EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV (EU) 2022/2556

av den 14 december 2022

om ändring av direktiven 2009/65/EG, 2009/138/EG, 2011/61/EU, 2013/36/EU, 2014/59/EU, 2014/65/EU, (EU) 2015/2366 och (EU) 2016/2341 vad gäller digital operativ motståndskraft för finanssektorn

(Text av betydelse för EES)

EUROPAPARLAMENTET OCH EUROPEISKA UNIONENS RÅD HAR ANTAGIT DETTA DIREKTIV

med beaktande av fördraget om Europeiska unionens funktionssätt, särskilt artiklarna 53.1 och 114,

med beaktande av Europeiska kommissionens förslag,

efter översändande av utkastet till lagstiftningsakt till de nationella parlamenten,

med beaktande av Europeiska centralbankens yttrande ([1]),

med beaktande av Europeiska ekonomiska och sociala kommitténs yttrande ([2]),

i enlighet med det ordinarie lagstiftningsförfarandet ([3]), och

av följande skäl:

(1) Unionen måste på ett lämpligt och heltäckande sätt ta itu med de digitala risker som uppstår för alla finansiella entiteter till följd av en ökad användning av informations- och kommunikationsteknik (IKT) vid tillhandahållande och konsumtion av finansiella tjänster, och därmed bidra till att förverkliga den digitala finanssektorns potential när det gäller att stimulera innovation och främja konkurrens i en säker digital miljö.

(2) Finansiella entiteter är mycket beroende av digital teknik i sin dagliga verksamhet. Det är därför ytterst viktigt att säkerställa att deras digitala transaktioner har en operativ motståndskraft mot IKT-risk. Detta behov har blivit allt större på grund av den ökade marknaden för banbrytande teknik, särskilt teknik som möjliggör att digitala representationer av värde eller rättigheter kan överföras och lagras elektroniskt, med hjälp av teknik för distribuerade liggare eller liknande teknik (kryptotillgångar) och för tjänster relaterade till sådana tillgångar.

([1]) EUT C 343, 26.8.2021, s. 1.
([2]) EUT C 155, 30.4.2021, s. 38.
([3]) Europaparlamentets ståndpunkt av den 10 november 2022 (ännu inte offentliggjord i EUT) och rådets beslut av den 28 november 2022.

(3) De krav som rör hantering av IKT-risk för finanssektorn på unionsnivå fastställs för närvarande i Europaparlamentets och rådets direktiv 2009/65/EG ([4]), 2009/138/EG ([5]), 2011/61/EU ([6]), 2013/36/EU ([7]), 2014/59/EU ([8]), 2014/65/EU ([9]), (EU) 2015/2366 ([10]) och (EU) 2016/2341 ([11]).

Dessa krav skiljer sig åt och är ibland ofullständiga. IKT-risk har i vissa fall endast behandlats indirekt som en del av den operativa risken, medan den i andra fall inte har behandlats över huvud taget. Dessa problem åtgärdas genom antagandet av Europaparlamentets och rådets förordning (EU) 2022/2554 ([12]). Dessa direktiv bör därför ändras för att säkerställa konsekvens med den förordningen. I detta direktiv antas en rad ändringar som är nödvändiga för att bringa rättslig klarhet och enhetlighet i fråga om hur de finansiella entiteter som auktoriseras och övervakas i enlighet med dessa direktiv ska tillämpa olika krav på digital operativ motståndskraft som är nödvändiga för att de ska kunna bedriva sin verksamhet och tillhandahålla tjänster och därigenom garantera en smidigt fungerande inre marknad. Det är nödvändigt att se till att dessa krav är förenliga med marknadsutvecklingen, samtidigt som proportionalitet uppmuntras, särskilt med avseende på de finansiella entiteternas storlek och de särskilda ordningar som är tillämpliga på dem, i syfte att minska efterlevnadskostnaderna.

(4) Inom området för banktjänster innehåller direktiv 2013/36/EU i dagsläget endast allmänna regler om intern styrning och operativ risk med krav på beredskaps- och kontinuitetsplaner vilka underförstått används som en grund för att hantera IKT-risk. För att uttryckligen och tydligt hantera IKT-risk bör dock kraven på beredskaps- och kontinuitetsplaner ändras så att de även innefattar kontinuitets- och åtgärds- och återställningsplaner även för IKT-risk, i enlighet med kraven i förordning (EU) 2022/2554. Dessutom ingår IKT-risk endast indirekt, som en del av den operativa risken, i den översyns- och utvärderingsprocess (ÖUP) som utförs av behöriga myndigheter, och kriterierna för deras bedömning fastställs för närvarande i riktlinjerna om IKT-riskbedömning inom ramen för översyns- och utvärderingsprocessen (ÖUP), utfärdade av den europeiska tillsynsmyndigheten (Europeiska bankmyndigheten, EBA), inrättad genom Europaparlamentets och rådets förordning (EU) nr 1093/2010 ([13]). För att skapa rättslig klarhet och säkerställa att banktillsynsmyndigheterna effektivt identifierar IKT-risk och övervakar finansiella entiteters hantering därav, i linje med den nya ramen för digital operativ motståndskraft, bör ÖUP:s

([4]) Europaparlamentets och rådets direktiv 2009/65/EG av den 13 juli 2009 om samordning av lagar och andra författningar som avser företag för kollektiva investeringar i överlåtbara värdepapper (fondföretag) (EUT L 302, 17.11.2009, s. 32).

