lögð fram hjá, skal upplýsa kvartandann um framvindu og niðurstöður vegna kvörtunarinnar, m.a. möguleikann á réttarúrræði skv. 78. gr.

78. gr.

Réttur til skilvirks úrræðis til að leita réttar síns gagnvart eftirlitsyfirvaldi

1. Hver einstaklingur eða lögaðili skal, án þess að það hafi áhrif á önnur stjórnsýsluúrræði eða úrræði utan dómstóla, hafa rétt til raunhæfs úrræðis vegna lagalega bindandi ákvörðunar eftirlitsyfirvalds sem hann varðar.

2. Hver skráður einstaklingur skal, án þess að það hafi áhrif á önnur stjórnsýsluúrræði eða úrræði utan dómstóla, hafa rétt til raunhæfs úrræðis til að leita réttar síns ef eftirlitsyfirvaldið, sem er lögbært skv. 55. og 56. gr., tekur kvörtun ekki til meðferðar eða upplýsir hinn skráða ekki innan þriggja mánaða um framvindu eða niðurstöður vegna kvörtunarinnar sem lögð var fram skv. 77. gr.

3. Mál gegn eftirlitsyfirvaldi skal höfðað fyrir dómstólum í aðildarríkinu þar sem eftirlitsyfirvaldið hefur staðfestu.

4. Ef mál er höfðað gegn ákvörðun eftirlitsyfirvalds eftir að persónuverndarráðið hefur lagt fram álit sitt eða ákvörðun í samræmingarkerfinu skal eftirlitsyfirvaldið framsenda viðkomandi álit eða ákvörðun til dómstólsins.

79. gr.

Réttur til skilvirks úrræðis til að leita réttar síns gagnvart ábyrgðaraðila eða vinnsluaðila

1. Sérhver skráður einstaklingur skal, án þess að það hafi áhrif á önnur fyrirliggjandi stjórnsýsluúrræði eða úrræði utan dómstóla, m.a. réttinn til að leggja fram kvörtun hjá eftirlitsyfirvaldi skv. 77. gr., hafa rétt til skilvirks úrræðis til að leita réttar síns ef hann telur að brotið hafi verið gegn réttindum sínum samkvæmt þessari reglugerð á grundvelli þess að vinnsla persónuupplýsinga um hann samrýmist ekki þessari reglugerð.

2. Höfða skal mál gegn ábyrgðaraðila eða vinnsluaðila fyrir dómstólum í aðildarríkinu þar sem ábyrgðaraðilinn eða vinnsluaðilinn hefur staðfestu. Að öðrum kosti er heimilt að höfða slíkt mál fyrir dómstólum aðildarríkisins þar sem hinn skráði hefur fasta búsetu nema ábyrgðaraðilinn eða vinnsluaðilinn sé opinbert yfirvald aðildarríkis sem fer með opinbert vald.

([1]) Reglugerð Evrópuþingsins og ráðsins (EB) nr. 1049/2001 frá 30. maí 2001 um almennan aðgang að skjölum Evrópuþingsins, ráðsins og framkvæmdastjórnarinnar (Stjtíð. EB L 145, 31.5.2001, bls. 43).

80. gr.

Fyrirsvar skráðra einstaklinga

1. Skráður einstaklingur skal hafa rétt til að veita stofnun, samtökum eða félagi, sem ekki eru rekin í hagnaðarskyni og sem stofnuð eru í samræmi við lög aðildarríkis, hafa lögboðin markmið í þágu almannahagsmuna og eru virk á sviði verndar réttinda og frelsis skráðra einstaklinga að því er varðar vernd persónuupplýsinga um þá, umboð til að leggja fram kvörtun fyrir sína hönd, að neyta þeirra réttinda sem um getur í 77., 78. og 79. gr., fyrir sína hönd og að neyta réttarins til skaðabóta, sem um getur í 82. gr., fyrir sína hönd ef kveðið er á um það í lögum aðildarríkisins.

