EBA/GL/2021/03

10. juni 2021

Reviderede retningslinjer

for indberetning af større hændelser i henhold til PSD2

1. Compliance- og indberetningsforpligtelser

Status for disse retningslinjer

1. Dette dokument indeholder retningslinjer, som er udstedt i henhold til artikel 16 i EBA-forordningen[1]. I henhold til artikel 16, stk. 3, i EBA-forordningen skal kompetente myndigheder og finansielle institutioner bestræbe sig bedst muligt på at efterleve disse retningslinjer.

2. Retningslinjerne fastlægger EBA's syn på hensigtsmæssig tilsynspraksis inden for Det Europæiske Finanstilsynssystem, eller hvordan EU-lovgivningen bør anvendes på et bestemt område. Kompetente myndigheder som defineret i artikel 4, stk. 2, i EBA-forordningen, og som er omfattet af retningslinjerne, bør efterleve disse ved i fornødent omfang at indarbejde dem i deres praksis (f.eks. ved at ændre deres retlige rammer eller deres tilsynsprocesser), også hvor retningslinjerne primært er rettet mod institutioner.

Indberetningskrav

3. I henhold til artikel 16, stk. 3, i EBA-forordningen skal kompetente myndigheder senest den (07.11.2021) underrette EBA om, hvorvidt de efterlever eller agter at efterleve disse retningslinjer, eller årsagen til eventuelt manglende efterlevelse. Hvis EBA ikke har modtaget underretning inden denne dato, anser EBA de kompetente myndigheder for ikke at efterleve retningslinjerne. Underretninger fremsendes ved hjælp af det skema, der er tilgængeligt på EBA's websted, med referencen "EBA/GL/2021/03". Underretninger fremsendes af personer med behørig beføjelse til at indberette efterlevelse på vegne af deres kompetente myndighed. Enhver ændring af status med hensyn til efterlevelse skal også meddeles EBA.

4. Underretninger offentliggøres på EBA's websted i henhold til artikel 16, stk. 3.

[1] 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).

2. Emne, anvendelsesområde og definitioner

Emne

5. Disse retningslinjer følger af det mandat, der er givet til EBA i artikel 96, stk. 3, i Europa-Parlamentets og Rådets direktiv (EU) 2015/2366 af 25. november 2015 om betalingstjenester i det indre marked, 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 (PSD2).

6. Navnlig fastsætter disse retningslinjer kriterierne for betalingstjenesteudbyderes klassificering af større drifts- eller sikkerhedshændelser samt det format og de procedurer, de bør følge til at underrette den kompetente myndighed i hjemlandet om sådanne hændelser i henhold til artikel 96, stk. 1, i PSD2.

7. Derudover omhandler retningslinjerne, hvordan disse kompetente myndigheder bør vurdere en hændelses relevans samt oplysningerne i de hændelsesrapporter, som de i henhold til artikel 96, stk. 2, i PSD2 skal videregive til andre nationale myndigheder.

8. Endvidere omhandler disse retningslinjer videregivelsen af relevante oplysninger vedrørende de indberettede hændelser til EBA og ECB med det formål at fremme en fælles og ensartet metode.

Anvendelsesområde

9. Disse retningslinjer finder anvendelse ved klassificering og indberetning af større drifts- eller sikkerhedshændelser i henhold til artikel 96 i PSD2.

10. Disse retningslinjer finder anvendelse på alle hændelser, der er omfattet af definitionen af "større drifts- eller sikkerhedshændelser", som omfatter både eksterne og interne hændelser, uanset om de er bevidst skadevoldende eller utilsigtede.

11. Disse retningslinjer gælder også, hvis den større drifts- eller sikkerhedshændelse er opstået uden for Unionen (f.eks. når en hændelse hidrører fra et moderselskab eller datterselskab, der er etableret udenfor Unionen) og berører de betalingstjenester, der leveres af en betalingstjenesteudbyder hjemmehørende i Unionen, enten direkte (en betalingsrelateret tjeneste udføres af den berørte tredjelandsvirksomhed) eller indirekte (betalingstjenesteudbyderens evne til at fortsætte sin betalingsaktivitet er på anden måde truet som følge af hændelsen).

12. Disse retningslinjer gælder også for større hændelser, der påvirker funktioner, som betalingstjenesteudbydere har outsourcet til tredjeparter.

Målgruppe

13. Det første sæt retningslinjer (afsnit 4) henvender sig til betalingstjenesteudbydere som defineret i artikel 4, stk. 11, i PSD2 og som omhandlet i artikel 4, stk. 1, i forordning (EU) 1093/2010.

14. Det andet og tredje sæt retningslinjer (afsnit 5 og 6) henvender sig til kompetente myndigheder som defineret i artikel 4, stk. 2, litra i), i forordning (EU) nr. 1093/2010.

Definitioner

15. Medmindre andet er angivet, har de termer, der er anvendt og defineret i PSD2, samme betydning i disse retningslinjer. I disse retningslinjer gælder endvidere følgende definitioner:

Drifts- eller sikkerhedshændelse	En enkeltstående begivenhed eller en række sammenhængende begivenheder, der ikke er planlagt af betalingstjenesteudbyderen, og som har fået eller formodes at få negativ indvirkning på betalingsrelaterede tjenesters integritet, tilgængelighed, fortrolighed og/eller ægthed.
Integritet	Den egenskab, at korrektheden og fuldstændigheden af aktiver (herunder data) varetages.
Tilgængelighed	Den egenskab, at betalingsrelaterede tjenester er til rådighed og anvendelige for betalingstjenestebrugere i henhold til anerkendte niveauer, som betalingstjenesteudbyderen har fastsat på forhånd.
Fortrolighed	Den egenskab, at oplysninger ikke gøres tilgængelige eller videregives til uautoriserede personer, virksomheder eller processer.
Ægthed	Den egenskab ved en kilde, at den er, hvad den hævder at være.
Betalingsrelaterede tjenester	Forretningsaktiviteter i den i artikel 4, stk. 3, i PSD2 anvendte forstand og alle de tekniske støttefunktioner, der er nødvendige for korrekt levering af betalingstjenester.

3. Gennemførelse

Anvendelsesdato

16. Disse retningslinjer finder anvendelse fra den 1. januar 2022.

Ophævelse

17. Følgende retningslinjer ophæves med virkning fra den 1. januar 2022:

Retningslinjer for indberetning af større hændelser i henhold til direktiv (EU) 2015/2366 (PSD2) (EBA/GL/2017/10)

4. Retningslinjer, der henvender sig til betalingstjenesteudbydere i forbindelse med indberetning af større drifts- eller sikkerhedshændelser til den kompetente myndighed i deres hjemland

Retningslinje 1: Klassificering som større hændelse

1.1. Betalingstjenesteudbydere bør klassificere drifts- eller sikkerhedshændelser som større, hvis de opfylder

a. et eller flere kriterier på det "højere indvirkningsniveau" eller

b. tre eller flere kriterier på det "lavere indvirkningsniveau"

som beskrevet i retningslinje 1.4, og i overensstemmelse med den vurdering, som er fastlagt i disse retningslinjer.

1.2. Betalingstjenesteudbydere bør vurdere en drifts- eller sikkerhedshændelse i forhold til følgende kriterier og deres underliggende indikatorer:

i. Berørte transaktioner

Betalingstjenesteudbydere bør fastslå den samlede værdi af de berørte transaktioner samt antallet af berørte betalinger som procentdel af det antal betalingstransaktioner, der normalt foretages med de berørte betalingstjenester.

ii. Berørte betalingstjenestebrugere

Betalingstjenesteudbydere bør fastslå det berørte antal betalingstjenestebrugere både i absolutte tal og som procentdel af det samlede antal betalingstjenestebrugere.

iii. Brud på sikkerheden i netværks- eller informationssystemer

Betalingstjenesteudbydere bør fastslå, om en ondsindet handling har skadet sikkerheden i netværks- eller informationssystemer med relation til levering af betalingstjenester.

iv. Tjenestens nedetid

Betalingstjenesteudbydere bør fastslå den periode, hvor tjenesten sandsynligvis vil være utilgængelig for betalingstjenestebrugeren, eller hvor betalingsordren i den i artikel 4, stk. 13, i den i PSD2 anvendte forstand ikke kan udføres af betalingstjenesteudbyderen.

v. Økonomisk indvirkning

Betalingstjenesteudbydere bør fastslå de samlede omkostninger, der er forbundet med hændelsen, og heri medregne både det absolutte beløb og, hvor det er relevant, omkostningernes relative betydning i forhold til betalingstjenesteudbyderens størrelse (dvs. betalingstjenesteudbyderens kernekapital).

vi. Højt niveau af intern eskalering

Betalingstjenesteudbydere bør fastslå, om hændelsen er blevet eller sandsynligvis vil blive indberettet til deres øverste ledelse.

vii. Andre betalingstjenesteudbydere eller relevante infrastrukturer, der potentielt kan være berørt

Betalingstjenesteudbydere bør fastslå de systemiske konsekvenser, som hændelsen sandsynligvis vil have, dvs. dens potentiale for at brede sig fra den indledningsvis berørte betalingstjenesteudbyder til andre betalingstjenesteudbydere, finansielle markeds infrastrukturer og/eller betalingsordninger.

viii. Indvirkning på omdømme

Betalingsudbydere bør fastslå, hvordan hændelsen kan underminere brugernes tillid til betalingstjenesteudbyderen selv og, mere generelt, til den underliggende tjeneste eller markedet som helhed.

1.3. Betalingstjenesteudbydere bør beregne indikatorernes værdi efter følgende metode:

i. Berørte transaktioner:

Som hovedregel bør betalingstjenesteudbydere ved "berørte transaktioner" forstå alle indenlandske og grænseoverskridende transaktioner, der er eller sandsynligvis vil blive direkte eller indirekte berørt af hændelsen, navnlig transaktioner, der ikke har kunnet initieres eller behandles, transaktioner, for hvilke betalingsmeddelelsens indhold er ændret, og transaktioner, der er bestilt i svigagtigt øjemed (uanset om midlerne er blevet tilbagebetalt eller ej), eller hvor korrekt udførelse forhindres eller vanskeliggøres på anden måde af hændelsen.

For driftshændelser, der påvirker evnen til at initiere og/eller behandle transaktioner, bør betalingstjenesteudbydere kun indberette hændelser af en varighed på mere end en time. Hændelsens varighed bør måles fra det øjeblik, hvor hændelsen opstår, til det øjeblik, hvor de normale aktiviteter/funktioner er blevet bragt tilbage til niveauet fra før hændelsen.

Desuden bør betalingstjenesteudbydere ved det normale niveau af betalingstransaktioner forstå den daglige mængde, beregnet som årsgennemsnit, af indenlandske og grænseoverskridende betalingstransaktioner, der udføres med de betalingstjenester, der er berørt af hændelsen, idet referenceperioden for beregningen er det foregående år. Hvis betalingstjenesteudbyderen ikke anser dette tal for repræsentativt (f.eks. på grund af sæsonudsving), bør udbyderen i stedet anvende en anden, mere repræsentativ målemetode,

og over for den kompetente myndighed begrunde denne metode i det tilhørende felt i skemaet (se bilaget).

ii. Berørte betalingstjenestebrugere

Betalingstjenesteudbydere bør ved "berørte betalingstjenestebrugere" forstå alle kunder (indenlandske eller udenlandske, forbrugere eller virksomheder), som har indgået en kontrakt om adgang til den berørte betalingstjeneste med den berørte betalingstjenesteudbyder, og som er eller sandsynligvis vil blive ramt af hændelsens konsekvenser. Betalingstjenesteudbydere bør anvende skøn baseret på tidligere aktivitet med henblik på at fastslå det antal betalingstjenestebrugere, der kan have brugt betalingstjenesten, mens hændelsen har stået på.