([5]) Europaparlamentets och rådets direktiv 2009/138/EG av den 25 november 2009 om upptagande och utövande av försäkrings- och återförsäkringsverksamhet (Solvens II) (EUT L 335, 17.12.2009, s. 1).

([6]) Europaparlamentets och rådets direktiv 2011/61/EU av den 8 juni 2011 om förvaltare av alternativa investeringsfonder samt om ändring av direktiv 2003/41/EG och 2009/65/EG och förordningarna (EG) nr 1060/2009 och (EU) nr 1095/2010 (EUT L 174, 1.7.2011, s. 1).

([7]) Europaparlamentets och rådets direktiv 2013/36/EU av den 26 juni 2013 om behörighet att utöva verksamhet i kreditinstitut och om tillsyn av kreditinstitut, om ändring av direktiv 2002/87/EG och om upphävande av direktiven 2006/48/EG och 2006/49/EG (EUT L 176, 27.6.2013, s. 338).

([8]) Europaparlamentets och rådets direktiv 2014/59/EU av den 15 maj 2014 om inrättande av en ram för återhämtning och resolution av kreditinstitut och värdepappersföretag och om ändring av rådets direktiv 82/891/EEG och Europaparlamentets och rådets direktiv 2001/24/EG, 2002/47/EG, 2004/25/EG, 2005/56/EG, 2007/36/EG, 2011/35/EU, 2012/30/EU och 2013/36/EU samt Europaparlamentets och rådets förordningar (EU) nr 1093/2010 och (EU) nr 648/2012 (EUT L 173, 12.6.2014, s. 190).

([9]) Europaparlamentets och rådets direktiv 2014/65/EU av den 15 maj 2014 om marknader för finansiella instrument och om ändring av direktiv 2002/92/EG och av direktiv 2011/61/EU (EUT L 173, 12.6.2014, s. 349).

([10]) Europaparlamentets och rådets direktiv (EU) 2015/2366 av den 25 november 2015 om betaltjänster på den inre marknaden, om ändring av direktiven 2002/65/EG, 2009/110/EG och 2013/36/EU samt förordning (EU) nr 1093/2010 och om upphävande av direktiv 2007/64/EG (EUT L 337, 23.12.2015, s. 35).

([11]) Europaparlamentets och rådets direktiv (EU) 2016/2341 av den 14 december 2016 om verksamhet i och tillsyn över tjänstepensionsinstitut (EUT L 354, 23.12.2016, s. 37).

([12]) Europaparlamentets och rådets förordning (EU) 2022/2554 av den 14 december 2022 om digital operativ motståndskraft för finanssektorn och om ändring av förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014, (EU) nr 909/2014 och (EU) 2016/1011 (se sidan 1 i detta nummer av EUT).

([13]) Europaparlamentets och rådets förordning (EU) nr 1093/2010 av den 24 november 2010 om inrättande av en europeisk tillsynsmyndighet (Europeiska bankmyndigheten), om ändring av beslut nr 716/2009/EG och om upphävande av kommissionens beslut 2009/78/EG (EUT L 331, 15.12.2010, s. 12).

tillämpningsområde även ändras så att det uttryckligen hänvisar till de krav som fastställs i förordning (EU) 2022/2554 och i synnerhet omfattar de risker som påvisats i rapporter om allvarliga IKT-relaterade incidenter och resultaten av den testning av digital operativ motståndskraft som finansiella entiteter utfört i enlighet med den förordningen.

(5) Digital operativ motståndskraft är nödvändigt för att upprätthålla en finansiell entitets kritiska funktioner och kärnaffärsområden i händelse av dess resolution och för att undvika störningar i realekonomin och det finansiella systemet. Allvarliga operativa incidenter kan hämma en finansiell entitets förmåga att fortsätta att driva sin verksamhet och kan äventyra resolutionsmålen. Vissa kontraktsmässiga arrangemang som rör användningen av IKT-tjänster är väsentliga för att säkerställa driftskontinuitet och tillhandahålla nödvändiga uppgifter i händelse av resolution. För att vara anpassat till målen för unionens ram för operativ motståndskraft bör direktiv 2014/59/EU ändras i enlighet med detta så att det säkerställs att information relaterad till operativ motståndskraft beaktas i samband med resolutionsplanering och bedömning av finansiella entiteters möjligheter till resolution.

