

REGULAS

KOMISIJAS REGULA (ES) Nr. 611/2013

(2013. gada 24. jūnijs)

par pasākumiem, kas piemērojami paziņošanai par personas datu aizsardzības pārkāpumiem saskaņā ar Eiropas Parlamenta un Padomes Direktīvu 2002/58/EK par privātumu un elektronisko komunikāciju

EIROPAS KOMISIJA,

ņemot vērā Līgumu par Eiropas Savienības darbību,

ņemot vērā Eiropas Parlamenta un Padomes 2002. gada 12. jūlija Direktīvu 2002/58/EK par personas datu apstrādi un privātās dzīves aizsardzību elektronisko komunikāciju nozarē (direktīva par privāto dzīvi un elektronisko komunikāciju) ⁽¹⁾ un jo īpaši tās 4. panta 5. punktu,

apspriedusies ar Eiropas Tiklu un informācijas drošības aģentūru (ENISA),

apspriedusies ar Darba grupu fizisku personu aizsardzībai attiecībā uz personas datu apstrādi, kas izveidota saskaņā ar 29. pantu Eiropas Parlamenta un Padomes 1995. gada 24. oktobra Direktīvā 95/46/EK par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un par šādu datu brīvu apriti ⁽²⁾ (29. pantā minētā darba grupa),

apspriedusies ar Eiropas Datu aizsardzības uzraudzītāju (EDAU),

tā kā:

- (1) Direktīva 2002/58/EK paredz dalībvalstu to noteikumu saskaņošanu, ar kuriem jānodrošina pamattiesību un pamatbrīvību līdzvērtīgs aizsardzības līmenis, un jo īpaši tiesības uz privāto dzīvi un konfidencialitāti saistībā ar personas datu apstrādi elektronisko komunikāciju nozarē, kā arī jānodrošina šo datu un elektronisko komunikāciju iekārtu un pakalpojumu brīva aprīte Savienībā.
- (2) Saskaņā ar Direktīvas 2002/58/EK 4. pantu publiski pieejamu elektronisko komunikāciju pakalpojumu sniedzējiem par personas datu aizsardzības pārkāpumu ir jāpaziņo kompetentajam valsts iestādēm un noteiktos gadījumos arī abonentiem un individuālajiem lietotājiem. Personas datu aizsardzības pārkāpums ir definēts Direktīvas 2002/58/EK 2. panta i) punktā kā drošības pārkāpums, kura rezultātā notiek nejauša vai nelikumīga nosūtīto, uzglabāto vai citādi apstrādāto personas datu iznīcināšana vai nejauša zaudēšana, pārveidošana, neat-

ļauta vai nelikumīga izpaušana vai piekļuve, un jebkurš cits nelikumīgs apstrādes veids, kas saistīts ar noteikumu par publiski pieejamiem komunikāciju pakalpojumiem Savienībā.

- (3) Lai nodrošinātu Direktīvas 2002/58/EK 4. panta 2., 3. un 4. punktā minēto pasākumu īstenošanas konsekveni, ar minētās direktīvas 4. panta 5. punktu Komisija ir pilnvarota pieņemt tehniskus īstenošanas pasākumus attiecībā uz attiecīgajā pantā minēto informēšanas un paziņošanas prasību piemērošanas apstākļiem, veidu un kārtību.
- (4) Šajā ziņā dažādas valstu prasības var novest pie tiesiskas nenoteiktības, sarežģītākām un apgrūtinātām procedūrām un ievērojamām administratīvām izmaksām tiem pakalpojumu sniedzējiem, kas darbojas pārrobežu režīmā. Tāpēc Komisija uzskata, ka ir nepieciešams pieņemt šādus tehniskus īstenošanas pasākumus.
- (5) Šī regula attiecas tikai uz paziņošanu par personas datu aizsardzības pārkāpumiem, tātad tajā nav izklāstīti tehniski īstenošanas pasākumi saistībā ar Direktīvas 2002/58/EK 4. panta 2. punktu par abonentu informēšanu tīkla drošības pārkāpuma īpaša riska gadījumā.
- (6) No Direktīvas 2002/58/EK 4. panta 3. punkta pirmās daļas izriet, ka pakalpojumu sniedzējiem būtu jāpaziņo kompetentajai valsts iestādei par visiem personas datu aizsardzības pārkāpumiem. Tas, vai paziņot kompetentajai valsts iestādei par personas datu aizsardzības pārkāpumu, nebūtu atstājams pakalpojumu sniedzēja ziņā. Tomēr minētais noteikums neliedz attiecīgajai kompetentajai valsts iestādei pēc saviem ieskatiem un saskaņā ar spēkā esošajiem tiesību aktiem noteikt, kuru konkrētu pārkāpumu izmeklēšana būtu uzskatāma par prioritāti, un veikt nepieciešamos pasākumus, lai ziņošana par personas datu aizsardzības pārkāpumiem nebūtu nepietiekama vai pārmērīga.
- (7) Būtu lietderīgi izstrādāt sistēmu, saskaņā ar kuru personas datu aizsardzības pārkāpumus paziņo kompetentajai valsts iestādei un kurai pie zināmiem nosacījumiem ir atšķirīgi līmeņi, uz katru no kuriem attiecas noteikti termiņi. Šādas sistēmas uzdevums būtu nodrošināt, ka kompetentā iestāde tiek informēta pēc iespējas agrāk un pilnīgāk, tomēr nevajadzīgi nekavējot pakalpojumu sniedzēja centienus izmeklēt pārkāpumu un veikt vajadzīgos pasākumus, lai to apturētu un likvidētu pārkāpuma sekas.