2. Aðildarríki er heimilt að mæla fyrir um að stofnun, samtök eða félag, sem um getur í 1. mgr. þessarar greinar, hafi rétt, óháð því hvort hinn skráði hefur veitt umboð til þess, til að leggja fram, í viðkomandi aðildarríki, kvörtun hjá því eftirlitsyfirvaldi sem er lögbært skv. 77. gr. og að neyta þeirra réttinda, sem um getur í 78. og 79. gr., hafi þau ástæðu til að ætla að réttindi skráðs einstaklings samkvæmt þessari reglugerð hafi verið brotin vegna vinnslunnar.

81. gr.

Frestun málsmeðferðar

1. Hafi lögbær dómstóll aðildarríkis fengið upplýsingar um dómsmál, sem varðar sama málefni vegna vinnslu af hálfu sama ábyrgðaraðila eða vinnsluaðila og er til meðferðar hjá dómstól í öðru aðildarríki, skal hann hafa samband við dómstólinn í því aðildarríki til að fá staðfest hvort um slíkt dómsmál er að ræða.

2. Ef mál um sama álitaefni vegna vinnslu sama ábyrgðaraðila eða vinnsluaðila er til meðferðar fyrir dómstóli í öðru aðildarríki getur hvaða þar til bær dómstóll sem er, annar en sá sem málið var fyrst höfðað fyrir, frestað málsmeðferð sinni.

3. Ef málið er til meðferðar á fyrsta dómstigi getur hvaða dómstóll sem er, annar en sá sem málið var fyrst höfðað fyrir, einnig vísað málinu frá samkvæmt kröfu eins málsaðilans ef sá dómstóll, sem mál er fyrst höfðað fyrir, hefur dómsvald um kröfurnar og lög, sem gilda við þann dómstól, heimila að skyldar kröfur séu sóttar sameiginlega.

82. gr.

Bótaréttur og bótaábyrgð

1. Hver sem hefur orðið fyrir eignatjóni eða óefnislegu tjóni vegna brots á ákvæðum þessarar reglugerðar skal eiga rétt á skaðabótum frá ábyrgðaraðila eða vinnsluaðila fyrir það tjón sem hann hefur orðið fyrir.

2. Ábyrgðaraðili, sem tekur þátt í vinnslu, skal bera ábyrgð á því tjóni sem hlýst af vinnslu sem brýtur í bága við þessa reglugerð. Vinnsluaðili skal því aðeins bera ábyrgð á tjóni, sem hlýst af vinnslu, hafi hann ekki uppfyllt skyldur samkvæmt þessari reglugerð, sem beinast sérstaklega að vinnsluaðilum, eða ef hann hefur ekki fylgt lögmætum fyrirmælum ábyrgðaraðilans eða farið gegn þeim.

3. Ábyrgðaraðili eða vinnsluaðili skal vera undanþeginn bótaábyrgð skv. 2. mgr. ef hann getur fært sönnur á að hann beri enga ábyrgð á atburðinum sem olli tjóninu.

4. Ef fleiri en einn ábyrgðaraðili eða vinnsluaðili, eða bæði ábyrgðaraðili og vinnsluaðili, koma að sömu vinnslu og ef þeir bera, skv. 2. og 3. mgr., ábyrgð á tjóni sem hlýst af vinnslu skal hver ábyrgðaraðili eða vinnsluaðili vera ábyrgur fyrir öllu tjóninu til að tryggja hinum skráða fullar skaðabætur.

5. Ef ábyrgðaraðili eða vinnsluaðili hefur greitt fullar skaðabætur vegna tjónsins, í samræmi við 4. mgr., skal hann eiga rétt á að krefjast þess að aðrir ábyrgðaraðilar eða vinnsluaðilar, sem komu að sömu vinnslu, endurgreiði þann hluta bótanna sem samsvarar hlutdeild þeirra í ábyrgð á tjóninu, í samræmi við skilyrðin sem sett eru fram í 2. mgr.

