MÄÄRUSED

KOMISJONI MÄÄRUS (EL) nr 611/2013,

24. juuni 2013,

meetmete kohta, mida kohaldatakse eraelu puutumatust ja elektroonilist sidet käsitleva Euroopa Parlamendi ja nõukogu direktiivi 2002/58/EÜ kohaselt isikuandmetega seotud rikkumiste teatamise suhtes

EUROOPA KOMISJON,

võttes arvesse Euroopa Liidu toimimise lepingut,

võttes arvesse Euroopa Parlamendi ja nõukogu 12. juuli 2002. aasta direktiivi 2002/58/EÜ, milles käsitletakse isikuandmete töötlemist ja eraelu puutumatuse kaitset elektroonilise side sektoris (eraelu puutumatust ja elektroonilist sidet käsitlev direktiiv), [1] eriti selle artikli 4 lõiget 5,

olles konsulteerinud Euroopa Võrgu- ja Infoturbeametiga (ENISA),

olles konsulteerinud Euroopa Parlamendi ja nõukogu 24. oktoobri 1995. aasta direktiivi 95/46/EÜ (üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta) [2] artikli 29 alusel asutatud üksikisikute kaitsmist isikuandmete töötlemisel käsitleva töörühmaga (artikli 29 töörühm),

olles konsulteerinud Euroopa Andmekaitseinspektoriga

ning arvestades järgmist:

(1) Direktiiviga 2002/58/EÜ nähakse ette nende siseriiklike sätete ühtlustamine, mis on vajalikud põhiõiguste ja -vabaduste, eelkõige eraelu puutumatuse ja konfidentsiaalsuse kaitse samaväärse taseme tagamiseks isikuandmete töötlemise puhul elektroonilise side sektoris ja selliste andmete ning elektrooniliste sideseadmete ja -teenuste vaba liikumise tagamiseks ELis.

(2) Direktiivi 2002/58/EÜ artikli 4 kohaselt on üldkasutatavate elektrooniliste sideteenuste osutajad kohustatud isikuandmetega seotud rikkumisest teavitama pädevaid riigiasutusi ning teatavatel juhtudel ka asjaomaseid abonente ja üksikisikuid. Isikuandmetega seotud rikkumine on direktiivi 2002/58/EÜ artikli 2 punktis i määratletud kui turvanõude rikkumine, mis toob seoses ELis üldkasutatava elektroonilise sideteenuse osutamisega kaasa edastatud, salvestatud või muul viisil töödeldud isikuandmete juhusliku või ebaseadusliku hävitamise, kaotsimineku, muutmise, ebaseadusliku avalikustamise või neile juurdepääsu.

(3) Direktiivi 2002/58/EÜ artikli 4 lõigetes 2, 3 ja 4 osutatud meetmete ühetaolise rakendamise tagamiseks on kõnealuse direktiivi artikli 4 lõikega 5 antud komisjonile õigus võtta vastu tehnilised rakendusmeetmed, milles käsitletakse kõnealuses artiklis osutatud teabe- ja teavitamisnõuetega seotud asjaolusid, vormi ja korda.

(4) Erinevad riigisisesed nõuded selles valdkonnas võivad põhjustada piiriüleselt tegutsevatele teenuseosutajatele õiguslikku ebakindlust, keerukamaid ja koormavamaid menetlusi ning olulisi halduskulusid. Seepärast peab komisjon vajalikuks võtta vastu sellised tehnilised rakendusmeetmed.

(5) Käesolev määrus piirdub isikuandmetega seotud rikkumistest teatamisega ning seepärast ei sätestata selles tehnilisi rakendusmeetmeid seoses direktiivi 2002/58/EÜ artikli 4 lõikega 2, milles käsitletakse abonentide teavitamist võrgu turvalisuse rikkumise konkreetsest ohust..