(6) I direktiv 2014/65/EU fastställs hårdare IKT-riskregler för värdepappersföretag och handelsplatser när dessa bedriver algoritmisk handel. Mindre utförliga krav tillämpas på datarapporteringstjänster och transaktionsregister. Dessutom hänvisas det i direktiv 2014/65/EU endast i begränsad mån till kontroll- och skyddssystem för informationsbehandlingssystem och användning av lämpliga system, resurser och förfaranden för att sörja för kontinuitet och regelbundenhet i affärstjänster. Det direktivet bör dessutom harmoniseras med förordning (EU) 2022/2554 i fråga om kontinuitet och regelbundenhet i tillhandahållandet av investeringstjänster och utförandet av investeringsverksamhet, operativ motståndskraft, handelssystemens kapacitet och effektiva arrangemang för kontinuitet och riskhantering.

(7) I direktiv (EU) 2015/2366 fastställs särskilda regler om IKT-relaterade säkerhetskontroll- och begränsningsaspekter för erhållande av en auktorisation att utföra betaltjänster. Dessa auktorisationsregler bör ändras för att anpassas till förordning (EU) 2022/2554. För att minska den administrativa bördan och undvika komplexitet och överlappande rapporteringskrav bör dessutom reglerna om incidentrapportering i det direktivet upphöra att tillämpas för betaltjänstleverantörer som regleras enligt det direktivet och som omfattas av förordning (EU) 2022/2554, vilket gör det möjligt för dessa betaltjänstleverantörer att dra nytta av en gemensam, fullständigt harmoniserad incidentrapporteringsmekanism med avseende på alla operativa incidenter eller säkerhetsincidenter, oavsett om sådana incidenter är IKT-relaterade.

(8) Direktiven 2009/138/EG och (EU) 2016/2341 fångar delvis upp IKT-risk i sina allmänna bestämmelser om styrning och riskhantering, vilket innebär att vissa krav ska specificeras genom delegerade akter med eller utan särskilda hänvisningar till IKT-risk. På samma sätt tillämpas endast mycket allmänna regler på förvaltare av alternativa investeringsfonder som omfattas av direktiv 2011/61/EU och förvaltningsbolag som omfattas av direktiv 2009/65/EG. Dessa direktiv bör därför anpassas till kraven i förordning (EU) 2022/2554 när det gäller förvaltningen av IKT-system och IKT-verktyg.

(9) Ytterligare IKT-krav har i många fall redan fastställts i delegerade akter och genomförandeakter, antagna utifrån förslag till tekniska tillsynsstandarder och tekniska standarder för genomförande vilka utarbetats av den behöriga europeiska tillsynsmyndigheten. Eftersom bestämmelserna i förordning (EU) 2022/2554 hädanefter utgör den rättsliga ramen för IKT-risk för finanssektorn bör vissa befogenheter att anta delegerade akter och genomförandeakter i direktiven 2009/65/EG, 2009/138/EG, 2011/61/EU och 2014/65/EU ändras för att stryka IKT-riskbestämmelserna från tillämpningsområdet för dessa befogenheter.

(10) För att säkerställa ett enhetligt genomförande av den nya ramen för digital operativ motståndskraft för finanssektorn bör medlemsstaterna tillämpa de bestämmelser i nationell rätt som införlivar detta direktiv från och med tillämpningsdagen för förordning (EU) 2022/2554.

(11) Direktiven 2009/65/EG, 2009/138/EG, 2011/61/EU, 2013/36/EU, 2014/59/EU, 2014/65/EU, (EU) 2015/2366 och (EU) 2016/2341 har antagits på grundval av artikel 53.1 eller artikel 114 i fördraget om Europeiska unionens funktionssätt (EUF-fördraget) eller båda. Ändringarna genom detta direktiv har tagits med i en och samma lagstiftningsakt på grund av det inbördes förhållandet mellan sakfrågan och ändringarnas syften. Följaktligen bör detta direktiv antas på grundval av såväl artikel 53.1 som artikel 114 i EUF-fördraget.

(12) Eftersom målen för detta direktiv inte i tillräcklig utsträckning kan uppnås av medlemsstaterna, eftersom de innebär en harmonisering av redan befintliga krav i direktiven, utan snarare, på grund av åtgärdens omfattning och verkningar, kan uppnås bättre på unionsnivå, kan unionen vidta åtgärder i enlighet med subsidiaritetsprincipen i artikel 5 i fördraget om Europeiska unionen. I enlighet med proportionalitetsprincipen i samma artikel går detta direktiv inte utöver vad som är nödvändigt för att uppnå dessa mål.

(13) I enlighet med den gemensamma politiska förklaringen av den 28 september 2011 från medlemsstaterna och kommissionen om förklarande dokument ([14]), har medlemsstaterna åtagit sig att, när det är motiverat, låta anmälan av införlivandeåtgärder åtföljas av ett eller flera dokument som förklarar förhållandet mellan de olika delarna i direktivet och motsvarande delar i de nationella instrumenten för införlivande. Lagstiftaren anser att det är motiverat att sådana dokument översänds avseende detta direktiv.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

Artikel 1

Ändringar av direktiv 2009/65/EG

Artikel 12 i direktiv 2009/65/EG ska ändras på följande sätt:

1. I punkt 1 andra stycket ska led a ersättas med följande:

”a) har sunda administrativa förfaranden och redovisningsrutiner, kontroll- och säkerhetsarrangemang för elektronisk databehandling, inbegripet när det gäller nätverks- och informationssystem som inrättas och förvaltas i enlighet med Europaparlamentets och rådets förordning (EU) 2022/2554 (*), samt lämpliga interna kontrollmekanismer, särskilt regler för de anställdas personliga transaktioner eller för innehav eller förvaltning av investeringar i finansiella instrument i syfte att placera på egna konton, och att det minst säkerställs att varje transaktion i vilken fondföretaget medverkar är möjlig att rekonstruera med avseende på dess ursprung, de deltagande parterna, dess art samt tiden och platsen då den ägde rum och att fondföretagets tillgångar som förvaltas av förvaltningsbolaget placeras i enlighet med fondbestämmelserna eller bolagsordningen samt gällande lagstiftning, och

(*) Europaparlamentets och rådets förordning (EU) 2022/2554 av den 14 december 2022 om digital operativ motståndskraft för finanssektorn och om ändring av förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014, (EU) nr 909/2014 och (EU) 2016/1011 (EUT L 333, 27.12.2022, s. 1).”

2. Punkt 3 ska ersättas med följande:

”3. Utan att det påverkar tillämpningen av artikel 116 ska kommissionen, genom delegerade akter i enlighet med artikel 112a, anta åtgärder som specificerar

a) de förfaranden och arrangemang som avses i punkt 1 andra stycket a, andra än de förfaranden och arrangemang som gäller nätverks- och informationssystem,

b) de strukturer och organisatoriska krav för att minimera intressekonflikter som avses i punkt 1 andra stycket b.”

([14]) EUT C 369, 17.12.2011, s. 14.

Artikel 2

Ändringar av direktiv 2009/138/EG

Direktiv 2009/138/EG ska ändras på följande sätt:

1. Artikel 41.4 ska ersättas med följande:

”4. Försäkrings- och återförsäkringsföretag ska vidta rimliga åtgärder för att säkerställa att deras verksamhet bedrivs med kontinuitet och på ett korrekt sätt, inklusive utvecklingen av beredskapsplaner. Företaget ska i detta syfte använda lämpliga och proportionella system, resurser och förfaranden och ska i synnerhet inrätta och förvalta nätverks- och informationssystem i enlighet med Europaparlamentets och rådets förordning (EU) 2022/2554 (*).

(*) Europaparlamentets och rådets förordning (EU) 2022/2554 av den 14 december 2022 om digital operativ motståndskraft för finanssektorn och om ändring av förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014, (EU) nr 909/2014 och (EU) 2016/1011 (EUT L 333, 27.12.2022, s. 1).”

2. I artikel 50.1 ska leden a och b ersättas med följande:

”a) Delarna i de system som avses i artiklarna 41, 44, särskilt de områden som förtecknas i artikel 44.2, och artiklarna 46 och 47, andra än de delar som avser hantering av informations- och kommunikationsteknisk risk.

b) De funktioner som avses i artiklarna 44, 46, 47 och 48, andra än de funktioner som avser hantering av informations- och kommunikationsteknisk risk.”

Artikel 3

Ändring av direktiv 2011/61/EU

Artikel 18 i direktiv 2011/61/EU ska ersättas med följande:

”*Artikel 18*

Allmänna principer

1. Medlemsstaterna ska kräva att AIF-förvaltare alltid ska använda tillfredsställande och lämpliga personella och tekniska resurser som krävs för att de ska kunna förvalta AIF-fonderna på ett korrekt sätt.

De behöriga myndigheterna i AIF-förvaltarens hemmedlemsstat ska, även med beaktande av arten av de AIF-fonder som AIF-förvaltaren förvaltar, särskilt kräva att AIF-förvaltaren har sunda administrativa förfaranden och redovisningsrutiner, kontroll- och säkerhetsarrangemang för elektronisk databehandling, inbegripet när det gäller nätverks- och informationssystem som upprättas och förvaltas i enlighet med Europaparlamentets och rådets förordning (EU) 2022/2554 (*) och tillfredsställande interna kontrollmekanismer, särskilt regler för de anställdas personliga transaktioner eller för innehav eller förvaltning av investeringar i syfte att investera för egen räkning, och att det åtminstone säkerställs att varje transaktion i vilken AIF-förvaltaren medverkar avseende AIF-fonderna är möjlig att rekonstruera med avseende på dess ursprung, de deltagande parterna, dess art samt tiden och platsen då den ägde rum, och att tillgångarna i de AIF-fonder som förvaltas av AIF-förvaltaren investeras i enlighet med fondbestämmelserna eller bolagsordningen samt gällande lagstiftning.

2. Kommissionen ska, genom delegerade akter i enlighet med artikel 56, och med förbehåll för villkoren i artiklarna 57 och 58, anta åtgärder för att närmare ange de förfaranden och arrangemang som avses i punkt 1 i den här artikeln, andra än de förfaranden och arrangemang som gäller nätverks- och informationssystem.

