KOMISIJAS DELEĢĒTĀ REGULA (ES) 2018/389

(2017. gada 27. novembris),

ar ko Eiropas Parlamenta un Padomes Direktīvu (ES) 2015/2366 papildina attiecībā uz regulatīvajiem tehniskajiem standartiem par drošu lietotāja autentificēšanu un vienotiem un drošiem atklātiem saziņas standartiem

(Dokuments attiecas uz EEZ)

EIROPAS KOMISIJA,

ņemot vērā Līgumu par Eiropas Savienības darbību,

ņemot vērā Eiropas Parlamenta un Padomes 2015. gada 25. novembra Direktīvu (ES) 2015/2366 par maksājumu pakalpojumiem iekšējā tirgū, ar ko groza Direktīvas 2002/65/EK, 2009/110/EK un 2013/36/ES un Regulu (ES) Nr. 1093/2010 un atceļ Direktīvu 2007/64/EK ([1]), un jo īpaši tās 98. panta 4. punkta otro daļu,

tā kā:

(1) Maksājumu pakalpojumi, kas tiek piedāvāti elektroniski, būtu jāveic drošā veidā, pielietojot tehnoloģijas, ar kurām var garantēt drošu lietotāja autentificēšanu un, cik iespējams, maksimāli samazināt krāpšanas risku. Autentificēšanas procedūrām būtu kopumā jāietver darījumu uzraudzības mehānismi, lai atklātu mēģinājumus izmantot maksājumu pakalpojumu lietotāja personalizētos drošības datus, kas ir pazaudēti, nozagti vai nelikumīgi piesavināti, un būtu arī jānodrošina, ka maksājumu pakalpojumu lietotājs ir likumīgas lietotājs un tāpēc dod piekrišanu naudas līdzekļu pārvešanai un piekļuvei tā konta informācijai, izmantojot personalizētos drošības datus parastos lietošanas apstākļos. Turklāt ir nepieciešams precizēt prasības par drošu lietotāja autentificēšanu, kas būtu piemērojamas ik reizi, kad maksātājs piekļūst savam maksājumu kontam tiešsaistē, iniciē elektronisku maksājuma darījumu vai veic kādu darbību, izmantojot attālinātu kanālu, kas varētu ietvert ar maksājumiem saistītas krāpšanas risku vai cita veida ļaunprātīgu izmantošanu, prasot ģenerēt autentifikācijas kodu, kuram vajadzētu būt noturīgam pret risku, ka tas tiks viltots kopumā vai ka tiks publiskots kāds no elementiem, pamatojoties uz ko kods tika ģenerēts.

(2) Tā kā krāpšanas metodes pastāvīgi mainās, prasībām par drošu klienta autentificēšanu būtu jāveicina tādu tehnisko risinājumu inovācijas, kas novērstu jaunus drošības apdraudējumus elektronisko maksājumu jomā. Lai nodrošinātu, ka nosakāmās prasības tiek pastāvīgi efektīvi īstenotas, ir lietderīgi arī pieprasīt, lai drošības pasākumi drošas klienta autentificēšanas piemērošanai un attiecīgie izņēmumi, pasākumi personalizēto drošības datu konfidencialitātes un integritātes aizsargāšanai un pasākumi vienotu un drošu atklātu saziņas standartu izveidošanai tiek dokumentēti, periodiski testēti, novērtēti un revidēti no tādu revidentu puses, kam ir zināšanas IT drošības un maksājumu jomā un kas ir operacionāli neatkarīgi. Lai kompetentās iestādes varētu uzraudzīt šo pasākumu pārskatīšanas kvalitāti, informācija par šādu pārskatīšanu būtu jādara tām pieejama pēc to pieprasījuma.

(3) Tā kā elektroniskiem attālinātajiem maksājumu darījumiem ir lielāks krāpšanas risks, ir nepieciešams ieviest papildu prasības attiecībā uz drošu klienta autentificēšanu šādos darījumos, nodrošinot, ka, uzsākot darījumu, elementi darījumu dinamiski sasaista ar summu un maksātāja norādīto maksājuma saņēmēju.

(4) Dinamiska sasaiste ir iespējama, ģenerējot autentificēšanas kodus, pamatojoties uz stingrām drošības prasībām. Lai saglabātu tehnoloģisko neitralitāti, nebūtu jāpieprasa specializēta autentificēšanas kodu ieviešanas tehnoloģija. Tādēļ autentificēšanas kodiem vajadzētu balstīties uz tādiem risinājumiem, kā piemēram, vienreizējas paroles ģenerēšana un validēšana, elektroniskie paraksti vai citi kriptogrāfiski derīguma apgalvojumi, kuros izmanto atslēgas vai kriptogrāfisku informāciju, kas tiek glabāta autentifikācijas elementos, ja tiek izpildītas drošības prasības.

([1]) OV L 337, 23.12.2015., 35. lpp.

(5) Ir nepieciešams noteikt īpašas prasības attiecībā uz situāciju, kad galīgā summa nav zināma brīdī, kad maksātājs iniciē elektronisku attālinātu maksājumu darījumu, lai nodrošinātu, ka drošā klienta autentificēšana attiecas uz maksimālo summu, kam maksātājs ir devis piekrišanu, kā minēts Direktīvā (ES) 2015/2366.

(6) Lai nodrošinātu, ka tiek piemērota droša klienta autentificēšana, ir svarīgi arī pieprasīt, lai būtu atbilstoši drošības parametri attiecībā uz drošas klienta autentificēšanas elementiem, ko kategorizē kā zināšanas (kaut kas, ko zina tikai lietotājs), piemēram, elementa garums vai sarežģītība, kā valdījumu (kaut kas, kas ir tikai lietotāja valdījumā), piemēram, algoritmu specifikācijas, atslēgas garums un entropija, un attiecībā uz ierīcēm un programmatūru, kas nolasa elementus, kuri klasificēti kā neatņemamas īpašības (kaut kas, kas lietotājs ir), piemēram, algoritmu specifikācijas, biometriskie sensori un veidnes aizsardzības elementi, jo īpaši lai mazinātu risku, ka nepiederošas personas šos elementus atklāj, izpauž un izmanto. Nepieciešams arī noteikt prasības, lai nodrošinātu, ka minētie elementi ir neatkarīgi, lai viena elementa drošības plaisa neapdraudētu citu elementu uzticamību, it īpaši tad, ja kāds no šiem elementiem tiek izmantots ar daudzfunkcionālas ierīces starpniecību, proti, ar tādas ierīces starpniecību kā planšetdators vai mobilais tālrunis, kurus var izmantot gan lai dotu rīkojumu veikt maksājumu, gan autentificēšanas procesā.

(7) Drošas klienta autentificēšanas prasības attiecas uz maksājumiem, ko iniciējis maksātājs, neatkarīgi no tā, vai maksātājs ir fiziska vai juridiska persona.

(8) Uz maksājumiem, kas veikti, izmantojot anonīmu maksājumu instrumentu, to būtības dēļ neattiecina drošas lietotāja autentificēšanas pienākumu. Gadījumos, ja šādu instrumentu anonimitāte tiek atcelta līgumisku vai juridisku iemeslu dēļ, maksājumiem piemēro drošības prasības, kas izriet no Direktīvas (ES) 2015/2366 un šā regulatīvā tehniskā standarta.

(9) Saskaņā ar Direktīvu (ES) 2015/2366 atbrīvojumi no principa par drošu klienta autentificēšanu ir noteikti, pamatojoties uz riska pakāpi, summu, atkārtošanos un maksājumu darījuma izpildei izmantoto maksājumu kanālu.

(10) Darbības, kas ietver piekļuvi maksājuma konta atlikumam un nesenajiem darījumiem, neizpaužot sensitīvus maksājumu datus, tādus regulārus maksājumus vieniem un tiem pašiem maksājumu saņēmējiem, kurus maksātājs ir iepriekš izveidojis vai apstiprinājis, izmantojot drošu klienta autentificēšanu, un maksājumus, kas saņemti no vienas un tās pašas fiziskas vai juridiskas personas vai sniegti tai, ja minētajai personai ir konti pie tā paša maksājumu pakalpojumu sniedzēja, rada zemu riska līmeni, tādējādi ļaujot maksājumu pakalpojumu sniedzējiem nepiemērot drošu klienta autentificēšanu. Tādējādi netiek ievērots, ka saskaņā ar Direktīvas (ES) 2015/2366 65., 66. un 67. pantu maksājumu iniciēšanas pakalpojumu sniedzējiem, maksājumu pakalpojumu sniedzējiem, kas izdod kartei piesaistītus maksājumu instrumentus, un konta informācijas pakalpojumu sniedzējiem nepieciešamā un būtiskā informācija no kontu apkalpojošā maksājumu pakalpojumu sniedzēja būtu jāprasa un jāsaņem tikai, lai sniegtu attiecīgo maksājumu pakalpojumu ar maksājumu pakalpojumu lietotāja piekrišanu. Šādu piekrišanu var sniegt atsevišķi par katru informācijas pieprasījumu vai par katru maksājumu, kas jāiniciē, vai konta informācijas pakalpojumu sniedzējiem kā pilnvaras attiecībā uz noteiktiem maksājumu kontiem un saistītajiem maksājumu darījumiem, kā noteikts līgumā ar maksājumu pakalpojumu lietotāju.

(11) Atbrīvojumi attiecībā uz tādiem nelielas vērtības bezkontakta maksājumiem tirdzniecības vietās, kuros ņem vērā arī secīgu darījumu maksimālo skaitu vai konkrētu, noteiktu maksimālo vērtību secīgiem darījumiem, nepiemērojot drošu klienta autentificēšanu, ļautu izstrādāt lietotājiem draudzīgus un zema riska maksājumu pakalpojumus, un tāpēc tie būtu jāparedz. Turklāt ir lietderīgi noteikt izņēmumu attiecībā uz elektronisko maksājumu darījumiem, kas iniciēti neuzraudzītos maksājumu terminālos, kur drošu klienta autentificēšanu ne vienmēr var būt viegli piemērot operacionālu iemeslu dēļ (piemēram, lai izvairītos no rindām un potenciāliem negadījumiem pie iekasēšanas barjerām, vai citu drošības vai drošuma risku dēļ).

(12) Līdzīgi atbrīvojumam attiecībā uz nelielas vērtības bezkontakta maksājumiem tirdzniecības vietā ir jānodrošina atbilstīgs līdzsvars starp paaugstinātas drošības interesēm attālinātu maksājumu gadījumā un maksājumu lietotāj-draudzīguma un pieejamības vajadzībām maksājumu e-komercijas jomā. Saskaņā ar minētajiem principiem robežvērtības, zem kurām nav nepieciešams piemērot drošu klienta autentificēšanu, būtu jānosaka piesardzīgā veidā, lai aptvertu tikai tiešsaistes pirkumus, kuru vērtība ir neliela. Robežvērtības attiecībā uz pirkumiem tiešsaistē būtu jānosaka piesardzīgāk, ņemot vērā, ka fakts, ka persona fiziski nav klāt pirkuma izdarīšanas brīdī, rada nedaudz lielāku drošības risku.

(13) Drošas klienta autentificēšanas prasības attiecas uz maksājumiem, ko iniciējis maksātājs, neatkarīgi no tā, vai maksātājs ir fiziska vai juridiska persona. Daudzi korporatīvie maksājumi tiek iniciēti, izmantojot īpašus procesus vai protokolus, kas garantē tādu augstu maksājumu drošības līmeni, ko Direktīva (ES) 2015/2366 cenšas panākt ar drošu klienta autentificēšanu. Ja kompetentās iestādes konstatē, ka minētie maksājumu procesi un protokoli, kas darīti pieejami tikai tiem maksātājiem, kas nav patērētāji, izpilda Direktīvas (ES) 2015/2366 mērķus attiecībā uz drošību, maksājumu pakalpojumu sniedzējus attiecībā uz šiem procesiem vai protokoliem var atbrīvot no prasības par drošu klientu autentificēšanu.