(6) Direktiivi 2002/58/EÜ artikli 4 lõike 3 esimesest lõigust tuleneb, et teenuseosutajad peaksid teavitama pädevat riigiasutust kõigist isikuandmetega seotud rikkumistest. Seepärast ei tuleks teenuseosutajale jätta kaalutlusõigust otsustamisel, kas pädevat riigiasutust teavitada või mitte. Siiski ei peaks see takistama asjaomast pädevat riigiasutust prioriseerimast teatavate rikkumiste uurimist viisil, mida ta peab sobivaks vastavalt kohaldatavale õigusele, ning võtmast vajaduse korral meetmeid, et vältida ülemäärast või liiga vähest isikuandmetega seotud rikkumistest teatamist.

(7) On asjakohane näha pädevale riigiasutusele isikuandmetega seotud rikkumistest teatamise jaoks ette süsteem, mis koosneb juhul, kui teatavad tingimused on täidetud, eri etappidest ja iga etapi suhtes on kehtestatud teatav ajaline piirang. Selle süsteemi eesmärk oleks tagada, et pädevat riigiasutust teavitatakse võimalikult vara ja võimalikult põhjalikult, ilma et see siiski põhjendamatult takistaks teenuseosutajal rikkumist uurida ja võtta vajalikud meetmed selle piiramiseks ja tagajärgede kõrvaldamiseks

[1] EÜT L 201, 31.7.2002, lk 37.
[2] EÜT L 281, 23.11.1995, lk 31.

(8) Lihtsat kahtlust selle kohta, et isikuandmetega seotud rikkumine on toimunud, ega ka intsidendi tuvastamist ilma piisava teabe olemasoluta ei tohiks teenuseosutaja pingutustest hoolimata lugeda piisavaks, et käsitada isikuandmetega seotud rikkumist tuvastatuks käesoleva määruse kohaldamisel. Erilist tähelepanu tuleks seoses sellega pöörata I lisas osutatud teabe olemasolule.

(9) Käesoleva määruse kohaldamise raames peaksid asjaomased riigiasutused tegema koostööd isikuandmetega seotud selliste rikkumiste korral, millel on piiriülene mõõde.

(10) Käesoleva määrusega ei nähta ette täiendavaid üksikasju seoses isikuandmetega seotud rikkumiste registriga, mida teenuseosutajad peavad pidama, kuna direktiivi 2002/58/EÜ artiklis 4 sätestatakse selle registri sisu ammendavalt. Teenuseosutajad võivad siiski osutada käesolevale määrusele, et määrata kindlaks registri vorm.

(11) Kõik pädevad riigiasutused peaksid tegema teenuseosutajatele kättesaadavaks turvalised elektroonilised vahendid isikuandmetega seotud rikkumistest teatamiseks sellises ühtses vormis, mis põhineb standardil, nagu XML, sisaldades 1. lisas sätestatud teavet asjaomastes keeltes, nii et see võimaldab kõigil teenuseosutajatel ELis järgida sarnast teatise saatmise menetlust, sõltumata sellest, kus nad asuvad või kus toimus isikuandmetega seotud rikkumine. Sellega seoses peaks komisjon hõlbustama turvaliste elektrooniliste vahendite rakendamist, korraldades vajaduse korral koosolekuid pädevate riigiasutustega.

(12) Selle hindamisel, kas isikuandmetega seotud rikkumine tõenäoliselt kahjustab abonendi või üksikisiku isikuandmeid või eraelu puutumatust, tuleks eelkõige arvesse võtta asjaomaste isikuandmete laadi ja sisu, seda eriti juhul, kui andmed on seotud finantsteabega, näiteks krediitkaardi andmed ja pangakonto andmed; direktiivi 95/46/EÜ artikli 8 lõikes 1 osutatud andmete eriliigid; ja teatavad andmed, mis on konkreetselt seotud telefoni- või internetiteenuste osutamisega, näiteks e-posti andmed, asukohaandmed, interneti logifailid, veebilehitsemise ajalugu ja üksikasjalikud kõnede väljavõtted.