⁽¹⁾ OV L 201, 31.7.2002., 37. lpp.

⁽²⁾ OV L 281, 23.11.1995., 31. lpp.

- (8) Vienkāršas aizdomas, ka ir noticis personas datu aizsardzības pārkāpums, vai vienkāršs konstatējums, ka ir noticis drošības incidents, bet par to nav pieejams pietiekami daudz informācijas par spīti pakalpojumu sniedzēja centieniem šajā sakarībā, nav pietiekams iemesls, lai uzskatītu, ka ir noticis personas datu aizsardzības pārkāpums šīs regulas izpratnē. Īpaša vērība saistībā ar minēto būtu jāpievērš tam, vai ir pieejama I pielikumā minētā informācija.
- (9) Piemērojot šo regulu, attiecīgajām kompetentajām valsts iestādēm būtu jāsadarbjas personas datu aizsardzības pārkāpumu lietās, kam ir pārrobežu raksturs.
- (10) Šī regula neparedz papildu specifikācijas attiecībā uz personas datu aizsardzības pārkāpumu reģistru, kas jāuztur pakalpojumu sniedzējam, jo tā saturs izsmeltoši precizēts Direktīvas 2002/58/EK 4. pantā. Tomēr pakalpojumu sniedzēji var atsaukties uz šo regulu, lai noteiktu reģistra formātu.
- (11) Visām kompetentajām valsts iestādēm būtu pakalpojumu lietotājiem jādara pieejami droši elektroniski līdzekļi, kā par personas datu aizsardzības pārkāpumiem sniegt paziņojumu vienotā formātā, kura pamatā ir noteikts standarts, piemēram, XML, un kurš satur I pielikumā norādīto informāciju attiecīgajās valodās, lai visi pakalpojumu sniedzēji Savienībā varētu ievērot līdzīgu informēšanas kārtību neatkarīgi no atrašanās vietas vai personas datu aizsardzības pārkāpuma norises vietas. Komisijai šajā sakarībā būtu jāveicina drošu elektronisko līdzekļu ieviešana, vajadzības gadījumā sasaucot sanāksmes ar kompetento valsts iestāžu piedalīšanos.
- (12) Izvērtējot, vai personas datu aizsardzības pārkāpums varētu negatīvi ietekmēt abonenta vai individuāla lietotāja personas datus vai privātumu, jo īpaši jāņem vērā attiecīgo personas datu būtība un saturs, proti, vai tie ir ar finanšu informāciju saistīti dati, piemēram, kredītkaršu vai bankas konta dati, Direktīvas 95/46/EK 8. panta 1. punktā minētās īpašās datu kategorijas un noteikti dati, kas specifiski saistīti ar telefonijas vai interneta pakalpojumu sniegšanu, t. i., e-pasta dati, atrašanās vietas dati, interneta žurnālfaili, tīmekļa pārlūkošanas vēsture un detalizēta zvanu informācija.
- (13) Ārkārtas apstākļos vajadzētu būt pieļaujamam, ka pakalpojumu sniedzējs abonentu vai individuālo lietotāju var informēt ar aizkavēšanos, ja abonenta vai individuālā lietotāja informēšana var apdraudēt personas datu aizsardzības pārkāpuma pienācīgu izmeklēšanu. Šajā kontekstā ārkārtas apstākļi var būt kriminālizmeklēšana, kā arī citi personas datu aizsardzības pārkāpumi, kas gan nav uzskatāmi par nopietnu noziegumu, bet kuru dēļ varētu būt lietderīgi paziņošanu atlikt. Jebkurā gadījumā kompetentajai valsts iestādei katrā gadījumā atsevišķi un ievērojot apstākļus būtu jāizvērtē, vai piekrist atlikšanai vai noteikt, ka par pārkāpumu ir jāpaziņo.