I tilfælde af grupper bør den enkelte betalingstjenesteudbyder kun tage højde for sine egne betalingstjenestebrugere. Hvis en betalingstjenesteudbyder tilbyder driftstjenester til andre, bør denne betalingstjenesteudbyder kun tage højde for sine eventuelle egne betalingstjenestebrugere, og de betalingstjenesteudbydere, der modtager disse driftstjenester, bør vurdere hændelsen i forhold til deres egne betalingstjenestebrugere.

For driftshændelser, der påvirker evnen til at initiere og/eller behandle transaktioner, bør betalingstjenesteudbydere kun indberette hændelser, der påvirker betalingstjenestebrugere og har en varighed på mere end en time. Hændelsens varighed bør måles fra det øjeblik, hvor hændelsen opstår, til det øjeblik, hvor de almindelige aktiviteter/funktioner er genetableret på niveauet fra før hændelsen.

Betalingstjenesteudbydere bør endvidere ved det samlede antal betalingstjenestebrugere forstå det samlede antal indenlandske og grænseoverskridende betalingstjenestebrugere, der er kontraktligt bundet til dem på tidspunktet for hændelsen (eller alternativt det seneste foreliggende antal) og har adgang til den berørte betalingstjeneste, uanset deres størrelse og om de regnes som aktive eller passive betalingstjenestebrugere.

iii. Brud på sikkerheden i netværks- eller informationssystemer

Betalingstjenesteudbydere bør fastslå, om en ondsindet handling har skadet tilgængeligheden, ægtheden, integriteten eller fortroligheden af netværks- eller informationssystemer (herunder data) med relation til levering af betalingstjenester.

iv. Tjenestens nedetid

Betalingstjenesteudbydere bør medregne det tidsrum, hvori en opgave, proces eller kanal med relation til levering af betalingstjenester, er eller sandsynligvis vil være nede og derved forhindrer i) initiering og/eller udførelse af en betalingstjeneste og/eller ii) adgang til en betalingskonto. Betalingstjenesteudbydere bør beregne nedetiden for tjenesten fra det øjeblik, hvor nedetiden begynder, og medregne både de perioder, hvor de holder åbent som påkrævet for gennemførelsen af betalingstransaktioner, og perioder, hvor de holder lukket, samt vedligeholdelsesperioder, når dette er relevant og muligt. Hvis betalingstjenesteudbydere ikke kan fastslå, hvornår nedetiden for tjenesten er begyndt, bør de undtagelsesvis beregne tjenestens nedetid fra det øjeblik, hvor den konstateres.

v. *Økonomisk indvirkning*

Betalingstjenesteudbydere bør medregne både de omkostninger, der kan sættes i forbindelse med hændelsen direkte, og omkostninger, der indirekte er relateret til hændelsen. Betalingsudbydere bør blandt andet medregne eksproprierede midler eller aktiver, omkostninger til udskiftning af hardware eller software, andre juridiske omkostninger og omkostninger til afhjælpning, gebyrer som følge af manglende overholdelse af kontraktlige forpligtelser, sanktioner, eksterne forpligtelser og tabte indtægter. Hvad angår indirekte omkostninger, bør betalingstjenesteudbydere kun medregne omkostninger, der allerede kendes eller med stor sandsynlighed vil påløbe.

vi. *Højt niveau af intern eskalering*

Betalingstjenesteudbydere bør tage stilling til, om ledelsesorganet som defineret i EBA's retningslinjer for IKT og sikkerhedsrisikostyring som følge af indvirkningen på betalingsrelaterede tjenester har modtaget eller sandsynligvis vil modtage underretning, i overensstemmelse med retningslinje 60, punkt d), i EBA's retningslinjer for IKT og sikkerhedsrisikostyring, om hændelsen uden for en periodisk notifikationsprocedure og løbende, mens hændelsen står på. Desuden bør betalingstjenesteudbydere tage stilling til, om der er eller sandsynligvis vil blive udløst en krisesituation som følge af hændelsens indvirkning på betalingsrelaterede tjenester.

vii. *Andre betalingstjenesteudbydere eller relevante infrastrukturer, der potentielt er berørt*

Betalingstjenesteudbydere bør vurdere hændelsens indvirkning på det finansielle marked, forstået som det finansielle markeds infrastrukturer og/eller betalingsordninger, der understøtter markedet og de øvrige betalingstjenesteudbydere. Betalingstjenesteudbydere bør navnlig vurdere, om hændelsen har gentaget sig eller sandsynligvis vil gentage sig hos andre betalingstjenesteudbydere, om den har påvirket eller sandsynligvis vil påvirke den smidige funktion af det finansielle markeds infrastrukturer, og om den har skadet eller sandsynligvis vil skade den smidige funktion af det finansielle system som helhed. Betalingstjenesteudbydere bør have en række forhold for øje, f.eks. om den berørte komponent/software er ejendomsretligt beskyttet eller er almindeligt tilgængelig, om det berørte netværk er et internt eller eksternt netværk, og om betalingstjenesteudbyderen er ophørt eller sandsynligvis vil ophøre med at opfylde sine forpligtelser i det finansielle markeds infrastrukturer, som udbyderen indgår i.

viii. *Indvirkning på omdømme*

Betalingstjenesteudbydere bør medregne den synlighed, som hændelsen efter deres bedste overbevisning har opnået eller sandsynligvis vil opnå på markedet. Navnlig bør betalingstjenesteudbydere tage højde for sandsynligheden for, at hændelsen vil være samfundsskadelig, som en indikator for dens potentiale til at påvirke deres omdømme. Betalingstjenesteudbydere bør tage højde for, om i) betalingstjenestebrugere og/eller betalingstjenesteudbydere har klaget over hændelsens negative indvirkning, ii) hændelsen har påvirket en synlig betalingstjenesterelateret proces og derfor sandsynligvis vil få eller allerede har fået presseomtale (ikke kun i de traditionelle medier som for eksempel aviser,

men også i blogs, sociale medier osv.), iii) kontraktlige forpligtelser er blevet eller sandsynligvis vil blive misligholdt med offentliggørelse af sagsanlæg mod betalingstjenesteudbyderen til følge, iv) lovkrav ikke er blevet efterlevet med iværksættelse af tilsynsforanstaltninger eller sanktioner til følge, der har været eller sandsynligvis vil blive gjort offentligt tilgængelige, og v) en lignende type hændelse er opstået tidligere.

1.4. Betalingstjenesteudbydere bør vurdere en hændelse ved, at de for de enkelte kriterier fastslår, om de pågældende tærskelværdier i tabel 1 er eller sandsynligvis vil blive nået, før hændelsen er afhjulpet.

Tabel 1: Tærskelværdier

Kriterier	Lavere indvirkningsniveau	Højere indvirkningsniveau
Berørte transaktioner	> 10 % af betalingstjenesteudbyderens normale transaktionsniveau (i antal transaktioner) **og** hændelsens varighed > 1 time* **eller** > 500 000 EUR **og** hændelsens varighed > 1 time*	> 25 % af betalingstjenesteudbyderens normale transaktionsniveau (i antal transaktioner) **eller** > 15 000 000 EUR
Berørte betalingstjenestebrugere	> 5 000 **og** hændelsens varighed > 1 time* **eller** > 10 % af betalingstjenesteudbyderens betalingstjenestebrugere **og** hændelsens varighed > 1 time*	> 50 000 **eller** > 25 % af betalingstjenesteudbyderens betalingstjenestebrugere
Tjenestens nedetid	> 2 timer	Ikke relevant
Brud på sikkerheden i netværks- eller informationssystemer	Ja	Ikke relevant
Økonomisk indvirkning	Ikke relevant	> Maks. (0,1 % kernekapital**, 200 000 EUR) **eller** > 5 000 000 EUR
Højt niveau af intern eskalering	Ja	Ja, og en krisesituation (eller tilsvarende) vil sandsynligvis blive udløst
Andre betalingstjenesteudbydere eller	Ja	Ikke relevant

relevante infrastrukturer, der potentielt er berørt		
Indvirkning på omdømme	Ja	Ikke relevant

* Tærskelværdien vedrørende hændelsens varighed i en periode på mere end en time gælder kun for driftshændelser, der påvirker betalingstjenesteudbyderens evne til at initiere og/eller behandle transaktioner.

**Kernekapital som defineret i artikel 25 i Europa-Parlamentets og Rådets forordning (EU) nr. 575/2013 af 26. juni 2013 om tilsynsmæssige krav til kreditinstitutter og investeringsselskaber og om ændring af forordning (EU) nr. 648/2012.

1.5. Betalingstjenesteudbydere bør anvende skøn, hvis de ikke har faktiske data som grundlag for deres vurdering af, om en given tærskelværdi er eller sandsynligvis vil blive nået, før hændelsen er afhjulpet (dette kan f.eks. ske i den indledende undersøgelsesfase).

1.6. Betalingsudbydere bør løbende foretage denne vurdering, mens hændelsen står på, for at identificere enhver mulig statusændring, enten opad (fra ikke-større til større) eller nedad (fra større til ikke-større). Enhver omklassificering af hændelsen fra større til ikke-større bør hurtigst muligt meddeles den kompetente myndighed i overensstemmelse med kravet i retningslinje 2.21.

Retningslinje 2: Anmeldelsesproces

2.1. Betalingstjenesteudbydere bør samle alle relevante oplysninger, udarbejde en hændelsesrapport ved hjælp af skemaet i bilaget, og indsende rapporten til den kompetente myndighed i hjemlandet. Betalingstjenesteudbydere bør udfylde alle felter i skemaet efter anvisningerne i bilaget.

2.2. Betalingstjenesteudbydere bør anvende det samme skema ved indsendelse af den indledende, den foreløbige og den endelige rapport vedrørende samme hændelse. Betalingstjenesteudbydere bør derfor udfylde et enkelt skema trinvis og, hvis relevant, opdatere oplysningerne i tidligere rapporter.

2.3. Betalingstjenesteudbydere bør, hvis det er relevant, desuden forelægge den kompetente myndighed i deres hjemland en kopi af de oplysninger, der er afgivet (eller vil blive afgivet) til deres brugere, som fastsat i artikel 96, stk. 1, andet afsnit, af det andet betalingstjenestedirektiv, så snart de foreligger.

2.4. Betalingstjenesteudbydere bør, på anmodning fra den kompetente myndighed i deres hjemland, udlevere eventuelle yderligere dokumenter, der supplerer de oplysninger, som er indsendt med standardskemaet. Betalingstjenesteudbydere bør følge op på alle anmodninger fra den kompetente myndighed i hjemlandet om at afgive supplerende oplysninger eller uddybe allerede indsendt dokumentation.

2.5. Eventuelle yderligere oplysninger, der er indeholdt i de dokumenter, betalingstjenesteudbydere udleverer til den kompetente myndighed, enten på betalingstjenesteudbyderens initiativ eller på den kompetente myndigheds anmodning i overensstemmelse med retningslinje 2.4, bør afspejles af betalingstjenesteudbyderen i skemaet under retningslinje 2.1.

2.6. Betalingstjenesteudbydere bør til enhver tid behandle de udvekslede oplysninger fortroligt og sikre disses integritet, og bør derudover sikre deres behørige autentifikation over for den kompetente myndighed i hjemlandet.

