REGLUGERÐ FRAMKVÆMDASTJÓRNARINNAR (ESB) nr. 611/2013 **2016/EES/52/31**

frá 24. júní 2013

um ráðstafanir sem gilda um tilkynningar um brot er varða persónuupplýsingar samkvæmt tilskipun Evrópuþingsins og ráðsins 2002/58/EB um friðhelgi einkalífsins og rafræn fjarskipti (*)

FRAMKVÆMDASTJORN EVROPUSAMBANDSINS HEFUR,

með hliðsjón af sáttmálanum um starfshætti Evrópusambandsins,

með hliðsjón af 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 ([1]), einkum 5. mgr. 4. gr.,

að höfðu samráði við Net- og upplýsingaöryggisstofnun Evrópu (ENISA),

að höfðu samráði við starfshóp um vernd einstaklinga í tengslum við vinnslu persónuupplýsinga, sem stofnaður var með 29. gr. tilskipunar Evrópuþingsins og ráðsins nr. 95/46/EB frá 24. október 1995 um vernd einstaklinga í tengslum við vinnslu persónuupplýsinga og um frjálsa miðlun slíkra upplýsinga ([2]) (starfshópurinn skv. 29. gr.),

að höfðu samráði við Evrópsku persónuverndarstofnunina,

og að teknu tilliti til eftirfarandi:

1) Í tilskipun 2002/58/EB er kveðið á um samhæfingu landsbundinna ákvæða til að tryggja sambærilega vernd grundvallarréttinda og mannfrelsis, einkum að því er varðar réttinn til friðhelgi einkalífsins og trúnaðarkvaða vegna vinnslu persónuupplýsinga á rafræna fjarskiptasviðinu og til að tryggja frjálsan flutning slíkra gagna og um rafrænan fjarskiptabúnað og -þjónustu í Sambandinu.

2) Samkvæmt 4. gr. tilskipunar 2002/58/EB ber veitendum rafrænnar fjarskiptaþjónustu, sem er aðgengileg öllum, skylda til að tilkynna lögbærum landsyfirvöldum og í vissum tilvikum einnig hlutaðeigandi áskrifendum og einstaklingum um brot er varðar persónuupplýsingar. Brot er varða persónuupplýsingar eru skilgreind í i-lið 2. gr. tilskipunar 2002/58/EB: sem brot á öryggi sem leiða til óviljandi eða ólöglegrar eyðileggingar persónuupplýsinga, sem eru sendar, geymdar eða unnar á einhvern hátt í tengslum við veitingu rafrænnar fjarskiptaþjónustu sem er aðgengileg öllum innan Sambandsins, eða að þær glatist, breytist, verði birtar eða veittur aðgangur að þeim í leyfisleysi.

3) Til að tryggja samræmi í framkvæmd ráðstafananna, sem um getur í 2., 3. og 4. mgr. 4. gr. tilskipunar 2002/58/EB, veitir 5. mgr. 4. gr. sömu tilskipunar framkvæmdastjórninni vald til að samþykkja tæknilegar framkvæmdarráðstafanir varðandi málavexti, snið og málsmeðferðarreglur sem eiga við um upplýsinga- og tilkynningarskyldu sem um getur í þeirri grein.

4) Mismunandi landsbundnar kröfur kunna í þessu tilliti að leiða til réttaróvissu, flóknari og þunglamalegri málsmeðferðar og umtalsverðs umsýslukostnaðar veitenda sem starfa yfir landamæri. Framkvæmdastjórnin telur því nauðsynlegt að samþykkja slíkar tæknilegar framkvæmdarráðstafanir.

5) Reglugerð þessi takmarkast við tilkynningu brota er varða persónuupplýsingar og í henni eru þar af leiðandi ekki settar fram tæknilegar framkvæmdarráðstafanir varðandi 2. mgr. 4. gr. tilskipunar 2002/58/EB um að upplýsa áskrifendur um það ef sérstök hætta er á því að netöryggi bregðist.