6. Dómsmál til að neyta réttarins til bóta skulu rekin fyrir dómstólum sem eru til þess bærir samkvæmt lögum aðildarríkisins sem um getur í 2. mgr. 72. gr.

83. gr.

Almenn skilyrði fyrir álagningu stjórnsýslusekta

1. Sérhvert eftirlitsyfirvald skal sjá til þess að álagning stjórnsýslusekta samkvæmt þessari grein vegna brota á reglugerð þessari, sem um getur í 4., 5. og 6. mgr., sé í hverju tilviki skilvirk, í réttu hlutfalli við brot og hafi varnaðaráhrif.

2. Leggja skal á stjórnsýslusektir, allt eftir aðstæðum í hverju tilviki, til viðbótar við eða í stað ráðstafana sem um getur í a- til h-lið og j-lið 2. mgr. 58. gr. Þegar ákveðið er hvort beita skuli stjórnsýslusekt og upphæð sektarinnar er ákveðin í hverju tilviki fyrir sig skal taka tilhlýðilegt tillit til eftirfarandi:

a) þess hvers eðlis, hversu alvarlegt og hversu langvarandi brotið er, með tilliti til eðlis, umfangs eða tilgangs vinnslunnar sem um er að ræða og fjölda skráðra einstaklinga sem urðu fyrir því og hversu alvarlegu tjóni þeir urðu fyrir,

b) þess hvort brotið var framið af ásetningi eða af gáleysi,

c) aðgerða sem ábyrgðaraðilinn eða vinnsluaðilinn hefur gripið til í því skyni að draga úr tjóni skráðra einstaklinga,

d) þess hversu mikla ábyrgð ábyrgðaraðili eða vinnsluaðili ber með tilliti til tæknilegra og skipulagslegra ráðstafana sem hann hefur komið til framkvæmda skv. 25. og 32. gr.,

e) fyrri brota ábyrgðaraðila eða vinnsluaðila sem máli skipta, ef einhver eru,

f) umfangs samvinnu við eftirlitsyfirvaldið til þess að bæta úr brotinu og draga úr mögulegum, skaðlegum áhrifum þess,

g) þess hvaða flokka persónuupplýsinga brotið hafði áhrif á,

h) þess með hvaða hætti eftirlitsyfirvaldinu var gert kunnugt um brotið, einkum hvort, og þá að hvaða leyti, ábyrgðaraðili eða vinnsluaðili tilkynnti um brotið,

i) fylgni við ráðstafanir, sem um getur í 2. mgr. 58. gr., ef áður hefur verið mælt fyrir um slíkar ráðstafanir gegn hlutaðeigandi ábyrgðaraðila eða vinnsluaðila að því er varðar sama efni,

j) fylgni við viðurkenndar hátternisreglur skv. 40. gr. eða viðurkennt vottunarfyrirkomulag skv. 42. gr. og

k) annarra íþyngjandi eða mildandi þátta sem varða kringumstæður málsins, s.s. hagnaðar sem fékkst eða taps sem komist var hjá, með beinum eða óbeinum hætti, vegna brotsins.

3. Ef ábyrgðaraðili eða vinnsluaðili brýtur, af ásetningi eða af gáleysi, gegn fleiri en einu ákvæði þessarar reglugerðar við sömu eða tengdar vinnsluaðgerðir skal heildarfjárhæð stjórnsýslusektarinnar ekki vera hærri en fjárhæðin sem er tilgreind fyrir alvarlegasta brotið.

4. Brot gegn eftirfarandi ákvæðum skulu, í samræmi við 2. mgr., varða stjórnsýslusektum sem nema allt að 10 000 000 evrum eða, ef um er að ræða fyrirtæki, allt að 2% af árlegri heildarveltu fyrirtækisins á heimsvísu á næstliðnu fjárhagsári, hvort heldur er hærra:

a) skyldum ábyrgðaraðila og vinnsluaðila skv. 8. gr., 11. gr., 25.–39. gr. og 42.–43. gr.,

b) skyldum vottunaraðila skv. 42. og 43. gr.,

c) skyldum eftirlitsaðila skv. 4. mgr. 41. gr.