(*) Europaparlamentets och rådets förordning (EU) 2022/2554 av den 14 december 2022 om digital operativ motståndskraft för finanssektorn och om ändring av förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014, (EU) nr 909/2014 och (EU) 2016/1011 (EUT L 333, 27.12.2022, s. 1).”

Artikel 4

Ändringar av direktiv 2013/36/EU

Direktiv 2013/36/EU ska ändras på följande sätt:

1. I artikel 65.3 ska led a vi ersättas med följande:

   ”vi) Tredje parter till vilka enheterna i leden i–iv har gett i uppdrag att utföra uppgifter eller verksamhet, inbegripet de tredjepartsleverantörer av IKT-tjänster som avses i kapitel V i Europaparlamentets och rådets förordning (EU) 2022/2554 (*).

   _____

   (*) Europaparlamentets och rådets förordning (EU) 2022/2554 av den 14 december 2022 om digital operativ motståndskraft för finanssektorn och om ändring av förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014, (EU) nr 909/2014 och (EU) 2016/1011 (EUT L333, 27.12.2022, s. 1).”

2. I artikel 74.1 ska första stycket ersättas med följande:

   ”Instituten ska ha en robust företagsstyrning, i vilket ingår en tydlig organisationsstruktur med väldefinierade, genomlysta och konsekventa ansvarskedjor, effektiva processer för att identifiera, hantera, övervaka och rapportera risker som instituten är eller kan bli exponerade för, tillfredsställande metoder för intern kontroll, inklusive sunda administrations- och redovisningsrutiner och nätverks- och informationssystem som inrättas och förvaltas i enlighet med förordning (EU) 2022/2554, samt ersättningspolicy och ersättningspraxis som är förenliga med och främjar sund och effektiv riskhantering.”

3. Artikel 85.2 ska ersättas med följande:

   ”2. De behöriga myndigheterna ska se till att instituten har lämpliga beredskaps- och kontinuitetspolicyer och -planer, inbegripet IKT-kontinuitetspolicyer och -planer samt IKT-relaterade åtgärds- och återställningsplaner för den teknik som de använder för meddelande av information, och att de planerna inrättas, förvaltas och testas i enlighet med artikel 11 i förordning (EU) 2022/2554, så att instituten kan fortsätta att bedriva sin verksamhet vid en allvarlig störning i verksamheten och begränsa de förluster som orsakas till följd av sådan störning.”

4. I artikel 97.1 ska följande led läggas till:

   ”d) risker som påvisats vid testning av digital operativ motståndskraft i enlighet med kapitel IV i förordning (EU) 2022/2554.”

Artikel 5

Ändringar av direktiv 2014/59/EU

Direktiv 2014/59/EU ska ändras på följande sätt:

1. Artikel 10 ska ändras på följande sätt:

   a) I punkt 7 ska led c ersättas med följande:

      ”c) En beskrivning av hur kritiska funktioner och kärnaffärsområden, i den utsträckning som krävs, skulle kunna avskiljas juridiskt och ekonomiskt från övriga funktioner för att säkerställa fortsatt verksamhet och digital operativ motståndskraft efter institutets fallissemang.”

   b) I punkt 7 ska led q ersättas med följande:

      ”q) En beskrivning av grundläggande operationer och system för kontinuerlig drift av institutets operativa processer, inbegripet nätverks- och informationssystem som avses i Europaparlamentets och rådets förordning (EU) 2022/2554 (*).

      _____

      (*) Europaparlamentets och rådets förordning (EU) 2022/2554 av den 14 december 2022 om digital operativ motståndskraft för finanssektorn och om ändring av förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014, (EU) nr 909/2014 och (EU) 2016/1011 (EUT L 333, 27.12.2022, s. 1).”

c) I punkt 9 ska följande stycke läggas till:

”I enlighet med artikel 10 i förordning (EU) nr 1093/2010 ska EBA se över och vid behov uppdatera de tekniska standarderna för tillsyn i syfte att bland annat ta hänsyn till bestämmelserna i kapitel II i förordning (EU) 2022/2554.”

2. Bilagan ska ändras på följande sätt:

a) I avsnitt A ska punkt 16 ersättas med följande:

”16. Arrangemang och åtgärder som är nödvändiga för att fortlöpande upprätthålla institutets operativa verksamhet, inbegripet nätverks- och informationssystem som inrättas och förvaltas i enlighet med förordning (EU) 2022/2554.”

b) Avsnitt B ska ändras på följande sätt:

i) Punkt 14 ska ersättas med följande:

”14. Uppgifter om ägarna till de system som avses i led 13, tillhörande servicenivåavtal och alla datorprogram, system eller verksamhetstillstånd, inklusive per juridiska enheter, kritisk verksamhet och centrala affärsområden samt uppgifter om kritiska tredjepartsleverantörer av IKT-tjänster enligt definitionen i artikel 3.23 i förordning (EU) 2022/2554.”

ii) Följande punkt ska införas:

”14a. Resultaten av institutionernas testning av digital operativ motståndskraft enligt förordning (EU) 2022/2554.”

c) Avsnitt C ska ändras på följande sätt:

i) Punkt 4 ska ersättas med följande:

”4. I vilken mån serviceavtal, inbegripet kontraktsmässiga arrangemang som rör användningen av IKT-tjänster, som institutet ingått är solida och kan hävdas om institutet avvecklas.”

ii) Följande punkt ska införas:

”4a. Den digitala operativa motståndskraften hos de nätverks- och informationssystem som stöder institutets kritiska funktioner och kärnaffärsområden, med beaktande av rapporter om allvarliga IKT-relaterade incidenter och resultaten av testning av digital operativ motståndskraft enligt förordning (EU) 2022/2554.”