(13) Erandlike asjaolude korral peaks teenuseosutajal olema lubatud saata abonendile või üksikisikule teatis hiljem, juhul kui teatise saatmine abonendile või üksikisikule võib seada ohtu isikuandmetega seotud rikkumise nõuetekohase uurimise. Seoses sellega võivad erandlikud asjaolud hõlmata kriminaaluurimisi ning ka muid isikuandmetega seotud rikkumisi, mis ei ole raske kuriteoga samaväärsed, kuid mille korral võib olla asjakohane teatise saatmine edasi lükata. Igal juhul peaks pädev riigiasutus hindama iga juhtumi korral eraldi ning asjaolusid arvesse võttes, kas nõustuda edasilükkamisega või nõuda teatise saatmist.

(14) Kuigi teenuseosutajatel peaks olema oma abonentide kontaktandmed, arvestades nende otsest lepingusuhet, ei tohi selline teave olemas olla teiste üksikisikute kohta, kellele isikuandmetega seotud rikkumisel on kahjulik mõju. Sellisel juhul peaks teenuseosutajal olema lubatud teavitada neid üksikisikuid esmalt teadaannete kaudu peamistes riiklikes või piirkondlikes meediakanalites (nt ajalehed), millele järgneb niipea kui võimalik käesoleva määrusega ette nähtud individuaalse teatise saatmine. Seepärast ei ole teenuseosutaja kohustatud teavitama meediakanalite kaudu, kuid pigem on tal lubatud soovi korral sel viisil tegutseda juhul, kui ta on ikka veel tegemas kindlaks kõiki kahjustatud üksikisikuid.

(15) Rikkumist käsitlevas teabes peaks keskenduma rikkumisele ning see ei tohiks olla seotud muid teemasid käsitleva teabega. Näiteks isikuandmetega seotud rikkumist käsitleva teabe esitamist korrapärases arves ei tohiks käsitada asjakohase vahendina isikuandmetega seotud rikkumisest teavitamisel.

(16) Käesolevas määruses ei sätestata konkreetseid tehnoloogilisi kaitsemeetmeid, mis õigustavad erandit kohustusest teavitada isikuandmetega seotud rikkumisest abonente või üksikisikuid, sest aja jooksul tehnoloogia arenedes need muutuvad. Komisjonil peaks siiski olema võimalik avaldada praeguse tava alusel selliste konkreetsete tehnoloogiliste kaitsemeetmete soovituslik loend.

(17) Krüpteerimist või räsi kasutamist ei tohiks üksinda pidada piisavaks, et teenuseosutajad saaksid väita üldisemalt, et nad on täitnud direktiivi 95/46/EÜ artiklis 17 sätestatud üldise turvalisuse kohustuse. Selleks peaksid teenuseosutajad rakendama ka asjakohaseid korralduslikke ja tehnilisi meetmeid, et vältida, tuvastada ja blokeerida isikuandmetega seotud rikkumisi. Teenuseosutajad peaksid arvesse võtma mis tahes jääkriski, mis võib alles jääda pärast kontrollide rakendamist, et mõista, kus võivad isikuandmetega seotud rikkumised aset leida.

(18) Kui teenuseosutaja kasutab teise teenuseosutaja teenuseid, et osutada osa teenusest, näiteks seoses arvete esitamise või juhtimisfunktsioonidega, ei peaks kõnealune teine

teenuseosutaja, kellel ei ole otsest lepingulist suhet lõppkasutajaga, olema kohustatud isikuandmetega seotud rikkumise korral teatisi esitama. Selle asemel peaks ta hoiatama ja teavitama teenuseosutajat, kellega tal on otsene lepingusuhe. See peaks kehtima ka elektroonilise sideteenuse hulgimüügi raames, kui tavaliselt hulgimüüjal ei ole lõppkasutajaga otsest lepingulist suhet.