5. Brot gegn eftirfarandi ákvæðum skulu, í samræmi við 2. mgr., varða stjórnsýslusektum sem nema allt að 20 000 000 evrum eða, ef um er að ræða fyrirtæki, allt að 4% af árlegri heildarveltu fyrirtækisins á heimsvísu á næstliðnu fjárhagsári, hvort heldur er hærra:

a) grundvallarreglum um vinnslu, þ.m.t. skilyrðum fyrir samþykki, skv. 5., 6., 7. og 9. gr.,

b) réttindum skráðra einstaklinga skv. 12.–22. gr.,

c) miðlun persónuupplýsinga til viðtakanda í þriðja landi eða alþjóðastofnunar skv. 44.–49. gr.,

d) skyldum samkvæmt lögum aðildarríkis sem samþykkt eru skv. IX. kafla,

e) ekki er farið að fyrirmælum eða tímabundinni eða varanlegri takmörkun á vinnslu eða tímabundinni stöðvun gagnaflæðis af hálfu eftirlitsyfirvaldsins skv. 2. mgr. 58. gr. eða ekki er farið að skyldu til að veita aðgang skv. 1. mgr. 58. gr.

6. Ef ekki er farið að fyrirmælum eftirlitsyfirvaldsins, eins og um getur í 2. mgr. 58. gr., skal það varða, í samræmi við 2. mgr. þessarar greinar, stjórnsýslusektum sem nema allt að 20 000 000 evrum eða, ef um er að ræða fyrirtæki, allt að 4% af árlegri heildarveltu fyrirtækisins á heimsvísu á næstliðnu fjárhagsári, hvort heldur er hærra.

7. Með fyrirvara um valdheimildir eftirlitsyfirvalda til að gera ráðstafanir til úrbóta skv. 2. mgr. 58. gr. er hverju aðildarríki heimilt að mæla fyrir um reglur um það hvort og að hve miklu leyti heimilt er að leggja stjórnsýslusektir á opinber yfirvöld og stofnanir með staðfestu í aðildarríkinu.

8. Beiting eftirlitsyfirvaldsins á valdheimildum sínum samkvæmt þessari grein skal lúta viðeigandi réttarfarsreglum í samræmi við lög Sambandsins og lög aðildarríkis, m.a. um skilvirka réttarvernd og sanngjarna málsmeðferð.

9. Ef ákvæði um stjórnsýslusektir er ekki að finna í réttarkerfi aðildarríkisins er heimilt að beita þessari grein þannig að lögbært eftirlitsyfirvald eigi frumkvæði að sektinni og þar til bærir landsdómstólar leggi hana á en jafnframt sé tryggt að þessi lagalegu úrræði séu skilvirk og hafi jafngild áhrif og stjórnsýslusektir sem eftirlitsyfirvöld leggja á. Álagðar sektir skulu þó ætíð vera skilvirkar, í réttu hlutfalli við brot og hafa varnaðaráhrif. Viðkomandi aðildarríki skulu tilkynna framkvæmdastjórninni eigi síðar en 25. maí 2018 um ákvæði laga sem þau samþykkja samkvæmt þessari málsgrein og skulu án tafar tilkynna um síðari breytingalög eða breytingar sem hafa áhrif á þau.

84. gr.

Viðurlög

1. Aðildarríkin skulu ákvarða reglur um önnur viðurlög við brotum gegn þessari reglugerð, einkum brotum sem varða ekki stjórnsýslusektum skv. 83. gr., og skulu gera allar nauðsynlegar ráðstafanir til að sjá til þess að þeim sé komið til framkvæmda. Slík viðurlög skulu vera skilvirk, í réttu hlutfalli við brot og hafa varnaðaráhrif.

2. Sérhvert aðildarríki skal tilkynna framkvæmdastjórninni eigi síðar en 25. maí 2018 um ákvæði landslaga sem þau hafa samþykkt skv. 1. mgr. og skulu án tafar tilkynna um síðari breytingar sem hafa áhrif á þau.