Artikel 6

Ändringar av direktiv 2014/65/EU

Direktiv 2014/65/EU ska ändras på följande sätt:

1. Artikel 16 ska ändras på följande sätt:

a) Punkt 4 ska ersättas med följande:

”4. Varje värdepappersföretag ska vidta rimliga åtgärder för att sörja för kontinuitet och regelbundenhet i tillhandahållandet av investeringstjänster och utförandet av investeringsverksamhet. Värdepappersföretaget ska i det syftet använda lämpliga och proportionella system, inbegripet informations- och kommunikationstekniska system (IKT-system) som inrättas och förvaltas i enlighet med artikel 7 i Europaparlamentets och rådets förordning (EU) 2022/2554 (*) samt lämpliga och proportionella resurser och förfaranden.

(*) Europaparlamentets och rådets förordning (EU) 2022/2554 av den 14 december 2022 om digital operativ motståndskraft för finanssektorn och om ändring av förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014, (EU) nr 909/2014 och (EU) 2016/1011 (EUT L333, 27.12.2022, s. 1).”

b) I punkt 5 ska andra och tredje styckena ersättas med följande:

”Varje värdepappersföretag ska tillämpa sunda förfaranden för förvaltning och redovisning samt ha mekanismer för internkontroll och effektiva riskbedömningsmetoder.

Utan att det påverkar behöriga myndigheters möjlighet att kräva tillgång till kommunikation i enlighet med detta direktiv och förordning (EU) nr 600/2014, ska ett värdepappersföretag ha inrättat sunda skyddsmekanismer för att, i enlighet med kraven i förordning (EU) 2022/2554, säkerställa skyddet och autentiseringen vid informationsöverföring, för att minimera risken för dataförvanskning och för obehörig åtkomst och för att förhindra informationsläckor så att uppgifterna därmed alltid behandlas konfidentiellt.”

2. Artikel 17 ska ändras på följande sätt:

a) Punkt 1 ska ersättas med följande:

”1. Ett värdepappersföretag som bedriver algoritmisk handel ska ha inrättat effektiva system och riskkontroller som är anpassade för den verksamhet som bedrivs, så att det säkerställs att dess handelssystem är motståndskraftiga och har tillräcklig kapacitet i enlighet med kraven i kapitel II i förordning (EU) 2022/2554, att de omfattas av lämpliga handelströsklar och handelslimiter och att de förhindrar att felaktiga order skickas eller att systemet på annat sätt fungerar så att det kan skapa eller bidra till en oordnad marknad.

Ett sådant företag ska också ha inrättat effektiva system och riskkontrollåtgärder för att säkerställa att handelssystemen inte kan användas för något ändamål som strider mot förordning (EU) nr 596/2014 eller mot reglerna för en handelsplats till vilken det är anslutet.

Värdepappersföretaget ska ha inrättat effektiva arrangemang för kontinuitet för att hantera alla avbrott i driften i sina handelssystem, inbegripet en IKT-kontinuitetspolicy och -planer samt IKT-relaterade åtgärds- och återställningsplaner för informations- och kommunikationsteknik som inrättas i enlighet med artikel 11 i förordning (EU) 2022/2554, och ska säkerställa att systemen är fullständigt testade och vederbörligen övervakade för att säkerställa att de uppfyller de allmänna krav som föreskrivs i denna punkt och eventuella särskilda krav i kapitlen II och IV i förordning (EU) 2022/2554.”

b) I punkt 7 ska led a ersättas med följande:

”a) Detaljerna i de organisatoriska krav som fastställs i punkterna 1–6, andra än de krav som rör IKT-riskhantering, och som ska föreskrivas för värdepappersföretag som tillhandahåller olika slags investeringstjänster, investeringsverksamheter, sidotjänster eller kombinationer därav, varigenom specifikationerna av de organisatoriska krav som fastställs i punkt 5 ska innehålla specifika krav för direkt marknadstillträde och för sponsrat tillträde så att det säkerställs att de kontroller som tillämpas på sponsrat tillträde åtminstone motsvarar dem som tillämpas på direkt marknadstillträde.”

3. Artikel 47.1 ska ändras på följande sätt:

a) Led b ska ersättas med följande:

”b) har tillräckliga förutsättningar för att kunna hantera de risker den är exponerad för, inbegripet att hantera IKT-risk i enlighet med kapitel II i förordning (EU) 2022/2554, vidtar lämpliga åtgärder och inför system för att identifiera betydande risker för dess verksamhet och vidtar effektiva åtgärder för att reducera sådana risker,”

b) Led c ska utgå.