- (14) Ņemot vērā tiesās līgumattiecības, pakalpojumu sniedzēju rīcībā vajadzētu būt abonentu kontaktinformācijai, taču šāda informācija var arī nebūt pieejama par citiem individuāliem lietotājiem, kurus negatīvi ietekmējis personas datu aizsardzības pārkāpums. Tādā gadījumā vajadzētu atļaut pakalpojumu sniedzējam šos individuālos lietotājus informēt, sākumā publicējot sludinājumus lielākajos valsts un reģionālajos plašsaziņas līdzekļos, piemēram, laikrakstos, un pēc tam pēc iespējas drīzāk tiem paziņot individuāli, kā paredzēts šajā regulā. Tādējādi informēt individuālos lietotājus ar plašsaziņas līdzekļu starpniecību nav pakalpojumu sniedzēja obligāts pienākums, bet, kamēr norit pārkāpuma skarto individuālo lietotāju identificēšana, būtu ieteicams rīkoties šādā veidā, ja pakalpojumu sniedzējs tā vēlas.
- (15) Informācijai par pārkāpumu vajadzētu attiekties tikai uz pārkāpumu, nevis uz kādu citu tematu. Piemēram, ja informāciju par personas datu aizsardzības pārkāpumu iekļauj kārtējā rēķinā, tas nebūtu uzskatāms par pienācīgu paņēmieni, kā paziņot par personas datu aizsardzības pārkāpumu.
- (16) Šajā regulā nav noteikti specifiski tehniski aizsardzības pasākumi, ar kuriem varētu pamatot atkāpes no pienākuma paziņot abonentiem vai individuāliem lietotājiem par personas datu aizsardzības pārkāpumiem, jo tehnikas attīstības gaitā šādi pasākumi var mainīties. Tomēr Komisijai vajadzētu būt iespējai publicēt šādu specifisku tehnisku aizsardzības pasākumu orientējošu sarakstu saskaņā ar pašreizējo praksi.
- (17) Šifrēšanas vai jaukšanas izmantošanu pašu par sevi nevarētu uzskatīt par pietiekamu, lai pakalpojumu sniedzēji varētu apgalvot, ka ir izpildījuši Direktīvas 95/46/EK 17. pantā noteikto vispārējo drošības pienākumu. Šajā sakarībā pakalpojumu sniedzējiem vajadzētu īstenot arī pienācīgus organizatoriskos un tehniskos pasākumus, lai nepieļautu, konstatētu un bloķētu personas datu aizsardzības pārkāpumus. Pakalpojumu sniedzējiem vajadzētu ņemt vērā visus neapzinātos apdraudējumus, kas var pastāvēt arī pēc tam, kad īstenoti kontroles pasākumi, lai izprastu, kur varētu notikt iespējamie personas datu aizsardzības pārkāpumi.
- (18) Ja pakalpojumu sniedzējs daļu no pakalpojuma, piemēram, rēķinu izrakstīšanu vai pārvaldības funkcijas, nodrošina ar cita pakalpojumu sniedzēja starpniecību, šim

citam pakalpojumu sniedzējam, kam nav tiešu līgumattiecību ar galalietotāju, nav pienākuma sniegt paziņojumus personas datu aizsardzības pārkāpumu gadījumā. Tā vietā tam ir jābrīdina un jāinformē pakalpojumu sniedzējs, ar kuru tam ir tiešas līgumattiecības. Šis noteikums ir spēkā arī elektronisko komunikāciju pakalpojumu vairumtirdzniecības piegādes kontekstā, kad vairumtirdzniecības pakalpojumu sniedzējam parasti nav tiešu līgumattiecību ar galalietotāju.

