

EUROPA-PARLAMENTETS OG RÅDETS DIREKTIV (EU) 2022/2556**af 14. december 2022****om ændring af direktiv 2009/65/EF, 2009/138/EF, 2011/61/EU, 2013/36/EU, 2014/59/EU, 2014/65/EU, (EU) 2015/2366 og (EU) 2016/2341 for så vidt angår digital operationel modstandsdygtighed i den finansielle sektor****(EØS-relevant tekst)**

EUROPA-PARLAMENTET OG RÅDET FOR DEN EUROPÆISKE UNION HAR —

under henvisning til traktaten om Den Europæiske Unions funktionsmåde, særlig artikel 53, stk. 1, og artikel 114,

under henvisning til forslag fra Europa-Kommissionen,

efter fremsendelse af udkast til lovgivningsmæssig retsakt til de nationale parlamenter,

under henvisning til udtalelse fra Den Europæiske Centralbank ⁽¹⁾,

under henvisning til udtalelse fra Det Europæiske Økonomiske og Sociale Udvalg ⁽²⁾,

efter den almindelige lovgivningsprocedure ⁽³⁾, og

ud fra følgende betragtninger:

- (1) Unionen skal på fyldestgørende og fuldstændig vis imødegå digitale risici for alle finansielle enheder som følge af en øget anvendelse af informations- og kommunikationsteknologi (IKT) i forbindelse med levering og forbrug af finansielle tjenesteydelser og dermed bidrage til realisering af det potentiale, der ligger i digital finansiering med hensyn til at styrke innovation og fremmekonkurrence i et sikkert digitalt miljø.
- (2) Finansielle enheder er stærkt afhængige af brugen af digitale teknologier i deres daglige aktiviteter. Det er derfor yderst vigtigt at sikre deres digitale aktiviteter operationelle modstandsdygtighed over for IKT-risiko. Dette behov er blevet endnu mere presserende på grund af væksten i banebrydende teknologier på markedet, og navnlig de teknologier, der skaber mulighed for, at digitale repræsentationer af værdier eller rettigheder, der skal overføres og lagres elektronisk ved hjælp af distributed ledger-teknologi eller lignende teknologi (kryptoaktiver), og i tjenesteydelser forbundet med disse aktiver.

⁽¹⁾ EUT C 343 af 26.8.2021, s. 1.

⁽²⁾ EUT C 155 af 30.4.2021, s. 38.

⁽³⁾ Europa-Parlamentets holdning af 10.11.2022 (endnu ikke offentliggjort i EUT) og Rådets afgørelse af 28.11.2022.

- (3) På EU-plan er kravene vedrørende styring af IKT-risikoen i den finansielle sektor fastsat i Europa-Parlamentets og Rådets direktiv 2009/65/EF⁽⁴⁾, 2009/138/EF⁽⁵⁾, 2011/61/EU⁽⁶⁾, 2013/36/EU⁽⁷⁾, 2014/59/EU⁽⁸⁾, 2014/65/EU⁽⁹⁾, (EU) 2015/2366⁽¹⁰⁾ og (EU) 2016/2341⁽¹¹⁾.

Disse krav er forskellige og i nogle tilfælde ufuldstændige. I visse tilfælde er IKT-risikoen kun implicit omhandlet som en del af den operationelle risiko, og den er i andre overhovedet ikke omhandlet. Disse problemer udbedres ved vedtagelsen af Europa-Parlamentets og Rådets forordning (EU) 2022/2554⁽¹²⁾. Nævnte direktiver bør derfor ændres for at sikre overensstemmelse med nævnte forordning. Nærværende direktiv introducerer en række ændringer, som forekommer nødvendige for at skabe juridisk klarhed og sammenhæng, når finansielle enheder, som er meddelt tilladelse og underlagt tilsyn i overensstemmelse med nævnte direktiver, anvender forskellige krav vedrørende digital operationel modstandsdygtighed, som er nødvendige for udøvelsen af deres aktiviteter og leveringen af ydelser og dermed garanterer et velfungerende indre marked. Det er nødvendigt at sikre, at disse krav er tilstrækkelige i forhold til markedsudviklingen, samtidig med at der tilskyndes til proportionalitet, navnlig med hensyn til de finansielle enheders størrelse og de specifikke ordninger som de er omfattet af, med henblik på at reducere overholdelsesomkostningerne.

- (4) På området for bankydelser fastsætter direktiv 2013/36/EU i øjeblikket kun generelle regler vedrørende intern ledelse og bestemmelser om operationel risiko, der omfatter krav vedrørende beredskabs- og kontinuitetsplaner, som implicit udgør grundlaget for håndtering af IKT-risiko. For at håndtere IKT-risiko eksplicit og tydeligt bør kravene vedrørende beredskabs- og kontinuitetsplaner imidlertid ændres, således at de også omfatter forretningskontinuitetsplaner samt planer for indsats- og genopretning vedrørende IKT-risiko i overensstemmelse med kravene i forordning (EU) 2022/2554. Desuden er IKT-risiko kun implicit medtaget, i forbindelse med operationelle risici, i den tilsynskontrol- og vurderingsproces (SREP), der udføres af de kompetente myndigheder, og kriterierne for vurderingen heraf er i øjeblikket fastlagt i Retningslinjer om IKT-risikovurdering under tilsynskontrol- og vurderingsprocessen (SREP), der er udstedt af Den Europæiske Tilsynsmyndighed (Den Europæiske Banktilsynsmyndighed) (EBA), som blev oprettet ved Europa-Parlamentets og Rådets forordning (EU) nr. 1093/2010⁽¹³⁾. Med henblik på at skabe juridisk klarhed og sikre, at banktilsynsmyndighederne rent faktisk afdækker IKT-risiko og