(14) Attiecībā uz reāllaika darījumu riska analīzi, kurā maksājuma darījums tiek kategorizēts kā zemas riska pakāpes darījums, ir lietderīgi arī ieviest atbrīvojumu attiecībā uz maksājumu pakalpojumu sniedzēju, kas neplāno piemērot drošu klienta autentificēšanu, pieņemot efektīvas un uz risku balstītas prasības, ar kurām tiek nodrošināta maksājumu pakalpojumu lietotāju naudas līdzekļu un personas datu drošība. Minētajām uz risku balstītajām prasībām būtu jāapkopo riska analīzes rezultāti, kas apstiprina, ka nav identificēti anormāli tēriņi vai maksātāja uzvedības modelis, ņemot vērā citus riska faktorus, tostarp informāciju par maksātāja un maksājuma saņēmēja atrašanās vietu ar monetārajiem robežlielumiem, kuru pamatā ir krāpšanas koeficienti, kas aprēķināti attiecībā uz attālinātiem maksājumiem. Ja, pamatojoties uz reāllaika darījumu riska analīzi, maksājumu nevar klasificēt kā tādu, kas rada zemu riska līmeni, maksājumu pakalpojumu sniedzējam vajadzētu pāriet uz drošu klienta autentificēšanu. Šāda uz risku balstīta atbrīvojuma maksimālā vērtība būtu jānosaka tādā veidā, lai nodrošinātu, ka atbilstīgais krāpšanas koeficients ir ļoti zems, arī salīdzinot ar visu maksājumu pakalpojumu sniedzēja maksājumu darījumu, tostarp to, kuri autentificēti ar drošu klienta autentificēšanu, krāpšanas koeficientu noteiktā laika periodā un regulāri.

(15) Lai nodrošinātu efektīvu izpildi, maksājumu pakalpojumu sniedzējiem, kas vēlas izmantot atbrīvojumus no drošas klientu autentificēšanas, būtu attiecībā uz katru maksājuma darījuma veidu regulāri jāuzrauga un kompetentajām iestādēm un Eiropas Banku iestādei (EBI) pēc to pieprasījuma jādara pieejama informācija par krāpniecisku vai neatļautu maksājumu darījumu summu un par novērotajiem krāpšanas koeficientiem attiecībā uz visiem to maksājumu darījumiem, neatkarīgi no tā, vai tie autentificēti, izmantojot drošu klienta autentificēšanu, vai veikti saskaņā ar attiecīgo atbrīvojumu.

(16) Šo jauno vēsturisko pierādījumu apkopošana par elektronisko maksājumu darījumu krāpšanas koeficientiem palīdzēs arī EBI, balstoties uz reāllaika darījumu riska analīzi, efektīvi pārskatīt robežvērtības tādiem atbrīvojumiem no prasības par drošu klientu autentificēšanu. EBI būtu jāpārskata un attiecīgā gadījumā jāiesniedz Komisijai šo regulatīvo tehnisko standartu atjauninājumu projekti, iesniedzot jaunus robežvērtību projektus un attiecīgos krāpšanas koeficientus, lai palielinātu attālināto elektronisko maksājumu drošību saskaņā ar Direktīvas (ES) 2015/2366 98. panta 5. punktu un Eiropas Parlamenta un Padomes Regulas (ES) Nr. 1093/2010 10. pantu ([1]).

(17) Maksājumu pakalpojumu sniedzējiem, kas izmanto kādu no paredzētajiem atbrīvojumiem, vajadzētu būt iespējai jebkurā laikā izvēlēties darbībām un attiecīgajos noteikumos minētajiem maksājumu darījumiem piemērot drošu klientu autentificēšanu.

(18) Pasākumiem, kas aizsargā personalizētu drošības datu konfidencialitāti un integritāti, kā arī autentificēšanas ierīcēm un programmatūrai būtu jāierobežo riski, kas saistīti ar krāpšanu, kura izriet no neatļautas vai krāpnieciskas maksājumu instrumentu izmantošanas un neatļautas piekļuves maksājumu kontiem. Šajā nolūkā ir jāievieš prasības par personalizēto drošības datu drošu izveidi un sniegšanu un to saistīšanu ar maksājumu pakalpojumu lietotāju un jāparedz nosacījumi par minēto datu atjaunošanu un dezaktivēšanu.

(19) Lai nodrošinātu efektīvu un drošu saziņu starp attiecīgajiem dalībniekiem saistībā ar konta informācijas pakalpojumiem, maksājumu iniciēšanas pakalpojumiem un apstiprinājumu par naudas līdzekļu pieejamību, ir nepieciešams precizēt prasības attiecībā uz vienotiem un drošiem atklātiem saziņas standartiem, kas jāievēro visiem attiecīgajiem maksājumu pakalpojumu sniedzējiem. Direktīvā (ES) 2015/2366 paredzēts, ka konta informācijas pakalpojumu sniedzēji var piekļūt maksājumu konta informācijai un to izmantot. Tādēļ ar šo regulu netiek mainīti noteikumi par piekļuvi kontiem, kas nav maksājumu konti.

([1]) Eiropas Parlamenta un Padomes 2010. gada 24. novembra Regula (ES) Nr. 1093/2010, ar ko izveido Eiropas Uzraudzības iestādi (Eiropas Banku iestādi), groza Lēmumu Nr. 716/2009/EK un atceļ Komisijas Lēmumu 2009/78/EK (OV L 331, 15.12.2010., 12. lpp.).

(20) Katram kontu apkalpojošajam maksājumu pakalpojumu sniedzējam, kam ir tiešsaistē pieejami maksājumu konti, būtu jāpiedāvā vismaz viena piekļuves saskarne, kas ļauj droši sazināties ar konta informācijas pakalpojumu sniedzējiem, maksājumu iniciēšanas pakalpojumu sniedzējiem un maksājumu pakalpojumu sniedzējiem, kas izdod kartei piesaistītus maksājumu instrumentus. Saskarnei būtu jāļauj konta informācijas pakalpojumu sniedzējiem, maksājumu iniciēšanas pakalpojumu sniedzējiem un maksājumu pakalpojumu sniedzējiem, kas izdod kartei piesaistītus maksājumu instrumentus, sevi identificēt kontu apkalpojošajam maksājumu pakalpojumu sniedzējam. Tai būtu arī jānodrošina, ka konta informācijas pakalpojumu sniedzēji un maksājumu iniciēšanas pakalpojumu sniedzēji var paļauties uz autentifikācijas procedūrām, kuras kontu apkalpojošais maksājumu pakalpojumu sniedzējs piedāvā maksājumu pakalpojumu lietotājam. Lai nodrošinātu tehnoloģiju un darījumdarbības modeļu neitralitāti, kontu apkalpojošajiem maksājumu pakalpojumu sniedzējiem būtu jādod iespēja brīvi izlemt, vai piedāvāt saskarni, kas paredzēta saziņai ar konta informācijas pakalpojumu sniedzējiem, maksājumu iniciēšanas pakalpojumu sniedzējiem un maksājumu pakalpojumu sniedzējiem, kas izdod kartei piesaistītus maksājumu instrumentus, vai ļaut šādai saziņai izmantot saskarni identifikācijai un saziņai ar kontu apkalpojošo maksājumu pakalpojumu sniedzēju maksājumu pakalpojumu lietotājiem.

(21) Lai konta informācijas pakalpojumu sniedzēji, maksājumu iniciēšanas pakalpojumu sniedzēji un maksājumu pakalpojumu sniedzēji, kas izdod kartei piesaistītus maksājumu instrumentus, varētu izstrādāt tehniskos risinājumus, saskarnes tehnisko specifikāciju vajadzētu pienācīgi dokumentēt un darīt publiski pieejamu. Turklāt kontu apkalpojošajam maksājumu pakalpojumu sniedzējam būtu jāparedz mehānisms, kas ļauj maksājumu pakalpojumu sniedzējiem tehniskos risinājumus testēt vismaz sešus mēnešus pirms šo standartu pieteikuma iesniegšanas dienas vai, ja saskarni laiž tirgū pēc šo standartu piemērošanas datuma, – pirms dienas, kurā saskarni laiž tirgū. Lai nodrošinātu dažādo tehnoloģisko saziņas risinājumu sadarbspēju, saskarnē būtu jāizmanto saziņas standarti, kurus izstrādājušas starptautiskās vai Eiropas standartizācijas organizācijas.

(22) Konta informācijas pakalpojumu sniedzēju un maksājumu iniciēšanas pakalpojumu sniedzēju sniegto pakalpojumu kvalitāte būs atkarīga no saskarņu, ko ieviesuši vai pielāgojuši kontu apkalpojošie maksājumu pakalpojumu sniedzēji, pareizas darbības. Tāpēc ir svarīgi, ka gadījumos, kad šādas saskarnes neatbilst standartos iekļautajiem noteikumiem, tiek veikti pasākumi, lai garantētu uzņēmējdarbības nepārtrauktību minēto pakalpojumu lietotājiem. Valstu kompetentajām iestādēm ir jābūt atbildīgām par to, lai maksājumu pakalpojumu sniedzēju un maksājumu iniciācijas pakalpojumu sniedzēju darbība netiek bloķēta vai traucēta to pakalpojumu sniegšanai.

(23) Ja piekļuvi maksājumu kontiem piedāvā, izmantojot specializētu saskarni, lai nodrošinātu maksājumu pakalpojumu lietotāju tiesības izmantot maksājumu iniciēšanas pakalpojumu sniedzējus un pakalpojumus, kas ļauj piekļūt konta informācijai, kā paredzēts Direktīvā (ES) 2015/2366, ir nepieciešams noteikt, ka specializētajām saskarnēm ir tāda paša līmeņa pieejamība un veiktspēja kā saskarnei, kas pieejama maksājumu pakalpojumu lietotājam. Kontu apkalpojošajiem maksājumu pakalpojumu sniedzējiem arī būtu jānosaka pārredzami galvenie darbības rādītāji un pakalpojuma līmeņa mērķi attiecībā uz specializētās saskarnes pieejamību un veiktspēju, kas ir vismaz tikpat stingri kā rādītāji un mērķi, kuri noteikti saskarnei, ko izmanto to maksājumu pakalpojumu lietotāji. Maksājumu pakalpojumu sniedzējiem būtu jātestē šīs specializētās saskarnes, kuras tie izmantos, un kompetentajām iestādēm būtu jāveic minēto saskarņu spriedzes testi un uzraudzība.

(24) Lai nodrošinātu, ka maksājumu pakalpojumu sniedzēji, kas izmanto specializēto saskarni, var turpināt sniegt savus pakalpojumus pieejamības problēmu vai nepienācīgas veiktspējas gadījumā, ir nepieciešams, ievērojot stingrus nosacījumus, nodrošināt rezerves mehānismu, kas ļautu šādiem pakalpojumu sniedzējiem izmantot saskarni, ko kontu apkalpojošais maksājumu pakalpojumu sniedzējs uztur, lai identificētu savus maksājumu pakalpojumu lietotājus un sazinātos ar tiem. Noteikti kontu apkalpojošie maksājumu pakalpojumu sniedzēji tiks atbrīvoti no prasības nodrošināt šādu rezerves mehānismu ar klientu saskarnēm, ja to kompetentās iestādes konstatē, ka specializētās saskarnes atbilst īpašajiem nosacījumiem, kas nodrošina netraucētu konkurenci. Ja specializētās saskarnes, kurām piemēro atbrīvojumu, neatbilst vajadzīgajiem nosacījumiem, attiecīgās kompetentās iestādes atsauc piešķirtos atbrīvojumus.