IX. KAFLI

Ákvæði sem varða sérstakar vinnsluaðstæður

85. gr.

Vinnsla og tjáningar- og upplýsingafrelsi

1. Aðildarríki skulu samkvæmt lögum samræma réttinn til verndar persónuupplýsingum samkvæmt þessari reglugerð og réttinn til tjáningar- og upplýsingafrelsis, þ.m.t. vinnslu vegna fréttamennsku og starfsemi fræðimanna eða listrænnar eða bókmenntalegrar tjáningar.

2. Að því er varðar vinnslu í þágu fréttamennsku eða starfsemi fræðimanna eða listrænnar eða bókmenntalegrar tjáningar skulu aðildarríkin kveða á um undanþágur eða frávik frá II. kafla (meginreglur), III. kafla (réttindi skráðs einstaklings), IV. kafla (ábyrgðaraðili og vinnsluaðili), V. kafla (miðlun persónuupplýsinga til þriðju landa eða alþjóðastofnana), VI. kafla (sjálfstæð eftirlitsyfirvöld), VII. kafla (samstarf og samræming) og IX. kafla (gagnavinnsla við tilteknar aðstæður) ef það er nauðsynlegt til þess að samræma réttinn til verndar persónuupplýsingum og réttinn til tjáningar- og upplýsingafrelsis.

3. Sérhvert aðildarríki skal tilkynna framkvæmdastjórninni um ákvæði landslaga sem þau hafa samþykkt skv. 2. mgr. og skulu þau án tafar tilkynna um síðari breytingalög eða breytingar sem hafa áhrif á þau.

86. gr.

Vinnsla og aðgangur almennings að opinberum skjölum

Opinberu yfirvaldi, opinberri stofnun eða einkaaðila er heimilt að afhenda persónuupplýsingar úr opinberum skjölum, sem yfirvaldið, stofnunin eða aðilinn hefur í sinni vörslu vegna framkvæmdar verkefnis í þágu almannahagsmuna, í samræmi við lög Sambandsins eða lög aðildarríkis sem opinbera yfirvaldið eða stofnunin heyrir undir, til þess að samræma aðgang almennings að opinberum skjölum og réttinn til verndar persónuupplýsingum samkvæmt þessari reglugerð.

87. gr.

Vinnsla landsbundins auðkennisnúmers

Aðildarríkjum er heimilt að ákvarða frekar hvaða sértæku skilyrði gilda um vinnslu landsbundinna auðkennisnúmera eða annarra almennra auðkenna. Í því tilviki skal því aðeins nota landsbundið auðkennisnúmer eða annað almennt auðkenni að gerðar séu viðeigandi verndarráðstafanir varðandi réttindi og frelsi hins skráða samkvæmt þessari reglugerð.

88. gr.

Vinnsla í atvinnutengdu samhengi

1. Aðildarríkjum er heimilt, með lögum eða kjarasamningum, að kveða á um sértækar reglur til að tryggja vernd réttinda og frelsis við vinnslu persónuupplýsinga starfsmanns í atvinnutengdu samhengi, einkum að því er varðar ráðningu, framkvæmd ráðningarsamnings, m.a. uppfyllingu skuldbindinga sem mælt er fyrir um í lögum eða kjarasamningum, stjórnun, undirbúning og skipulagningu vinnunnar, jafnrétti og fjölbreytileika á vinnustaðnum, heilbrigði og öryggi á vinnustað, vernd eigna vinnuveitanda eða viðskiptavinar og það að starfstengd réttindi og fríðindi séu nýtt og þeirra notið sameiginlega eða einstaklingsbundið, sem og í þeim tilgangi að ljúka ráðningarsambandi.

2. Þessar reglur skulu ná yfir viðeigandi og sértækar ráðstafanir til að vernda mannlega reisn hins skráða, lögmæta hagsmuni hans og grundvallarréttindi, með sérstöku tilliti til gagnsæis vinnslunnar, miðlunar persónuupplýsinga innan fyrirtækjasamstæðu eða hóps fyrirtækja sem stunda sameiginlega atvinnustarfsemi og vöktunarkerfa á vinnustað.