⁽⁴⁾ Europa-Parlamentets og Rådets direktiv 2009/65/EF af 13. juli 2009 om samordning af love og administrative bestemmelser om visse institutter for kollektiv investering i værdipapirer (investeringsinstitutter) (EUT L 302 af 17.11.2009, s. 32).

⁽⁵⁾ Europa-Parlamentets og Rådets direktiv 2009/138/EF af 25. november 2009 om adgang til og udøvelse af forsikrings- og genforsikringsvirksomhed (Solvens II) (EUT L 335 af 17.12.2009, s. 1).

⁽⁶⁾ Europa-Parlamentets og Rådets direktiv 2011/61/EU af 8. juni 2011 om forvaltere af alternative investeringsfonde og om ændring af direktiv 2003/41/EF og 2009/65/EF samt forordning (EF) nr. 1060/2009 og (EU) nr. 1095/2010 (EUT L 174 af 1.7.2011, s. 1).

⁽⁷⁾ Europa-Parlamentets og Rådets direktiv 2013/36/EU af 26. juni 2013 om adgang til at udøve virksomhed som kreditinstitut og om tilsyn med kreditinstitutter og investeringsselskaber, om ændring af direktiv 2002/87/EF og om ophævelse af direktiv 2006/48/EF og 2006/49/EF (EUT L 176 af 27.6.2013, s. 338).

⁽⁸⁾ Europa-Parlamentets og Rådets direktiv 2014/59/EU af 15. maj 2014 om et regelsæt for genopretning og afvikling af kreditinstitutter og investeringsselskaber og om ændring af Rådets direktiv 82/891/EØF og Europa-Parlamentets og Rådets direktiv 2001/24/EF, 2002/47/EF, 2004/25/EF, 2005/56/EF, 2007/36/EF, 2011/35/EU, 2012/30/EU og 2013/36/EU samt forordning (EU) nr. 1093/2010 og (EU) nr. 648/2012 (EUT L 173 af 12.6.2014, s. 190).

⁽⁹⁾ Europa-Parlamentets og Rådets direktiv 2014/65/EU af 15. maj 2014 om markeder for finansielle instrumenter og om ændring af direktiv 2002/92/EF og direktiv 2011/61/EU (EUT L 173 af 12.6.2014, s. 349).

⁽¹⁰⁾ Europa-Parlamentets og Rådets direktiv (EU) 2015/2366 af 25. november 2015 om betalingstjenester i det indre marked, og om ændring af direktiv 2002/65/EF, 2009/110/EF og 2013/36/EU og forordning (EU) nr. 1093/2010 og om ophævelse af direktiv 2007/64/EF (EUT L 337 af 23.12.2015, s. 35).

⁽¹¹⁾ Europa-Parlamentets og Rådets direktiv (EU) 2016/2341 af 14. december 2016 om arbejdsmarkedsrelaterede pensionskassers (IORP'ers) aktiviteter og tilsynet hermed (EUT L 354 af 23.12.2016, s. 37).

⁽¹²⁾ Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor og om ændring af forordning (EF) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 og (EU) 2016/1011 (se side 1 i denne EUT).

⁽¹³⁾ Europa-Parlamentets og Rådets forordning (EU) nr. 1093/2010 af 24. november 2010 om oprettelse af en europæisk tilsynsmyndighed (Den Europæiske Banktilsynsmyndighed), om ændring af afgørelse nr. 716/2009/EF og om ophævelse af Kommissionens afgørelse 2009/78/EF (EUT L 331 af 15.12.2010, s. 12).

overvåger finansielle enheders styring heraf i overensstemmelse med den nye ramme for digital operationel modstandsdygtighed, bør anvendelsesområdet for SREP også ændres, så det eksplicit henviser til kravene i forordning (EU) 2022/2554 og navnlig dækker de risici, der afdækkes i indberetninger om større IKT-relaterede hændelser og af resultaterne af de test af den digitale operationelle modstandsdygtighed, som de finansielle enheder udfører i overensstemmelse med nævnte forordning.