(25) Lai kompetentajām iestādēm dotu iespēju efektīvi uzraudzīt un pārraudzīt saziņas saskarņu ieviešanu un pārvaldību, kontu apkalpojošiem maksājumu pakalpojumu sniedzējiem būtu jāizveido to tīmekļa vietnē pieejams attiecīgās dokumentācijas kopsavilkums un pēc pieprasījuma jāiesniedz kompetentajām iestādēm dokumentācija par risinājumiem ārkārtas situācijās. Kontu apkalpojošajiem maksājumu pakalpojumu sniedzējiem būtu jādara publiski pieejama statistika par minētās saskarnes pieejamību un veiktspēju.

(26) Lai nodrošinātu datu konfidencialitāti un integritāti, ir jānodrošina, ka saziņas sesijas starp kontus apkalpojošajiem maksājumu pakalpojumu sniedzējiem, konta informācijas pakalpojumu sniedzējiem, maksājumu iniciēšanas pakalpojumu sniedzējiem un maksājumu pakalpojumu sniedzējiem, kas izdod kartei piesaistītus maksājumu

instrumentus, ir drošas. Jo īpaši ir jāpieprasa, lai starp konta informācijas pakalpojumu sniedzējiem, maksājumu iniciēšanas pakalpojumu sniedzējiem, maksājumu pakalpojumu sniedzējiem, kas izdod kartei piesaistītus maksājumu instrumentus, un kontu apkalpojošajiem maksājumu pakalpojumu sniedzējiem datu apmaiņas laikā tiktu piemērota šifrēšana.

(27) Lai uzlabotu lietotāju uzticēšanos un nodrošinātu drošu lietotāju autentificēšanu, būtu jāņem vērā elektroniskās identifikācijas līdzekļu un uzticamības pakalpojumu izmantošana, kā noteikts Eiropas Parlamenta un Padomes Regulā (ES) Nr. 910/2014 ([1]), it īpaši attiecībā uz paziņotām elektroniskās identifikācijas shēmām.

(28) Lai nodrošinātu saskaņotus piemērošanas datumus, šī regula būtu jāpiemēro no tā paša datuma, no kura dalībvalstīm ir jāpiemēro drošības pasākumi, kas minēti Direktīvas (ES) 2015/2366 65., 66., 67. un 97. pantā.

(29) Šī regula balstās uz regulatīvo tehnisko standartu projektu, ko Komisijai iesniegusi Eiropas Banku iestāde (EBI).

(30) EBI ir veikusi atklātu un pārredzamu sabiedrisko apspriešanu par šīs regulas pamatā esošo regulatīvo tehnisko standartu projektu, izvērtējusi iespējamās saistītās izmaksas un ieguvumus un pieprasījusi saskaņā ar Regulas (ES) Nr. 1093/2010 37. pantu izveidotās Banku nozares ieinteresēto personu grupas atzinumu,

IR PIEŅĒMUSI ŠO REGULU.

I NODAĻA

VISPĀRĪGI NOTEIKUMI

1. pants

Priekšmets

Ar šo regulu nosaka prasības, kas maksājumu pakalpojumu sniedzējiem jāievēro, lai īstenotu drošības pasākumus, kas tiem ļauj rīkoties šādi:

a) piemērot drošas lietotāju autentificēšanas procedūru saskaņā ar Direktīvas (ES) 2015/2366 97. pantu;

b) atbrīvot no drošas lietotāju autentificēšanas drošības prasības piemērošanas saskaņā ar konkrētiem un ierobežotiem nosacījumiem, kas balstīti uz riska pakāpi, maksājumu darījumu summas un atkārtošanās un to izpildei izmantotā maksājumu kanāla;

c) aizsargāt maksājumu pakalpojumu lietotāja personalizēto drošības datu konfidencialitāti un integritāti;

d) izstrādāt vienotus un drošus atklātos standartus attiecībā uz saziņu starp kontu apkalpojošajiem maksājumu pakalpojumu sniedzējiem, maksājumu iniciēšanas pakalpojumu sniedzējiem, konta informācijas pakalpojumu sniedzējiem, maksātājiem, maksājumu saņēmējiem un citiem maksājumu pakalpojumu sniedzējiem saistībā ar maksājumu pakalpojumu sniegšanu un izmantošanu, piemērojot Direktīvas (ES) 2015/2366 IV sadaļu.

2. pants

Vispārīgas autentificēšanas prasības

1. Maksājumu pakalpojumu sniedzējiem ir darījumu uzraudzības mehānismi, kas tiem ļauj atklāt neatļautus vai krāpnieciskus maksājumu darījumus nolūkā īstenot drošības pasākumus, kas minēti 1. panta a) un b) apakšpunktā.

([1]) Eiropas Parlamenta un Padomes 2014. gada 23. jūlija Regula (ES) Nr. 910/2014 par elektronisko identifikāciju un uzticamības pakalpojumiem elektronisko darījumu veikšanai iekšējā tirgū un ar ko atceļ Direktīvu 1999/93/EK (OV L 257, 28.8.2014., 53. lpp.).

Šie mehānismi ir balstīti uz analīzi par maksājumu darījumiem, ņemot vērā elementus, kas ir raksturīgi maksājumu pakalpojumu lietotājam personalizēto drošības datu parastas lietošanas apstākļos.

2. Maksājumu pakalpojumu sniedzēji nodrošina, ka darījumu uzraudzības mehānismos ir ņemti vērā vismaz katrs no šiem riska faktoriem:

a) saraksti ar kompromitētiem vai nozagtiem autentifikācijas elementiem;

b) katra maksājumu darījuma summa;

c) zināmie krāpšanas scenāriji maksājumu pakalpojumu sniegšanas jomā;

d) ļaunprogrammatūras infekcijas pazīmes kādā autentifikācijas procedūru sesijā;

e) ja piekļuves ierīci vai programmatūru nodrošina maksājumu pakalpojumu sniedzējs, reģistrs ar maksājumu pakalpojumu lietotājam sniegtās piekļuves ierīces vai programmatūras izmantojumu un piekļuves ierīces vai programmatūras anormālu izmantojumu.

3. pants

Drošības pasākumu pārskatīšana

1. Regulas 1. pantā minēto drošības pasākumu īstenošanu dokumentē, periodiski testē, novērtē un saskaņā ar maksājumu pakalpojumu sniedzēja piemērojamo tiesisko regulējumu revidē revidenti, kam ir zināšanas IT drošības un maksājumu jomā un kas ir operacionāli neatkarīgi maksājumu pakalpojumu sniedzēja ietvaros vai no tā.

2. Laikposmus starp 1. punktā minētajām revīzijām nosaka, ņemot vērā attiecīgo grāmatvedības un tiesību aktos noteiktās revīzijas sistēmu, ko piemēro maksājumu pakalpojumu sniedzējam.

Tomēr maksājumu pakalpojumu sniedzējiem, kuri izmanto 18. pantā minēto atbrīvojumu, vismaz reizi gadā veic revīziju attiecībā uz metodoloģiju, modeļiem un paziņotajiem krāpšanas gadījumu rādītājiem. Revidentam, kas veic šādu revīziju, ir specializētas zināšanas par IT drošību un maksājumiem un operacionālā neatkarība maksājumu pakalpojumu sniedzēja ietvaros vai no tā. Pirmā gada laikā, kad tiek izmantots atbrīvojums saskaņā ar 18. pantu, un pēc tam vismaz reizi trijos gados vai biežāk pēc kompetentās iestādes pieprasījuma, šo revīziju veic neatkarīgs un kvalificēts ārējais revidents.

3. Šajā revīzijā sniedz novērtējumu un ziņojumu par maksājumu pakalpojumu sniedzēja drošības pasākumu atbilstību šajā regulā izklāstītajām prasībām.

Visu pārskatu dara pieejamu kompetentām iestādēm pēc to pieprasījuma.

II NODAĻA

DROŠĪBAS PASĀKUMI DROŠAS LIETOTĀJU AUTENTIFICĒŠANAS PIEMĒROŠANAI

4. pants

Autentifikācijas kods

1. Ja maksājumu pakalpojumu sniedzēji piemēro drošu lietotāju autentificēšanu saskaņā ar Direktīvas (ES) 2015/2366 97. panta 1. punktu, autentificēšanu balsta uz diviem vai vairākiem elementiem, kurus kategorizē kā zināšanas, valdījumu un neatņemamas īpašības un kuru rezultātā tiek ģenerēts autentifikācijas kods.

Maksājumu pakalpojumu sniedzējs autentifikācijas kodu pieņem tikai tad, kad maksātājs izmanto autentifikācijas kodu, lai piekļūtu savam maksājumu kontam tiešsaistē, sāktu elektronisku maksājuma darījumu vai veiktu kādu darbību, izmantojot attālinātu kanālu, kas varētu ietvert ar maksājumiem saistītas krāpšanas risku vai cita veida ļaunprātīgu rīcību.

2. Šā panta 1. punkta vajadzībām maksājumu pakalpojumu sniedzēji veic drošības pasākumus, lai nodrošinātu, ka ir izpildītas visas šādas prasības:

a) ja autentifikācijas kods tiek izpausts, no tā nevar izsecināt informāciju par kādu no 1. punktā minētajiem elementiem;

b) nav iespējams ģenerēt jaunu autentifikācijas kodu, pamatojoties uz informāciju par kādu citu iepriekš ģenerētu autentifikācijas kodu;

c) autentifikācijas kodu nevar viltot.

3. Maksājumu pakalpojumu sniedzēji nodrošina, ka autentifikācija, izmantojot autentifikācijas koda ģenerēšanu, ietver katru no turpmāk minētajiem pasākumiem:

a) ja attālinātas piekļuves, attālinātu elektronisko maksājumu un citu darbību autentifikācijas laikā, izmantojot attālinātu kanālu, kas varētu ietvert ar maksājumiem saistītas krāpšanas risku vai cita veida ļaunprātīgu rīcību, nav izdevies ģenerēt autentifikācijas kodu 1. punkta nolūkos, nav iespējams noteikt, kuri no šajā punktā minētajiem elementiem bija nepareizi;

b) neveiksmīgu pēc kārtas veiktu autentifikācijas mēģinājumu skaits, pēc kura Direktīvas (ES) 2015/2366 97. panta 1. punktā minētās darbības tiek uz laiku vai pastāvīgi bloķētas, nedrīkst pārsniegt piecus mēģinājumus noteiktā laika periodā;

c) saskaņā ar V nodaļas prasībām saziņas sesijas ir aizsargātas pret autentifikācijas laikā nosūtīto autentifikācijas datu pārtveršanu un pret nepiederīgu personu manipulācijām;

d) lai piekļūtu savam maksājumu kontam tiešsaistē, maksimālais maksātāja bezdarbības laiks pēc autentificēšanās nedrīkst pārsniegt piecas minūtes.

4. Ja 3. punkta b) apakšpunktā minētais bloks ir uz laiku, minētā bloka ilgumu un atkārtošanas iespēju skaitu nosaka, pamatojoties uz maksātājam sniegtā pakalpojuma iezīmēm un visiem attiecīgajiem iesaistītajiem riskiem, ņemot vērā vismaz 2. panta 2. punktā norādītos faktorus.