Indledende rapport

2.7. Betalingstjenesteudbydere bør indsende en indledende rapport til den kompetente myndighed i hjemlandet, efter at en drifts- eller sikkerhedshændelse er blevet klassificeret som større. Kompetente myndigheder bør hurtigst muligst bekræfte modtagelsen af den indledende rapport og give hændelsen en unik referencekode, der identificerer hændelsen entydigt. Betalingstjenesteudbydere bør angive denne referencekode, når de indsender en opdatering til den indledende rapport eller til den foreløbige eller den endelige rapport vedrørende samme hændelse, medmindre den foreløbige og den endelige rapport indsendes sammen med den indledende rapport.

2.8. Betalingstjenesteudbydere bør sende den indledende rapport til den kompetente myndighed senest fire timer efter det øjeblik, hvor drifts- eller sikkerhedshændelsen er blevet klassificeret som større. Hvis den kompetente myndigheds indberetningskanaler vides ikke at være tilgængelige eller i drift på det tidspunkt, bør betalingstjenesteudbydere sende den indledende rapport, så snart kanalerne er tilgængelige/i drift igen.

2.9. Betalingstjenesteudbydere bør i overensstemmelse med retningslinje 1.1. og 1.4 klassificere hændelsen, hurtigst muligt efter at hændelsen er blevet konstateret, dog senest 24 timer efter konstatering af hændelsen, og hurtigst muligt efter at de oplysninger, der er nødvendige for at klassificere hændelsen, foreligger for betalingstjenesteudbyderen. Hvis der er behov for længere tid til at klassificere hændelsen, bør betalingstjenesteudbydere redegøre for årsagen til dette i den indledende rapport, der sendes til den kompetente myndighed.

2.10. Betalingsudbydere bør endvidere indsende en indledende rapport til den kompetente myndighed i hjemlandet, når en tidligere ikke-større hændelse er blevet omklassificeret til en større hændelse. I dette særlige tilfælde bør betalingstjenesteudbydere sende den indledende rapport til den kompetente myndighed, straks efter at statusændringen konstateres, eller — hvis den kompetente myndigheds indberetningskanaler på dette tidspunkt vides ikke at være tilgængelige eller i drift — så snart de er tilgængelige/i drift igen.

2.11. Betalingstjenesteudbydere bør i deres indledende rapport medtage oplysninger på overskriftsniveau (dvs. afsnit A i skemaet) for at vise nogle grundlæggende karakteristika ved

hændelsen og dens forventede konsekvenser på grundlag af de foreliggende oplysninger straks efter dens klassificering som større. Betalingstjenesteudbydere bør anvende skøn, hvis der ikke foreligger faktiske data.

Foreløbig rapport

2.12. Når de normale aktiviteter er genoptaget, og driften igen er normal, bør betalingstjenesteudbydere indsende den foreløbige rapport og underrette den kompetente myndighed om dette. Betalingstjenesteudbydere bør betragte driften som værende normal igen, når aktiviteten/funktionerne er bragt tilbage på det niveau af service/betingelser, som er fastlagt af betalingstjenesteudbyderen eller fastlagt eksternt gennem en serviceleveranceaftale (behandlingstider, kapacitet, sikkerhedskrav m.m.), og beredskabsforanstaltninger ikke længere er i kraft. Den foreløbige rapport bør indeholde en mere detaljeret beskrivelse af hændelsen og dens konsekvenser (afsnit B i skemaet).

2.13. Hvis de normale aktiviteter endnu ikke er genoptaget, bør betalingstjenesteudbydere indsende en foreløbig rapport til den kompetente myndighed senest tre dage efter indsendelsen af den indledende rapport.

2.14. Betalingstjenesteudbydere bør opdatere de oplysninger, der allerede er givet i skemaets afsnit A og B, når de får kendskab til betydelige ændringer siden indsendelsen af den tidligere rapport (f.eks. om hændelsen er eskaleret eller deeskaleret, og om der er konstateret nye årsager eller iværksat tiltag til at løse problemet). Dette omfatter tilfælde, hvor hændelsen ikke er blevet afhjulpet inden for tre arbejdsdage, hvilket vil forpligte betalingstjenesteudbydere til at indsende en yderligere foreløbig rapport. Under alle omstændigheder bør betalingstjenesteudbydere indsende en ny foreløbig rapport på anmodning af den kompetente myndighed i hjemlandet.

2.15. Ligesom for indledende rapporter bør betalingstjenesteudbydere anvende skøn, når der ikke foreligger faktiske data.

2.16. Såfremt driften igen er normal senest fire timer efter at hændelsen er blevet klassificeret som større, bør betalingstjenesteudbydere bestræbe sig på at indsende både den indledende og den foreløbige rapport samtidig (dvs. med udfyldelse af skemaets afsnit A og B) inden for fristen på fire timer.

Endelig rapport

2.17. Betalingstjenesteudbydere bør indsende en endelig rapport, når årsagsanalysen er blevet gennemført (uanset om der allerede er iværksat afbødende foranstaltninger, eller om den endelige grundlæggende årsag er påvist), og der foreligger faktiske tal i stedet for potentielle skøn.

2.18. Betalingstjenesteudbydere bør indsende den endelige rapport til den kompetente myndighed, højst 20 arbejdsdage, efter at driften anses for igen at være normal.

Betalingstjenesteudbydere, der har brug for en forlængelse af denne frist (f.eks. hvis der endnu ikke foreligger faktiske tal for indvirkningen, eller de grundlæggende årsager endnu ikke er påvist), bør inden fristens udløb kontakte den kompetente myndighed og give en fyldestgørende begrundelse for forsinkelsen og angive en ny forventet dato for den endelige rapport.

2.19. Hvis betalingstjenesteudbydere kan levere alle de påkrævede oplysninger i den endelige rapport (dvs. skemaets afsnit C) inden for firetimersfristen, efter at hændelsen blev klassificeret som større, bør de bestræbe sig på at indsende oplysningerne vedrørende den indledende, foreløbige og endelige rapport sammen.

2.20. Betalingstjenesteudbydere bør i deres endelige rapport medtage fuldstændige oplysninger, dvs. i) faktiske tal om indvirkningen i stedet for skøn (samt andre nødvendige opdateringer i afsnit A og B i skemaet), og ii) skemaets afsnit C, som omfatter den grundlæggende årsag, hvis denne allerede kendes, og en sammenfatning af de foranstaltninger, der er vedtaget eller planlægges vedtaget for at løse problemet og forhindre, at det gentager sig i fremtiden.

2.21. Betalingstjenesteudbydere bør desuden indsende en endelig rapport, hvis de som et resultat af den løbende vurdering af hændelsen konstaterer, at en allerede indberettet hændelse ikke længere opfylder kriterierne for at blive betragtet som en større hændelse og ikke forventes at opfylde dem, før hændelsen er afhjulpet. I så fald bør betalingstjenesteudbydere indsende den endelige rapport, så snart dette forhold konstateres, og under alle omstændigheder senest inden udløbet af fristen for indsendelse af den næste rapport. I denne særlige situation bør betalingstjenesteudbydere i stedet for at udfylde afsnit C i skemaet afkrydse feltet "hændelse omklassificeret til ikke-større" og redegøre for årsagerne til denne omklassificering.

Retningslinje 3: Delegeret og konsolideret indberetning

3.1. Hvis den kompetente myndighed tillader det, bør betalingstjenesteudbydere, der ønsker at delegere indberetningsforpligtelser i henhold til PSD2 til en tredjepart, underrette den kompetente myndighed i hjemlandet og sikre, at følgende betingelser er opfyldt:

a. Den formelle kontrakt eller, efter omstændighederne, en koncerns eksisterende interne ordninger, der understøtter delegeret indberetning mellem betalingstjenesteudbyderen og tredjeparten, fastlægger entydigt ansvarsfordelingen mellem alle parter. Navnlig fremgår det klart af kontrakten eller ordningerne, at den berørte betalingstjenesteudbyder — uafhængigt af den eventuelle delegering af indberetningsforpligtelser — fortsat er fuldt ansvarlig for opfyldelse af kravene i artikel 96 i PSD2 og for indholdet af de oplysninger, der afgives til den kompetente myndighed i hjemlandet.

b. Delegeringen opfylder de krav til outsourcing af vigtige driftsmæssige funktioner, som er fastlagt i:

i. artikel 19, stk. 6, i PSD2, hvad angår betalingsinstitutter og udstedere af e-penge, og som finder tilsvarende anvendelse i henhold til artikel 3 i direktiv 2009/110/EF, eller

ii. EBA's retningslinjer om ordninger for outsourcing (EBA/GL/2019/02) vedrørende alle betalingstjenesteudbydere.

c. Oplysningerne indsendes på forhånd til den kompetente myndighed i hjemlandet og under alle omstændigheder under overholdelse af de frister og procedurer, der måtte være fastsat af den kompetente myndighed.

d. Fortroligheden af følsomme data og kvaliteten, sammenhængen, integriteten og pålideligheden af de oplysninger, der gives til den kompetente myndighed, er forsvarligt forsikret.

3.2. Betalingstjenesteudbydere, der ønsker at tillade den udpegede tredjepart at opfylde indberetningsforpligtelserne i konsolideret form (dvs. i form af en enkelt rapport, der vedrører flere betalingstjenesteudbydere, som er berørt af den samme større drifts- eller sikkerhedshændelse), bør underrette den kompetente myndighed i hjemlandet, angive kontaktoplysninger i skemaet under "Berørt betalingstjenesteudbyder" og sørge for, at følgende betingelser er opfyldt:

a. Medtage denne bestemmelse i den kontrakt, der understøtter delegeret indberetning.

b. Gøre den konsoliderede indberetning betinget af, at hændelsen skyldes en afbrydelse af de tjenester, der leveres af tredjeparten.

c. Begrænse den konsoliderede indberetning til betalingstjenesteudbydere, der er etableret i samme medlemsstat.

d. Medsende en liste over alle betalingstjenesteudbydere, der er berørt af hændelsen.

e. Sikre, at tredjeparten vurderer hændelsens væsentlighed for de enkelte berørte betalingstjenesteudbydere og i den konsoliderede rapport kun medtager de betalingstjenesteudbydere, for hvilke hændelsen er klassificeret som større; desuden sikre, at en betalingstjenesteudbyder — i tvivlstilfælde — medtages i den konsoliderede rapport, så længe der ikke er dokumentation for andet.

f. Sørge for, når der er felter i skemaet, hvor det ikke er muligt at give et fælles svar (f.eks. afsnit B2, B4 og C3), at tredjeparten enten i) udfylder dem individuelt for de berørte betalingstjenesteudbydere og specificerer identiteten af de enkelte betalingstjenesteudbydere, som oplysningerne vedrører, eller ii) angiver de kumulative værdier, der er iagttaget eller skønnet for betalingstjenesteudbyderne.

g. Sikre, at tredjeparten holder betalingstjenesteudbyderen løbende underrettet om alle relevante oplysninger om hændelsen og alle de interaktioner, som tredjeparten måtte have med den kompetente myndighed, samt indholdet heraf, dog kun i det omfang, dette ikke udgør et brud på fortroligheden af oplysninger, der vedrører andre betalingstjenesteudbydere.

3.3. Betalingstjenesteudbydere bør ikke delegere deres indberetningsforpligtelser, før de har underrettet den kompetente myndighed i hjemlandet eller fået oplyst, at aftalen om outsourcing ikke opfylder kravene i retningslinje 3.1, litra b).

3.4. Betalingstjenesteudbydere, der ønsker at trække delegeringen af deres indberetningsforpligtelser tilbage, bør underrette den kompetente myndighed i hjemlandet om dette under overholdelse af de frister og procedurer, myndigheden har fastsat. Betalingstjenesteudbydere bør desuden underrette den kompetente myndighed i hjemlandet om enhver væsentlig forandring, der berører den udpegede tredjepart og dennes evne til at opfylde indberetningsforpligtelserne.