- (5) Digital operationel modstandsdygtighed er en væsentlig forudsætning for at opretholde en finansiell enheds kritiske funktioner og centrale forretningsområder i tilfælde af dens afvikling og derved undgå forstyrrelser af realøkonomien og i det finansielle system. Større operationelle hændelser kan hæmme en finansiell enheds evne til at fortsætte driften og kan true afviklingsmålene. Visse kontraktlige ordninger for brugen af IKT-tjenester er vigtige for at sikre operationel kontinuitet og at levere de nødvendige data i tilfælde af afvikling. Med henblik på tilpasning til målene i EU's ramme for operationel modstandsdygtighed bør direktiv 2014/59/EU ændres i overensstemmelse hermed for at sikre, at oplysninger vedrørende operationel modstandsdygtighed tages i betragtning i forbindelse med afviklingsplanlægning og vurdering af finansieringsenheders afviklingsmuligheder.
- (6) Direktiv 2014/65/EU fastsætter kun strengere regler med hensyn til IKT-risiko for investeringsselskaber og markedspladser, der er involveret i algoritmisk handel. Der gælder mindre detaljerede krav for dataindberetnings-tjenester og transaktionsregistre. Direktiv 2014/65/EU omhandler også kun i begrænset omfang kontrol- og sikkerhedsforanstaltninger på edb-området og anvendelsen af passende systemer, ressourcer og procedurer til sikring af kontinuiteten og regelmæssigheden i forbindelse med erhvervs-tjenester. Desuden bør nævnte direktiv bringes i overensstemmelse med forordning (EU) 2022/2554 for så vidt angår kontinuitet og regelmæssighed i ydelsen af investeringsservice og udførelsen af investeringsaktiviteter, operationel modstandsdygtighed, handelssystemers kapacitet og effektivitet i forbindelse med ordninger til sikring af driftsstabilitet og risikostyring.
- (7) Direktiv (EU) 2015/2366 fastsætter særlige regler for IKT-sikkerhedskontroller og begrænsende elementer med henblik på tilladelse til at udbyde betalingstjenester. Disse regler om tilladelse bør ændres, så de bliver bragt i overensstemmelse med forordning (EU) 2022/2554. For at mindske den administrative byrde og undgå kompleksitet og overlappende indberetningskrav bør reglerne om indberetning af hændelser i nævnte direktiv desuden ophøre med at finde anvendelse på betalingstjenesteudbydere, der reguleres i henhold til nævnte direktiv og også er omfattet af forordning (EU) 2022/2554, således at disse betalingstjenesteudbydere kan benytte sig af en fælles og fuldt ud harmoniseret mekanisme til indberetning af hændelser med hensyn til alle operationelle hændelser eller sikkerhedsmæssig betalingsrelaterede hændelser, uanset om sådanne hændelser er IKT-relaterede.
- (8) Direktiv 2009/138/EF og (EU) 2016/2341 omfatter delvis IKT-risiko i de almindelige bestemmelser om ledelse og risikostyring, idet visse krav skal præciseres i delegerede retsakter med eller uden specifik henvisning til IKT-risiko. På tilsvarende vis er de regler, der finder anvendelse på forvaltere af alternative investeringsfonde som omhandlet i direktiv 2011/61/EU og administrations-selskaber som omhandlet i direktiv 2009/65/EF, udelukkende meget generelle. Nævnte direktiver bør derfor bringes i overensstemmelse med de krav, der er fastsat i forordning (EU) 2022/2554 for så vidt angår styringen af IKT-systemer og -værktøjer.
- (9) I mange tilfælde er der allerede fastlagt krav til IKT-risiko i delegerede retsakter og gennemførelsesretsakter, som er vedtaget på grundlag af udkast til reguleringsmæssige tekniske standarder og udkast til gennemførelsesmæssige tekniske standarder, som er udviklet af den kompetente europæiske tilsynsmyndighed. Eftersom bestemmelserne i forordning (EU) 2022/2554 fremover udgør den retlige ramme for IKT-risiko i den finansielle sektor, bør visse beføjelser til at vedtage delegerede retsakter og gennemførelsesretsakter i direktiv 2009/65/EF, 2009/138/EF, 2011/61/EU og 2014/65/EU ændres, således at bestemmelserne om IKT-risiko fjernes fra anvendelsesområdet for de pågældende beføjelser.
- (10) For at sikre en sammenhængende gennemførelse af den nye ramme for digital operationel modstandsdygtighed i den finansielle sektor, bør medlemsstaterne anvende bestemmelserne i national ret om gennemførelse af dette direktiv fra datoen for anvendelse af forordning (EU) 2022/2554.

- (11) Direktiv 2009/65/EF, 2009/138/EF, 2011/61/EU, 2013/36/EU, 2014/59/EU, 2014/65/EU, (EU) 2015/2366 og (EU) 2016/2341 er vedtaget på grundlag af artikel 53, stk. 1, eller artikel 114 i traktaten om Den Europæiske Unions funktionsmåde (TEUF), eller begge. Ændringerne i nærværende direktiv er blevet indarbejdet i én enkelt lovgivningsmæssig retsakt, da genstanden for og målene med ændringerne er indbyrdes forbundet. Nærværende direktiv bør derfor vedtages på grundlag af både artikel 53, stk. 1, og artikel 114 i TEUF.
- (12) Målene for dette direktiv kan ikke i tilstrækkelig grad opfyldes af medlemsstaterne, da de indebærer harmonisering af krav, der allerede er indeholdt i direktiver, men kan på grund af foranstaltningens omfang og virkninger bedre nås på EU-plan; Unionen kan derfor vedtage foranstaltninger i overensstemmelse med nærhedsprincippet, jf. artikel 5 i traktaten om Den Europæiske Union. I overensstemmelse med proportionalitetsprincippet, jf. nævnte artikel, går dette direktiv ikke videre, end hvad der er nødvendigt for at nå disse mål.
- (13) I henhold til den fælles politiske erklæring af 28. september 2011 fra medlemsstaterne og Kommissionen om forklarende dokumenter⁽¹⁴⁾ har medlemsstaterne forpligtet sig til i tilfælde, hvor det er berettiget, at lade meddelelsen af gennemførelsesforanstaltninger ledsage af et eller flere dokumenter, der forklarer forholdet mellem et direktivs bestanddele og de tilsvarende dele i de nationale gennemførelsesinstrumenter. I forbindelse med dette direktiv finder lovgiver, at fremsendelse af sådanne dokumenter er berettiget —