4. Artikel 48 ska ändras på följande sätt:

a) Punkt 1 ska ersättas med följande:

”1. Medlemsstaterna ska kräva att en reglerad marknad inrättar och upprätthåller en operativ motståndskraft i enlighet med kraven i kapitel II i förordning (EU) 2022/2554 för att säkerställa att dess handelssystem är motståndskraftiga, har tillräcklig kapacitet för att kunna hantera toppbelastning i fråga om order- och meddelandevolymer, kan säkerställa ordnad handel under svåra förhållanden på marknaden, är till fullo testade för att säkerställa att sådana villkor är uppfyllda och omfattas av effektiva arrangemang för kontinuitet, inbegripet en IKT-kontinuitetspolicy och -planer samt IKT-relaterade åtgärds- och återställningsplaner som inrättas i enlighet med artikel 11 i förordning (EU) 2022/2554, för att säkerställa kontinuitet i sin verksamhet vid eventuella driftsavbrott i sina handelssystem.”

b) Punkt 6 ska ersättas med följande:

”6. Medlemsstaterna ska kräva att en reglerad marknad har inrättat effektiva system, förfaranden och arrangemang, bland annat krav på medlemmar eller deltagare att utföra lämpliga tester av algoritmer och att tillhandahålla miljöer för att underlätta sådana tester, i enlighet med kraven i kapitlen II och IV i förordning (EU) 2022/2554, för att säkerställa att algoritmiska handelssystem inte kan skapa eller bidra till otillbörliga marknadsförhållanden på marknaden och att hantera eventuella otillbörliga marknadsförhållanden som kan uppstå till följd av sådana algoritmiska handelssystem, inbegripet system för att begränsa andelen ej utförda order i förhållande till transaktionerna som kan läggas in i systemet av en medlem eller en deltagare, för att det ska vara möjligt att bromsa orderflödet om det finns en risk för att systemkapaciteten ska uppnås och för att begränsa och genomdriva den minsta tick-size som får tillämpas på marknaden.”

c) Punkt 12 ska ändras på följande sätt:

i) Led a ska ersättas med följande:

”a) kraven för att säkerställa att handelssystem på reglerade marknader är motståndskraftiga och har tillräcklig kapacitet, förutom kraven rörande digital operativ motståndskraft,”.

ii) Led g ska ersättas med följande:

”g) kraven för att säkerställa lämplig testning av algoritmer, annat än testning av digital operativ motståndskraft, så att det kan säkerställas att algoritmiska handelssystem inbegripet system för algoritmisk högfrekvenshandel inte kan skapa eller bidra till otillbörliga marknadsförhållanden på marknaden.”

Artikel 7

Ändring av direktiv (EU) 2015/2366

Direktiv (EU) 2015/2366 ska ändras på följande sätt:

1. I artikel 3 ska led j ersättas med följande:

”j) Tjänster som tillhandahålls av leverantörer av tekniska tjänster som stöder tillhandahållandet av betaltjänster, utan att de vid någon tidpunkt kommer i besittning av de medel som ska överföras, inklusive behandling och lagring av uppgifter, förtroendeskapande tjänster och integritetsskydd, autentisering av uppgifter och enheter, tillhandahållande av nät för informations- och kommunikationsteknik (IKT) och kommunikationsnät samt tillhandahållande och underhåll av terminaler och utrustning för betaltjänster, med undantag för tjänster för betalningsinitiering och kontoinformationstjänster.”

2. Artikel 5.1 ska ändras på följande sätt:

a) Första stycket ska ändras på följande sätt:

i) Led e ska ersättas med följande:

”e) En beskrivning av den sökandes styrsystem och interna kontrollmekanismer, inklusive förvaltnings-, riskhanterings- och redovisningsförfaranden samt arrangemang för användning av IKT-tjänster i enlighet med Europaparlamentets och rådets förordning (EU) 2022/2554 (*), vilken ska visa att dessa styrsystem och interna kontrollmekanismer är proportionella, lämpliga, sunda och tillräckliga.

(*) Europaparlamentets och rådets förordning (EU) 2022/2554 av den 14 december 2022 om digital operativ motståndskraft för finanssektorn och om ändring av förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014, (EU) nr 909/2014 och (EU) 2016/1011 ((EUT L333, 27.12.2022, s. 1).”

ii) Led f ska ersättas med följande:

”f) En beskrivning av de förfaranden som finns för att övervaka, hantera och följa upp säkerhetsincidenter och säkerhetsrelaterade kundklagomål, inklusive en rapporteringsmekanism för incidenter som beaktar betalningsinstitutets informationsskyldigheter enligt kapitel III i förordning (EU) 2022/2554.”

iii) Led h ska ersättas med följande:

”h) En beskrivning av arrangemang för verksamhetens kontinuitet, inklusive en tydlig angivelse av kritiska verksamheter, en effektiv IKT-kontinuitetspolicy och -planer samt effektiva IKT-relaterade åtgärds- och återställningsplaner och ett förfarande för att regelbundet kontrollera och se över dessa planers lämplighet och effektivitet i enlighet med förordning (EU) 2022/2554.”