Maksātāju brīdina, pirms bloks kļūst pastāvīgs.

Ja bloks ir kļuvis pastāvīgs, ievieš drošu procedūru, kas maksātājam ļauj atgūt bloķētā elektronisko maksājumu instrumenta izmantojumu.

5. pants

Dinamiskā sasaiste

1. Ja maksājumu pakalpojumu sniedzēji piemēro drošu lietotāju autentificēšanu saskaņā ar Direktīvas (ES) 2015/2366 97. panta 2. punktu, papildus šīs regulas 4. panta prasībām tie pieņem arī drošības pasākumus, kas atbilst visām šādām prasībām:

a) maksātājs jāinformē par maksājumu darījuma summu un maksājuma saņēmēju;

b) ģenerētais autentifikācijas kods ir specifisks maksājumu darījuma summai un maksājuma saņēmējam, par kuru maksātājs ir vienojies, uzsākot darījumu;

c) maksājumu pakalpojumu sniedzēja pieņemtais autentifikācijas kods atbilst sākotnējai maksājumu darījuma specifiskajai summai un saņēmēja identitātei, par kuru maksātājs ir vienojies;

d) ja mainās summa vai maksājuma saņēmējs, ģenerētais autentifikācijas kods vairs nav spēkā.

2. Šā panta 1. punkta vajadzībām maksājumu pakalpojumu sniedzēji veic drošības pasākumus, kas nodrošina konfidencialitāti, autentiskumu un integritāti attiecībā uz:

a) darījuma summu un maksājuma saņēmēju visos autentifikācijas posmos;

b) informāciju, kas maksātājam redzama visu autentificēšanas posmu laikā, tostarp autentifikācijas koda ģenerēšanas, nosūtīšanas un izmantošanas laikā.

3. Šā panta 1. punkta b) apakšpunkta nolūkā un ja maksājumu pakalpojumu sniedzēji piemēro drošu lietotāju autentificēšanu saskaņā ar Direktīvas (ES) 2015/2366 97. panta 2. punktu, attiecībā uz autentifikācijas kodu piemēro šādas prasības:

a) attiecībā uz kartei piesaistītu maksājuma darījumu, kuram maksātājs ir devis piekrišanu attiecībā uz bloķējamo līdzekļu precīzu summu saskaņā ar minētās direktīvas 75. panta 1. punktu, autentifikācijas kods ir specifisks attiecībā uz summu, kuru maksātājs ir piekritis bloķēt un par kuru maksātājs ir vienojies, iniciējot darījumu;

b) attiecībā uz maksājumu darījumiem, kuriem maksātājs ir devis piekrišanu izpildīt partiju ar attālinātiem elektronisko maksājumu darījumiem ar vienu vai vairākiem maksājumu saņēmējiem, autentifikācijas kods ir specifisks maksājumu darījumu partijas kopsummai un konkrētajiem maksājumu saņēmējiem.

6. pants

Prasības attiecībā uz elementiem, kas kategorizēti kā zināšanas

1. Maksājumu pakalpojumu sniedzēji veic pasākumus, lai mazinātu risku, ka nepiederīgas personas atklāj vai tām tiek izpausti drošas lietotāju autentifikācijas elementi, kas kategorizēti kā zināšanas.

2. Maksātāja šo elementu izmantojumam piemēro mazinošus pasākumus, lai novērstu, ka elementi tiek izpausti neatļautām personām.

7. pants

Prasības attiecībā uz elementiem, kas kategorizēti kā turējums

1. Maksājumu pakalpojumu sniedzēji veic pasākumus, lai mazinātu risku, ka nepiederīgas personas atklāj vai tām tiek izpausti drošas lietotāju autentifikācijas elementi, kas kategorizēti kā turējums.

2. Maksātāja šo elementu izmantojumam piemēro pasākumus, kuru mērķis ir novērst elementu replicēšanu.

8. pants

Prasības attiecībā uz ierīcēm un programmatūru, kas saistīta ar elementiem, kuri kategorizēti kā neatņemamas īpašības

1. Maksājumu pakalpojumu sniedzēji veic pasākumus, lai mazinātu risku, ka nepiederīgas personas atklāj autentifikācijas elementus, kas kategorizēti kā neatņemamas īpašības un ko nolasa maksātājam sniegtās piekļuves iekārtas un programmatūra. Maksājumu pakalpojumu sniedzēji nodrošina vismaz to ka, ir ļoti neliela varbūtība, ka nepiederīga persona minētajās piekļuves ierīcēs un programmatūrā autentificējas kā maksātājs.

2. Maksātāja šo elementu izmantojumam piemēro pasākumus, ar ko nodrošina, ka minētās ierīces un programmatūra garantē aizsardzību pret elementu neatļautu izmantojumu, piekļūstot ierīcēm un programmatūrai.

9. pants

Elementu neatkarība

1. Maksājumu pakalpojumu sniedzēji nodrošina, ka drošas lietotāju autentificēšanas elementiem, kas minēti 6., 7. un 8. pantā, piemēro pasākumus, ar ko nodrošina, ka tehnoloģiju, algoritmu un parametru ziņā drošības plaisa vienā no elementiem neapdraud pārējo elementu uzticamību.

2. Maksājumu pakalpojumu sniedzēji pieņem drošības pasākumus, ja kāds no drošas lietotāju autentificēšanas elementiem vai pats autentifikācijas kods tiek izmantots daudzfunkcionālā ierīcē, lai mazinātu risku, kas rastos, ja šī daudzfunkcionālā ierīce tiktu kompromitēta.

3. 2. punkta nolūkos riska mazināšanas pasākumi ietver katru no šiem elementiem:

a) atdalītas, drošas izpildes vides izmantošana ar daudzfunkcionālajā ierīcē uzstādītas programmatūras starpniecību;

b) mehānismi, lai nodrošinātu, ka maksātājs vai trešā persona nav mainījuši programmatūru vai ierīci;

c) ja ir notikušas izmaiņas – mehānismi to seku mazināšanai.

III NODAĻA

ATBRĪVOJUMI NO PRASĪBAS PAR DOŠU LIETOTĀJU AUTENTIFICĒŠANU

10. pants

Maksājumu konta informācija

1. Maksājumu pakalpojumu sniedzējiem ir ļauts nepiemērot drošu lietotāju autentificēšanu, ja ir ievērotas 2. pantā un šā panta 2. punktā noteiktās prasības un ja maksājumu pakalpojumu lietotājs var piekļūt tikai vienam vai abiem no šiem posteņiem tiešsaistē, neizpaužot sensitīvus maksājumu datus:

a) viena vai vairāku noteiktu maksājumu kontu atlikums;

b) maksājumu darījumi, kas pēdējo 90 dienu laikā veikti, izmantojot vienu vai vairākus noteiktus maksājumu kontus.

2. Šā panta 1. punkta vajadzībām maksājumu pakalpojumu sniedzējiem nedrīkst piemērot atbrīvojumu no drošas lietotāju autentificēšanas, ja ir izpildīts kāds no šādiem nosacījumiem:

a) maksājumu pakalpojumu lietotājs pirmo reizi tiešsaistē piekļūst informācijai, kas minēta 1. punktā;

b) kopš pēdējās reizes, kad maksājumu pakalpojumu lietotājs tiešsaistē piekļuva informācijai, kas noteikta 1. punkta b) apakšpunktā, un izmantoja drošu lietotāja autentificēšanu, ir pagājušas vairāk nekā 90 dienas.

11. pants

Bezkontakta maksājumi tirdzniecības vietā

Maksājumu pakalpojumu sniedzējiem ir atļauts nepiemērot drošu lietotāja autentificēšanu (ja ir ievērotas 2. pantā noteiktās prasības) gadījumos, kad maksātājs iniciē bezkontakta elektronisko maksājumu darījumu, ar noteikumu, ka ir izpildīti šādi nosacījumi:

a) bezkontakta elektroniskā maksājumu darījuma atsevišķā vērtība nepārsniedz EUR 50; un

b) iepriekšējo bezkontakta elektronisko maksājumu darījumu, kas iniciēti ar maksājumu instrumentu, kam ir bezkontakta funkcionalitāte, kumulatīvā summa, skaitot no drošas lietotāju autentificēšanas pēdējā piemērošanas datuma, nepārsniedz EUR 150; vai

c) secīgo bezkontakta elektronisko maksājumu darījumu, kas iniciēti ar maksājumu instrumentu, kam ir bezkontakta funkcionalitāte, skaits kopš drošas lietotāju autentificēšanas pēdējās piemērošanas, nepārsniedz piecus.

12. pants

Neuzraudzīti maksājumu termināļi transporta maksām un stāvvietas izmantošanas maksām

Maksājumu pakalpojumu sniedzējiem ir atļauts nepiemērot drošu lietotāja autentificēšanu (ja ir nodrošināta atbilstība 2. pantā noteiktajām prasībām) gadījumos, kad maksātājs iniciē elektronisku maksājumu darījumu neuzraudzītā terminālī, lai samaksātu transporta maksu vai stāvvietas izmantošanas maksu.

13. pants

Uzticami saņēmēji

1. Maksājumu pakalpojumu sniedzēji piemēro drošu lietotāju autentificēšanu, ja maksātājs, izmantojot maksātāja kontu apkalpojošo maksājumu pakalpojumu sniedzēju, izveido vai groza sarakstu ar uzticamiem saņēmējiem.

2. Maksājumu pakalpojumu sniedzējiem ir atļauts nepiemērot drošu lietotāju autentificēšanu (ja ir ievērotas vispārīgās autentificēšanas prasības) gadījumā, kad maksātājs iniciē maksājumu darījumu un saņēmējs ir iekļauts uzticamo maksājumu saņēmēju sarakstā, ko iepriekš izveidojis maksātājs.

14. pants

Atkārtoti maksājumi

1. Maksājumu pakalpojumu sniedzēji piemēro drošu lietotāju autentificēšanu, ja maksātājs pirmo reizi rada, groza vai iniciē virkni atkārtotu darījumu ar vienādu summu un tam pašam maksājuma saņēmējam.

2. Maksājumu pakalpojumu sniedzējiem ir atļauts nepiemērot drošu lietotāju autentificēšanu (ja ir ievērotas vispārīgās autentificēšanas prasības), lai iniciētu visus pēctecīgos maksājumu darījumus, kas iekļauti 1. punktā minēto maksājumu darījumu sarakstā.

15. pants

Kredītpārvedumi starp vienas un tās pašas fiziskas vai juridiskas personas kontiem

Maksājumu pakalpojumu sniedzējiem ir atļauts nepiemērot drošu lietotāju autentificēšanu (ja ir ievērotas 2. pantā noteiktās prasības) gadījumā, kad maksātājs ierosina kredītpārvedumu apstākļos, kuros maksātājs un maksājuma saņēmējs ir viena un tā pati fiziska vai juridiska persona, un abus maksājumu kontus tur viens un tas pats kontu apkalpojošais maksājumu pakalpojumu sniedzējs.

16. pants

Zemas vērtības darījumi

Maksājumu pakalpojumu sniedzējiem ir atļauts nepiemērot drošu lietotāja autentificēšanu gadījumos, kad maksātājs iniciē attālinātu elektronisko maksājumu darījumu, ja ir izpildīti šādi nosacījumi:

a) elektroniskā maksājumu darījuma vērtība nepārsniedz EUR 30; un

b) iepriekšējo attālinātu elektronisko maksājumu darījumu, kurus maksātājs iniciējis kopš pēdējās drošas lietotāju autentificēšanas izmantošanas, kumulatīvā vērtība nepārsniedz EUR 100; vai

c) iepriekšējo attālinātu elektronisko maksājumu darījumu, kurus maksātājs iniciējis kopš pēdējās drošas lietotāju autentificēšanas izmantošanas, skaits nepārsniedz piecus secīgus, atsevišķus attālinātos elektronisko maksājumu darījumus.