3. Sérhvert aðildarríki skal tilkynna framkvæmdastjórninni eigi síðar en 25. maí 2018 um ákvæði landslaga sem þau hafa samþykkt skv. 1. mgr. og skulu án tafar tilkynna um síðari breytingar sem hafa áhrif á þau.

89. gr.

Verndarráðstafanir og undanþágur sem varða vinnslu vegna skjalavistunar í þágu almannahagsmuna, rannsókna á sviði vísinda eða sagnfræði eða í tölfræðilegum tilgangi

1. Vinnsla vegna skjalavistunar í þágu almannahagsmuna, rannsókna á sviði vísinda eða sagnfræði eða í tölfræðilegum tilgangi skal vera háð viðeigandi ráðstöfunum til verndar réttindum og frelsi hins skráða í samræmi við þessa reglugerð. Þessar verndarráðstafanir skulu tryggja að tæknilegar og skipulagslegar ráðstafanir séu gerðar, einkum til þess að tryggja að farið sé að

meginreglunni um lágmörkun gagna. Notkun gerviauðkenna getur verið á meðal þessara ráðstafana, að því tilskildu að ná megi þessum markmiðum með þeim hætti. Ef hægt er að ná umræddum markmiðum með frekari vinnslu sem leyfir ekki, eða leyfir ekki lengur, persónugreiningu skráðra einstaklinga skal þessum markmiðum náð með þeim hætti.

2. Þegar vinnsla persónuupplýsinga fer fram í þágu rannsókna á sviði vísinda eða sagnfræði eða í tölfræðilegum tilgangi geta lög Sambandsins eða lög aðildarríkis kveðið á um undanþágur frá þeim réttindum sem um getur í 15., 16., 18. og 21. gr., með fyrirvara um skilyrði og verndarráðstafanir sem um getur í 1. mgr. þessarar greinar, að svo miklu leyti sem telja má að slík réttindi geri það ómögulegt eða hamli því verulega að unnt sé að ná viðkomandi markmiðum og slíkar undanþágur eru nauðsynlegar til að þeim verði náð.

3. Þegar vinnsla persónuupplýsinga fer fram vegna skjalavistunar í þágu almannahagsmuna geta lög Sambandsins eða lög aðildarríkis kveðið á um undanþágur frá þeim réttindum, sem um getur í 15., 16., 18., 19., 20. og 21. gr., með fyrirvara um skilyrði og verndarráðstafanir sem um getur í 1. mgr. þessarar greinar, að svo miklu leyti sem telja má að þessi réttindi geri það ómögulegt eða hamli því verulega að unnt sé að ná viðkomandi markmiðum og slíkar undanþágur eru nauðsynlegar til að þeim verði náð.

4. Þegar vinnsla, sem um getur í 2. og 3. mgr., þjónar á sama tíma öðrum tilgangi skulu undanþágurnar aðeins gilda um vinnslu í þeim tilgangi sem um getur í þeim málsgreinum.

90. gr.

Þagnarskylda

1. Aðildarríkin geta samþykkt sértækar reglur til að ákvarða valdheimildir eftirlitsyfirvaldanna, sem mælt er fyrir um í e- og f-lið 1. mgr. 58. gr., með tilliti til ábyrgðaraðila eða vinnsluaðila, sem falla undir þagnarskyldu samkvæmt lögum Sambandsins eða lögum aðildarríkis eða reglum sem þar til bærir innlendir aðilar setja, eða aðrar jafngildar skuldbindingar um leynd þegar slíkt reynist nauðsynlegt og hóflegt til að samræma réttinn til verndar persónuupplýsingum og þagnarskyldu. Þessar reglur skulu aðeins gilda með hliðsjón af persónuupplýsingum sem ábyrgðaraðili eða vinnsluaðili hefur fengið í hendur í kjölfar eða við starfsemi sem fellur undir þessa þagnarskyldu.