VEDTAGET DETTE DIREKTIV:

Artikel 1

Ændringer af direktiv 2009/65/EF

I artikel 12 i direktiv 2009/65/EF foretages følgende ændringer:

1) Stk. 1, andet afsnit, litra a), affattes således:

- »a) har en sund administrativ og regnskabsmæssig praksis, kontrol- og sikringsforanstaltninger på edb-området, herunder hvad angår net- og informationssystemer, som oprettes og styres i overensstemmelse med Europa-Parlamentets og Rådets forordning (EU) 2022/2554 (*), samt fyldestgørende interne kontrolprocedurer, herunder navnlig regler for de ansattes personlige transaktioner eller for besiddelse eller administration af investeringer i finansielle instrumenter med henblik på investering for egen regning, som mindst sikrer, at enhver transaktion, der implicerer investeringsinstituttet, kan rekonstrueres med hensyn til oprindelse, implicerede parter, art samt tid og sted for gennemførelsen, og at aktiver i investeringsinstitutter, der administreres af administrationselskaber, investeres i overensstemmelse med fondsbestemmelserne eller vedtægterne og gældende ret

(*) Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor og om ændring af forordning (EF) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 og (EU) 2016/1011 (EUT L 333 af 27.12.2022, s. 1).«

2) Stk. 3 affattes således:

»3. Uden at det berører artikel 116, vedtager Kommissionen ved hjælp af delegerede retsakter i overensstemmelse med artikel 112a, foranstaltninger, der fastlægger

- a) de procedurer og de foranstaltninger, der er omhandlet i stk. 1, andet afsnit, litra a), bortset fra de procedurer og foranstaltninger, der vedrører net- og informationssystemer
- b) de strukturer og organisatoriske krav med henblik på minimering af interessekonflikter, som er omhandlet i stk. 1, andet afsnit, litra b).«

(14) EUT C 369 af 17.12.2011, s. 14.

Artikel 2

Ændringer af direktiv 2009/138/EF

I direktiv 2009/138/EF foretages følgende ændringer:

1) Artikel 41, stk. 4, affattes således:

»4. Forsikrings- og genforsikringselskaber træffer passende foranstaltninger til at sikre kontinuitet og regelmæssighed i udøvelsen af deres virksomhed, inklusive udarbejdelse af beredskabsplaner. Selskabet anvender med henblik herpå hensigtsmæssige og rimeligt afpassede systemer, ressourcer og procedurer og opretter og styrer navnlig net- og informationssystemer i overensstemmelse med i Europa-Parlamentets og Rådets forordning (EU) 2022/2554 (*).

(*) Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor og om ændring af forordning (EF) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 og (EU) 2016/1011 (EUT L 333 af 27.12.2022, s. 1).«

2) Artikel 50, stk. 1, litra a) og b), affattes således:

- a) elementerne i de systemer, der er omhandlet i artikel 41, artikel 44, navnlig de områder, der er omhandlet i artikel 44, stk. 2, og artikel 46 og 47, bortset fra de elementer, der vedrører risikostyring i forbindelse med informations- og kommunikationsteknologi
- b) de funktioner, der er omhandlet i artikel 44, 46, 47 og 48, bortset fra de funktioner, der vedrører risikostyring i forbindelse med informations- og kommunikationsteknologi.«

Artikel 3

Ændring af direktiv 2011/61/EU

Artikel 18 i direktiv 2011/61/EU affattes således:

»Artikel 18

Generelle principper

1. Medlemsstaterne kræver, at FAIF'er til enhver tid anvender tilstrækkelige og egnede menneskelige og tekniske ressourcer for at sikre korrekt forvaltning af AIF'er.

Især skal de kompetente myndigheder i FAIF'ens hjemland under hensyntagen til karakteren af de AIF'er, der forvaltes af FAIF'en, kræve, at FAIF'en har sunde administrative og regnskabsmæssige praksis, kontrol- og sikringsforanstaltninger på edb-området, herunder hvad angår net- og informationssystemer, som oprettes og styres i overensstemmelse med Europa-Parlamentets og Rådets forordning (EU) 2022/2554 (*), samt fyldestgørende interne kontrolmekanismer, herunder navnlig regler for sine arbejdstageres personlige transaktioner eller for besiddelse eller forvaltning af investeringer med henblik på investering for egen regning, som mindst sikrer, at enhver transaktion, der implicerer AIF'er, kan rekonstrueres med hensyn til oprindelse, involverede parter, art samt tid og sted for gennemførelsen, og at aktiver i de AIF'er, som forvaltes af FAIF'en, investeres i overensstemmelse med AIF'ens regler eller vedtægter og gældende ret.