6) Af fyrstu undirgrein 3. mgr. 4. gr. tilskipunar 2002/58/EB leiðir að veitendur ættu að tilkynna lögbærum landsyfirvöldum um öll brot er varða persónuupplýsingar. Þar af leiðir að veitandinn ætti ekki að fá að ákveða hvort slíkt er tilkynnt til lögbærs landsyfirvalds. Þetta ætti þó ekki að koma í veg fyrir að hlutaðeigandi lögbært landsyfirvald forgangsraði rannsókn tiltekinna brota á þann hátt sem það telur viðeigandi í samræmi við gildandi lög og geri ráðstafanir sem eru nauðsynlegar til að komast hjá of mikilli eða of lítill skýrslugjöf um brot er varða persónuupplýsingar.

7) Rétt er að taka upp kerfi fyrir tilkynningar um brot er varða persónuupplýsingar til lögbærs landsyfirvalds sem, að tilteknum skilyrðum uppfylltum, er samsett úr mismunandi stigum með tímamörkum fyrir hvert stig. Kerfinu er ætlað að tryggja að lögbærum landsyfirvöldum sé tilkynnt um brot eins fljótt og eins nákvæmlega og auðið er, þó án þess að hindra veitandann í viðleitni sinni til að rannsaka brotið og gera nauðsynlegar ráðstafanir til að takmarka það og bæta fyrir afleiðingar þess.

(*) Þessi ESB-gerð birtist í Stjtíð. ESB L 173, 26.6.2013, bls. 2. Hennar var getið í ákvörðun sameiginlegu EES-nefndarinnar nr. 154/2016 frá 8. júlí 2016 um breytingu á XI. viðauka (Fjarskiptaþjónusta) við EES-samninginn, biður birtingar.

([1]) Stjtíð. ESB L 201, 31.7.2002, bls. 37.

([2]) Stjtíð. EB L 281, 23.11.1995, bls. 31.

8) Hvorki einfaldur grunur um að brot er varðar persónuupplýsingar hafi átt sér stað né að uppvíst hafi orðið um atvik án þess að nægar upplýsingar liggi fyrir, þrátt fyrir að veitandinn hafi gert það sem hann mögulega gat til að afla slíkra upplýsinga, nægir til að telja að uppvíst hafi orðið um brot er varðar persónuupplýsingar hvað þessa reglugerð varðar. Í þessu samhengi ber að taka sérstakt tillit til þess að hve miklu leyti upplýsingarnar, sem um getur í I. viðauka, eru aðgengilegar.

9) Lögbær landsyfirvöld ættu að hafa samstarf um beitingu þessarar reglugerðar í tilvikum þegar brot er varða persónuupplýsingar ná yfir landamæri.

10) Í þessari reglugerð eru engar viðbótarforskriftir fyrir skrána yfir brot er varða persónuupplýsingar, sem veitendum ber að halda, þar eð tæmandi lýsing á innihaldinu er gefin í 4. gr. tilskipunar 2002/58/EB. Veitendur geta þó vísað til þessarar reglugerðar til þess að ákveða snið skrárinnar.

11) Öll lögbær landsyfirvöld ættu að sjá veitendum fyrir öruggri rafrænni aðferð til að þeir geti tilkynnt um brot er varða persónuupplýsingar á sameiginlegu sniði, sem er byggt á staðli á borð við XML, með þeim upplýsingum sem eru tilgreindar í I. viðauka á viðeigandi tungumálum, þannig að allir veitendur í Sambandinu geti fylgt svipaðri málsmeðferð við tilkynningu, burtséð frá því hvar þeir eru staddir eða hvar brotið er varðar persónuupplýsingar átti sér stað. Framkvæmdastjórnin ætti í þessu sambandi að auðvelda framkvæmd á öruggri rafrænni aðferð með því að boða til funda með lögbærum landsyfirvöldum þegar nauðsyn krefur.

12) Við mat á því hvort líkur eru á að brot er varðar persónuupplýsingar hafi skaðleg áhrif á persónuupplýsingarnar eða einkalíf áskrifanda eða einstaklings ætti einkum að taka tillit til eðlis og efnis viðkomandi persónuupplýsinga, sér í lagi ef gögnin varða fjárhagsupplýsingar, s.s. um kreditkort og bankareikning, sérstaka flokka upplýsinga sem um getur í 1. mgr. 8. gr. tilskipunar 95/46/EB og tilteknar upplýsingar sem sérstaklega varða veitingu talsíma- eða Netþjónustu, þ.e. tölvupóst, staðsetningargögn, gagnadagbækur, vefsíður sem hafa verið skoðaðar og sundurliðaðar skrár yfir upphringingar.