(19) Direktiiviga 95/46/EÜ määratakse kindlaks Euroopa Liidus isikuandmete kaitse üldine raamistik. Komisjon on esitanud Euroopa Parlamendi ja nõukogu määruse ettepaneku, et asendada direktiiv 95/46/EÜ (andmekaitsemäärus). Kavandatud andmekaitsemäärusega kehtestataks kõigile vastutavatele töötlejatele kohustus teavitada isikuandmetega seotud rikkumistest, tuginedes direktiivi 2002/58/EÜ artikli 4 lõikele 3. Käesolev komisjoni määrus on kavandatud meetmega täielikult kooskõlas.

(20) Kavandatud andmekaitsemäärusega tehakse ka piiratud arv tehnilisi kohandusi direktiivi 2002/58/EÜ, et võtta arvesse direktiivi 95/46/EÜ muutmist määruseks. Uue määrusega kaasnevad sisulised õiguslikud tagajärjed, mis on seotud direktiiviga 2002/58/EÜ, vaatab komisjoni läbi.

(21) Käesoleva määruse kohaldamine tuleks läbi vaadata kolm aastat pärast selle jõustumist ning selle sisu läbivaatamisel tuleks arvesse võtta sel ajal kehtivat õigusraamistikku, sealhulgas kavandatud andmekaitsemäärust. Käesoleva määruse läbivaatamine tuleks võimaluse korral siduda direktiivi 2002/58/EÜ mis tahes tulevase läbivaatamisega.

(22) Käesoleva määruse kohaldamise hindamisel võib muu hulgas aluseks võtta mis tahes statistika, mida pädevad riigiasutused omavad isikuandmetega seotud selliste rikkumiste kohta, millest neid teavitatakse. See statistika võib hõlmata näiteks teavet pädevale riigiasutusele teatatud isikuandmetega seotud rikkumiste arvu kohta, abonendile või üksikisikule teatatud isikuandmetega seotud rikkumiste arvu kohta, isikuandmetega seotud rikkumise lahendamiseks kulunud aja kohta ning kas võetud oli tehnoloogilisi kaitsemeetmeid. See statistika peaks andma komisjonile ja liikmesriikidele järjepidevad ja võrreldavad statistilised andmed ega tohiks paljastada teatava teenuseosutaja ega asjaomaste abonentide või üksikisikute andmeid. Komisjon võib sel eesmärgil korraldada ka korrapäraseid koosolekuid pädevate riigiasutuste ja muude huvitatud sidusrühmadega.

(23) Käesoleva määrusega ettenähtud meetmed on kooskõlas sidekomitee arvamusega,

ON VASTU VÕTNUD KÄESOLEVA MÄÄRUSE:

Artikkel 1

Reguleerimisala

Käesolevat määrust kohaldatakse üldkasutatava elektroonilise sideteenuse osutaja (edaspidi „teenuseosutaja") poolt isikuandmetega seotud rikkumistest teatamise suhtes.

Artikkel 2

Pädevale riigiasutusele saadetav teatis

1. Teenuseosutaja teavitab pädevat riigiasutust kõigist isikuandmetega seotud rikkumistest.

2. Teenuseosutaja teavitab pädevat riigiasutust isikuandmetega seotud rikkumisest võimaluse korral hiljemalt 24 tundi pärast isikuandmetega seotud rikkumise tuvastamist.

Teenuseosutaja esitab pädevale riigiasutusele saadetavas teatises I lisas sätestatud teabe.

Isikuandmetega seotud rikkumine tuleb lugeda tuvastatuks, kui teenuseosutaja on seoses aset leidnud turvaintsidendiga, mis on seadnud ohtu isikuandmed, saanud piisavalt teavet, et koostada käesoleva määrusega nõutud sisukas teatis.

3. Kui kogu I lisas sätestatud teave ei ole kättesaadav ning nõutav on isikuandmetega seotud rikkumise täiendav uurimine, on teenuseosutajal lubatud esitada pädevale riigiasutusele esialgne teatis hiljemalt 24 tunni jooksul alates isikuandmetega seotud rikkumise tuvastamisest. Pädevale riigiasutusele saadetud esialgne teatis sisaldab I lisa 1. jaos sätestatud teavet. Teenuseosutaja saadab pädevale riigiasutusele teise teatise nii ruttu kui võimalik ning hiljemalt kolme päeva jooksul pärast esialgset teatist. Teine teatis sisaldab I lisa 2. jaos sätestatud teavet ning vajaduse korral juba esitatud teabe ajakohastamist.