3.5. Betalingstjenesteudbydere bør i videst muligt omfang opfylde deres indberetningsforpligtelser uden brug af ekstern bistand, hvis den udpegede tredjepart undlader at underrette den kompetente myndighed i hjemlandet om en større drifts- eller sikkerhedshændelse i overensstemmelse med artikel 96 i PSD2 og med disse retningslinjer. Betalingstjenesteudbydere bør også sikre, at en hændelse ikke indberettes to gange, dels af den nævnte betalingstjenesteudbyder, dels igen af tredjeparten.

3.6. I situationer, hvor en hændelse skyldes en afbrydelse af de tjenester, der leveres af en udbyder af tekniske tjenester (eller en infrastruktur), og hvor afbrydelsen påvirker flere betalingstjenesteudbydere, bør betalingstjenesteudbydere sikre, at den delegerede indberetning henviser til betalingstjenesteudbyderens individuelle data (bortset fra i tilfælde af konsolideret indberetning).

Retningslinje 4: Drifts- og sikkerhedspolitik

4.1. Betalingstjenesteudbydere bør sikre, at deres generelle drifts- og sikkerhedspolitik klart fastlægger alle ansvarsområder vedrørende indberetning af hændelser i henhold til PSD2 samt de processer, der er implementeret for at opfylde kravene i disse retningslinjer.

5. Retningslinjer for kompetente myndigheder om kriterierne for vurdering af hændelsens relevans og de oplysninger i hændelsesrapporterne, der skal videregives til andre myndigheder i hjemlandet

Retningslinje 5: Vurdering af hændelsens relevans

5.1. Kompetente myndigheder i hjemlandet bør vurdere en større drifts- eller sikkerhedshændelses relevans for andre nationale myndigheder på grundlag af deres eget ekspertskøn og med følgende kriterier som primære indikatorer for hændelsens betydning:

a. Årsagerne til hændelsen hører under den anden nationale myndigheds ansvarsområde (dvs. dens kompetenceområde).
b. Hændelsens konsekvenser har indvirkning på en anden national myndigheds målsætninger (f.eks. varetagelse af finansiel stabilitet).
c. Hændelsen berører eller kan berøre betalingstjenestebrugere i vid udstrækning.
d. Hændelsen vil sandsynligvis få eller har fået omfattende presseomtale.

5.2. Kompetente myndigheder i hjemlandet bør foretage denne vurdering løbende, mens hændelsen står på, så de kan identificere enhver mulig ændring, der kan gøre en hændelse relevant, selv om den ikke tidligere er blevet anset for at være relevant.

Retningslinje 6: Oplysninger til videregivelse

6.1. Uanset eventuelle andre lovkrav om at videregive hændelsesrelaterede oplysninger til andre nationale myndigheder bør kompetente myndigheder videregive oplysninger om større drifts- eller sikkerhedshændelser til de relevante nationale myndigheder, som er identificeret ved anvendelse af retningslinje 5.1, i det mindste på tidspunktet for modtagelse af den indledende rapport (eller alternativt den rapport, der har ført til videregivelse af oplysninger) og når de underrettes om, at driften igen er normal (dvs. den foreløbige rapport).

6.2. Kompetente myndigheder bør indsende de oplysninger, der er påkrævet for at give et klart billede af det skete og de mulige konsekvenser heraf, til de relevante nationale myndigheder. Til det formål bør de som minimum videregive de oplysninger, der er anført af betalingstjenesteudbyderen i følgende af skemaets felter (i den indledende eller den foreløbige rapport):

- Dato og klokkeslæt for klassificering af hændelsen som større.
- Dato og klokkeslæt for konstatering af hændelsen.
- Dato og klokkeslæt for hændelsens opståen.
- Dato og klokkeslæt, hvor hændelsen er blevet afhjulpet eller forventes afhjulpet.
- En kort beskrivelse af hændelsen (herunder ikkefølsomme dele af den detaljerede beskrivelse).
- En kort beskrivelse af iværksatte eller planlagte foranstaltninger til afhjælpning af hændelsen.
- En beskrivelse af, hvordan hændelsen kan påvirke andre betalingstjenesteudbydere og/eller infrastrukturer.
- En beskrivelse af eventuel presseomtale.
- Årsagen til hændelsen.

6.3. Kompetente myndigheder bør sikre behørig anonymisering i det omfang, det er nødvendigt, og udelade oplysninger, der kan være omfattet af begrænsninger vedrørende fortrolighed eller intellektuel ejendomsret, inden de videregiver hændelsesrelaterede oplysninger til de relevante nationale myndigheder. Kompetente myndigheder bør dog oplyse den indberettende betalingstjenesteudbyders navn og adresse til de relevante nationale myndigheder, forudsat at disse kan garantere, at oplysningerne behandles fortroligt.

6.4. Kompetente myndigheder bør til enhver tid behandle de opbevarede og udvekslede oplysninger fortroligt og sikre disses integritet, og bør sikre deres behørige autentifikation over for de relevante nationale myndigheder. Navnlig bør kompetente myndigheder behandle alle oplysninger, de modtager i henhold til disse retningslinjer, i overensstemmelse med tavshedspligten som fastlagt i PSD2, med forbehold af gældende EU-lovgivning og nationale krav.

6. Retningslinjer for kompetente myndigheder om kriterierne for vurdering af de relevante oplysninger i hændelsesrapporterne, der skal videregives til EBA og ECB, og om formatet af og procedurerne for deres kommunikation.

Retningslinje 7: Oplysninger til videregivelse

7.1. Kompetente myndigheder bør altid til EBA og ECB fremsende alle rapporter, der er modtaget fra (eller på vegne af) betalingstjenesteudbydere, som er berørt af en større drifts- eller sikkerhedshændelse, ved at anvende en standardiseret fil, der kan findes på EBA's websted.

Retningslinje 8: Kommunikation

8.1. Kompetente myndigheder bør til enhver tid behandle de opbevarede og udvekslede oplysninger fortroligt og sikre disses integritet, og bør sikre deres behørige autentifikation over for EBA og ECB. Navnlig bør kompetente myndigheder behandle alle oplysninger, de modtager i henhold til disse retningslinjer, i overensstemmelse med tavshedspligten som fastsat i PSD2, med forbehold af gældende EU-lovgivning og nationale krav.

8.2. For at undgå forsinkelser i overførslen af hændelsesrelaterede oplysninger til EBA/ECB og bidrage til at mindske risikoen for driftsforstyrrelser bør kompetente myndigheder være i besiddelse af relevante kommunikationsmidler.

Bilag 1 — Indberetningsskema for betalingstjenesteudbydere

Indledende rapport

Indledende rapport	senest fire timer efter hændelsens klassificering som større hændelse	Nulstil valg i rullemenu
Indberetningsdato *(DD.MM.ÅÅÅÅ)*		Klokkeslæt *(TT.MM)*
Hændelsens referencekode		

A — Indledende rapport						
A 1 — GENERELLE OPLYSNINGER						
Type rapport						
Type rapport						
Berørt betalingstjenesteudbyder						
Betalingstjenesteudbyders navn						
Betalingstjenesteudbyders nationale identifikationsnummer						
Ledende enhed i koncern, hvis relevant						
Land(e) berørt af hændelsen	☐ AT ☐ BE ☐ BG ☐ CY ☐ CZ	☐ DE ☐ DK ☐ EE ☐ ES ☐ FI	☐ FR ☐ LI ☐ GR ☐ HR ☐ HU	☐ IE ☐ IS ☐ IT ☐ LT ☐ LU	☐ LV ☐ MT ☐ NL ☐ NO ☐ PL	☐ PT ☐ RO ☐ SE ☐ SI ☐ SK
Primær kontaktperson		E-mail		Telefon		
Sekundær kontaktperson		E-mail		Telefon		
Indberettende enhed (udfyld denne del, hvis den indberettende enhed ikke er den berørte betalingstjenesteudbyder i tilfælde af delegeret indberetning						
Den indberettende enheds navn						
Nationalt identifikationsnummer						
Primær kontaktperson		E-mail		Telefon		
Sekundær kontaktperson		E-mail		Telefon		
A 2 — KONSTATERING og KLASSIFICERING af HÆNDELSE						
Dato og klokkeslæt for konstatering af hændelsen *(DD.MM.ÅÅÅÅ TT.MM)*						
Dato og klokkeslæt for klassificering af hændelsen *(DD.MM.ÅÅÅÅ TT.MM)*						
Hændelsen blev konstateret af		Hvis "Andet", bedes du uddybe svaret:				
Hændelsens art	☐ Berørte transaktioner ☐ betalingstjenestebruger ☐ Tjenestens nedetid ☐ Brud på sikkerheden i netværks- eller ☐ Økonomisk indvirkning ☐ Højt niveau af intern eskalering ☐ Andre betalingstjenesteudbyder eller relevante ☐ Indvirkning på infrastrukturer, der potentielt					
Kriterier, der udløser rapporten om en større hændelse						
En kort og generel beskrivelse af hændelsen						
Eventuel indvirkning i andre EU-medlemsstater						
Indberetning til andre myndigheder		Hvis "Ja", bedes du uddybe svaret:				
Årsager til for sen indsendelse af den indledende rapport						

Foreløbig rapport

Indberetning af en større hændelse

Foreløbig rapport	senest tre arbejdsdage efter indsendelse af den indledende rapport	Nulstil valg i rullemenu

Indberetningsdato *(DD.MM.ÅÅÅÅ)* | Klokkeslæt *(TT.MM)*

Hændelsens referencekode

B — Foreløbig rapport

B 1 — GENERELLE OPLYSNINGER

En mere detaljeret beskrivelse af hændelsen:

Hvad er det konkrete problem?			
Hvordan opstod hændelsen?			
Hvordan udviklede den sig?			
Hvad er konsekvenserne (navnlig for betalingstjenestebrugere)?			
Blev betalingstjenestebrugere underrettet om hændelsen?		Hvis "Ja", bedes du uddybe svaret:	
Er hændelsen relateret til (en) tidligere hændelse(r)?		Hvis "Ja", bedes du uddybe svaret:	
Har andre tjenesteudbydere/tredjeparter været berørt eller involveret?		Hvis "Ja", bedes du uddybe svaret:	
Er der indledt krisestyring (internt og/eller eksternt)?		Hvis "Ja", bedes du uddybe svaret:	
Dato og klokkeslæt for hændelsens opståen (hvis allerede fastslået) *(DD.MM.ÅÅÅÅ TT.MM)*			
Dato og klokkeslæt, hvor hændelsen er afhjulpet eller forventes afhjulpet *(DD.MM.ÅÅÅÅ TT.MM)*			
Berørte funktionsområder	☐ Autentifikation/godkendelse ☐ Direkte afvikling ☐ Kommunikation ☐ Indirekte afvikling ☐ Clearing ☐ Andet	Hvis "Andet", bedes du ud	
Ændringer foretaget i tidligere rapporter			

B 2 — KLASSFICERING AF HÆNDELSE/OPLYSNINGER OM HÆNDELSE

Berørte transaktioner[2)]	Indvirkningsniveau Antal berørte transaktioner I % af det normale antal transaktioner Værdi af berørte transaktioner i EUR Hændelsens varighed (kun relevant for driftshændelser) Bemærkninger		
Berørte betalingstjenestebrugere[3)]	Indvirkningsniveau Antal berørte betalingstjenestebrugere I % af det samlede antal betalingstjenestebrugere		
Brud på sikkerheden i netværks- eller informationssystemer	Beskriv, hvordan netværks- eller informationssystemer er berørt		
Tjenestens nedetid	Den samlede nedetid:	Dage: Timer: Minutter:	
Økonomisk indvirkning	Indvirkningsniveau Direkte omkostninger i EUR Indirekte omkostninger i EUR		
Højt niveau af intern eskalering	Beskriv niveauet for hændelsens interne eskalering med angivelse af, om den har udløst eller sandsynligvis vil udløse en krisesituation (eller tilsvarende), og redegør i givet fald for dette		
Andre betalingstjenesteudbydere eller relevante infrastrukturer, der potentie	Beskriv, hvordan hændelsen kan berøre andre betalingstjenesteudbydere og/eller infrastrukturer		
Indvirkning på omdømme	Beskriv, hvordan hændelsen kan påvirke betalingstjenesteudbyderens omdømme (f.eks. presseomtale, offentliggørelse af sagsanlæg eller		