13) Við sérstakar aðstæður ætti veitandi að hafa leyfi til að fresta tilkynningu til áskrifanda eða einstaklings ef slík tilkynning getur stofnað viðeigandi rannsókn á broti er varðar persónuupplýsingar í hættu. Þannig geta sérstakar aðstæður tekið til rannsóknar á sakamáli ásamt öðrum brotum er varða persónuupplýsingar þar sem ekki er um alvarlegt afbrot að ræða en þar sem gæti verið hagkvæmt að fresta tilkynningu. Í öllum kringumstæðum skal það vera lögbærra landsyfirvalda í hverju tilviki fyrir sig og í ljósi aðstæðna að meta hvort samþykkja beri frestun eða fara fram á tilkynningu.

14) Veitendur ættu, í ljósi beinna samningsbundinna tengsla, að hafa samskiptaupplýsingar áskrifenda sinna en ekki er víst að slíkar upplýsingar liggi fyrir um aðra einstaklinga sem verða fyrir skaðlegum áhrifum af broti er varðar persónuupplýsingar. Í því tilviki ætti veitanda að vera heimilt að byrja á því að tilkynna þessum einstaklingum með auglýsingum í helstu landsbundnu eða svæðisbundnu fjölmiðlum, s.s. dagblöðum, og fylgja þeim eftir eins fljótt og unnt er með tilkynningu til hvers einstaklings eins og kveðið er á um í þessari reglugerð. Veitanda er því ekki skylt að setja tilkynningu í fjölmiðla en getur kosið að hafa þann háttinn á þegar því ferli að greina alla einstaklinga, sem hafa orðið fyrir áhrifum, er enn ólokið.

15) Upplýsingar um brotið ættu eingöngu að varða það brot og ekki innihalda upplýsingar um önnur mál. Það ætti t.d. ekki að teljast viðunandi aðferð við að tilkynna brot er varðar persónuupplýsingar að setja upplýsingar um það á venjulegan reikning.

16) Með þessari reglugerð eru ekki tilgreindar neinar sértækar, tæknilegar verndarráðstafanir, sem réttlæta að vikið sé frá skyldunni um að tilkynna brot er varða persónuupplýsingar til áskrifenda eða einstaklinga, þar eð þær geta breyst með tímanum samhliða tækniþróun. Framkvæmdastjórnin ætti þó að geta birt viðmiðunarskrá yfir slíkar sértækar, tæknilegar verndarráðstafanir samkvæmt gildandi venjum.

17) Notkun dulkóðunar eða tætingar (e. hashing) ætti í sjálfu sér ekki að nægja til að veitendur geti fullyrt í víðari skilningi að þeir hafi fullnægt almennri öryggisskyldu, sem sett er fram í 17. gr. tilskipunar 95/46/EB. Hvað þetta snertir ættu veitendur einnig að gera viðunandi skipulags- og tækniráðstafanir til að koma í veg fyrir, greina og stöðva brot er varða persónuupplýsingar. Eftir að hafa gert varnarráðstafanir ættu veitendur að íhuga þá hættu, sem enn kann að vera fyrir hendi, til þess að skilja hvar brot er varða persónuupplýsingar geta hugsanlega átt sér stað.

18) Ef veitandi fær annan veitanda til að taka að sér hluta þjónustunnar, t.d. í tengslum við reikningagerð eða stjórnunarstörf, ætti þessum öðrum veitanda, sem hefur engin bein samningsbundin tengsl við endanlegan notanda, ekki að vera skylt að gefa út tilkynningar þegar brot er varðar persónuupplýsingar á sér stað. Þess í stað ætti hann að gera veitandanum, sem hann er í beinum samningsbundin tengslum við, viðvart og

upplýsa hann. Þetta ætti einnig að gilda í tengslum við veitingu rafrænnar fjarskiptaþjónustu í heildsölu, þar sem heildsalinn hefur alla jafna ekki bein samningsbundin tengsl við endanlegan notanda.