2. Kommissionen vedtager ved hjælp af delegerede retsakter i overensstemmelse med artikel 56 og på de i artikel 57 og 58 anførte betingelser foranstaltninger til præcisering af de procedurer og foranstaltninger, der er omhandlet i nærværende artikels stk. 1, bortset fra de procedurer og foranstaltninger, der vedrører net- og informationssystemer.

(*) Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor og om ændring af forordning (EF) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 og (EU) 2016/1011 (EUT L 333 af 27.12.2022, s. 1).«

Artikel 4

Ændringer af direktiv 2013/36/EU

I direktiv 2013/36/EU foretages følgende ændringer:

1) Artikel 65, stk. 3, litra a), nr. vi), affattes således:

- »vi) tredjeparter, som de enheder, der er omhandlet i nr. i)-iv), har outsourcet funktioner eller aktiviteter til, herunder tredjepartsudbydere af IKT-tjenester som omhandlet i kapitel V i Europa-Parlamentets og Rådets forordning (EU) 2022/2554 (*)

(*) Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor og om ændring af forordning (EF) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 og (EU) 2016/1011 (EUT L 333 af 27.12.2022, s. 1).«

2) Artikel 74, stk. 1, første afsnit, affattes således:

»Institutter skal have robuste ledelsesordninger, hvilket omfatter en klar organisatorisk struktur med en veldefineret, gennemsigtig og konsekvent ansvarsfordeling og effektive procedurer til at identificere, styre, overvåge og indberette de risici, som institutterne er eller kan blive eksponeret for, fyldestgørende interne kontrolmekanismer, herunder en sund administrativ og regnskabsmæssig praksis samt net- og informationssystemer, der etableres og styres i overensstemmelse med forordning (EU) 2022/2554, og en aflønningspolitik og -praksis, som er i overensstemmelse med og fremmer en forsvarlig og effektiv risikostyring.«

3) Artikel 85, stk. 2, affattes således:

»2. De kompetente myndigheder sikrer, at institutterne råder over fyldestgørende beredskabs- og kontinuitetspolitikker og planer, herunder politikker og planer for IKT-driftsstabilitet og planer for IKT-indsats- og genopretning i forbindelse med den teknologi, som de anvender til formidling af oplysninger, og at disse planer udarbejdes, forvaltes og testes i overensstemmelse med artikel 11 i forordning (EU) 2022/2554, med henblik på at gøre det muligt for institutterne at videreføre driften i tilfælde af alvorlige driftsforstyrrelser og begrænse tab som følge af sådanne forstyrrelser.«

4) I artikel 97, stk. 1, tilføjes følgende litra:

- »d) de risici, som afsløres ved test af digital operationel modstandsdygtighed i overensstemmelse med kapitel IV i forordning (EU) 2022/2554.«

Artikel 5

Ændringer af direktiv 2014/59/EU

I direktiv 2014/59/EU foretages følgende ændringer:

1) I artikel 10 foretages følgende ændringer:

a) Stk. 7, litra c), affattes således:

- »c) en beskrivelse af, hvordan kritiske funktioner og centrale forretningsområder i nødvendigt omfang vil kunne adskilles juridisk og økonomisk fra andre funktioner for at sikre deres videreførelse og digitale operationelle modstandsdygtighed i tilfælde af, at instituttet bliver nødlidende«.

b) Stk. 7, litra q), affattes således:

- »q) en beskrivelse af de aktiviteter og systemer, der har afgørende betydning for opretholdelsen af den fortsatte gennemførelse af instituttets operationelle procedurer, herunder net- og informationssystemer som omhandlet i Europa-Parlamentets og Rådets forordning (EU) 2022/2554 (*)

(*) Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor og om ændring af forordning (EF) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 og (EU) 2016/1011 (EUT L 333 af 27.12.2022, s. 1).«

c) I stk. 9 tilføjes følgende afsnit:

»EBA gennemgår og ajourfører om nødvendigt de reguleringsmæssige tekniske standarder i overensstemmelse med artikel 10 i forordning (EU) nr. 1093/2010 for bl.a. at tage højde for bestemmelserne i kapitel II i forordning (EU) 2022/2554.«

2) I bilaget foretages følgende ændringer:

a) Afsnit A, punkt 16), affattes således:

»16) ordninger og foranstaltninger, som er nødvendige for at bevare den fortsatte drift af instituttets operationelle procedurer, herunder net- og informationssystemer, som oprettes og styres i overensstemmelse med forordning (EU) 2022/2554.«

b) I afsnit B foretages følgende ændringer:

i) Punkt 14) affattes således:

»14) identifikation af ejerne af de i punkt 13) anførte systemer, tilknyttede serviceleveranceaftaler og software og systemer eller licenser, herunder en oversigt pr. deres juridiske enheder, kritiske funktioner og centrale forretningsområder samt identifikation af kritiske tredjepartsudbydere af IKT-tjenester som defineret i artikel 3, nr. 23), i forordning (EU) 2022/2554.«

ii) Følgende punkt indsættes:

»14a) resultaterne af institutternes test af digital operationel modstandsdygtighed i henhold til forordning (EU) 2022/2554.«

c) I afsnit C foretages følgende ændringer:

i) Punkt 4) affattes således:

»4) hvorvidt de serviceaftaler, som instituttet har indgået, herunder kontraktlige ordninger for brugen af IKT-tjenester, er robuste og kan håndhæves fuldt ud i tilfælde af afvikling af instituttet.«

ii) Følgende punkt indsættes:

»4a) den digitale operationelle modstandsdygtighed for de net- og informationssystemer, der understøtter instituttets kritiske funktioner og centrale forretningsområder, under hensyntagen til indberetninger om større IKT-relaterede hændelser og resultaterne af test af digital operationel modstandsdygtighed i henhold til forordning (EU) 2022/2554.«

Artikel 6

Ændringer af direktiv 2014/65/EU

I direktiv 2014/65/EU foretages følgende ændringer:

1) I artikel 16 foretages følgende ændringer:

a) Stk. 4 affattes således:

»4. Et investeringsselskab skal, inden for rimelighedens grænser, træffe sådanne foranstaltninger, som måtte være nødvendige for at sikre kontinuitet og regelmæssighed i ydelsen af investeringsservice og udførelsen af investeringsaktiviteter. Investeringsselskabet anvender med henblik herpå hensigtsmæssige og forholdsmæssigt afpassede systemer, herunder informations- og kommunikationsteknologisystemer (»IKT-systemer«), som oprettes og styres i overensstemmelse med artikel 7 i Europa-Parlamentets og Rådets forordning (EU) 2022/2554 (*), samt hensigtsmæssige og forholdsmæssigt afpassede ressourcer og procedurer.

(*) Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor og om ændring af forordning (EF) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 og (EU) 2016/1011 (EUT L 333 af 27.12.2022, s. 1).«

b) Stk. 5, andet og tredje afsnit, affattes således:

»Et investeringsselskab skal have en sund administrativ og regnskabsmæssig praksis, interne kontrolmekanismer og effektive procedurer til risikovurdering.

Uden at det berører kompetente myndigheders mulighed for at kræve adgang til kommunikation i overensstemmelse med dette direktiv og forordning (EU) nr. 600/2014 skal et investeringsselskab have etableret forsvarlige sikkerhedsmekanismer med henblik på i overensstemmelse med kravene i forordning (EU) 2022/2554 at garantere sikring og autentificering af midlerne til overførsel af information, at minimere risikoen for dataforvanskning og uautoriseret adgang og forhindre lækage af oplysninger, således at datasikkerheden garanteres til enhver tid.«

2) I artikel 17 foretages følgende ændringer:

a) Stk. 1 affattes således:

»1. Et investeringsselskab, der benytter sig af algoritmisk handel, skal have effektive systemer og risikokontrolforanstaltninger, som svarer til den virksomhed, som selskabet driver, med henblik på at sikre, at dets handelssystemer er modstandsdygtige og har tilstrækkelig kapacitet i overensstemmelse med kravene i kapitel II i forordning (EU) 2022/2554, er underlagt passende handelstærskler og -begrænsninger og forhindrer, at der afgives fejlagtige ordrer, eller at systemerne på anden måde fungerer dårligt, så det skaber eller bidrager til forstyrrelser på markedet.

Et sådant selskab skal også have effektive systemer og risikokontrolforanstaltninger med henblik på at sikre, at handelssystemerne ikke kan anvendes til formål, som strider mod forordning (EU) nr. 596/2014 eller mod de regler, der gælder for en markedsplads, som det er knyttet til.

Investeringsselskabet skal have effektive ordninger for forretningskontinuitet med henblik på at kunne håndtere en brist i dets handelssystemer, herunder politikker og planer for IKT-driftsstabilitet og planer for IKT-indsats- og genopretning, som er udarbejdet i overensstemmelse med artikel 11 i forordning (EU) 2022/2554, og skal desuden sørge for, at dets systemer er grundigt afprøvet og underlagt behørig overvågning med henblik på at sikre, at de opfylder kravene fastsat i dette stykke og eventuelle specifikke krav fastsat i kapitel II og IV i forordning (EU) 2022/2554.«

b) Stk. 7, litra a), affattes således:

»a) enkelthederne i de i stk. 1-6 fastsatte organisatoriske krav, bortset fra de organisatoriske krav, der vedrører IKT-risikostyring, som skal opfyldes af investeringsselskaber, som udfører forskellige former for investeringsservice, investeringsaktiviteter, accessoriske tjenesteydelser eller kombinationer heraf, hvorved præciseringerne vedrørende de organisatoriske krav i stk. 5 skal fastlægge de specifikke krav for direkte markedsadgang og sponsoreret adgang, således at det sikres, at kontrolforanstaltningerne i forbindelse med sponsoreret adgang mindst svarer til dem, der anvendes i forbindelse med direkte markedsadgang«.