17. pants

Droši korporatīvo maksājumu procesi un protokoli

Maksājumu pakalpojumu sniedzējiem ir atļauts nepiemērot drošu lietotāju autentificēšanu attiecībā uz juridiskajām personām, kas iniciē elektronisko maksājumu darījumus, izmantojot specializētus maksāšanas procesus vai protokolus, kas ir pieejami tikai tiem maksātājiem, kas nav patērētāji, ja kompetentās iestādes ir pārliecinātas, ka šie procesi vai protokoli nodrošina vismaz līdzvērtīgu drošības līmeni tam, kas paredzēts Direktīvā (ES) 2015/2366.

18. pants

Darījuma riska analīze

1. Maksājumu pakalpojumu sniedzējiem ir atļauts nepiemērot drošu lietotāju autentificēšanu, ja maksātājs iniciē attālinātu elektronisku maksājumu darījumu, ko maksājumu pakalpojumu sniedzējs identificē kā tādu, kas rada zemu riska līmeni saskaņā ar darījumu uzraudzības mehānismiem, kas minēti 2. pantā un šā panta 2. punkta c) apakšpunktā.

2. Elektronisku maksājuma darījumu, kas minēts 1. punktā, uzskata par tādu, kas rada zema līmeņa risku, ja ir izpildīti visi šādi nosacījumi:

a) attiecībā uz šāda veida darījumu krāpšanas līmenis, par ko maksājumu pakalpojumu sniedzējs ziņo un kas aprēķināts saskaņā ar 19. pantu, ir vienāds ar krāpšanas atsauces koeficientu, kas norādītas pielikuma tabulā "attālināti, elektroniski, kartēm piesaistīti maksājumi" un "attālināti, elektroniski kredītpārvedumi", vai zemāks par to;

b) darījuma summa nepārsniedz attiecīgo atbrīvojuma robežvērtību ("AR"), kas norādīta pielikuma tabulā;

c) maksājumu pakalpojumu sniedzēji reāllaika riska analīzes rezultātā nav konstatējuši nevienu no šādām iezīmēm:

   i) anormāli tēriņi vai maksātāja uzvedības modelis;

   ii) neparasta informācija par maksātāja piekļuves ierīci/programmatūru;

   iii) ļaunprogrammatūras infekcija kādā autentifikācijas procedūru sesijā;

   iv) zināms krāpšanas scenārijs maksājumu pakalpojumu sniegšanā;

   v) anormāla maksātāja atrašanās vieta;

   vi) maksātāja atrašanās vieta ir augsta riska vieta.

3. Maksājumu pakalpojumu sniedzēji, kas plāno elektroniskiem attālinātajiem maksājumu darījumiem piemērot atbrīvojumu no drošas lietotāju autentificēšanas, pamatojoties uz to, ka tie rada nelielu risku, ņem vērā vismaz šādus riska faktorus:

a) atsevišķā maksājumu pakalpojumu lietotāja tēriņu modelis;

b) katra maksājumu pakalpojumu sniedzēja maksājumu pakalpojumu lietotāja maksājumu darījumu vēsture;

c) maksātāja un maksājuma saņēmēja atrašanās vieta maksājumu darījuma brīdī gadījumos, kad maksājumu pakalpojumu sniedzējs nodrošina piekļuves ierīci vai programmatūru;

d) maksājumu pakalpojumu lietotāja anormāla maksājumu modeļa apzināšana lietotāja maksājumu darījumu vēsturē.

Maksājumu pakalpojumu sniedzēja izvērtējumā visus šos riska faktorus apvieno riska novērtējumā par katru atsevišķo darījumu, lai noteiktu, vai konkrēts maksājums būtu jāatļauj bez drošas lietotāju autentificēšanas.

19. pants

Krāpšanas koeficientu aprēķināšana

1. Katram darījumu veidam, kas minēts pielikuma tabulā, maksājumu pakalpojumu sniedzējs nodrošina, ka kopējais krāpšanas koeficients, kas attiecas gan uz maksājumu darījumiem, kuri autentificēti ar drošu lietotāju autentificēšanu, gan tie, kuri veikti saskaņā ar kādu no 13. līdz 18. pantā minētajiem atbrīvojumiem, ir līdzvērtīgs vai zemāks par krāpšanas atsauces koeficientu tāda paša veida maksājumu darījumam, kas norādīts pielikuma tabulā.

Kopējo krāpšanas koeficientu katram darījumu veidam aprēķina kā neatļautu vai krāpniecisku attālināto maksājumu darījumu kopējo vērtību (neatkarīgi no tā, vai līdzekļi ir atgūti vai nē), kas dalīta ar kopējo vērtību visiem tāda paša veida attālinātajiem maksājumu darījumiem (neatkarīgi no tā, vai tie autentificēti, piemērojot drošu klientu autentificēšanu, vai izpildīti saskaņā ar 13. līdz 18. pantā minētajiem atbrīvojumiem), katru ceturksni (90 dienas).

2. Krāpšanas koeficientu aprēķinu un izrietošos skaitļus novērtē 3. panta 2. punktā minētajā revīzijas pārbaudē, kurā pārliecinās, ka rādītāji un skaitļi ir pilnīgi un precīzi.

3. Metodoloģiju un modeli, ko maksājumu pakalpojumu sniedzējs izmanto, lai aprēķinātu krāpšanas koeficientus, kā arī pašus krāpšanas koeficientus, pienācīgi dokumentē un dara pilnībā pieejamus kompetentajām iestādēm un EBI, iepriekš nosūtot paziņojumu attiecīgajai kompetentajai iestādei vai kompetentajām iestādēm pēc to pieprasījuma.

20. pants

Uz darījumu riska analīzes balstītu atbrīvojumu piemērošanas pārtraukšana

1. Maksājumu pakalpojumu sniedzēji, kas izmanto 18. pantā minēto atbrīvojumu, nekavējoties ziņo kompetentajām iestādēm, ja kāds no viņu uzraudzītajiem krāpšanas koeficientiem attiecībā uz jebkādu pielikuma tabulā norādīto maksājumu darījumu veidu pārsniedz piemērojamo krāpšanas atsauces koeficientu, un kompetentajām iestādēm iesniedz aprakstu par pasākumiem, kurus tie plāno pieņemt, lai atjaunotu to uzraudzīto krāpšanas koeficientu atbilstību piemērojamajiem krāpšanas atsauces koeficientiem.

2. Maksājumu pakalpojumu sniedzēji nekavējoties pārtrauc izmantot 18. pantā minēto atbrīvojumu attiecībā uz visu veidu maksājumu darījumiem, kas norādīti pielikuma tabulā īpašo atbrīvojuma robežvērtību diapazonā, ja to uzraudzītie krāpšanas koeficienti divus ceturkšņus pēc kārtas pārsniedz krāpšanas atsauces koeficientu, ko piemēro attiecīgajam maksājuma instrumentam vai maksājumu darījumu veidam attiecīgajā atbrīvojuma robežvērtību diapazonā.

3. Pēc 18. pantā minētā atbrīvojuma piemērošanas pārtraukšanas saskaņā ar šā panta 2. punktu maksājumu pakalpojumu sniedzēji minēto atbrīvojumu nedrīkst atkal izmantot, līdz to aprēķinātais krāpšanas koeficients vienu ceturksni ir vienāds ar krāpšanas atsauces koeficientu, ko piemēro šāda veida darījumiem attiecīgajā atbrīvojuma robežvērtību diapazonā, vai zemāks par to.

4. Ja maksājumu pakalpojumu sniedzējs plāno atkal izmantot 18. pantā minēto atbrīvojumu, tas saprātīgā termiņā par to paziņo kompetentajām iestādēm, un pirms atbrīvojuma atkārtotas izmantošanas iesniedz pierādījumus par to, ka uzraudzītā krāpšanas koeficienta atbilstība attiecīgā atbrīvojuma robežvērtību diapazonā piemērojamajam krāpšanas koeficientam ir atjaunota saskaņā ar šā panta 3. punktu.

21. pants

Uzraudzība

1. Lai izmantotu 10. līdz 18. pantā noteiktos atbrīvojumus, maksājumu pakalpojumu sniedzēji vismaz reizi ceturksnī reģistrē un uzrauga šādus datus par katru maksājumu darījumu veidu, norādot gan attālinātos, gan neattālinātos maksājumu darījumus:

a) kopējā vērtība neatļautiem vai krāpnieciskiem maksājumu darījumiem saskaņā ar Direktīvas (ES) 2015/2366 64. panta 2. punktu, kopējā vērtība visiem maksājumu darījumiem un izrietošais krāpšanas koeficients, tostarp tādu maksājumu darījumu sadalījums, kas iniciēti, izmantojot drošu lietotāju autentificēšanu un saskaņā ar katru no atbrīvojumiem;

b) vidējā darījumu vērtība, tostarp tādu maksājumu darījumu sadalījums, kas iniciēti, izmantojot drošu lietotāju autentificēšanu un saskaņā ar katru no atbrīvojumiem;

c) maksājumu darījumu skaits, kuros piemērots katrs atbrīvojums, un to procentuālā daļa attiecībā pret maksājumu darījumu kopskaitu.

2. Maksājumu pakalpojumu sniedzēji uzraudzības rezultātus saskaņā ar 1. punktu dara pieejamus kompetentajām iestādēm un EBI, pēc to pieprasījuma iepriekš nosūtot paziņojumu attiecīgajai kompetentajai iestādei vai kompetentajām iestādēm.

IV NODAĻA

MAKSĀJUMU PAKALPOJUMU LIETOTĀJU PERSONALIZĒTO DROŠĪBAS DATU KONFIDENCIALITĀTE UN INTEGRITĀTE

22. pants

Vispārīgas prasības

1. Maksājumu pakalpojumu sniedzēji nodrošina maksājumu pakalpojumu lietotāja personalizēto drošības datu, tostarp autentificēšanas kodu, konfidencialitāti un integritāti visos autentifikācijas posmos.

2. Šā panta 1. punkta vajadzībām maksājumu pakalpojumu sniedzēji nodrošina, ka ir izpildītas visas šādas prasības:

a) personalizētie drošības dati uz displeja ir anonimizēti un nav salasāmi pilnā apjomā, kad maksājumu pakalpojumu lietotājs tos ievada autentificēšanas laikā;

b) personalizēti drošības dati datu formātā, kā arī kriptogrāfiska informācija saistībā ar personalizēto drošības datu šifrēšanu netiek glabāta nešifrētā tekstā;

c) slepena kriptogrāfiska informācija ir aizsargāta no neatļautas izpaušanas.

3. Maksājumu pakalpojumu sniedzēji pilnībā dokumentē procesu saistībā ar tādas kriptogrāfiskas informācijas pārvaldību, ko izmanto, lai šifrētu vai kā citādi padarītu par nesalasāmiem personalizētos drošības datus.

4. Maksājumu pakalpojumu sniedzēji nodrošina, ka personalizēto drošības datu un saskaņā ar II nodaļu ģenerēto autentificēšanas kodu maršrutēšana un apstrāde notiek drošā vidē saskaņā ar spēcīgiem un plaši atzītiem nozares standartiem.

23. pants

Personīgo drošības datu izveide un nosūtīšana

Maksājumu pakalpojumu sniedzēji nodrošina, ka personīgo drošības datu izveide notiek drošā vidē.