B 3 — BESKRIVELSE AF HÆNDELSE

Hændelsens art		
Hændelsens årsag	☐ Undersøgelse pågår ☐ Ondsindet handling ☐ Procesfejl ☐ Systemfejl ☐ Menneskelige fejl ☐ Eksterne forhold ☐ Andet	Hvis "Andet", bedes du uddybe svare
Har hændelsen påvirket dig direkte, eller indirekte via en tjenesteudbyder?		Hvis "Indirekte", bedes du anføre tjenesteudbyderens navn:

B 4 — HÆNDELSENS INDVIRKNING

Samlet indvirkning	☐ Integritet ☐ Tilgængelighe	☐ Fortrolighed ☐ Autenticitet	
Berørte kommercielle kanaler	☐ Filialer ☐ Netbank ☐ E-handel	☐ Telefonbank ☐ Mobilbank ☐ Pengeautomater	☐ Salgsterminal ☐ Andet
	Hvis "Andet", bedes du uddybe svaret:		
Berørte betalingstjenester	☐ Kontantindbetaling på en betalingskonto ☐ Udbetaling af kontantbeløb fra en betalingskonto ☐ Handlinger, der er nødvendige for at have en ☐ Indløsning af betalingstransaktioner	☐ Kreditoverførsel ☐ Direkte debitering ☐ Kortbetalinger ☐ Udstedelse af betalingsinstrumenter	☐ Betalingsoverførsl ☐ Betalingsinitierings ☐ Kontooplysningstjenester

B 5 — BEGRÆSNING AF HÆNDELSENS INDVIRKNING

Hvilke handlinger/foranstaltninger er hidtil blevet iværksat eller planlagt for at afhjælpe hændelsen?	
Er beredskabsplanen og/eller katastrofeberedskabsplanen bragt i anvendelse?	
I givet fald, hvornår? *(DD.MM.ÅÅÅÅ TT.MM)*	
I givet fald bedes du redegøre nærmere herfor	

Endelig rapport

Rapport om en større hændelse

Vælg rapportart:

senest 20 arbejdsdage efter indsendelse af den foreløbige rapport

Beskriv:
(gælder for hændelser, der omklassificeres til ikke-større hændelser)

Nulstil valg i rullemenu

Indberetningsdato *(DD/MM/ÅÅÅÅ)* Klokkeslæt *(TT:MM)*
Hændelsens referencekode

C – Endelig rapport

Hvis der ikke er sendt en foreløbig rapport, skal afsnit B også udfyldes.

C 1 — GENERELLE OPLYSNINGER

Opdatering af oplysningerne fra den indledende rapport og de(n) foreløbige rapport(er)	
Ændringer foretaget i tidligere rapporter	
Andre relevante oplysninger.	
Er alle oprindelige kontroller etableret? Hvis "Nej", skal du angive, hvilke kontroller der er tale om, og hvor lang tid ekstra det krævede at genetablere dem.	

C 2 — ÅRSAGSANALYSE OG OPFØLGNING

Hvad er den grundlæggende årsag (hvis allerede kendt)?	☐ Ondsindet handling	☐ Procesfejl	☐ Systemfejl	☐ Menneskelig fejl	☐ Eksterne forhold	☐ Andet
Uddyb venligst dit svar:	☐ Ondsindet kode ☐ Informationsindsamling ☐ Indtrængen ☐ Distributed denial of service-angreb/denial of service-angreb ☐ Bevidste interne handlinger ☐ Bevidst ekstern fysisk skade ☐ Informationsindholds sikkerhed ☐ Svigagtige ☐ Andet	☐ Mangelfuld overvågning og kontrol ☐ Kommunikationsproblemer ☐ Ukorrekt betjening ☐ Mangelfuld forandringsledelse ☐ Mangelfuldhed i interne procedurer og dokumentation ☐ Genetableringsproblemer ☐ Andet	☐ Hardwarefejl ☐ Netværksfejl ☐ Databaseproblem ☐ Software-/applikationsfejl ☐ Fysisk skade ☐ Andet	☐ Utilstrækkelige ☐ Manglende ☐ Utilstrækkelige ressourcer ☐ Andet	☐ Fejl hos en leverandør/udbyder af tekniske tjenester ☐ Force majeure ☐ Andet	
	Hvis "Andet", bedes du uddybe svaret:					
Andre relevante oplysninger om den grundlæggende årsag						
Vigtigste korrigerende handlinger/foranstaltninger, der er iværksat eller planlagt for at forebygge en gentagelse af hændelsen, hvis de allerede kendes:						

C 3 — YDERLIGERE OPLYSNINGER

Er andre betalingstjenesteudbydere blevet underrettet om hændelsen?	Hvis "Ja", uddybes dette:	
Er der taget retlige skridt mod betalingstjenesteudbyderen?	Hvis "Ja", uddybes dette:	
Vurdering af effektiviteten af de handlinger, der er iværksat	Redegør nærmere for dette:	

VEJLEDNING TIL UDFYLDELSE AF SKEMAET

Betalingstjenesteudbydere bør udfylde det relevante afsnit i skemaet, afhængigt af hvilken indberetningsfase de befinder sig i: afsnit A for den indledende rapport, afsnit B for foreløbige rapporter og afsnit C for den endelige rapport. Betalingstjenesteudbydere bør anvende det samme skema ved indsendelse af den indledende, den foreløbige og den endelige rapport vedrørende samme hændelse. Alle felter skal udfyldes, medmindre andet tydeligt er angivet.

Overskrift

Indledende rapport: Denne indberetning er den første, betalingstjenesteudbyderen indsender til den kompetente myndighed i hjemlandet.

Foreløbig rapport: Den foreløbige rapport indeholder en mere detaljeret beskrivelse af hændelsen og dennes konsekvenser. Den er en opdatering af den indledende rapport (og, efter omstændighederne, af en tidligere foreløbig rapport) om den samme hændelse.

Endelig rapport: Den endelige rapport er den sidste rapport, betalingstjenesteudbyderen sender vedrørende hændelsen, da i) der allerede er udført en årsagsanalyse, og de skønnede tal kan erstattes af faktiske tal, eller ii) hændelsen ikke længere anses for større og skal omklassificeres.

Hændelse omklassificeret til ikke-større: Hændelsen opfylder ikke længere kriterierne for at blive anset for større og forventes ikke at opfylde dem, før den er afhjulpet. Betalingstjenesteudbydere bør redegøre for årsagerne til denne omklassificering.

Indberetningsdato og -tidspunkt: Den nøjagtige dato og det nøjagtige klokkeslæt for indsendelse af rapporten til den kompetente myndighed.

Hændelsens referencekode (anvendes for foreløbige og endelige rapporter samt for opdateringer til den indledende rapport): Den referencekode, der er tildelt af den kompetente myndighed på tidspunktet for den indledende rapport, og som identificerer hændelsen entydigt. Den enkelte myndighed bør som præfiks anvende hjemlandets tocifrede ISO-kode[2].

A - Indledende rapport

A 1 - Generelle oplysninger

Rapportens art:

Enkeltstående: Rapporten omfatter en enkelt betalingstjenesteudbyder.

Konsolideret: Rapporten omfatter flere betalingstjenesteudbydere i samme medlemsstat, der er berørt af den samme større drifts- eller sikkerhedshændelse, og hvor betalingstjenesteudbyderne gør brug af konsolideret indberetning. Felterne under "Berørt betalingstjenesteudbyder" bør være tomme (med undtagelse af feltet "Land(e), der er berørt af hændelsen"), og der bør medtages en liste over de betalingstjenesteudbydere, som rapporten omfatter, ved at udfylde den tilhørende tabel "Konsolideret rapport — liste over berørte betalingstjenesteudbydere".

Berørt betalingstjenesteudbyder: Henviser til den betalingstjenesteudbyder, der er ramt af hændelsen.

Betalingstjenesteudbyderens navn: Det fulde navn på den betalingstjenesteudbyder, som indberetningen vedrører, således som det fremgår af det relevante officielle nationale register over betalingstjenesteudbydere.

Betalingstjenesteudbyderens nationale identifikationsnummer: Det unikke nationale identifikationsnummer, der anvendes af den kompetente myndighed i hjemlandet i dennes nationale register for at identificere betalingstjenesteudbyderen entydigt.

Ledende enhed i koncern: Hvad angår grupper af enheder som defineret i artikel 4, nr. 40, i PSD2, angives navnet på den ledende enhed.

[2] Vedrørende alfa-2-landekoder i ISO-3166 henvises til https://www.iso.org/iso-3166-country-codes.html

Land(e) berørt af hændelsen: Land(e), hvor indvirkningen af hændelsen har udmøntet sig (f.eks. hvis flere filialer af en betalingstjenesteudbyder, der er etableret i forskellige lande, er berørt), uafhængigt af hændelsens alvorsgrad i de(t) øvrige land(e). Dette kan være, men behøver ikke være, samme land som hjemlandet.

Primær kontaktperson: For- og efternavn på den person, der er ansvarlig for indberetning af hændelsen, eller, hvis en tredjepartstjenesteudbyder indberetter på vegne af den berørte betalingstjenesteudbyder, for- og efternavn på den person, der er ansvarlig for håndtering af hændelser/risikoafdelingen eller tilsvarende område hos den berørte betalingstjenesteudbyder.

E-mail: Den e-mailadresse, som eventuelle anmodninger om uddybning kan rettes til. Dette kan være en personlig eller virksomhedens e-mailadresse.

Telefon: Det telefonnummer, som eventuelle anmodninger om uddybning, kan rettes til. Dette kan være en persons eller en virksomheds telefonnummer.

Sekundær kontaktperson: For- og efternavn på en anden person, som den kompetente myndighed kan kontakte for at forhøre sig om en hændelse, hvis den primære kontaktperson ikke er til stede. Hvis en tredjepartstjenesteudbyder indberetter på vegne af den berørte betalingstjenesteudbyder, anføres for- og efternavn på den anden person, der er ansvarlig for håndtering af hændelser/risikoafdelingen eller tilsvarende område hos den berørte betalingstjenesteudbyder.

E-mail: E-mailadresse på den anden kontaktperson, som eventuelle anmodninger om uddybning kan rettes til. Dette kan være en personlig eller virksomhedens e-mailadresse.

Telefon: E-mailadresse på den anden kontaktperson, som eventuelle anmodninger om uddybning kan rettes til. Dette kan være en persons eller en virksomheds telefonnummer.

Indberettende enhed: Dette afsnit bør udfyldes, hvis en tredjepart opfylder indberetningsforpligtelserne på vegne af den berørte betalingstjenesteudbyder, hvor det er relevant.

Den indberettende enheds navn: Det fulde navn på den enhed, der indberetter hændelsen, således som navnet fremgår af det relevante officielle nationale virksomhedsregister.

Nationalt identifikationsnummer: Det unikke nationale identifikationsnummer, der anvendes i det land, hvor tredjeparten er etableret, til entydigt at identificere den enhed, der indberetter hændelsen. Hvis den indberettende tredjepart er en betalingstjenesteudbyder, bør det nationale identifikationsnummer være betalingstjenesteudbyderens unikke nationale identifikationsnummer, der anvendes af den kompetente myndighed i hjemlandet i dettes nationale register.