3) I artikel 47, stk. 1, foretages følgende ændringer:

a) Litra b) affattes således:

»b) er tilstrækkelig rustet til at styre de risici, markedet udsættes for, herunder til at styre IKT-risiko i overensstemmelse med kapitel II i forordning (EU) 2022/2554, anvender fyldestgørende ordninger og systemer med henblik på at påvise væsentlige risici for markedets drift og har indført effektive foranstaltninger til at mindske disse risici.«

b) Litra c) udgår.

4) I artikel 48 foretages følgende ændringer:

a) Stk. 1 affattes således:

»1. Medlemsstaterne stiller krav om, at et reguleret marked skal etablere og opretholde sin operationelle modstandsdygtighed i overensstemmelse med kravene i kapitel II i forordning (EU) 2022/2554 for at sikre, at dets handelssystemer er modstandsdygtige, har tilstrækkelig kapacitet til at klare spidsbelastninger med hensyn til ordrer og meddelelser, kan sikre korrekt handel i tilfælde af alvorlig markedsstress, er fuldt gennemprøvede for at sikre, at sådanne betingelser er opfyldt, og er omfattet af effektive ordninger til sikring af driftsstabilitet, herunder politikker og planer for IKT-driftsstabilitet og planer for IKT-indsats- og genopretning udarbejdet i overensstemmelse med artikel 11 i forordning (EU) 2022/2554, til at sikre opretholdelsen af markedets tjenester i tilfælde af et svigt af dets handelssystemer.«

b) Stk. 6 affattes således:

»6. Medlemsstaterne stiller krav om, at et reguleret marked skal have etableret effektive systemer, procedurer og ordninger, som bl.a. kræver, at medlemmer eller deltagere gennemfører passende test af algoritmer, og skaber rammer, der letter en sådan test i overensstemmelse med kravene i kapital II og IV i forordning (EU) 2022/2554 til at sikre, at algoritmiske handelssystemer ikke kan skabe eller bidrage til ureglementerede handelsvilkår på markedet og til at håndtere eventuelle ureglementerede handelsvilkår, der opstår på grund af sådanne algoritmiske handelssystemer, herunder systemer, der begrænser forholdet mellem ikkeudførte ordrer og transaktioner, der kan indføres i systemet af et medlem eller en deltager, således at det bliver muligt at bremse ordrestrømmen, hvis der er risiko for, at man når op på systemets maksimale kapacitet, og at den minimumskursændring (tick size), der kan anvendes på markedet, begrænses og håndhæves.«

c) I stk. 12 foretages følgende ændringer:

i) Litra a) affattes således:

»a) forpligtelserne til at sikre, at regulerede markeders handelssystemer er fleksible og har en tilstrækkelig kapacitet, med undtagelse af de forpligtelser, som vedrører digital operationel modstandsdygtighed.«

ii) Litra g) affattes således:

»g) forpligtelserne til at sikre passende test af algoritmer, bortset fra test af digital operationel modstandsdygtighed, med henblik på at sikre, at algoritmiske handelssystemer, herunder algoritmiske højfrekvenshandelssystemer, ikke kan skabe eller bidrage til ureglementerede handelsvilkår på markedet.«

Artikel 7

Ændring af direktiv (EU) 2015/2366

I direktiv (EU) 2015/2366 foretages følgende ændringer:

1) Artikel 3, litra j), affattes således:

»j) tjenester leveret af udbydere af tekniske tjenester, der understøtter udbuddet af betalingstjenester, uden at udbyderne på noget tidspunkt kommer i besiddelse af de midler, som skal overføres, herunder behandling og lagring af data, tillidsskabende tjenester og tjenester til beskyttelse af privatlivets fred, autentifikation af data og enheder, levering af informations- og kommunikationsteknologi (IKT) og kommunikationsnetværk, levering og vedligeholdelse af terminaler og anordninger til brug for betalingstjenester, med undtagelse af betalingsinitieringstjenester og kontooplysningstjenester.«

2) I artikel 5, stk. 1, foretages følgende ændringer:

a) I første afsnit foretages følgende ændringer:

i) Litra e) affattes således:

»e) en beskrivelse af ansøgerens forvaltningsordninger og interne kontrolmekanismer, herunder administrative, risikostyringsmæssige og regnskabsmæssige procedurer samt ordninger for brug af IKT-tjenester i overensstemmelse med Europa-Parlamentets og Rådets forordning (EU) 2022/2554 (*), der dokumenterer, at disse forvaltningsordninger og interne kontrolmekanismer er proportionale, passende, forsvarlige og tilstrækkelige

(*) Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor og om ændring af forordning (EF) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 og (EU) 2016/1011 (EUT L 333 af 27.12.2022, s. 1).«

ii) Litra f) affattes således:

»f) en beskrivelse af den procedure, der er indført for at håndtere og følge op på sikkerhedshændelser og sikkerhedsrelaterede kundeklager, herunder en ordning for indberetning af hændelser, hvori der er taget højde for betalingsinstituttets indberetningsforpligtelser, jf. kapitel III i forordning (EU) 2022/2554.«

iii) Litra h) affattes således:

- »h) en beskrivelse af ordningerne for forretningskontinuitet, herunder en klar fastlæggelse af de kritiske funktioner, effektive politikker og planer for IKT-driftsstabilitet og planer for IKT-indsats- og genopretning og en procedure til regelmæssigt at teste og evaluere, om sådanne planer er tilstrækkelige og effektive, i overensstemmelse med forordning (EU) 2022/2554.«

b) Tredje afsnit affattes således:

»Det skal i tilknytning til de i første afsnits litra j) omhandlede sikkerhedskontrolforanstaltninger og begrænsende foranstaltninger angives, hvordan de sikrer et højt niveau af digital operationel modstandsdygtighed i overensstemmelse med kapitel II i forordning (EU) 2022/2554, navnlig med hensyn til teknisk sikkerhed og databeskyttelse, herunder vedrørende de software- og IKT-systemer, der anvendes af ansøgeren eller de virksomheder, som ansøgeren outsourcer hele eller dele af sine aktiviteter til. Disse foranstaltninger skal også omfatte de sikkerhedsforanstaltninger, der er fastsat i dette direktivs artikel 95, stk. 1. Foranstaltningerne skal tage højde for EBA's retningslinjer om sikkerhedsforanstaltninger som omhandlet i dette direktivs artikel 95, stk. 3, når de foreligger.«

3) Artikel 19, stk. 6, andet afsnit, affattes således:

»Vigtige driftsmæssige funktioner, herunder IKT-systemer, må ikke outsources på en måde, der i væsentlig grad forringer kvaliteten af betalingsinstituttets interne kontrol og de kompetente myndigheders mulighed for at kunne overvåge og spore, om betalingsinstituttet overholder alle forpligtelserne i dette direktiv.«

4) I artikel 95, stk. 1, tilføjes følgende afsnit:

»Første afsnit berører ikke anvendelsen af kapitel II i forordning (EU) 2022/2554 på:

- a) betalingstjenesteudbydere som omhandlet i dette direktivs artikel 1, stk. 1, litra a), b) og d)
- b) kontooplysningstjenesteudbydere, jf. dette direktivs artikel 33, stk. 1
- c) betalingsinstitutter, der er undtaget i henhold til dette direktivs artikel 32, stk. 1, og
- d) e- pengeinstitutter, der er omfattet af en undtagelse, som omhandlet i artikel 9, stk. 1, i direktiv 2009/110/EF.«

5) I artikel 96 tilføjes følgende stykke:

»7. Medlemsstaterne sikrer, at nærværende artikels stk. 1-5 ikke finder anvendelse på:

- a) betalingstjenesteudbydere som omhandlet i dette direktivs artikel 1, stk. 1, litra a), b) og d)
- b) kontooplysningstjenesteudbydere, jf. dette direktivs artikel 33, stk. 1
- c) betalingsinstitutter, der er undtaget i henhold til dette direktivs artikel 32, stk. 1, og
- d) e- pengeinstitutter, der er omfattet af en undtagelse som omhandlet i artikel 9, stk. 1, i direktiv 2009/110/EF.«

6) Artikel 98, stk. 5, affattes således:

»5. EBA gennemgår og ajourfører om nødvendigt regelmæssigt de reguleringsmæssige tekniske standarder i overensstemmelse med artikel 10 i forordning (EU) nr. 1093/2010 for bl.a. at tage højde for innovation og den teknologiske udvikling og for bestemmelserne i kapitel II i forordning (EU) 2022/2554.«

Artikel 8

Ændring af direktiv (EU) 2016/2341

Artikel 21, stk. 5, i direktiv (EU) 2016/2341 affattes således:

- »5. Medlemsstaterne sikrer, at IORP'er træffer passende foranstaltninger til at sikre kontinuitet og regelmæssighed i udøvelsen af deres virksomhed, herunder udarbejdelse af beredskabsplaner. IORP'er anvender med henblik herpå

hensigtsmæssige og rimeligt afpassede systemer, ressourcer og procedurer og opretter og styrer navnlig net- og informationssystemer i overensstemmelse med Europa-Parlamentets og Rådets forordning (EU) 2022/2554 (*), hvis det er relevant.

(*) Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstanddygtighed i den finansielle sektor og om ændring af forordning (EF) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 og (EU) 2016/1011 (EUT L 333 af 27.12.2022, s. 1).«

Artikel 9

Gennemførelse

1. Medlemsstaterne vedtager og offentliggør senest den 17. januar 2025 de bestemmelser, der er nødvendige for at efterkomme dette direktiv. De underretter straks Kommissionen herom.

De anvender disse bestemmelser fra den 17. januar 2025.

Disse bestemmelser skal ved vedtagelsen indeholde en henvisning til dette direktiv eller skal ved offentliggørelsen ledsages af en sådan henvisning. De nærmere regler for henvisningen fastsættes af medlemsstaterne.

2. Medlemsstaterne meddeler Kommissionen teksten til de vigtigste nationale love og bestemmelser, som de udsteder på det område, der er omfattet af dette direktiv.

Artikel 10

Ikrafttræden

Dette direktiv træder i kraft på tyvendedagen efter offentliggørelsen i *Den Europæiske Unions Tidende*.

Artikel 11

Adressater

Dette direktiv er rettet til medlemsstaterne.

Udfærdiget i Strasbourg, den 14. december 2022.

På Europa-Parlamentets vegne

R. METSOLA

Formand

På Rådets vegne

M. BEK

Formand