Tie mazina riskus, kas saistīti ar personalizēto drošības datu un autentificēšanas ierīču un programmatūras neatļautu izmantošanu nozaudēšanas, zādzības vai kopēšanas gadījumā pirms to piegādes maksātājam.

24. pants

Saistīšana ar maksājumu pakalpojumu lietotāju

1. Maksājumu pakalpojumu sniedzēji nodrošina, ka tikai maksājumu pakalpojumu lietotājs ir drošā veidā saistīts ar personalizētajiem drošības datiem, autentifikācijas ierīcēm un programmatūru.

2. Šā panta 1. punkta vajadzībām maksājumu pakalpojumu sniedzēji nodrošina, ka ir izpildītas visas šādas prasības:

a) maksājumu pakalpojumu lietotāja identitātes saistīšana ar personalizētajiem drošības datiem, autentifikācijas ierīcēm un programmatūru tiek veikta drošā vidē, kas saskaņā ar maksājumu pakalpojumu sniedzēja atbildību sastāv vismaz no maksājumu pakalpojumu sniedzēja telpām, maksājumu pakalpojumu sniedzēja nodrošinātas interneta vides vai citas līdzīgas drošas tīmekļa vietnes, ko izmanto maksājumu pakalpojumu sniedzējs un tā bankomātu pakalpojumi, un ņemot vērā riskus, kas saistīti ar ierīcēm un sastāvdaļām, ko izmanto sasaistīšanas procesa laikā un par ko neatbild maksājumu pakalpojumu sniedzējs;

b) maksājumu pakalpojuma lietotāja identitātes sasaistīšanu, izmantojot attālinātu kanālu, ar personalizētajiem drošības datiem un autentifikācijas ierīcēm vai programmatūru veic, izmantojot lietotāju autentificēšanu.

25. pants

Personalizēto drošības datu, autentifikācijas ierīču un programmatūras piegāde

1. Maksājumu pakalpojumu sniedzēji nodrošina, ka personalizētie drošības dati, autentifikācijas ierīces un programmatūra, maksājumu pakalpojumu lietotājam tiek piegādāta drošā veidā, lai novērstu riskus saistībā ar to neatļautu izmantošanu pazaudēšanas, zādzības vai kopēšanas gadījumā.

2. Šā panta 1. punkta vajadzībām maksājumu pakalpojumu sniedzēji piemēro vismaz katru no šiem pasākumiem:

a) efektīvi un droši piegādes mehānismi, ar ko nodrošina, ka personalizētie drošības dati, autentifikācijas ierīces un programmatūra tiek piegādāta likumīgajam maksājumu pakalpojumu lietotājam;

b) mehānismi, kas dod iespēju maksājumu pakalpojumu sniedzējam pārbaudīt maksājumu pakalpojumu lietotājam pa internetu piegādātās autentifikācijas programmatūras autentiskumu;

c) pasākumi, ar ko nodrošina, ka gadījumā, ja personalizēto drošības datu piegāde notiek ārpus maksājumu pakalpojumu sniedzēja telpām vai izmantojot attālinātu kanālu:

   i) nepiederošas personas nevar iegūt vairāk nekā vienu personalizēto drošības datu, autentifikācijas ierīces vai programmatūras iezīmi, ja to piegādā, izmantojot to pašu kanālu;

   ii) piegādātie personalizētie drošības dati, autentifikācijas ierīces vai programmatūras pirms izmantošanas ir jāaktivizē;

d) pasākumi, ar ko nodrošina, ka gadījumos, kad personalizētie drošības dati, autentifikācijas ierīces vai programmatūra ir jāaktivizē pirms to pirmās izmantošanas, aktivizācija notiek drošā vidē saskaņā ar 24. pantā minēto procedūru.

26. pants

Personalizēto drošības datu atjaunošana

Maksājumu pakalpojumu sniedzēji nodrošina, ka personalizēto drošības datu atjaunošana vai atkārtota aktivizācija atbilst personīgo drošības datu un autentifikācijas ierīču izveides, saistīšanas un piegādes procedūrām saskaņā ar 23., 24. un 25. pantu.

27. pants

Iznīcināšana, deaktivizācija un atsaukšana

Maksājumu pakalpojumu sniedzēji nodrošina, ka tiem ir efektīvi procesi, lai piemērotu katru no šādiem drošības pasākumiem:

a) personalizēto drošības datu, autentifikācijas ierīču un programmatūras droša iznīcināšana, dezaktivēšana vai atsaukšana;

b) ja maksājumu pakalpojumu sniedzējs izplata atkārtoti izmantojamas autentifikācijas ierīces un programmatūru, ierīces vai programmatūras drošu atkārtotu izmantošanu nosaka, dokumentē un īsteno, pirms tās dara pieejamas citam maksājumu pakalpojumu lietotājam;

c) informācijas, kas saistīta personalizēto drošības datu, kas tiek glabāti maksājumu pakalpojumu sniedzēja sistēmās un datubāzēs, un attiecīgā gadījumā valsts reģistros, dezaktivēšana vai atsaukšana.

V NODAĻA

KOPĪGI UN DROŠI ATKLĀTI SAZIŅAS STANDARTI

1. iedaļa

Vispārīgas prasības attiecībā uz saziņu

28. pants

Prasības par identifikāciju

1. Maksājumu pakalpojumu sniedzēji nodrošina drošu identifikāciju saziņā starp maksātāja ierīci un maksājuma saņēmēja elektronisko maksājumu pieņemšanas ierīcēm, tostarp (bet ne tikai) maksājumu termināliem.

2. Maksājumu pakalpojumu sniedzēji nodrošina, ka tiek efektīvi mazināts risks, ka mobilajās lietotnēs un citās maksājumu pakalpojumu lietotāju saskarnēs, kas piedāvā elektronisko maksājumu pakalpojumus, saziņa tiks nepareizi novirzīta nepiederīgām personām.

29. pants

Izsekojamība

1. Maksājumu pakalpojumu sniedzējiem ir procesi, ar ko nodrošināt, ka visi maksājumu darījumi un citas mijiedarbības ar maksājumu pakalpojumu lietotāju, citiem maksājumu pakalpojumu sniedzējiem un citām struktūrām, tostarp tirgotājiem, saistībā ar maksājumu pakalpojumu sniegšanu ir izsekojamas, nodrošinot *ex post* informāciju par visiem pasākumiem, kas ir būtiski elektroniskajam darījumam visās stadijās.

2. Šā panta 1. punkta vajadzībām maksājumu pakalpojumu sniedzēji nodrošina, ka visas saziņas sesijas ar maksājumu pakalpojumu lietotāju, citiem maksājumu pakalpojumu sniedzējiem un citām struktūrām, tostarp tirgotājiem, ir balstītas uz visu turpmāk minēto:

a) unikāls sesijas identifikators;

b) drošības mehānismi, lai detalizēti reģistrētu darījumu, ieskaitot darījuma numuru, laika zīmogus un visus attiecīgos datus par darījumu;

c) laika zīmogi, kas balstās uz vienotu laika atsauces sistēmu un kas ir sinhronizēti saskaņā ar oficiālu laika signālu.

2. iedaļa

Īpašas prasības kopīgiem un drošiem atklātiem saziņas standartiem

30. pants

Vispārīgi pienākumi piekļuvei saskarnēm

1. Kontu apkalpojošiem maksājumu pakalpojumu sniedzējiem, kas maksātājam piedāvā tiešsaistē pieejamu maksājumu kontu, ir vismaz viena saskarne, kas atbilst visām šādām prasībām:

a) konta informācijas pakalpojumu sniedzēji, maksājumu iniciēšanas pakalpojumu sniedzēji un maksājumu pakalpojumu sniedzēji, kas izdod kartei piesaistītus maksājumu instrumentus, var sevi identificēt kontu apkalpojošajam maksājumu pakalpojumu sniedzējam;

b) konta informācijas pakalpojumu sniedzēji spēj droši sazināties, lai pieprasītu un saņemtu informāciju par vienu vai vairākiem maksājumu kontiem un saistītiem maksājumu darījumiem;

c) maksājumu iniciēšanas pakalpojumu sniedzēji spēj droši sazināties, lai iniciētu maksājuma uzdevumu no maksātāja maksājumu konta un saņemtu visu informāciju par maksājumu darījuma uzsākšanu un visu informāciju, kas kontu apkalpojošajam maksājumu pakalpojumu sniedzējiem pieejama saistībā ar maksājumu darījuma izpildi.

2. Lai autentificētu maksājumu pakalpojuma lietotāju, 1. punktā minētā saskarne nodrošina, ka konta informācijas pakalpojumu sniedzēji un maksājumu iniciēšanas pakalpojumu sniedzēji var paļauties uz visām autentifikācijas procedūrām, kuras kontu apkalpojošais maksājumu pakalpojumu sniedzējs piedāvā maksājumu pakalpojumu lietotājam.

Saskarnes atbilst vismaz visām šādām prasībām:

a) maksājumu iniciēšanas pakalpojumu sniedzējs vai konta informācijas pakalpojumu sniedzējs spēj kontu apkalpojošajam maksājumu pakalpojumu sniedzējam dot norādījumus sākt autentifikāciju, pamatojoties uz maksājumu pakalpojumu lietotāja piekrišanu;

b) saziņas sesijas starp kontu apkalpojošajiem maksājumu pakalpojumu sniedzējiem, konta informācijas pakalpojumu sniedzēju, maksājumu iniciēšanas pakalpojumu sniedzēju un jebkuru attiecīgo maksājumu pakalpojumu lietotāju izveido un uztur ar autentifikācijas starpniecību;

c) nodrošina personalizēto drošības datu un maksājumu iniciēšanas pakalpojumu sniedzēja vai konta informācijas pakalpojumu sniedzēja (vai caur to) nosūtīto autentifikācijas kodu integritāti un konfidencialitāti.

3. Kontu apkalpojošie maksājumu pakalpojumu sniedzēji nodrošina, ka to saskarnēs tiek izmantoti saziņas standarti, ko izdevušas starptautiska vai Eiropas mēroga standartizācijas organizācijas.

Kontu apkalpojošie maksājumu pakalpojumu sniedzēji nodrošina arī to, ka visu saskarņu tehniskās specifikācijas tiek dokumentētas, precizējot režīmu, protokolu un instrumentu kopumu, kas vajadzīgi maksājumu iniciēšanas pakalpojumu sniedzējiem, konta informācijas pakalpojumu sniedzējiem un maksājumu pakalpojumu sniedzējiem, kas izdod kartei piesaistītus maksājumu instrumentus, lai to programmatūras un lietojumprogrammas būtu sadarbspējīgas ar kontu apkalpojošo maksājumu pakalpojumu sniedzēju sistēmām.

Kontu apkalpojošie maksājumu pakalpojumu sniedzēji vismaz vienu un ne mazāk kā sešus mēnešus pirms pieteikuma iesniegšanas datuma, kas minēts 38. panta 2. punktā, vai pirms mērķa datuma, kurā paredzēts laist tirgū piekļuves saskarni, ja laišana tirgū notiek pēc 38. panta 2. punktā minētās dienas, bez maksas un pēc atļauju saņēmušu maksājumu iniciēšanas pakalpojumu sniedzēju, konta informācijas pakalpojumu sniedzēju un maksājumu pakalpojumu sniedzēju, kas izdod kartei piesaistītus maksājumu instrumentus, vai maksājumu pakalpojumu sniedzēju, kuri ir pieteikušies savās kompetentajās iestādēs, lai saņemtu attiecīgo atļauju, pieprasījuma dara pieejamu dokumentāciju un minētās dokumentācijas kopsavilkumu dara publiski pieejamu savā tīmekļa vietnē.