Kui teenuseosutaja ei suuda, olenemata oma uurimisest, esitada kogu teavet kolmepäevase ajavahemiku jooksul alates esialgse teatise esitamisest, esitab teenuseosutaja selle ajavahemiku jooksul nii palju teavet, kui ta omab, ning esitab pädevale riigiasutusele põhjenduse, miks ülejäänud teave saadetakse pärast seda ajavahemikku. Teenuseosutaja saadab pädevale riigiasutusele ülejäänud teabe ning vajaduse korral ajakohastab juba esitatud teavet nii ruttu kui võimalik.

4. Pädev riigiasutus teeb kõigile asjaomases liikmesriigis asuvatele teenuseosutajatele kättesaadavaks turvalised elektroonilised vahendid isikuandmetega seotud rikkumistest teatamiseks ning teabe sellele juurdepääsu saamise ja selle kasutamise korra kohta. Vajaduse korral korraldab komisjon käesoleva sätte kohaldamise hõlbustamiseks pädevate riigiasutustega koosolekuid.

5. Kui isikuandmetega seotud rikkumine kahjustab abonente või üksikisikuid, kes asuvad muudes liikmesriikides kui see, kus asub pädev riigiasutus, kellele on teatatud isikuandmetega seotud rikkumisest, teavitab pädev riigiasutus teisi asjaomaseid riigiasutusi.

Käesoleva sätte kohaldamise hõlbustamiseks koostab komisjon pädevate riigiasutuste ja asjakohaste kontaktisikute nimekirja ning haldab seda.

Artikkel 3

Abonendile või üksikisikule saadetav teatis

1. Kui isikuandmetega seotud rikkumine võib tõenäoliselt kahjustada abonendi või üksikisiku isikuandmeid ja eraelu puutumatust, saadab teenuseosutaja lisaks artiklis 2 osutatud teatisele sellise rikkumise teatise ka abonendile või üksikisikule.

2. Selle hindamisel, kas isikuandmetega seotud rikkumine võib tõenäoliselt kahjustada abonendi või üksikisiku isikuandmeid või eraelu puutumatust, võetakse arvesse eelkõige järgmisi asjaolusid:

a) asjaomaste isikuandmete olemus ja sisu, eelkõige juhul, kui andmed sisaldavad finantsteavet, nende puhul on tegemist direktiivi 95/46/EÜ artikli 8 lõikes 1 osutatud andmete eriliigiga või need on asukohaandmed, interneti logifailid, veebilehitsemise ajalugu, e-posti andmed või üksikasjalikud kõnede väljavõtted;

b) isikuandmetega seotud rikkumise tõenäolised tagajärjed asjaomase abonendi või üksikisiku jaoks, eelkõige juhul, kui rikkumise tagajärjeks võib olla identiteedivargus või pettus, tervisekahjustus, psühholoogilised kannatused, alandamine või maine kahjustamine; ning

c) isikuandmetega seotud rikkumise asjaolud eelkõige juhul, kui andmed on varastatud või kui teenuseosutaja teab, et andmed on volitamata kolmanda isiku omanduses.

3. Teatis saadetakse abonendile või üksikisikule põhjendamatu viivituseta pärast isikuandmetega seotud rikkumise tuvastamist, nagu on sätestatud artikli 2 lõike 2 kolmandas lõigus. See ei tohi sõltuda pädevale riigiasutusele artiklis 2 osutatud isikuandmetega seotud rikkumisest teatamisest.

4. Teenuseosutaja esitab abonendile või üksikisikule saadetavas teatises II lisas sätestatud teabe. Abonendile või üksikisikule saadetav teatis koostatakse selges ja kergesti mõistetavas keeles. Teenuseosutaja ei kasuta teatist uute või täiendavate teenuste edendamise või reklaamimise võimalusena.