Primær kontaktperson: For- og efternavn på den person, der er ansvarlig for indberetning af hændelsen.

E-mail: Den e-mailadresse, som eventuelle anmodninger om uddybning kan rettes til. Dette kan være en personlig eller virksomhedens e-mailadresse.

Telefon: Det telefonnummer, som eventuelle anmodninger om uddybning kan rettes til. Dette kan være en persons eller en virksomheds telefonnummer.

Sekundær kontaktperson: For- og efternavn på en anden person i den enhed, der indberetter hændelsen, og som kan kontaktes af den kompetente myndighed, når den primære kontaktperson ikke er til stede.

E-mail: E-mailadresse på den anden kontaktperson, som eventuelle anmodninger om uddybning kan rettes til. Dette kan være en personlig e-mailadresse eller virksomhedens e-mailadresse.

Telefon: E-mailadresse på den anden kontaktperson, som eventuelle anmodninger om uddybning kan rettes til. Dette kan være en persons eller en virksomheds telefonnummer.

A 2 - Konstatering og klassificering af hændelse

Dato og tidspunkt for konstatering af hændelsen: Dato og tidspunkt for konstatering af hændelsen.

Dato og tidspunkt for klassificering: Dato og tidspunkt for klassificering af sikkerheds- eller driftshændelsen som større.

Hændelse konstateret af: Angiv, om hændelsen blev konstateret af en betalingstjenestebruger, en instans hos betalingstjenesteudbyderen (f.eks. den interne revisionsfunktion) eller en anden ekstern part (f.eks. tjenesteudbyder). Hvis det ikke var nogen af disse, redegøres der for dette i det tilhørende felt.

Hændelsens art: Angiv, efter din bedste overbevisning, og hvis oplysningen er tilgængelig, om der er tale om en drifts- eller sikkerhedshændelse.

> **Driftshændelse:** Hændelse, der skyldes mangelfulde processer eller procesfejl, menneskelige fejl eller systemfejl, eller tilfælde af force majeure, der berører betalingsrelaterede tjenesters integritet, tilgængelighed, fortrolighed og/eller ægthed.
>
> **Sikkerhed:** Uautoriseret adgang, anvendelse, offentliggørelse, afbrydelse, ændring eller ødelæggelse af betalingstjenesteudbyderens aktiver, som påvirker betalingsrelaterede tjenesters integritet, tilgængelighed, fortrolighed og/eller ægthed. Dette kan for eksempel være tilfældet, hvis betalingstjenesteudbyderen er ramt af et brud på sikkerheden i netværks- eller informationssystemer.

Kriterier, der udløser rapporten om en større hændelse: Angiv, hvilke kriterier der har udløst rapporten om en større hændelse. Der kan vælges flere svar blandt følgende kriterier: Berørte transaktioner, berørte betalingstjenestebrugere, tjenestes nedetid, brud på sikkerheden i netværks- eller informationssystemer, økonomisk indvirkning, højt niveau af intern eskalering, andre betalingstjenesteudbydere eller relevante infrastrukturer, der potentielt er berørt, og/eller indvirkning på omdømme.

En kort og generel beskrivelse af hændelsen: Redegør kort for de mest relevante problemer ved hændelsen, herunder dens mulige årsager, umiddelbare konsekvenser osv.

Eventuel indvirkning i andre EU-medlemsstater: Redegør kort for den indvirkning, hændelsen har haft i en anden EU-medlemsstat (f.eks. på betalingstjenestebrugere, betalingstjenesteudbydere og/eller betalingsinfrastrukturer). Hvis det er muligt inden for den gældende indberetningsfrist vedhæftes en engelsk oversættelse.

Indberetning til andre myndigheder: Angiv, om hændelsen har været/vil blive indberettet til andre myndigheder inden for andre rammer for indberetning af hændelser, hvis dette vides på tidspunktet for indberetning. I givet fald anføres de pågældende myndigheder.

Årsager til for sen indsendelse af den indledende rapport: Redegør for årsagerne til, at hændelsen først har kunnet klassificeres efter 24 timer.

B Foreløbig rapport

B 1 – Generelle oplysninger

En mere detaljeret beskrivelse af hændelsen: Beskriv hændelsens væsentligste punkter omfattende som minimum oplysninger om det konkrete problem og baggrunden for dette, hvordan hændelsen opstod og udviklede sig samt konsekvenserne, navnlig for betalingstjenestebrugere osv. Anfør også, hvis relevant, oplysninger om kommunikationen med betalingstjenestebrugere.

Er hændelsen relateret til (en) tidligere hændelse(r)?: Angiv, hvis dette vides, om hændelsen er relateret til (en) tidligere hændelse(r). Hvis hændelsen er relateret til (en) tidligere hændelse(r), angives hvilke(n).

Har andre tjenesteudbydere/tredjeparter været berørt eller involveret?: Angiv, hvis dette vides, om hændelsen har berørt eller involveret andre tjenesteudbydere/tredjeparter. Hvis hændelsen har berørt eller involveret andre tjenesteudbydere/tredjeparter, anføres disse, og der redegøres nærmere for dette.

Er der indledt krisestyring (internt og/eller eksternt)?: Angiv, om der er indledt krisestyring (internt og/eller eksternt). Hvis der har været indledt krisestyring, redegøres der nærmere for dette.

Dato og klokkeslæt for hændelsens opståen: Dato og klokkeslæt for hændelsens opståen, hvis dette kendes.

Dato og klokkeslæt, hvor hændelsen er afhjulpet eller forventes afhjulpet: Angiv datoen og klokkeslættet, hvor hændelsen er kommet eller forventes at komme under kontrol, og driften er blevet eller forventes igen at være normal.

Berørte funktionsområder: Angiv de(t) trin i betalingsprocessen, der er berørt af hændelsen, som for eksempel autentifikation/godkendelse, kommunikation, clearing, direkte afvikling, indirekte afvikling og andet.

Autentifikation/godkendelse: En procedure, der giver betalingstjenesteudbyderen mulighed for at verificere identiteten af en betalingstjenestebruger eller validiteten af brugen af et specifikt betalingsinstrument, herunder brugen af brugerens personaliserede sikkerhedsoplysninger og samtykket fra betalingstjenestebrugeren (eller en tredjepart, der handler på dennes vegne) til at overføre midler.

Kommunikation: Informationsstrøm til identifikation, autentifikation, underretning og information mellem kontoførende betalingstjenesteudbydere og udbydere af betalingsinitieringstjenester, udbydere af kontooplysningstjenester, betalere, betalingsmodtagere og andre betalingstjenesteudbydere.

Clearing: Proces til overførsel, afstemning og undertiden bekræftelse af overførselsordrer forud for afviklingen, eventuelt også modregning af ordrer og beregning af slutpositioner til afvikling.

Direkte afvikling: Gennemførelse af en transaktion eller behandling med henblik på at opfylde deltagernes forpligtelser gennem overførsel af midler, når denne handling udføres af den berørte betalingstjenesteudbyder selv.

Indirekte afvikling: Gennemførelse af en transaktion eller behandling med henblik på at opfylde deltagernes forpligtelser gennem overførsel af midler, når denne handling udføres af en anden betalingstjenesteudbyder på vegne af den berørte betalingstjenesteudbyder.

Andet: Det berørte funktionsområde er ikke et af ovennævnte. Yderligere oplysninger tilføjes i fritekstfeltet.

Ændringer foretaget i tidligere rapporter: Angiv ændringer foretaget i oplysningerne i tidligere rapporter vedrørende samme hændelse (f.eks. den indledende rapport eller, efter omstændighederne, en foreløbig rapport).

B 2 – Klassificering af hændelse/Oplysninger om hændelse

Berørte transaktioner: Betalingstjenesteudbydere bør angive, hvilke tærskelværdier der er eller sandsynligvis vil blive nået som følge af hændelsen og de tilhørende tal: antal berørte transaktioner, procentdel af berørte transaktioner i forhold til antal betalingstransaktioner, der er udført med de betalingstjenester, der er berørt af hændelsen, og transaktionernes samlede værdi. Betalingstjenesteudbydere bør angive konkrete værdier for disse variabler i form af faktiske tal eller skøn. Som hovedregel bør betalingstjenesteudbydere ved "berørte transaktioner" forstå alle indenlandske og grænseoverskridende transaktioner, der direkte eller indirekte er eller sandsynligvis vil blive berørt af hændelsen, navnlig de transaktioner, der ikke har kunnet initieres eller behandles, transaktioner, for hvilke betalingsmeddelelsens indhold er ændret, og transaktioner, der er bestilt i svigagtigt øjemed (uanset om midlerne er blevet tilbagebetalt eller ej). Endvidere bør betalingstjenesteudbydere ved det normale niveau af betalingstransaktioner forstå årsgennemsnittet af daglige indenlandske og grænseoverskridende betalingstransaktioner, der udføres med de betalingstjenester, der er ramt af hændelsen, idet det foregående år er referenceperiode. Anser betalingstjenesteudbydere ikke dette tal for at være repræsentativt (f.eks. på grund af sæsonudsving), bør de i stedet anvende en anden, mere repræsentativ, målemetode og over for den kompetente myndighed begrunde denne metode i feltet "Kommentarer". I tilfælde, hvor betalingstransaktioner i ikkeeurovalutaer er berørt af hændelsen, bør berørte betalingstjenesteudbydere ved beregning af tærskelværdier og indberetning af transaktionernes værdi omregne transaktionsbeløbet i en ikkeeurovaluta til euro på grundlag af ECB's daglige referencekurs på den dag, der går forud for dagen, hvor hændelsesrapporten indsendes.

Berørte betalingstjenestebrugere: Betalingstjenesteudbydere bør angive, hvilke tærskler der er eller sandsynligvis vil blive berørt af hændelsen, og de tilhørende tal: samlet antal betalingstjenestebrugere der er berørt, og procentdelen af betalingstjenestebrugere der er berørt i forhold til det samlede antal betalingstjenestebrugere. Betalingstjenesteudbydere bør angive konkrete værdier for disse variabler i form af faktiske tal eller skøn. Betalingstjenesteudbydere bør ved "berørte betalingstjenestebrugere" forstå alle kunder (indenlandske eller udenlandske, forbrugere eller virksomheder), der har indgået en kontrakt med den berørte betalingstjenesteudbyder og derved har adgang til den berørte betalingstjeneste, og som er eller sandsynligvis vil blive ramt af konsekvenserne af hændelsen. Betalingstjenesteudbydere bør anvende skøn baseret på tidligere aktivitet for at fastslå det antal betalingstjenestebrugere, der kan have anvendt betalingstjenesten, mens hændelsen har stået på. For koncerners vedkommende bør den enkelte betalingstjenesteudbyder kun medregne sine egne betalingstjenestebrugere. Hvis en betalingstjenesteudbyder tilbyder driftstjenester til andre, bør denne betalingstjenesteudbyder kun medregne sine eventuelle egne betalingstjenestebrugere, og betalingstjenesteudbydere, der modtager disse driftstjenester, bør også vurdere hændelsen i forhold til deres egne betalingstjenestebrugere. Desuden bør betalingstjenesteudbydere ved det samlede antal betalingstjenestebrugere forstå det samlede antal indenlandske og grænseoverskridende betalingstjenestebrugere, der på hændelsestidspunktet er kontraktligt bundet til dem (eller alternativt det seneste foreliggende antal) og har adgang til den berørte betalingstjeneste, uanset deres størrelse og om de anses for aktive eller passive betalingstjenestebrugere.