4. Papildus 3. punktā noteiktajam kontu apkalpojošie maksājumu pakalpojumu sniedzēji nodrošina, ka, izņemot ārkārtas situācijās, visas izmaiņas to saskarnes tehniskajā specifikācijā ir iepriekš, pēc iespējas drīz un ne vēlāk kā trīs mēnešus pirms izmaiņu ieviešanas pieejamas atļauju saņēmušiem maksājumu iniciēšanas pakalpojumu sniedzējiem, konta informācijas pakalpojumu sniedzējiem un maksājumu pakalpojumu sniedzējiem, kas izdod kartei piesaistītus maksājumu instrumentus, vai maksājumu pakalpojumu sniedzējiem, kuri ir pieteikušies savās kompetentajās iestādēs, lai saņemtu attiecīgo atļauju.

Maksājumu pakalpojumu sniedzēji dokumentē ārkārtas situācijas, kurās izmaiņas tika īstenotas, un dokumentāciju dara pieejamu kompetentajām iestādēm pēc to pieprasījuma.

5. Kontu apkalpojošie maksājumu pakalpojumu sniedzēji dara pieejamu testēšanas mehānismu, tostarp atbalstu, pieslēguma un funkcionālai testēšanai, lai atļauju saņēmuši maksājumu iniciēšanas pakalpojumu sniedzēji, maksājumu pakalpojumu sniedzēji, kas izdod kartei piesaistītus maksājumu instrumentus, un konta informācijas pakalpojumu sniedzēji vai maksājumu pakalpojumu sniedzēji, kuri ir pieteikušies uz attiecīgo atļauju, varētu pārbaudīt savu programmatūru un lietojumprogrammas, ko izmanto, lai lietotājiem piedāvātu maksājumu pakalpojumus. Šis testēšanas mehānisms būtu jādara pieejams ne vēlāk kā sešus mēnešus pirms pieteikuma iesniegšanas datuma, kas minēts 38. panta 2. punktā, vai pirms mērķa datuma, kurā paredzēts laist tirgū piekļuves saskarni, ja tirgū laišanas diena ir pēc 38. panta 2. punktā minētās dienas.

Tomēr caur testēšanas mehānismu nedrīkst apmainīties ar jutīgu informāciju.

6. Kompetentās iestādes nodrošina, ka kontu apkalpojošie maksājumu pakalpojumu sniedzēji vienmēr ievēro pienākumus, kuri noteikti minētajos standartos attiecībā uz saskarni(-ēm), ko tie ievieš. Gadījumā, ja kontu apkalpojošais maksājumu pakalpojumu sniedzējs neizpilda prasības, kas attiecībā uz saskarnēm noteiktas minētajos standartos, kompetentās iestādes nodrošina, ka maksājumu iniciēšanas pakalpojumu un konta informācijas pakalpojumu sniegšana netiek kavēta vai traucēta, ciktāl attiecīgie šādu pakalpojumu sniedzēji atbilst nosacījumiem, kas noteikti saskaņā ar 33. panta 5. punktu.

31. pants

Piekļuves saskarnes opcijas

Kontu apkalpojošie maksājumu pakalpojumu sniedzēji izveido 30. pantā minēto saskarni(-es), izmantojot specializētu saskarni vai ļaujot 30. panta 1. punktā minētajiem maksājumu pakalpojumu sniedzējiem izmantot saskarnes, kas lietotas kontu apkalpojošo maksājumu pakalpojumu sniedzēju un maksājumu pakalpojumu lietotāju autentificēšanai un saziņai ar tiem.

32. pants

Pienākumi saistībā ar specializētu saskarni

1. Ja ir ievērots 30. un 31. pants, kontu apkalpojošie maksājumu pakalpojumu sniedzēji, kas ir ieviesuši specializētu saskarni, nodrošina, ka specializētā saskarne vienmēr ir tik pat pieejama un darbspējīga (tostarp sniedz atbalstu) kā saskarnes, kas maksājumu pakalpojumu lietotājam darītas pieejamas tiešai piekļuvei tā maksājumu kontam tiešsaistē.

2. Kontu apkalpojošie maksājumu pakalpojumu sniedzēji, kas ir ieviesuši specializētu saskarni, nosaka pārredzamus galvenos darbības rādītājus un pakalpojumu līmeņa mērķus, kuri gan pieejamības ziņā un attiecībā uz datiem, kas iesniegti saskaņā ar 36. pantu, ir vismaz tikpat stingri kā tie, kas noteikti saskarnei, ko izmanto to maksājumu pakalpojumu lietotāji. Kompetentās iestādes šīs saskarnes, rādītājus un mērķus uzrauga un pakļauj stresa testiem.

3. Kontu apkalpojošie maksājumu pakalpojumu sniedzēji, kas ir ieviesuši specializētu saskarni, nodrošina, ka šī saskarne nerada šķēršļus maksājumu iniciēšanas un konta informācijas pakalpojumu nodrošināšanai. Šādi šķēršļi citstarp var ietvert šķērsli 30. panta 1. punktā minētajiem maksājumu pakalpojumu sniedzējiem izmantot personalizētos drošības datus, ko kontu apkalpojošie maksājumu pakalpojumu sniedzēji ir izsnieguši saviem lietotājiem, liekot pārorientēties uz kontu apkalpojošā maksājumu pakalpojumu sniedzēja autentifikāciju vai citām funkcijām, kam nepieciešamas papildu atļaujas un reģistrācija papildus tam, kas paredzēts Direktīvas (ES) 2015/2366 11., 14. un 15. pantā, vai pieprasot papildu pārbaudes par piekrišanu, ko maksājumu pakalpojumu lietotāji devuši maksājumu iniciēšanas un konta informācijas pakalpojumu sniedzējiem.

4. Šā panta 1. un 2. punkta nolūkā kontu apkalpojošie maksājumu pakalpojumu sniedzēji uzrauga specializētās saskarnes pieejamību un veiktspēju. Kontu apkalpojošie maksājumu pakalpojumu sniedzēji savā tīmekļa vietnē publicē ceturkšņa statistiku par specializētās saskarnes un to maksājumu pakalpojumu lietotāju izmantotās saskarnes pieejamību un veiktspēju.

33. pants

Ārkārtas pasākumi specializētai saskarnei

1. Kontu apkalpojošie maksājumu pakalpojumu sniedzēji, izstrādājot specializēto saskarni, ietver ārkārtas pasākumu stratēģiju un plānus gadījumam, ja saskarne nedarbojas saskaņā ar 32. pantu, ja saskarne neplānoti ir nepieejama un ja notiek sistēmas pārrāvums. Pieņem, ka neplānota nepieejamība vai sistēmas pārrāvums ir notikuši, ja uz pieciem secīgiem pieprasījumiem par piekļuvi informācijai, lai snigtu maksājumu iniciēšanas pakalpojumus vai konta informācijas pakalpojumus, nav atbildēts 30 sekunžu laikā.

2. Ārkārtas pasākumi ietver saziņas plānus, lai maksājumu pakalpojumu sniedzējus, kas izmanto specializēto saskarni, informētu par pasākumiem, ar ko atjaunot sistēmu, un aprakstu par nekavējoties pieejamām alternatīvām iespējām, kas maksājumu pakalpojumu sniedzējiem var būt pieejamas attiecīgajā brīdī.

3. Gan kontu apkalpojošais maksājumu pakalpojumu sniedzējs, gan 30. panta 1. punktā minētie maksājumu pakalpojumu sniedzēji savām attiecīgajām kompetentajām valsts iestādēm nekavējoties ziņo par problēmām saistībā ar specializētajām saskarnēm, kā aprakstīts 1. punktā.

4. Ārkārtas pasākumu mehānisma ietvaros 30. panta 1. punktā minētajiem maksājumu pakalpojumu sniedzējiem ir atļauts izmantot saskarnes, kas darītas pieejamas maksājumu pakalpojumu lietotājiem, lai tie autentificētos un sazinātos ar savu kontu apkalpojošo maksājumu pakalpojumu sniedzēju, līdz specializētās saskarnes pieejamība un veiktspēja tiek atjaunota līmenī, kas paredzēts 32. pantā.

5. Šajā nolūkā kontu apkalpojošais maksājumu pakalpojumu sniedzējs nodrošina, ka 30. panta 1. punktā minētos maksājumu pakalpojumu sniedzējus var identificēt un ka tie var paļauties uz autentifikācijas procedūrām, kuras kontu apkalpojošais maksājumu pakalpojumu sniedzējs ir nodrošinājis maksājumu pakalpojumu lietotājam. Ja 30. panta 1. punktā minētie maksājumu pakalpojumu sniedzēji izmanto 4. punktā minēto saskarni, tie:

a) veic vajadzīgos pasākumus, lai nodrošinātu, ka tiem nav piekļuves, uzglabā vai apstrādā datus citos nolūkos nekā pakalpojuma sniegšana, kā to pieprasījis maksājumu pakalpojumu lietotājs;

b) turpina izpildīt saistības, kas izriet no attiecīgi Direktīvas (ES) 2015/2366 66. panta 3. punkta un 67. panta 2. punkta;

c) reģistrē datus, kam piekļūts, izmantojot saskarni, ko uztur kontu apkalpojošais maksājumu pakalpojumu sniedzējs saviem maksājumu pakalpojumu lietotājiem, un pēc pieprasījuma un bez liekas kavēšanās iesniedz žurnālfailus savai kompetentajai valsts iestādei;

d) savai kompetentajai valsts iestādei pēc pieprasījuma un bez nepamatotas kavēšanās pienācīgi pamato saskarnes, kas darīta pieejama maksājumu pakalpojumu lietotājiem, izmantošanu, lai tieši piekļūtu savam maksājumu kontam tiešsaistē;

e) attiecīgi informē kontu apkalpojošo maksājumu pakalpojumu sniedzēju.

6. Kompetentās iestādes pēc apspriešanās ar EBI, lai nodrošinātu šādu nosacījumu konsekventu piemērošanu, atbrīvo kontu apkalpojošos maksājumu pakalpojumu sniedzējus, kuri ir izvēlējušies specializēto saskarni, no pienākuma izveidot 4. punktā aprakstīto ārkārtas mehānismu, ja specializētā saskarne atbilst visiem šādiem nosacījumiem:

a) tā atbilst visiem 32. pantā specializētām saskarnēm paredzētajiem noteikumiem;

b) tā ir izstrādāta un testēta saskaņā ar 30. panta 5. punktu par labu maksājumu pakalpojumu sniedzējiem, kas minēti pantā;

c) maksājumu pakalpojumu sniedzēji to ir plaši izmantojuši vismaz trīs mēnešu garumā, lai sniegtu konta informācijas pakalpojumu un maksājumu iniciēšanas pakalpojumu un lai sniegtu apstiprinājumu par naudas līdzekļu pieejamību uz kartēm piesaistītiem maksājumiem;

d) visas problēmas, kas saistītas ar specializēto saskarni, ir atrisinātas bez liekas kavēšanās.

7. Kompetentās iestādes atsauc 6. punktā minēto atbrīvojumu, ja kontu apkalpojošais maksājumu pakalpojumu sniedzējs vairāk nekā divas secīgas kalendārās nedēļas nav izpildījis a) un d) apakšpunkta nosacījumus. Kompetentās iestādes informē EBI par šo atcelšanu un nodrošina, ka kontu apkalpojošais maksājumu pakalpojumu sniedzējs pēc iespējas īsākā termiņā un vēlākais divu mēnešu laikā izveido ārkārtas mehānismu, kas minēts 4. punktā.