5. Erandlike asjaolude korral, kui teatise saatmine abonendile või üksikisikule võib ohtu seada isikuandmetega seotud rikkumise nõuetekohase uurimise, on teenuseosutajal lubatud pärast pädevalt riigiasutuselt loa saamist viivitada abonendile või üksikisikule teatise saatmisega ajani, mida pädev riigiasutus peab võimalikuks, et teavitada isikuandmetega seotud rikkumisest vastavalt käesolevale artiklile.

6. Teenuseosutaja teavitab abonenti või üksikisikut isikuandmetega seotud rikkumisest sidevahendi abil, millega tagatakse teabe kiire kättesaamine ja mis on nõuetekohaselt turvatud vastavalt tehnika tasemele. Rikkumist käsitlevas teabes keskendutakse rikkumisele ning see ei ole seotud muud teemat käsitleva teabega.

7. Kui teenusosutaja, kellel on otsene lepinguline suhe lõppkasutajaga, ei suuda, olenemata tehtud mõistlikest püüdlustest, teha lõikes 3 osutatud ajavahemiku jooksul kindlaks kõiki üksikisikuid, keda isikuandmetega seotud rikkumine tõenäoliselt kahjustab, võib teenuseosutaja teavitada selle ajavahemiku jooksul kõnealuseid üksikisikuid teadaannete kaudu asjaomase liikmesriigi peamistes riiklikes või piirkondlikes meediakanalites. Need teadaanded peavad sisaldama II lisas sätestatud teavet, vajaduse korral kokkuvõtlikul kujul. Sel juhul jätkab teenuseosutaja kõigi mõistlike meetmete võtmist, et määrata need üksikisikud kindlaks ja edastada neile II lisas sätestatud teave võimalikult kiiresti.

Artikkel 4

Tehnoloogilised kaitsemeetmed

1. Erandina artikli 3 lõikest 1 ei ole vaja isikuandmetega seotud rikkumisest asjaomasele abonendile või üksikisikule teatada, kui teenuseosutaja on tõendanud pädevale riigiasutusele rahuldaval viisil, et ta on rakendanud kohaseid tehnoloogilisi kaitsemeetmeid ning neid meetmeid rakendati turvanõuete rikkumisega seotud andmete suhtes. Sellised tehnoloogilised kaitsemeetmed muudavad andmed loetamatuks kõigile isikutele, kellel puuduvad volitused andmetele juurdepääsuks.

2. Andmeid käsitatakse loetamatuna juhul, kui:

a) need on standarditud algoritmi abil turvaliselt krüptitud; andmete dekrüptimiseks kasutatav võti ei ole turvanõuete mis tahes rikkumise tõttu ohtu sattunud ning andmete dekrüptimiseks kasutatav võti on loodud nii, et seda ei saa kasutuses olevate tehnoloogiate abil kindlaks teha ükski isik, kellel ei ole luba võtmele juurdepääsuks; või

b) need on asendatud andmete räsiväärtusega, mis on arvutatud krüptograafilise võtmega standardse räsifunktsiooni abil; andmete räsimiseks kasutatav võti ei ole turvanõuete mis tahes rikkumise tõttu ohtu sattunud ning andmete räsimiseks kasutatav võti on loodud nii, et seda ei saa kasutuses olevate tehnoloogiate abil kindlaks teha ükski isik, kellel ei ole luba võtmele juurdepääsuks.

3. Olles konsulteerinud artikli 29 töörühma kaudu pädevate riigiasutustega, Euroopa Võrgu- ja Infoturbeameti ning Euroopa andmekaitseinspektoriga, võib komisjon avaldada praeguse tava alusel lõikes 1 osutatud asjakohaste tehnoloogiliste kaitsemeetmete soovitusliku loendi.