- (19) Direktīvā 95/46/EK noteikta vispārēja personas datu aizsardzības kārtība Eiropas Savienībā. Komisija ir iesniegusi priekšlikumu Eiropas Parlamenta un Padomes regulai, ar kuru aizstātu Direktīvu 95/46/EK (Datu aizsardzības regula). Ar ierosināto datu aizsardzības regulu tiktu noteikts, ka visiem datu kontrolētājiem ir pienākums paziņot par personas datu aizsardzības pārkāpumiem, pamatojoties uz Direktīvas 2002/58/EK 4. panta 3. punktu. Līdzšinējā Komisijas regula ir pilnībā saderīga ar ierosināto pasākumu.
- (20) Ar ierosināto Datu aizsardzības regulu tiks veikti arī daži tehniski pielāgojumi Direktīvā 2002/58/EK, ņemot vērā Direktīvas 95/46/EK pārveidošanu par regulu. Komisija veiks pārskatīšanu par to, kādas būtiskas juridiskās sekas uz Direktīvu 2002/58/EK atstās jaunā regula.
- (21) Šīs regulas piemērošana būtu jāpārskata trīs gadus pēc tās stāšanās spēkā, un tās saturs būtu jāpārskata, ņemot vērā tajā laikā spēkā esošo tiesisko regulējumu, tostarp ierosināto Datu aizsardzības regulu. Šīs regulas pārskatīšana, ja iespējams, būtu jāveic saistībā ar jebkādu Direktīvas 2002/58/EK pārskatīšanu nākotnē.
- (22) Šīs regulas piemērošanu var novērtēt, *inter alia* balstoties uz statistiku, ko savākušas kompetentās valsts iestādes par tām paziņotajiem personas datu aizsardzības pārkāpumiem. Šāda statistika var būt, piemēram, informācija par kompetentajai valsts iestādei paziņoto personas datu aizsardzības pārkāpumu skaitu, informācija par abonentiem vai individuāliem lietotājiem paziņoto personas datu aizsardzības pārkāpumu skaitu, personas datu aizsardzības pārkāpuma atrisināšanai patērētais laiks un tas, vai tika izmantoti tehniski aizsardzības pasākumi. Šādai statistikai būtu jānodrošina Komisija un dalībvalstis ar konsekventiem un salīdzināmiem statistikas datiem, un tai nevajadzētu atklāt ne ziņotāja pakalpojumu sniedzēja, ne iesaistīto abonentu vai individuālo lietotāju identitāti. Komisija šajā nolūkā var rīkot regulāras sanāksmes ar kompetento valsts iestāžu un citu ieinteresēto personu piedalīšanos.
- (23) Šajā regulā paredzētie pasākumi ir saskaņā ar Komunikācijas komitejas atzinumu,

IR PIENĒMUSI ŠO REGULU.

1. pants

Darbības joma

Šī regula attiecas uz to, kā publiski pieejamu elektronisko komunikāciju pakalpojumu sniedzēji ("pakalpojumu sniedzējs") paziņo par personas datu aizsardzības pārkāpumiem.

2. pants

Paziņošana kompetentajai valsts iestādei

1. Par visiem personas datu aizsardzības pārkāpumiem pakalpojumu sniedzējs paziņo kompetentajai valsts iestādei.

2. Ja iespējams, pakalpojumu sniedzējs kompetentajai valsts iestādei par personas datu aizsardzības pārkāpumu paziņo ne vēlāk kā 24 stundu laikā pēc tam, kad konstatēts personas datu aizsardzības pārkāpums.

Pakalpojumu sniedzējs paziņojumā kompetentajai valsts iestādei iekļauj I pielikumā norādīto informāciju.

Personas datu aizsardzības pārkāpuma konstatēšanu uzskata par notikušu brīdī, kad pakalpojumu sniedzējs ir guvis pietiekamu pārliecību, lai saskaņā ar šo regulu sniegtu pamatotu paziņojumu, ka ir noticis drošības incidents, kas izraisījis personas datu apdraudējumu.