2. Sérhvert aðildarríki skal tilkynna framkvæmdastjórninni eigi síðar en 25. maí 2018 um reglur sem það hefur samþykkt skv. 1. mgr. og skal án tafar tilkynna um síðari breytingar sem hafa áhrif á þær.

91. gr.

Reglur kirkjudeilda og trúarsamtaka um vernd persónuupplýsinga

1. Ef kirkjudeildir og trúarsamtök eða trúfélög í aðildarríki beita víðtækum reglum, þegar þessi reglugerð öðlast gildi, er varða vernd einstaklinga í tengslum við vinnslu, geta slíkar reglur gilt áfram, að því tilskildu að þær séu færðar til samræmis við þessa reglugerð.

2. Kirkjudeildir og trúarsamtök, sem beita víðtækum reglum í samræmi við 1. mgr. þessarar greinar, skulu sæta eftirliti sjálfstæðs eftirlitsyfirvalds, sem getur verið sértækt, að því tilskildu að það fullnægi skilyrðunum sem mælt er fyrir um í VI. kafla þessarar reglugerðar.

X. KAFLI

Framseldar gerðir og framkvæmdargerðir

92. gr.

Beiting framsals

1. Framkvæmdastjórninni er falið vald til að samþykkja framseldar gerðir, sbr. þó skilyrðin sem mælt er fyrir um í þessari grein.

2. Það framsal valds, sem um getur í 8. mgr. 12. gr. og 8. mgr. 43. gr., skal falið framkvæmdastjórninni um óákveðinn tíma frá 24. maí 2016.

3. Evrópuþinginu eða ráðinu er hvenær sem er heimilt að afturkalla framsal valds sem um getur í 8. mgr. 12. gr. og 8. mgr. 43. gr. Með ákvörðun um afturköllun skal bundinn endi á framsal þess valds sem tilgreint er í þeirri ákvörðun. Hún öðlast gildi daginn eftir birtingu hennar í *Stjórnartíðindum Evrópusambandsins*, eða síðar, eftir því sem tilgreint er í ákvörðuninni. Hún skal ekki hafa áhrif á gildi framseldra gerða sem þegar eru í gildi.

4. Um leið og framkvæmdastjórnin samþykkir framselda gerð skal hún jafnframt tilkynna það Evrópuþinginu og ráðinu.

5. Framseld gerð, sem er samþykkt skv. 8. mgr. 12. gr. og 8. mgr. 43. gr., skal því aðeins öðlast gildi að Evrópuþingið eða ráðið hafi ekki haft uppi nein andmæli innan þriggja mánaða frá tilkynningu um gerðina til Evrópuþingsins og ráðsins eða ef bæði Evrópuþingið og ráðið hafa upplýst framkvæmdastjórnina, áður en fresturinn er liðinn, um þá fyrirætlan sína að hreyfa ekki andmælum. Þessi frestur skal framlengdur um þrjá mánuði að frumkvæði Evrópuþingsins eða ráðsins.

93. gr.

Nefndarmeðferð

1. Framkvæmdastjórnin skal njóta aðstoðar nefndar. Þessi nefnd skal vera nefnd í skilningi reglugerðar (ESB) nr. 182/2011.

2. Þegar vísað er til þessarar málsgreinar gilda ákvæði 5. gr. reglugerðar (ESB) nr. 182/2011.

3. Þegar vísað er til þessarar málsgreinar gildir 8. gr. reglugerðar (ESB) nr. 182/2011 í tengslum við 5. gr. hennar.

XI. KAFLI

Lokaákvæði

94. gr.

Niðurfelling á tilskipun 95/46/EB

1. Tilskipun 95/46/EB er felld úr gildi frá og með 25. maí 2018.

2. Líta ber á tilvísanir í niðurfelldu tilskipunina sem tilvísanir í þessa reglugerð. Líta ber á tilvísanir í starfshópinn um vernd einstaklinga í tengslum við vinnslu persónuupplýsinga, sem komið var á fót með 29. gr. tilskipunar 95/46/EB, sem tilvísanir í Evrópska persónuverndarráðið sem komið er á fót með þessari reglugerð.