19) Í tilskipun 95/46/EB er skilgreindur almennur rammi fyrir vernd persónuupplýsinga í Evrópusambandinu. Framkvæmdastjórnin hefur lagt fram tillögu að reglugerð Evrópuþingsins og ráðsins í stað tilskipunar 95/46/EB (reglugerðin um gagnavernd). Með fyrirhugaðri reglugerð um gagnavernd verður öllum ábyrgðaraðilum gagna skylt að tilkynna brot er varða persónuupplýsingar, með skírskotun til 3. mgr. 4. gr. tilskipunar 2002/58/EB. Þessi reglugerð framkvæmdastjórnarinnar er í fullu samræmi við þessa fyrirhuguðu ráðstöfun.

20) Í fyrirhugaðri reglugerð um gangavernd er einnig gerður takmarkaður fjöldi tæknilegra breytinga á tilskipun 2002/58/EB til að taka tillit til umbreytingar á tilskipun 95/46/EB í reglugerð. Framkvæmdastjórnin mun kanna efnisleg réttaráhrif nýrrar reglugerðar á tilskipun 2002/58/EB.

21) Endurskoða ætti beitingu þessarar reglugerðar þremur árum eftir gildistöku hennar og endurskoða efni hennar í ljósi þágildandi lagaramma, þ.m.t. fyrirhugaðrar reglugerðar um gagnavernd. Endurskoðun þessarar reglugerðar ætti ef unnt er að tengja við síðari endurskoðun tilskipunar 2002/58/EB.

22) Beitingu þessarar reglugerðar má meta m.a. á grundvelli tölfræðilegra upplýsinga frá landsbundnum lögbærum landsyfirvöldum um þau brot er varða persónuupplýsingar sem tilkynnt hafa verið til þeirra. Þessar tölfræðilegu upplýsingar geta m.a. tekið til upplýsinga um fjölda brota er varða persónuupplýsingar sem tilkynnt hafa verið til lögbærs landsyfirvalds, fjölda brota er varða persónuupplýsingar sem tilkynnt hafa verið til áskrifanda eða einstaklings, þess tíma sem það hefur tekið að bæta úr broti er varðar persónuupplýsingar og hvort tæknilegar verndarráðstafanir hafa verið gerðar. Með þessum tölfræðilegu upplýsingum ættu framkvæmdastjórnin og aðildarríkin að fá samræmd og samanburðarhæf tölfræðileg gögn sem hvorki afhjúpa þann veitanda sem er tilkynnandi né þá áskrifendur eða einstaklinga sem hlut eiga að máli. Framkvæmdastjórnin getur einnig í þessu skyni haldið reglubundna fundi með lögbærum landsyfirvöldum og öðrum hagsmunaaðilum.

23) Ráðstafanirnar, sem kveðið er á um í þessari reglugerð, eru í samræmi við álit fjarskiptanefndarinnar,

SAMÞYKKT REGLUGERÐ ÞESSA:

1. gr.

Gildissvið

Reglugerð þessi gildir um tilkynningar, sem koma frá veitendum rafrænnar fjarskiptaþjónustu sem er aðgengileg öllum („veitandi“), um brot er varða persónuupplýsingar.

2. gr.

Tilkynningar til lögbærs landsyfirvalds

1. Veitandi skal tilkynna öll brot er varða persónuupplýsingar til lögbærs landsyfirvalds.

2. Veitandi skal tilkynna brot er varðar persónuupplýsingar til lögbærs landsyfirvalds eigi síðar en 24 klukkustundum eftir að uppvíst verður um brot er varðar persónuupplýsingar, sé það gerlegt.

Veitandi skal í tilkynningu sinni til lögbærs landsyfirvalds tilgreina þær upplýsingar sem settar eru fram í I. viðauka.

Brot er varðar persónuupplýsingar telst hafa átt sér stað þegar veitandi hefur fengið næga vitneskju um váatvik, sem hefur stefnt öryggi persónuupplýsinganna í hættu, til að geta samið marktæka tilkynningu í samræmi við þessa reglugerð.