3. Ja visa I pielikumā norādītā informācija nav pieejama un ir nepieciešama turpmāka izmeklēšana par personas datu aizsardzības pārkāpumu, pakalpojumu sniedzējam ir atļauts sniegt kompetentajai valsts iestādei sākotnējo paziņojumu ne vēlāk kā 24 stundu laikā pēc tam, kad konstatēts personas datu aizsardzības pārkāpums. Šajā sākotnējā paziņojumā kompetentajai valsts iestādei iekļauj I pielikuma 1. iedaļā norādīto informāciju. Pakalpojumu sniedzējs sniedz otru paziņojumu kompetentajai valsts iestādei pēc iespējas drīzāk, bet ne vēlāk kā trīs dienu laikā pēc sākotnējā paziņojuma. Šajā otrajā paziņojumā iekļauj I pielikuma 2. iedaļā norādīto informāciju un vajadzības gadījumā atjaunina agrāk sniegto informāciju.

Ja pakalpojumu sniedzējs, neraugoties uz veikto izmeklēšanu, nespēj sniegt visu informāciju trīs dienu laikā kopš sākotnējā paziņojuma, pakalpojumu sniedzējs sniedz informāciju, kas šajā laikā ir tā rīcībā, un sniedz kompetentajai iestādei pamatotu skaidrojumu par pārējās informācijas vēlāku iesniegšanu. Pakalpojumu sniedzējs pārējo informāciju kompetentajai valsts iestādei paziņo pēc iespējas drīzāk un vajadzības gadījumā pēc iespējas drīzāk atjaunina agrāk sniegto informāciju.

4. Kompetentā valsts iestāde visiem pakalpojumu sniedzējiem, kas reģistrēti attiecīgajā dalībvalstī, nodrošina drošus elektroniskus līdzekļus, kā paziņot par personas datu aizsardzības pārkāpumiem, un sniedz informāciju par procedūram, kā šiem līdzekļiem piekļūt un kā tos izmantot. Vajadzības gadījumā Komisija sasauc sanāksmes ar kompetento valsts iestāžu piedalīšanos, lai veicinātu šā nosacījuma piemērošanu.

5. Ja personas datu aizsardzības pārkāpums skar abonētus vai individuālus lietotājus no citām dalībvalstīm, nevis no tās, kuras kompetentajai valsts iestādei paziņots par personas datu aizsardzības pārkāpumu, šī kompetentā valsts iestāde sniedz informāciju pārējām skartajām valsts iestādēm.

Lai veicinātu minētā nosacījuma piemērošanu, Komisija izveido un uztur kompetento valsts iestāžu un attiecīgo kontaktpunktu sarakstu.

3. pants

Paziņojums abonentam vai individuālam lietotājam

1. Ja personas datu aizsardzības pārkāpums varētu negatīvi ietekmēt abonenta vai individuāla lietotāja personas datus vai privātumu, pakalpojumu sniedzējs papildus 2. pantā minētajam paziņojumam paziņo par pārkāpumu abonentam vai individuālam lietotājam.

2. To, vai personas datu aizsardzības pārkāpums varētu negatīvi ietekmēt abonenta vai individuāla lietotāja personas datus vai privātumu, izvērtē, ņemot vērā īpaši šādus apstākļus:

- a) attiecīgo personas datu būtība un saturs, proti, vai tie ir ar finanšu informāciju saistīti dati, Direktīvas 95/46/E 8. panta 1. punktā minētās īpašās datu kategorijas, kā arī atrašanās vietas dati, interneta žurnālfaili, tīmekļa pārlūkošanas vēsture, e-pasta dati un detalizēta zvanu informācija;
- b) personas datu aizsardzības pārkāpuma iespējamās sekas attiecīgajam abonentam vai individuālam lietotājam, jo īpaši – ja pārkāpums var būt par iemeslu identitātes zādzībai vai krāpšanai, fiziskam kaitējumam, psiholoģiskam diskomfortam, pazemojumam vai reputācijas graušanai; kā arī
- c) personas datu aizsardzības pārkāpuma apstākļi, konkrētāk, kur dati nozagti vai kad pakalpojumu sniedzējam kļuvis zināms, ka dati ir nepilnvarotas trešās personas rīcībā.

3. Paziņojumu abonentam vai individuālam lietotājam sniedz bez liekas kavēšanās pēc personas datu aizsardzības pārkāpuma konstatēšanas, kā noteikts 2. panta 2. punkta trešajā daļā. Minēto paziņojumu sniedz neatkarīgi no 2. pantā minētā paziņojuma kompetentajai valsts iestādei par personas datu aizsardzības pārkāpumu.