34. pants

Sertifikāti

1. Identifikācijas nolūkā, kā minēts 30. panta 1. punkta a) apakšpunktā, maksājumu pakalpojumu sniedzēji kā elektroniskos zīmogus izmanto kvalificētus sertifikātus, kā minēts Regulas (ES) Nr. 910/2014 3. panta 30. punktā, vai tīmekļa vietņu autentifikācijai, kā noteikts minētās regulas 3. panta 39. punktā.

2. Šīs regulas nolūkā reģistrācijas numurs, kā norādīts oficiālos reģistros saskaņā ar Regulas (ES) Nr. 910/2014 III pielikuma c) punktu vai IV pielikuma c) punktu, ir maksājumu pakalpojumu sniedzēja, kas izdod kartei piesaistītus maksājumu instrumentus, konta informācijas pakalpojumu sniedzēju un maksājumu iniciēšanas pakalpojumu sniedzēju, tostarp kontu apkalpojošo maksājumu pakalpojumu sniedzēju, kas sniedz šādus pakalpojumus, atļaujas numurs, kas saskaņā ar Direktīvas (ES) 2015/2366 14. pantu pieejams izcelsmes dalībvalsts publiskajā reģistrā vai kas izriet no paziņojumiem par katru atļauju, kas piešķirta saskaņā ar Eiropas Parlamenta un Padomes Direktīvas 2013/36/ES 8. pantu ([1]) atbilstīgi minētās direktīvas 20. pantam.

3. Šīs regulas nolūkos kvalificēti sertifikāti elektroniskajiem zīmogiem vai tīmekļa vietņu autentifikācijai, kā minēts 1. punktā, iekļauj – valodā, kuru parasti lieto starptautisko finanšu jomā – papildu īpašas iezīmes saistībā ar katru no turpmāk minētajiem elementiem:

a) maksājumu pakalpojumu sniedzēja loma, kura varbūt viena vai vairākas no šādām lomām:

   i) konta apkalpošana;

   ii) maksājumu iniciēšana;

   iii) konta informācija;

   iv) kartei piesaistītu maksājumu instrumentu izdošana;

b) to kompetento iestāžu nosaukums, kurās maksājumu pakalpojumu sniedzējs ir reģistrēts.

4. Raksturlielumi, kas minēti 3. punktā, neietekmē kvalificēto sertifikātu sadarbspēju un atzīšanu elektroniskiem zīmogiem vai tīmekļa vietņu autentifikācijai.

([1]) Eiropas Parlamenta un Padomes Direktīva 2013/36/ES (2013. gada 26. jūnijs) par piekļuvi kredītiestāžu darbībai un kredītiestāžu un ieguldījumu brokeru sabiedrību prudenciālo uzraudzību, ar ko groza Direktīvu 2002/87/EK un atceļ Direktīvas 2006/48/EK un 2006/49/EK (OV L 176, 27.6.2013., 338. lpp.).

35. pants

Saziņas sesijas drošība

1. Kontu apkalpojošie maksājumu pakalpojumu sniedzēji, maksājumu pakalpojumu sniedzēji, kas izdod kartei piesaistītus maksājumu instrumentus, konta informācijas pakalpojumu sniedzēji un maksājumu iniciēšanas pakalpojumu sniedzēji nodrošina, ka, ja datu apmaiņa tiek veikta, izmantojot internetu, starp saziņā esošajām personām attiecīgās saziņas sesijas laikā piemēro drošu datu šifrēšanu, lai nodrošinātu datu konfidencialitāti un integritāti, izmantojot spēcīgus un plaši atzītus šifrēšanas paņēmienus.

2. Maksājumu pakalpojumu sniedzēji, kas izdod kartei piesaistītus maksājumu instrumentus, konta informācijas pakalpojumu sniedzēji un maksājumu iniciēšanas pakalpojumu sniedzēji kontu apkalpojošo maksājumu pakalpojumu sniedzēju piedāvātās piekļuves sesijas patur pēc iespējas īsas un aktīvi pārtrauc jebkādas šādas sesijas, tiklīdz pieprasītā darbība ir pabeigta.

3. Uzturot paralēlas tīkla sesijas ar kontu apkalpojošo maksājumu pakalpojumu sniedzēju, konta informācijas pakalpojumu sniedzēji un maksājumu iniciēšanas pakalpojumu sniedzēji nodrošina, ka tās ir droši saistītas ar attiecīgajām sesijām, kas ieviestas ar maksājumu pakalpojumu lietotāju(-iem), lai nepieļautu iespēju, ka kāds ziņojums vai informācija, kas nodots starp tiem, varētu tikt novirzīts.

4. Konta informācijas pakalpojumu sniedzēji, maksājumu iniciēšanas pakalpojumu sniedzēji un maksājumu pakalpojumu sniedzēji, kas izdod kartei piesaistītus maksājumu instrumentus ar kontu apkalpojošo maksājumu pakalpojumu sniedzēju, ietver nepārprotamas atsauces uz katru no šiem punktiem:

a) maksājumu pakalpojumu lietotājs vai lietotāji un attiecīgā saziņas sesija, lai atšķirtu vairākus pieprasījumus no viena un tā paša maksājumu pakalpojumu lietotāja vai lietotājiem;

b) attiecībā uz maksājumu iniciēšanas pakalpojumiem – unikāli identificētais maksājuma darījums, kas iniciēts;

c) attiecībā uz apstiprinājumu par līdzekļu pieejamību – identificēts pieprasījums saistībā ar summu, kas vajadzīga, lai izpildītu kartei piesaistīto maksājumu darījumu.

5. Kontu apkalpojošie maksājumu pakalpojumu sniedzēji, konta informācijas pakalpojumu sniedzēji, maksājumu iniciēšanas pakalpojumu sniedzēji un maksājumu pakalpojumu sniedzēji, kas izdod kartei piesaistītus maksājumu instrumentus, nodrošina, ka gadījumā, kad tie sniedz personalizētus drošības datus un autentificēšanas kodus, darbinieki nevienā brīdī tos nevar tieši vai netieši nolasīt.

Ja personalizēti drošības dati, kas ir pakalpojumu sniedzēju kompetences jomā, zaudē konfidencialitāti, šie pakalpojumu sniedzēji bez liekas kavēšanās informē maksājumu pakalpojumu lietotāju, kas ar tiem saistīts, un personalizēto drošības datu izdevēju.

36. pants

Apmaiņa ar datiem

1. Kontu apkalpojošie maksājumu pakalpojumu sniedzēji atbilst visām šādām prasībām:

a) viņi sniedz konta informācijas pakalpojumu sniedzējiem to pašu informāciju no specializētiem maksājumu kontiem un saistītiem maksājumu darījumiem, kas darīta pieejama maksājumu pakalpojumu lietotājam, kad tieši pieprasīta piekļuve konta informācijai, ja šī informācija neietver sensitīvus maksājumu datus;

b) tie tūlīt pēc maksājuma uzdevuma saņemšanas sniedz maksājumu iniciēšanas pakalpojumu sniedzējiem to pašu informāciju par maksājuma darījumu iniciēšanu un izpildi, kas maksājumu pakalpojumu lietotājam ir pieejama, kad tas darījumu iniciē tieši;

c) tie pēc pieprasījuma nekavējoties sniedz maksājuma pakalpojuma sniedzējiem apstiprinājumu vienkāršā "jā" vai "nē" formātā par to, vai daudzums, kas vajadzīgs maksājuma darījuma izpildei, ir pieejams maksātāja maksājumu kontā.

2. Ja identifikācijas, autentifikācijas vai datu elementu apmaiņas laikā notiek neparedzēts notikums vai kļūda, kontu apkalpojošais maksājumu pakalpojumu sniedzējs nosūta paziņojumu maksājumu iniciēšanas pakalpojumu sniedzējam vai konta informācijas pakalpojumu sniedzējam un maksājumu pakalpojumu sniedzējam, kas izdod kartei piesaistītus maksājumu instrumentus, izskaidrojot negaidītā notikuma vai kļūdas iemeslu.

Ja kontu apkalpojošais maksājumu pakalpojumu sniedzējs piedāvā speciālu saskarni saskaņā ar 32. pantu, saskarnē tiek paredzēti paziņojumi par negaidītiem notikumiem vai kļūdām, par kurām maksājumu pakalpojumu sniedzējs, kurš konstatē attiecīgo notikumu vai kļūdu, paziņo pārējiem maksājumu pakalpojumu sniedzējiem, kas piedalās saziņas sesijā.

3. Konta informācijas pakalpojumu sniedzējiem ir piemēroti un efektīvi mehānismi, kas neļauj piekļūt citai informācijai, kā tikai informācijai, kas izriet no kontiem, kas nav specializēti maksājumu konti, un saistītiem maksājumu darījumiem saskaņā ar lietotāja nepārprotamu piekrišanu.

4. Maksājumu iniciēšanas pakalpojumu sniedzēji sniedz kontu apkalpojošajiem maksājumu pakalpojumu sniedzējiem to pašu informāciju, kas pieprasīta no maksājumu pakalpojumu lietotāja maksājumu darījuma tiešas iniciēšanas brīdī.

5. Konta informācijas pakalpojumu sniedzējiem ir iespēja piekļūt informācijai, kas izriet no specializētiem maksājumu kontiem un saistītiem maksājumu darījumiem, ko tur kontu apkalpojošie maksājumu pakalpojumu sniedzēji, lai veiktu konta informācijas pakalpojumu, ja tiek izpildīts kāds no šādiem nosacījumiem:

a) maksājumu pakalpojumu lietotājs aktīvi pieprasa šo informāciju;

b) maksājumu pakalpojumu lietotājs nav aktīvi pieprasījis šādu informāciju, proti, pieprasījumu biežums ir ne vairāk kā četras reizes 24 stundu periodā, ja vien konta informācijas pakalpojumu sniedzējs un kontu apkalpojošais maksājumu pakalpojumu sniedzējs ar maksājumu pakalpojumu lietotāja piekrišanu nav vienojušies par lielāku biežumu.

VI NODAĻA

NOBEIGUMA NOTEIKUMI

37. pants

Pārskatīšana

Neskarot Direktīvas (ES) 2015/2366 98. panta 5. punktu, EBI šīs regulas pielikumā minētos krāpšanas koeficientus un saskaņā ar 33. panta 6. punktu piešķirtos atbrīvojumus saistībā ar specializētām saskarnēm pārskata ne vēlāk kā līdz 2021. gada 14. martam un attiecīgā gadījumā Komisijai iesniedz to atjauninājumu projektus saskaņā ar Regulas (ES) Nr. 1093/2010 10. pantu.

38. pants

Stāšanās spēkā

1. Šī regula stājas spēkā nākamajā dienā pēc tās publicēšanas *Eiropas Savienības Oficiālajā Vēstnesī.*

2. Šo regulu piemēro no 2019. gada 14. septembra.

3. Tomēr 30. panta 3. un 5. punktu piemēro no 2019. gada 14. marta

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

Briselē, 2017. gada 27. novembrī

Komisijas vārdā –
priekšsēdētājs
Jean-Claude JUNCKER

PIELIKUMS

	Krāpšanas atsauces koeficients (%):	
Atbrīvojuma robežvērtība ("AR")	Attālināti, elektroniski, kartēm piesaistīti maksājumi	Attālināti, elektroniski kredītpārvedumi
EUR 500	0,01	0,005
EUR 250	0,06	0,01
EUR 100	0,13	0,015