b) Tredje stycket ska ersättas med följande:

”I samband med de säkerhetskontroll- och begränsningsåtgärder som avses i första stycket j ska det anges på vilket sätt de säkrar en hög nivå av digital operativ motståndskraft i enlighet med kapitel II i förordning (EU) 2022/2554, särskilt när det gäller teknisk säkerhet och dataskydd, däribland för de programvaru- och IKT-system som används av sökanden eller de företag till vilka denne utkontrakterar hela eller delar av sin verksamhet. Dessa åtgärder ska också omfatta de säkerhetsåtgärder som fastställs i artikel 95.1 i detta direktiv. I samband med dessa åtgärder ska hänsyn tas till EBA:s riktlinjer för säkerhetsåtgärder som avses i artikel 95.3 i detta direktiv när dessa har införts.”

3. I artikel 19.6 ska andra stycket ersättas med följande:

”Utkontraktering av viktiga operativa funktioner, inbegripet IKT-system, får inte ske på så sätt att det väsentligt försämrar kvaliteten på betalningsinstitutets interna kontroll och de behöriga myndigheternas möjligheter att övervaka och följa upp att betalningsinstitutet fullgör alla skyldigheter enligt detta direktiv.”

4. I artikel 95.1 ska följande stycke läggas till:

”Första stycket påverkar inte tillämpningen av kapitel II i förordning (EU) 2022/2554 på

a) betaltjänstleverantörer som avses i artikel 1.1 a, b och d i detta direktiv,

b) leverantörer av kontoinformationstjänster som avses i artikel 33.1 i detta direktiv,

c) betalningsinstitut som är undantagna enligt artikel 32.1 i detta direktiv, och

d) institut för elektroniska pengar som omfattas av ett undantag enligt artikel 9.1 i direktiv 2009/110/EG.”

5. I artikel 96 ska följande punkt läggas till:

”7. Medlemsstaterna ska säkerställa att punkterna 1–5 i denna artikel inte tillämpas på

a) betaltjänstleverantörer som avses i artikel 1.1 a, b och d i detta direktiv,

b) leverantörer av kontoinformationstjänster som avses i artikel 33.1 i detta direktiv,

c) betalningsinstitut som är undantagna enligt artikel 32.1 i detta direktiv, och

d) institut för elektroniska pengar som omfattas av ett undantag enligt artikel 9.1 i direktiv 2009/110/EG.”

6. Artikel 98.5 ska ersättas med följande:

”5. I enlighet med artikel 10 i förordning (EU) nr 1093/2010 ska EBA se över och vid behov regelbundet uppdatera de tekniska standarderna för tillsyn i syfte att bland annat ta hänsyn till innovation och teknisk utveckling, samt till bestämmelserna i kapitel II i förordning (EU) 2022/2554.”

Artikel 8

Ändring av direktiv (EU) 2016/2341

Artikel 21.5 i direktiv (EU) 2016/2341 ska ersättas med följande:

”5. Medlemsstaterna ska säkerställa att tjänstepensionsinstituten vidtar rimliga åtgärder för att säkerställa att deras verksamhet bedrivs med kontinuitet och på ett korrekt sätt, inklusive utarbetandet av beredskapsplaner. Tjänstepen-

sionsinstitutet ska i detta syfte använda lämpliga och proportionella system, resurser och förfaranden, och ska i synnerhet inrätta och förvalta nätverks- och informationssystem i enlighet med Europaparlamentets och rådets förordning (EU) 2022/2554 (*), i tillämpliga fall.

(*) Europaparlamentets och rådets förordning (EU) 2022/2554 av den 14 december 2022 om digital operativ motståndskraft för finanssektorn och om ändring av förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014, (EU) nr 909/2014 och (EU) 2016/1011 (EUT L 333, 27.12.2022, s. 1).”

Artikel 9

Införlivande

1. Medlemsstaterna ska senast den 17 januari 2025 anta och offentliggöra de bestämmelser som är nödvändiga för att följa detta direktiv. De ska genast underrätta kommissionen om detta.

De ska tillämpa dessa bestämmelser från och med den 17 januari 2025.

När en medlemsstat antar dessa bestämmelser ska de innehålla en hänvisning till detta direktiv eller åtföljas av en sådan hänvisning när de offentliggörs. Närmare föreskrifter om hur hänvisningen ska göras ska varje medlemsstat själv utfärda.

2. Medlemsstaterna ska underrätta kommissionen om texten till de centrala bestämmelser i nationell rätt som de antar inom det område som omfattas av detta direktiv.

Artikel 10

Ikraftträdande

Detta direktiv träder i kraft den tjugonde dagen efter det att det har offentliggjorts i *Europeiska unionens officiella tidning*.

Artikel 11

Adressater

Detta direktiv riktar sig till medlemsstaterna.

Utfärdat i Strasbourg den 14 december 2022.

På Europaparlamentets vägnar	*På rådets vägnar*
R. METSOLA	M. BEK
Ordförande	*Ordförande*