4. Pakalpojumu sniedzējs paziņojumā abonentam vai individuālam lietotājam iekļauj II pielikumā norādīto informāciju. Paziņojumu abonentam vai individuālam lietotājam formulē skaidri un viegli saprotamā valodā. Pakalpojumu sniedzējs neizmanto šādu paziņošanu kā izdevību reklamēt vai popularizēt jaunus vai papildu pakalpojumus.

5. Ārkārtas apstākļos, kad abonenta vai individuāla lietotāja informēšana var apdraudēt personas datu aizsardzības pārkāpuma pienācīgu izmeklēšanu, pakalpojumu sniedzējam, ja tas saņēmis kompetentās valsts iestādes piekrišanu, ir atļauts abonenta vai individuāla lietotāja informēšanu atlikt līdz brīdim,

kamēr kompetentā valsts iestāde uzskata par iespējamu informēt par personas datu aizsardzības pārkāpumu saskaņā ar šo pantu.

6. Pakalpojumu sniedzējs abonentam vai individuālam lietotājam par personas datu aizsardzības pārkāpumu paziņo, izmantojot tādas saziņas līdzekļus, kas nodrošina tūlītēju informācijas saņemšanu un ir pietiekami droši atbilstīgi jaunākajām tehnoloģijām. Informācija par pārkāpumu attiecas tikai uz pārkāpumu, nevis uz kādu citu tematu.

7. Ja pakalpojumu sniedzējs, kam ir tiesas līgumattiecības ar galalietotāju, ir pielicis saprātīgas pūles, tomēr 3. punktā minētajā termiņā nespēj identificēt visus individuālos lietotājus, kurus varētu negatīvi ietekmēt personas datu aizsardzības pārkāpums, pakalpojumu sniedzējs par pārkāpumu var šiem individuālajiem lietotājiem paziņot, minētajā termiņā publicējot sludinājumus lielākajos valsts mēroga un reģionālajos plašsaziņas līdzekļos attiecīgajās dalībvalstīs. Šajos sludinājumos iekļauj II pielikumā norādīto informāciju, vajadzības gadījumā saīsinātā formā. Tādā gadījumā pakalpojumu sniedzējs turpina pielikt saprātīgas pūles, lai pēc iespējas drīzāk identificētu šos individuālos lietotājus un paziņotu tiem II pielikumā norādīto informāciju.

4. pants

Tehniski aizsardzības pasākumi

1. Atkāpjoties no 3. panta 1. punkta, abonentam vai attiecīgajam individuālam lietotājam nav jāpaziņo par personas datu aizsardzības pārkāpumu, ja pakalpojumu sniedzējs kompetentajai valsts iestādei ir uzskatāmi pierādījis, ka tas ir īstenojis atbilstīgus tehniskus aizsardzības pasākumus un ka šie pasākumi tikuši piemēroti datiem, ko skāris drošības pārkāpums. Ar šādiem tehniskiem aizsardzības pasākumiem datus padara nesaprotamus personām, kurām nav pilnvaru piekļūt datiem.

2. Datus uzskata par nesaprotamiem, ja:

- a) tie ir droši šifrēti ar standartizētu algoritmu, datu atšifrēšanas atslēgu nav skāris nekāds drošības pārkāpums un datu atšifrēšanas atslēga ir ģenerēta tā, ka to ar pieejamiem tehniskajiem līdzekļiem nevar noskaidrot neviens, kam nav pilnvaru piekļūt atslēgai; vai
- b) dati ir aizstāti ar to jaucējvērtību (hešvērtību), kas aprēķināta ar standartizētu kriptogrāfisku jaucējfunkciju ar atslēgu, datu jaukšanas atslēgu nav skāris nekāds drošības pārkāpums un datu jaukšanas atslēga ir ģenerēta tā, ka to ar pieejamiem tehniskajiem līdzekļiem nevar noskaidrot neviens, kam nav pilnvaru piekļūt atslēgai.

3. Komisija pēc apspriešanās ar kompetentajām valsts iestādēm 29. pantā minētās darba grupas ietvaros, Eiropas Tīklu un informācijas drošības aģentūru un Eiropas Datu aizsardzības uzraudzītāju var publicēt 1. punktā minēto tehnisko aizsardzības pasākumu orientējošu sarakstu saskaņā ar pašreizējo praksi.