Brud på sikkerheden i netværks- eller informationssystemer: Betalingstjenesteudbydere bør fastslå, om en ondsindet handling har skadet tilgængeligheden, ægtheden, integriteten eller fortroligheden af netværks- eller informationssystemer (herunder data) med relation til levering af betalingstjenester.

Tjenestens nedetid: Betalingstjenesteudbydere bør angive, om tærskelværdien er eller sandsynligvis vil blive nået på grund af hændelsen, og det tilhørende tal: tjenestens samlede nedetid. Betalingstjenesteudbydere bør for denne variabel angive konkrete værdier, som kan være faktiske tal eller skøn. Betalingstjenesteudbydere bør medregne det tidsrum, hvori en opgave, proces eller kanal, der er relateret til levering af betalingstjenester, er eller sandsynligvis vil være nede og derved forhindrer i) initiering og/eller udførelse af en betalingstjeneste og/eller ii) adgang til en betalingskonto. Betalingstjenesteudbydere bør beregne nedetiden for tjenesten fra det øjeblik, nedetiden begynder, og tage højde for både de perioder, hvor de holder åbent som påkrævet for gennemførelsen af betalingstransaktioner, og de perioder, hvor de holder lukket, samt vedligeholdelsesperioder, når det er relevant og muligt. Hvis betalingstjenesteudbydere ikke kan fastslå, hvornår nedetiden for tjenesten er begyndt, bør de undtagelsesvis beregne tjenestens nedetid fra det øjeblik, hvor nedetiden konstateres.

Økonomisk indvirkning: Betalingstjenesteudbydere bør angive, om tærskelværdien er eller sandsynligvis vil blive nået som følge af hændelsen, og de tilhørende tal: direkte omkostninger og indirekte omkostninger. Betalingstjenesteudbydere bør angive konkrete værdier for disse variabler, i form af faktiske tal eller skøn. Betalingstjenesteudbydere bør medregne både de omkostninger, der kan relateres til hændelsen direkte, og omkostninger, der er indirekte relateret til hændelsen. Betalingstjenesteudbydere bør blandt andet medregne eksproprierede midler eller aktiver, omkostninger til udskiftning af hardware eller software, andre juridiske omkostninger og omkostninger til afhjælpning, gebyrer som følge af manglende overholdelse af kontraktlige forpligtelser, sanktioner, eksterne forpligtelser og tabte indtægter. Hvad angår indirekte omkostninger, bør betalingstjenesteudbydere kun medregne omkostninger, der allerede kendes eller højst sandsynligt vil påløbe. I de tilfælde, hvor omkostningerne er i ikkeeurovalutaer ved beregning af tærskelværdien og indberetning af værdien af den økonomiske indvirkning, bør betalingstjenesteudbydere omregne omkostningsbeløbet i en ikkeeurovaluta til euro på grundlag af ECB's daglige referencekurs på den dag, der går forud for dagen, hvor hændelsesrapporten indsendes.

Direkte omkostninger: Omkostninger (i euro), der direkte skyldes hændelsen, herunder udgifter til afhjælpning af hændelsen (f.eks. eksproprierede midler eller aktiver, udgifter til udskiftning af hardware og software, gebyrer som følge af manglende overholdelse af kontraktlige forpligtelser).

Indirekte omkostninger: Omkostninger (i euro), der indirekte skyldes hændelsen (f.eks. udgifter til godtgørelse af kunder, potentielle retsomkostninger).

Højt niveau af intern eskalering: Betalingstjenesteudbydere bør tage stilling til, om ledelsesorganet som defineret i EBA's retningslinjer for IKT og sikkerhedsrisikostyring som følge af indvirkningen på betalingsrelaterede tjenester har eller sandsynligvis vil modtage underretning i overensstemmelse med retningslinje 60, punkt d), i EBA's retningslinjer for IKT og sikkerhedsrisikostyring om hændelsen uden for en periodisk notifikationsprocedure og løbende, mens hændelsen står på. Desuden bør betalingstjenesteudbydere tage stilling til, om der er eller sandsynligvis vil blive udløst en krisesituation som følge af hændelsens indvirkning på betalingsrelaterede tjenester.

Andre betalingstjenesteudbydere eller relevante infrastrukturer, der potentielt er berørt: Betalingstjenesteudbydere bør vurdere hændelsens indvirkning på det finansielle marked, forstået som det finansielle markeds infrastrukturer og/eller betalingsordninger, der er grundlag for markedet og de øvrige betalingstjenesteudbydere. Betalingstjenesteudbydere bør navnlig vurdere, om hændelsen har gentaget sig eller sandsynligvis vil gentage sig hos andre betalingstjenesteudbydere, om den har påvirket eller sandsynligvis vil påvirke den smidige funktion af det finansielle markeds infrastrukturer, og om den har skadet eller sandsynligvis vil skade soliditeten af det finansielle system som helhed. Betalingstjenesteudbydere bør være opmærksomme på en række forhold, f.eks. om den berørte komponent/software er omfattet af ejendomsret eller er almindeligt tilgængelig, om det berørte netværk er et internt eller eksternt netværk, og om betalingstjenesteudbyderen er ophørt med eller sandsynligvis vil ophøre med at opfylde sine forpligtelser i det finansielle markeds infrastrukturer, udbyderen indgår i.

Indvirkning på omdømme: Betalingstjenesteudbydere bør vurdere det synlighedsniveau, som hændelsen efter deres bedste overbevisning har fået eller sandsynligvis vil få på markedet. Navnlig bør betalingstjenesteudbydere vurdere sandsynligheden for, at hændelsen er samfundsskadelig, som en indikator for dens potentiale til at påvirke deres omdømme. Betalingstjenesteudbydere bør tage højde for, om i) betalingstjenestebrugere og/eller betalingstjenesteudbydere har klaget over hændelsens negative indvirkning, ii) hændelsen har påvirket en synlig betalingstjenesterelateret proces og derfor sandsynligvis vil få eller allerede har fået presseomtale (ikke kun i de traditionelle medier som for eksempel aviser, men også i blogs, sociale medier osv.; ved presseomtale i denne kontekst forstås dog ikke blot et par negative kommentarer fra følgere; der skal være tale om en velfunderet redegørelse eller et betydeligt antal negative kommentarer/klager), iii) kontraktlige forpligtelser er blevet eller sandsynligvis vil blive misligholdt med offentliggørelse af sagsanlæg mod betalingstjenesteudbyderen til følge, iv) lovkrav ikke er blevet efterlevet med tilsynsforanstaltninger eller sanktioner til følge, der har været eller sandsynligvis vil blive gjort offentligt tilgængelige, og v) en lignende type hændelse er opstået tidligere.

B 3 – Beskrivelse af hændelse

Hændelsens art: Drifts- eller sikkerhedshændelse. Der kan redegøres yderligere for dette i det tilhørende felt i den indledende rapport.

Hændelsens årsag: Angiv hændelsens årsag eller, hvis denne endnu ikke kendes, den mest sandsynlige årsag. Der er flere svarmuligheder.

Undersøgelse pågår: Sæt kryds i feltet, hvis årsagen p.t. ikke er kendt.

Ondsindet handling: Handlinger, der bevidst er rettet mod betalingstjenesteudbyderen. Dette omfatter ondsindet kode, informationsindsamling, uvedkommende personers indtrængen, distributed denial of service-angreb/denial of service-angreb (DDoS-angreb/DoS-angreb),

bevidste interne handlinger, bevidst ekstern fysisk skade, informationsindholds sikkerhed, svigagtige handlinger osv. Se afsnit C2 i dette skema for yderligere oplysninger.

Procesfejl: Årsagen til hændelsen er mangelfuldhed, hvad angår design eller gennemførelse af betalingsprocessen, proceskontrollerne og/eller de understøttende processer (for eksempel proces til ændring/migration, test, konfigurering, kapacitet, overvågning).

Systemfejl: Hændelsen er relateret til mangelfuldhed, hvad angår design, gennemførelse, komponenter, specifikationer, integration eller kompleksitet af de systemer, netværk, infrastrukturer og databaser, der understøtter betalingsaktiviteten.

Menneskelige fejl: Hændelsen skyldes en utilsigtet menneskelig fejl, hvad enten der var tale om en del af betalingsproceduren (f.eks. upload af den forkerte betalingsbatchfil til betalingssystemet) eller årsagen på anden måde er relateret dertil (f.eks. en strømafbrydelse ved et uheld, der medfører, at betalingsaktiviteten stilles i bero).

Eksterne forhold: Årsagen er relateret til forhold, der generelt ligger uden for organisationens direkte kontrol (f.eks. naturkatastrofer, fejl hos en udbyder af tekniske tjenester).

Andet: Intet af ovennævnte er årsag til hændelsen. Yderligere oplysninger tilføjes i fritekstfeltet.

Har hændelsen påvirket dig direkte, eller indirekte via en tjenesteudbyder?: Angiv, om hændelsen har ramt betalingstjenesteudbyderen direkte eller påvirker denne indirekte gennem en tredjepart, hvis dette vides. I tilfælde af indirekte indvirkning angives navnet på tjenesteudbyderen eller -udbyderne.

B 4 – Hændelsens indvirkning

Samlet indvirkning: Angiv, hvilke funktioner der er påvirket af drifts- eller sikkerhedshændelsen. Der er flere svarmuligheder.

Integritet: Sikring af aktivers (herunder datas) rigtighed og fuldstændighed.

Tilgængelighed: Det forhold ved betalingsrelaterede tjenester, at de er fuldt ud tilgængelige og anvendelige for betalingstjenestebrugere, i henhold til anerkendte, på forhånd fastsatte niveauer.

Fortrolighed: Det forhold, at oplysninger ikke gøres tilgængelige eller videregives til uautoriserede personer, enheder eller processer.

Ægthed: Det forhold ved en kilde, at den er, hvad den hævder at være.

Berørte kommercielle kanaler: Angiv de(n) kanal(er), hvor der har været interaktion med betalingstjenestebrugere, og som hændelsen har berørt. Der kan afkrydses flere felter.

Filialer: Forretningssted (bortset fra hovedkontoret), som tilhører en betalingstjenesteudbyder, og som ikke er en juridisk person, men direkte udfører nogle af eller alle de transaktioner, der hører med til en betalingstjenesteudbyders virksomhed. Alle forretningssteder, der er oprettet i samme medlemsstat af en betalingstjenesteudbyder med hovedsæde i en anden medlemsstat, regnes for én filial.

Netbank: Finansielle transaktioner, der gennemføres via internettet ved hjælp af computere.

Telefonbank: Finansielle transaktioner, der gennemføres telefonisk.

Mobilbank: Finansielle transaktioner, der gennemføres ved hjælp af en særlig bankapplikation på en smartphone eller lignende enhed.

Pengeautomater: Elektromekaniske apparater, der gør det muligt for betalingstjenestebrugere at få udbetalt kontanter fra deres konto og/eller få adgang til andre tjenester.

Salgsterminal: Fysiske lokaler tilhørende den forretningsdrivende, hvor betalingstransaktionen er initieret.

E-handel: Betalingstransaktionen er initieret ved et virtuelt salgssted (f.eks. for betalinger initieret via internettet ved hjælp af kreditoverførsler, betalingskort, overførsel af elektroniske penge mellem e-pengekonti).

Andet: Den berørte kommercielle kanal er ikke en af ovennævnte. Yderligere oplysninger tilføjes i fritekstfeltet.

Berørte betalingstjenester: Angiv de betalingstjenester, der som følge af hændelsen ikke fungerer korrekt. Der kan afkrydses flere felter.

Kontant indbetaling på en betalingskonto: Indbetaling af et kontant beløb til en betalingstjenesteudbyder med henblik på indsættelse på en betalingskonto.