95. gr.

Tengsl við tilskipun 2002/58/EB

Í þessari reglugerð skal ekki leggja viðbótarskyldur á herðar einstaklingum eða lögaðilum í tengslum við veitingu rafrænnar fjarskiptaþjónustu, sem er öllum aðgengileg, á almennum fjarskiptanetum í Sambandinu að því er varðar málefni þar sem þeir falla undir sértækar skyldur með sama markmið og sett er fram í tilskipun 2002/58/EB.

96. gr.

Tengsl við áður gerða samninga

Alþjóðasamningar, sem taka til miðlunar persónuupplýsinga til þriðju landa eða alþjóðastofnana, sem aðildarríkin gerðu fyrir 24. maí 2016 og samrýmast lögum Sambandsins, sem giltu fyrir þennan dag, skulu gilda áfram uns þeim er breytt, þeir eru leystir af hólmi eða afturkallaðir.

97. gr.

Skýrslur framkvæmdastjórnarinnar

1. Framkvæmdastjórnin skal, eigi síðar en 25. maí 2020 og á fjögurra ára fresti eftir það, leggja skýrslu fyrir Evrópuþingið og ráðið um mat og endurskoðun þessarar reglugerðar. Skýrslurnar skulu gerðar opinberar.

2. Framkvæmdastjórnin skal, í tengslum við matið og endurskoðunina sem um getur í 1. mgr., einkum kanna beitingu og framkvæmd:

a) V. kafla um miðlun persónuupplýsinga til þriðju landa eða alþjóðastofnana, með sérstöku tilliti til ákvarðana sem samþykktar eru skv. 3. mgr. 45. gr. þessarar reglugerðar og ákvarðana sem eru samþykktar á grundvelli 6. mgr. 25. gr. tilskipunar 95/46/EB,

b) VII. kafla um samstarf og samræmingu.

3. Að því er 1. mgr. varðar getur framkvæmdastjórnin óskað eftir upplýsingum frá aðildarríkjum og eftirlitsyfirvöldum.

4. Þegar framkvæmdastjórnin framkvæmir mat og endurskoðun, sem um getur í 1. og 2. mgr., skal hún taka tillit til afstöðu og niðurstaðna Evrópuþingsins, ráðsins og annarra viðeigandi aðila eða heimilda.

5. Framkvæmdastjórnin skal, ef nauðsyn krefur, leggja fram viðeigandi tillögur að breytingum á þessari reglugerð, einkum með tilliti til þróunar á sviði upplýsingatækni og í ljósi framfara í upplýsingasamfélaginu.

98. gr.

Endurskoðun annarra réttargerða Sambandsins á sviði persónuverndar

Framkvæmdastjórnin skal, ef við á, leggja fram tillögur að nýrri löggjöf með það fyrir augum að breyta öðrum réttargerðum Sambandsins um vernd persónuupplýsinga til að tryggja samræmda og samhæfða vernd einstaklinga með tilliti til vinnslu. Þetta á einkum við um reglur um vernd einstaklinga með tilliti til vinnslu stofnana, aðila, skrifstofa og sérstofnana Sambandsins og um frjálsa miðlun slíkra upplýsinga.

99. gr.

Gildistaka og beiting

1. Reglugerð þessi öðlast gildi á tuttugasta degi eftir að hún birtist í *Stjórnartíðindum Evrópusambandsins*.

2. Hún kemur til framkvæmda frá og með 25. maí 2018.

Reglugerð þessi er bindandi í heild sinni og gildir í öllum aðildarríkjunum án frekari lögfestingar.

Gjört í Brussel 27. apríl 2016.

Fyrir hönd Evrópuþingsins,	*Fyrir hönd ráðsins,*
M. SCHULZ	J.A. HENNIS-PLASSCHAERT
forseti.	*forseti.*