3. Ef ekki liggja fyrir allar upplýsingar, sem tilgreindar eru í I. viðauka, og þörf er á frekari rannsókn á broti er varðar persónuupplýsingar skal veitandi hafa leyfi til að skila upphaflegri tilkynningu til lögbærs landsyfirvalds eigi síðar en 24 klukkustundum eftir að uppvíst er um brot er varðar persónuupplýsingar. Þessi upphaflega tilkynning til lögbær landsyfirvalds skal innihalda þær upplýsingar sem settar eru fram í 1. þætti I. viðauka. Veitandi skal skila annarri tilkynningu til lögbær landsyfirvalds eins skjótt og unnt er og innan þriggja daga frá upphaflegu tilkynningunni. Þessi önnur tilkynning verður að innihalda þær upplýsingar sem eru tilgreindar í 2. þætti I. viðauka og, ef nauðsyn krefur, uppfærslu á þeim upplýsingum sem þegar hafa verið veittar.

Ef veitandi, þrátt fyrir rannsóknir sínar, getur ekki veitt allar upplýsingar innan þriggja daga frá upphaflegu tilkynningunni skal hann veita allar þær upplýsingar sem hann hefur tiltækar innan þess tímaramma og skal gefa lögbæra landsyfirvaldinu rökstudda ástæðu fyrir seinkun á tilkynningu á eftirstandandi upplýsingum. Veitandi skal eins skjótt og auðið er leggja eftirstandandi upplýsingar fyrir lögbært landsyfirvald og, ef nauðsyn krefur, uppfæra þær upplýsingar, sem þegar hafa verið veittar.

4. Lögbært landsyfirvald skal sjá öllum veitendum, sem hafa staðfestu í viðkomandi aðildarríki, fyrir öruggri rafrænni aðferð við að tilkynna brot er varða persónuupplýsingar ásamt upplýsingum um aðgang að henni og notkun. Ef nauðsyn krefur skal framkvæmdastjórnin boða til funda með lögbærum landsyfirvöldum til að auðvelda beitingu þessa ákvæðis.

5. Ef brot er varðar persónuupplýsingar hefur áhrif á áskrifendur eða einstaklinga frá öðrum aðildarríkjum en aðildarríki lögbæra landsyfirvaldsins, sem hefur verið tilkynnt um brotið er varðar persónuupplýsingar, skal lögbæra landsyfirvaldið upplýsa önnur hlutaðeigandi landsyfirvöld.

Til að auðvelda beitingu þessa ákvæðis skal framkvæmdastjórnin semja og viðhalda skrá yfir lögbær landsyfirvöld og viðeigandi tengiliði.

3. gr.

Tilkynningar til áskrifanda eða einstaklings

1. Þegar gera má ráð fyrir að brot er varðar persónuupplýsingar hafi skaðleg áhrif á persónuupplýsingar eða einkalíf áskrifanda eða einstaklings skal veitandi, auk þeirrar tilkynningar sem um getur í 2. gr., einnig tilkynna brotið til áskrifandans eða einstaklingsins.

2. Við mat á því hvort líkur eru á að brot er varðar persónuupplýsingar hafi skaðleg áhrif á persónuupplýsingar eða einkalíf áskrifanda eða einstaklings skal einkum taka tillit til eftirfarandi aðstæðna:

a) eðlis og efnis viðkomandi persónuupplýsinga, sér í lagi ef gögnin varða fjárhagsupplýsingar, sérstaka flokka upplýsinga sem um getur í 1. mgr. 8. gr. tilskipunar 95/46/EB ásamt staðsetningargögnum, Netgagnadagbókum, vefsíðum sem hafa verið skoðaðar, tölvupóstgögnum og sundurliðuðum skrám yfir upphringingar,

b) líklegra afleiðinga af brotum er varða persónuupplýsingar fyrir viðkomandi áskrifanda eða einstakling, einkum ef brotið getur leitt til auðkennisþjófnaðar eða svika, líkamstjóns, sálarangistar, niðurlægingar eða mannorðstjóns og

c) aðstæðna við brot er varðar persónuupplýsingar, einkum þegar upplýsingunum hefur verið stolið eða veitanda er kunnugt að þriðji aðili hefur upplýsingarnar undir höndum í leyfisleysi.

3. Tilkynning til áskrifanda eða einstaklings skal vera án ótilhlýðilegrar tafar eftir að uppvíst hefur orðið um brot er varðar persónuupplýsingar, eins og tilgreint er í þriðju undirgrein 2. mgr. 2. gr. Þetta skal ekki vera háð tilkynningunni um brot er varðar persónuupplýsingar til lögbærs landsyfirvalds sem um getur í 2. gr.