Udbetaling af kontantbeløb fra en betalingskonto: Anmodning, der modtages af en betalingstjenesteudbyder fra dennes betalingstjenestebruger, om at udbetale et kontant beløb og debitere brugerens betalingskonto for beløbet.

Nødvendige handlinger i forbindelse med at føre en betalingskonto: Handlinger, der er nødvendige til at aktivere, deaktivere og/eller føre en betalingskonto (f.eks. åbning eller spærring).

Indløsning af betalingstransaktioner: En betalingstjeneste, der udbydes af en betalingstjenesteudbyder, som indgår en aftale med en betalingsmodtager om at modtage og behandle betalingstransaktioner, og som fører til overførsel af penge til betalingsmodtageren.

Kreditoverførsel: En betalingstjeneste til at kreditere en betalingsmodtagers betalingskonto med en betalingstransaktion eller en række betalingstransaktioner fra en betalers betalingskonto foretaget af den betalingstjenesteudbyder, der forvalter betalerens betalingskonto, på grundlag af en instruks fra betaleren.

Direkte debitering: En betalingstjeneste til at debitere en betalers betalingskonto, hvor en betalingstransaktion initieres af betalingsmodtageren på grundlag af betalerens samtykke til betalingsmodtageren, til betalingsmodtagerens betalingstjenesteudbyder eller til betalerens egen betalingstjenesteudbyder

Kortbetaling: En betalingstjeneste, der er baseret på en betalingskortordnings infrastruktur og forretningsbetingelser for betalingstransaktioner ved hjælp af kort, telekommunikation, digitalt udstyr eller IT-udstyr, eller ved hjælp af software, hvis dette resulterer i en debet- eller kreditkorttransaktion. Kortbaserede betalingstransaktioner omfatter ikke transaktioner baseret på andre former for betalingstjenester.

Udstedelse af betalingsinstrumenter: En betalingstjeneste udbudt af en betalingstjenesteudbyder, som har indgået en aftale om at stille et betalingsinstrument til rådighed for en betaler med henblik på at initiere og behandle betalerens betalingstransaktioner.

Pengeoverførsel: En betalingstjeneste, hvor der modtages midler fra en betaler, uden at der oprettes en betalingskonto i betalerens eller betalingsmodtagerens navn, alene med det formål at overføre et tilsvarende beløb til en betalingsmodtager eller en anden betalingstjenesteudbyder på betalingsmodtagerens vegne, og/eller hvor sådanne midler modtages på betalingsmodtagerens vegne og stilles til rådighed for denne.

Betalingsinitieringstjeneste: En tjeneste til initiering af en betalingsordre på anmodning af betalingstjenestebrugeren med hensyn til en betalingskonto hos en anden betalingstjenesteudbyder

Kontooplysningstjeneste: En onlinetjeneste, der leverer konsoliderede oplysninger om en eller flere betalingskonti, som betalingstjenestebrugeren har hos enten en anden betalingstjenesteudbyder eller hos flere end én betalingstjenesteudbyder.

B 5 – Begrænsning af hændelsens indvirkning

Hvilke handlinger/foranstaltninger er hidtil blevet iværksat eller planlagt for at afhjælpe hændelsen?: Redegør for handlinger, der er eller planlægges iværksat for at afhjælpe hændelsen foreløbigt.

Er beredskabsplanen og/eller katastrofeberedskabsplanen bragt i anvendelse?: Angiv, om dette har været tilfældet, og i givet fald de vigtigste oplysninger om det skete (dvs. hvornår de(n) blev bragt i anvendelse, og hvad de(n) bestod i).

C – Endelig rapport

C 1 – Generelle oplysninger

Opdatering af oplysningerne fra den indledende rapport og de(n) foreløbige rapport(er) (sammenfatning): Redegør nærmere for hændelsen, herunder de konkrete ændringer, der er foretaget i oplysningerne i den foreløbige rapport. Andre relevante oplysninger medtages.

Er alle oprindelige kontroller etableret?: Angiv, om betalingstjenesteudbyderen har været nødsaget til at aflyse eller begrænse nogle kontroller på et tidspunkt, mens hændelsen har stået på. I givet fald anføres det, om alle kontroller er genetableret, og, hvis det ikke er tilfældet, redegøres der i fritekstfeltet for, hvilke kontroller der ikke er genetableret, samt for den yderligere tid, der er nødvendig for at genetablere dem.

C 2 – Årsagsanalyse og opfølgning

Hvad er den grundlæggende årsag, hvis den kendes?: Angiv, hvad der er den grundlæggende årsag til hændelsen, eller, hvis den endnu ikke kendes, den mest sandsynlige årsag. Der er flere svarmuligheder. (Bemærk, at der bør skelnes mellem den grundlæggende årsag til hændelsen og hændelsens indvirkning.)

Ondsindet handling: Eksterne eller interne handlinger, der bevidst er rettet mod betalingstjenesteudbyderen. De opdeles i følgende kategorier:

Ondsindet kode: Virus, orm, trojansk hest, spyware m.m.

Informationsindsamling: Scanning, sniffing, social manipulation m.m.

Indtrængning: Uautoriseret adgang til privilegeret konto, uautoriseret adgang til ikkeprivilegeret konto, uautoriseret adgang via applikation, bot m.m.

Distributed denial of service-angreb/denial of service-angreb (DDoS-angreb/DoS-angreb): Forsøg på at gøre en onlinetjeneste utilgængelig ved at overbelaste den med trafik fra flere kilder.

Bevidste interne handlinger: Sabotage, tyveri m.m.

Bevidst ekstern fysisk skade: Sabotage, fysisk angreb på lokaler/datacentre m.m.

Informationsindholds sikkerhed: Uautoriseret adgang til oplysninger, uautoriseret ændring af oplysninger).

Svigagtige handlinger: Uautoriseret anvendelse af ressourcer, ophavsret, falsk identitet, phishing.

Andet (uddybes): Intet af ovennævnte er årsag til hændelsen. Yderligere oplysninger tilføjes i fritekstfeltet.

Procesfejl: Årsagen til hændelsen er mangelfuldhed, hvad angår design eller gennemførelse af betalingsprocessen, proceskontrollerne og/eller de underliggende processer (for eksempel proces til ændring/migration, test, konfigurering, kapacitet, overvågning). De opdeles i følgende kategorier:

Mangelfuld overvågning og kontrol: Vedrørende drift, certifikaters udløbsdato, licensers udløbsdato, udløbsdato for programrettelser, tællerværdiers definerede maksimum, mængden af data i databasen, administration af brugerrettigheder, dual control-princip m.m.

Kommunikationsproblemer: Mellem f.eks. markedsdeltagere eller inden for organisationen.

Ukorrekt betjening: Ingen udskiftning af certifikater, fuld cache m.m.

Mangelfuld forandringsledelse: Identificerede konfigurationsfejl, udrulning inklusive opdateringer, serviceproblemer, uventede fejl m.m.

Mangelfuldhed i interne procedurer og dokumentation: Manglende gennemsigtighed i funktionaliteter, processer og forekomst af fejlfunktioner, manglende dokumentation m.m.

Genetableringsproblemer: Beredskabsstyring, mangelfuld redundans m.m.

Andet (uddybes): Intet af ovennævnte er årsag til hændelsen. Yderligere oplysninger tilføjes i fritekstfeltet.

Systemfejl: Hændelsen er relateret til mangelfuldhed, hvad angår design, gennemførelse, komponenter, specifikationer, integration eller kompleksitet af de systemer, netværk, infrastrukturer og databaser, der understøtter betalingsaktiviteten. De opdeles i følgende kategorier:

Hardwarefejl: Fejl i fysisk teknologisk udstyr, der afvikler processerne og/eller lagrer de data, betalingstjenesteudbydere skal bruge til at gennemføre deres betalingsrelaterede aktivitet (f.eks. fejl på harddiske, i datacentre, i anden infrastruktur).

Netværksfejl: Fejl i de telekommunikationsnet, enten offentlige eller private, der muliggør udveksling af data og oplysninger (f.eks. via internettet) under betalingsprocessen.

Databaseproblemer: Datastruktur, der lagrer de person- og betalingsoplysninger, der er påkrævet for at udføre betalingstransaktioner.

Software-/applikationsfejl: Fejl i programmer, operativsystemer osv., der understøtter betalingstjenesteudbyderes levering af betalingstjenester (f.eks. fejlfunktioner, ukendte funktioner).

Fysisk skade: Utilsigtet skade forårsaget af mangelfulde forhold, anlægsarbejde m.m.

Andet (uddybes): Intet af ovennævnte er årsag til hændelsen. Yderligere oplysninger tilføjes i fritekstfeltet.

Menneskelig fejl: Hændelsen skyldes en utilsigtet menneskelig fejl, hvad enten der har været tale om en del af betalingsproceduren (f.eks. upload af den forkerte betalingsbatchfil til betalingssystemet), eller årsagen på anden måde er relateret dertil (f.eks. en strømafbrydelse ved et uheld, der medfører, at betalingsaktiviteten stilles i bero). De opdeles i følgende kategorier:

Utilsigtet: Fejl, udeladelser, manglende erfaring og kendskab m.m.

Manglende handling: Som følge af manglende færdigheder, kendskab, erfaring, oplysning m.m.

Utilstrækkelige ressourcer: Manglende menneskelige ressourcer, medarbejderes tilgængelighed m.m.

Andet (uddybes): Intet af ovennævnte er årsag til hændelsen. Yderligere oplysninger tilføjes i fritekstfeltet.

Eksterne forhold: Årsagen er relateret til forhold, der generelt ligger uden for organisationens kontrol. De opdeles i følgende kategorier:

Fejl hos leverandør/udbyder af tekniske tjenester: Strømafbrydelse, netnedbrud, juridiske problemer, forretningsmæssige problemer, afhængighedsforhold mellem tjenester m.m.

Force majeure: Strømsvigt, brand, naturfænomener som for eksempel jordskælv, oversvømmelse, kraftig nedbør, stærk blæst m.m.

Andet (uddybes): Intet af ovennævnte er årsag til hændelsen. Yderligere oplysninger tilføjes i fritekstfeltet.

Andet: Intet af ovennævnte er årsag til hændelsen. Yderligere oplysninger tilføjes i fritekstfeltet.

Andre relevante oplysninger om den grundlæggende årsag: Redegør nærmere for den grundlæggende årsag, herunder de foreløbige konklusioner af årsagsanalysen.

Vigtigste korrigerende handlinger/foranstaltninger, der er iværksat eller planlagt for at forebygge en gentagelse af hændelsen, hvis de allerede kendes: Beskriv de vigtigste handlinger, der er iværksat eller planlagt for at forebygge, at hændelsen gentager sig.

C 3 – Yderligere oplysninger

Er andre betalingstjenesteudbydere blevet underrettet om hændelsen? Oplys, hvilke betalingstjenesteudbydere der er blevet kontaktet formelt eller uformelt for at underrette dem om hændelsen, med oplysning om de betalingstjenesteudbydere, der er blevet underrettet, de oplysninger, disse har modtaget, samt begrundelsen for at give dem disse oplysninger.

Er der taget retlige skridt mod betalingstjenesteudbyderen?: Angiv, om der på tidspunktet for udarbejdelsen af den endelige rapport er taget retlige skridt mod betalingstjenesteudbyderen (f.eks. sagsanlæg eller inddragelse af autorisation) som følge af hændelsen.

Vurdering af effektiviteten af de handlinger, der er iværksat: Medtag om muligt en selvevaluering af effektiviteten af de handlinger, der er iværksat, mens hændelsen har stået på, herunder de erfaringer, der er gjort.