Artikkel 5

Teise teenuseosutaja teenuste kasutamine

Kui teine teenuseosutaja osutab allhankena osa elektroonilisest sideteenusest ilma, et ta oleks abonentidega otseses lepingulises suhtes, teavitab kõnealune teine teenuseosutaja isikuandmetega seotud rikkumise korral kohe allhankivat teenuseosutajat.

Artikkel 6

Aruandlus ja läbivaatamine

Komisjon esitab kolme aasta jooksul alates käesoleva määruse jõustumisest aruande määruse kohaldamise, selle tulemuslikkuse ning teenuseosutjatele, abonentidele ja üksikisikutele avalduva mõju kohta. Komisjon vaatab määruse läbi kõnealuse aruande alusel.

Artikkel 7

Jõustumine

Käesolev määrus jõustub 25. augustil 2013.

Käesolev määrus on tervikuna siduv ja vahetult kohaldatav kõikides liikmesriikides.

Brüssel, 24. juuni 2013

Komisjoni nimel
president
José Manuel BARROSO

I LISA

Pädevale riigiasutusele saadetava teatise sisu

1. jagu

Teenuseosutaja andmed

1. Teenuseosutaja nimi

2. Andmekaitseametniku nimi ja kontaktandmed või mõni muu kontaktpunkt, kust võib saada täiendavat teavet

3. Kas see on seotud esimese või teise teatisega

Esialgne teave isikuandmetega seotud rikkumise kohta (vajaduse korral täitetakse hilisemates teatistes)

4. Juhtumi kuupäev ja kellaaeg (kui teada; vajaduse korral võib esitada hinnangu) ning juhtumi tuvastamise kuupäev ja kellaaeg

5. Isikuandmetega seotud rikkumise asjaolud (nt kaotsiminek, vargus, koopia tegemine)

6. Asjaomaste isikuandmete laad ja sisu

7. Tehnilised ja korralduslikud meetmed, mida teenuseosutaja kohaldas (või kohaldab) kahjustatud isikuandmete suhtes

8. Teiste teenuseosutajate asjaomaste teenuste kasutamine (kui kohaldatav)

2. jagu

Täiendav teave isikuandmetega seotud rikkumise kohta

9. Isikuandmetega seotud rikkumise põhjustanud intsidendi kokkuvõte (sealhulgas rikkumise füüsiline asukoht ja asjaomane andmekandja)

10. Asjaomaste abonentide või üksikisikute arv

11. Võimalikud tagajärjed ja võimalik kahjulik mõju abonentidele või üksikisikutele

12. Tehnilised ja korralduslikud meetmed, mida teenuseosutaja on võtnud võimaliku kahjuliku mõju leevendamiseks

Abonentidele või üksikisikutele saadetav võimalik täiendav teatis

13. Teatise sisu

14. Kasutatud sidevahendid

15. Teatise saanud abonentide või üksikisikute arv

Võimalikud piiriülesed küsimused

16. Isikuandmetega seotud rikkumine, mis hõlmab muudes liikmesriikides asuvaid abonente või üksikisikuid

17. Muude pädevate riigiasutuste teavitamine

II LISA

Abonendile või üksikisikule saadetava teatise sisu

1. Teenuseosutaja nimi

2. Andmekaitseametniku nimi ja kontaktandmed või mõni muu kontaktpunkt, kust võib saada täiendavat teavet

3. Isikuandmetega seotud rikkumise põhjustanud juhtumi kokkuvõte

4. Juhtumi hinnanguline kuupäev

5. Asjaomaste isikuandmete laad ja sisu, nagu on osutatud artikli 3 lõikes 2

6. Isikuandmetega seotud rikkumise tõenäolised tagajärjed asjaomase abonendi või üksikisiku jaoks, nagu on osutatud artikli 3 lõikes 2

7. Isikuandmetega seotud rikkumise asjaolud, nagu on osutatud artikli 3 lõikes 2

8. Teenuseosutaja poolt isikuandmetega seotud rikkumise lahendamiseks võetud meetmed

9. Teenuseosutaja soovitatud meetmed võimaliku kahjustava mõju leevendamiseks