4. Veitandi skal í tilkynningu sinni til áskrifanda eða einstaklings tilgreina þær upplýsingar sem eru í II. viðauka. Tilkynning til áskrifanda eða einstaklings skal vera á skýru og auðskiljanlegu máli. Veitandi skal ekki nota tilkynninguna sem tækifæri til að kynna eða auglýsa nýja þjónustu eða viðbótarþjónustu.

5. Við sérstakar aðstæður, ef tilkynning til áskrifanda eða einstaklings getur stofnað viðeigandi rannsókn á broti er varðar persónuupplýsingar í hættu, skal veitandi, að fengnu samþykki lögbærs landsyfirvalds, hafa leyfi til að fresta tilkynningu til áskrifanda eða einstaklings þar til lögbært landsyfirvald telur mögulegt að tilkynna brotið er varðar persónuupplýsingar í samræmi við þessa grein.

6. Veitandi skal tilkynna brot er varðar persónuupplýsingar til áskrifanda eða einstaklings með samskiptaaðferð sem tryggir skjóta viðtöku upplýsinganna og þar sem öryggis er gætt samkvæmt nýjustu tækni. Upplýsingar um brot skulu eingöngu varða það brot og ekki innihalda upplýsingar um önnur mál.

7. Ef veitandi, sem hefur bein samningsbundin tengsl við endanlegan notanda, getur ekki þrátt fyrir að hafa lagt sig fram, innan tímarammans sem um getur í 3. mgr., borið kennsl á alla einstaklinga, sem líkur eru á að verði fyrir skaðlegum áhrifum af broti er varðar persónuupplýsingar, getur hann tilkynnt þessum einstaklingum það með auglýsingum í helstu landsbundnu eða svæðisbundnu fjölmiðlum í viðkomandi aðildarríkjum innan þess tímaramma. Þessar auglýsingar skulu innihalda upplýsingarnar, sem eru tilgreindar í II. viðauka, í styttri útgáfu ef nauðsyn krefur. Í því tilviki skal veitandi áfram af fremsta megni leitast við að bera kennsl á þá einstaklinga og veita þeim upplýsingarnar, sem eru tilgreindar í II. viðauka, eins skjótt og auðið er.

4. gr.

Tæknilegar verndarráðstafanir

1. Þrátt fyrir 1. mgr. 3. gr. er þess ekki krafist að brot er varðar persónuupplýsingar gegn áskrifanda eða einstaklingi tilkynnist viðkomandi ef veitandinn hefur sýnt lögbæru landsyfirvaldi með fullnægjandi hætti að gerðar hafi verið viðeigandi tæknilegar verndarráðstafanir, og að þær ráðstafanir hafi verið gerðar varðandi þau gögn sem öryggisbrotið snerti. Slíkar tæknilegar verndarráðstafanir skulu gera gögnin óskiljanleg hverjum þeim sem ekki er heimilaður aðgangur að þeim.

2. Upplýsingar teljast óskiljanlegar ef:

a) þær hafa verið dulkóðaðar á öruggan hátt með stöðluðu reikniriti, lyklinum til að dulráða upplýsingarnar hefur ekki verið stefnt í hættu í öryggisbroti og lykillinn til að dulráða upplýsingarnar er þannig gerður að ekki er hægt að lesa hann með tiltækri tækniþekkingu af einstaklingi sem ekki hefur heimild til að fá aðgang að lyklinum eða

b) í hans stað hefur komið tætt gildi hans, reiknað út með stöðluðu dulritunartætifalli, lyklinum sem er notaður til að tæta upplýsingarnar hefur ekki verið stefnt í hættu í öryggisbroti og lykillinn sem notaður er til að tæta upplýsingarnar er þannig gerður að ekki er hægt að lesa hann með tiltækri tækniþekkingu af einstaklingi sem ekki hefur aðgang að lyklinum.

3. Framkvæmdastjórnin getur, að höfðu samráði við lögbær landsyfirvöld fyrir milligöngu starfshópsins skv. 29. gr., Net- og upplýsingaöryggisstofnun Evrópu og Evrópsku persónuverndarstofnunina, birt viðmiðunarskrá um viðeigandi tæknilegar verndarráðstafanir, sem um getur í 1. mgr., samkvæmt gildandi venju.

5. gr.