*5. pants***Cita pakalpojumu sniedzēja iesaistīšana**

Ja ir nolīgts cits pakalpojumu sniedzējs, lai tas sniegtu daļu elektroniskās komunikācijas pakalpojumu, nenodibinot tiešas līgumattiecības ar abonentiem, šis cits pakalpojumu sniedzējs nekavējoties informē to nolīgušo pakalpojumu sniedzēju par personas datu aizsardzības pārkāpumu.

*6. pants***Ziņošana un pārskatīšana**

Trīs gadu laikā no šīs regulas spēkā stāšanās dienas Komisija sniedz ziņojumu par šīs regulas piemērošanu, tās efektivitāti un ietekmi uz pakalpojumu sniedzējiem, abonentiem un individuālajiem lietotājiem. Uz minētā ziņojuma pamata Komisija veic šīs regulas pārskatīšanu.

*7. pants***Stāšanās spēkā**

Šī regula stājas spēkā 2013. gada 25. augustā.

Šī regula uzliek saistības kopumā un ir tieši piemērojama visās dalībvalstīs.

Briselē, 2013. gada 24. jūnijā

Komisijas vārdā –
priekšsēdētājs
José Manuel BARROSO

I PIELIKUMS

Kompetentajai valsts iestādei nosūtāmā paziņojuma saturs**1. iedaļa***Pakalpojumu sniedzēja identifikācija*

1. Pakalpojumu sniedzēja nosaukums
2. Datu aizsardzības inspektora vai cita kontaktpunkta, kur var iegūt papildu informāciju, identitāte un kontaktinformācija
3. Ziņas par to, vai informācija attiecas uz pirmo vai otro paziņojumu

Sākotnējais paziņojums par personas datu aizsardzības pārkāpumu (attiecīgā gadījumā papildināms ar vēlākiem paziņojumiem)

4. Incidenta datums un laiks (ja zināms; vajadzības gadījumā var veikt aplēsi) un incidenta konstatēšanas laiks
5. Personas datu aizsardzības pārkāpuma apstākļi (piemēram, zudums, zādzība, kopēšana)
6. Skarto personas datu būtība un saturs
7. Tehniskie un organizatoriskie pasākumi, ko pakalpojumu sniedzējs piemērojis (vai gatavojas piemērot) skartajiem personas datiem
8. Citu pakalpojumu sniedzēju iesaistīšana (vajadzības gadījumā)

2. iedaļa*Sīkāka informācija par personas datu aizsardzības pārkāpumu*

9. Kopsavilkums par incidentu, kas izraisījis personas datu aizsardzības pārkāpumu (tostarp pārkāpuma norises fiziskā vieta un izmantotie datu nesēji)
10. Skarto abonentu vai individuālo lietotāju skaits
11. Potenciālās sekas un iespējamā negatīvā ietekme uz abonentiem vai individuālajiem lietotājiem
12. Tehniskie un organizatoriskie pasākumi, ko pakalpojumu sniedzējs veicis, lai mazinātu iespējamo negatīvo ietekmi

Iespējams papildu paziņojums abonentiem vai individuālajiem lietotājiem

13. Paziņojuma saturs
14. Izmantotie saziņas līdzekļi
15. Informēto abonentu vai individuālo lietotāju skaits

Iespējamie pārrobežu jautājumi

16. Personas datu aizsardzības pārkāpums skar abonentus vai individuālos lietotājus citās dalībvalstīs
17. Paziņošana citām kompetentajām valstu iestādēm

*II PIELIKUMS***Abonentam vai individuālajam lietotājam nosūtāmā paziņojuma saturs**

1. Pakalpojumu sniedzēja nosaukums
 2. Datu aizsardzības inspektora vai cita kontaktpunkta, kur var iegūt papildu informāciju, identitāte un kontaktinformācija
 3. Kopsavilkums par incidentu, kas izraisījis personas datu aizsardzības pārkāpumu
 4. Aptuvenais incidenta datums un laiks
 5. Skarto personas datu būtība un saturs, kā minēts 3. panta 2. punktā
 6. Personas datu aizsardzības pārkāpuma iespējamās sekas abonentam vai individuālajam lietotājam, kā minēts 3. panta 2. punktā
 7. Personas datu aizsardzības pārkāpuma apstākļi, kā minēts 3. panta 2. punktā
 8. Pakalpojumu sniedzēja veiktie pasākumi saistībā ar personas datu aizsardzības pārkāpumu
 9. Pakalpojumu sniedzēja ieteiktie pasākumi, lai mazinātu iespējamo negatīvo ietekmi
-