Að nota annan veitanda

Ef samið er við annan veitanda um að afhenda hluta rafrænnar fjarskiptaþjónustu, án þess að um bein samningsbundin tengsl við áskrifendur sé að ræða, skal sá veitandi þegar í stað tilkynna samningsbundna veitandanum um brot er varða persónuupplýsingar.

6. gr.

Skýrslugjöf og endurskoðun

Innan þriggja ára frá gildistöku þessarar reglugerðar skal framkvæmdastjórnin leggja fram skýrslu um beitingu þessarar reglugerðar, árangurinn af henni og áhrif á veitendur, áskrifendur og einstaklinga. Á grundvelli þeirrar skýrslu skal framkvæmdastjórnin endurskoða þessa reglugerð.

7. gr.

Gildistaka

Reglugerð þessi öðlast gildi 25. ágúst 2013.

Reglugerð þessi er bindandi í heild sinni og gildir í öllum aðildarríkjunum án frekari lögfestingar.

Gjört í Brussel 24. júní 2013.

Fyrir hönd framkvæmdastjórnarinnar,

forseti.

José Manuel BARROSO

I. VIÐAUKI

Efni tilkynningar til lögbærs landsyfirvalds

1. þáttur

Auðkenning veitanda

1. Heiti veitanda

2. Auðkenni og samskiptaupplýsingar gagnaverndarfulltrúa eða annars tengiliðar þar sem hægt er að fá frekari upplýsingar

3. Hvort um er að ræða fyrstu eða aðra tilkynningu

Frumupplýsingar um brot er varðar persónuupplýsingar (fyllist út í síðari tilkynningum eftir atvikum)

4. Dagsetning og tímasetning atviksins (ef þekkt; ef nauðsyn krefur má leggja á það mat) og þegar uppvíst varð um atvikið

5. Aðstæður við brot er varðar persónuupplýsingar (t.d. þær glatast, þjófnaður, afritun)

6. Eðli og efni viðkomandi persónuupplýsinga

7. Tækni- og skipulagsráðstafanir sem gerðar eru (eða verða gerðar) af veitanda þeirra persónuupplýsinga sem um ræðir

8. Viðeigandi notkun annarra veitenda (eftir atvikum)

2. þáttur

Nánari upplýsingar um brotið er varðar persónuupplýsingar

9. Samantekt um atvikið sem olli broti er varðar persónuupplýsingar (þ.m.t. staðinn þar sem brotið á sér stað og geymslumiðil sem um ræðir)

10. Fjöldi áskrifenda eða einstaklinga sem um ræðir

11. Mögulegar afleiðingar og möguleg skaðleg áhrif á áskrifendur eða einstaklinga

12. Tækni- og skipulagsráðstafanir sem veitandi gerir til að milda möguleg, skaðleg áhrif

Mögulegar viðbótartilkynningar til áskrifenda eða einstaklinga

13. Efni tilkynningar

14. Samskiptaaðferðir sem notaðar eru

15. Fjöldi áskrifenda eða einstaklinga sem um ræðir

Möguleg mál sem ná yfir landamæri

16. Brot er varða persónuupplýsingar sem varða áskrifendur eða einstaklinga í öðrum aðildarríkum

17. Tilkynningar til annarra lögbærra landsyfirvalda

———

II. VIÐAUKI

Efni tilkynningar til áskrifanda eða einstaklings

1. Heiti veitanda
2. Auðkenni og samskiptaupplýsingar gagnaverndarfulltrúa eða annars tengiliðar þar sem hægt er að fá frekari upplýsingar
3. Samantekt um atvikið sem olli broti er varðar persónuupplýsingar
4. Áætluð dagsetning atviks
5. Eðli og efni viðkomandi persónuupplýsinga eins og um getur í 2. mgr. 3. gr.
6. Líklegar afleiðingar af broti er varðar persónuupplýsingar fyrir áskrifanda eða einstakling sem um ræðir, eins og um getur í 2. mgr. 3. gr.
7. Aðstæður við brot er varðar persónuupplýsingar eins og um getur í 2. mgr. 3. gr.
8. Ráðstafanir sem veitandi gerir til að bæta úr broti er varðar persónuupplýsingar
9. Ráðstafanir, sem veitandi ráðleggur, til að milda möguleg, skaðleg áhrif

_____