EBA/GL/2017/10

18/12/2017

# Retningslinjer

## for indberetning af større hændelser i henhold til direktiv (EU) 2015/2366 (PSD2)

# 1. Compliance- og indberetningsforpligtelser

## Status for disse retningslinjer

1. Dette dokument indeholder retningslinjer, der er udstedt i henhold til artikel 16 i forordning (EU) nr. 1093/2010[1]. I henhold til artikel 16, stk. 3, i forordning (EU) nr. 1093/2010 skal de kompetente myndigheder og finansielle institutioner bestræbe sig på at efterleve disse retningslinjer bedst muligt.

2. Retningslinjerne afspejler EBA's syn på passende tilsynspraksis inden for det europæiske finanstilsynssystem eller på, hvordan EU-retten bør anvendes inden for et bestemt område. De kompetente myndigheder, som er omhandlet i artikel 4, stk. 2, i forordning (EU) nr. 1093/2010, 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 forordning (EU) nr. 1093/2010 skal de kompetente myndigheder senest den 19.02.2018 underrette EBA om, hvorvidt de efterlever eller agter at efterleve disse retningslinjer, eller begrunde en eventuel manglende efterlevelse. Hvis EBA ikke er blevet underrettet 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, til compliance@eba.europa.eu med referencen "EBA/GL/2017/10". Underretninger fremsendes af personer med behørig beføjelse til at indberette efterlevelse på vegne af deres kompetente myndigheder. 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. Genstand, anvendelsesområde og definitioner

## Genstand

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 nævnte direktiv.

7. Derudover omhandler retningslinjerne, hvordan disse kompetente myndigheder bør vurdere hændelsens relevans og detaljerne i de hændelsesindberetninger, som de i henhold til artikel 96, stk. 2, i nævnte direktiv bør dele med andre indenlandske myndigheder.

8. Endvidere omhandler disse retningslinjer delingen med EBA og ECB af de relevante detaljer vedrørende de indberettede hændelser med det formål at fremme en fælles og ensartet tilgang.

## Anvendelsesområde

9. Disse retningslinjer finder anvendelse ved klassificering og indberetning af større drifts- eller sikkerhedshændelser i henhold til artikel 96 i direktiv (EU) 2015/2366.

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 har sin oprindelse 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 betalingstjenesteleverandør hjemmehørende i Unionen, enten direkte (en betalingsrelateret tjeneste udføres af den berørte tredjelandsvirksomhed) eller indirekte (betalingstjenesteleverandørens evne til at fortsætte sin betalingsaktivitet er på anden måde truet som følge af hændelsen).

## Målgrupper

12. Det første sæt retningslinjer (afsnit 4) henvender sig til betalingstjenesteudbydere som defineret i artikel 4, stk. 11, i direktiv (EU) 2015/2366 og som omhandlet i artikel 4, stk. 1, i forordning (EU) 1093/2010.

13. 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

14. Medmindre andet er angivet, har de termer, der anvendes og er defineret i direktiv (EU) 2015/2366, samme betydning i retningslinjerne. I denne vejledning finder følgende definitioner endvidere anvendelse:

| | |
|---|---|
| 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, ægthed og/eller kontinuitet. |
| Integritet | Den egenskab, at korrektheden og fuldstændigheden af aktiver (herunder data) varetages. |
| Tilgængelig | Den egenskab, at betalingsrelaterede tjenester er til rådighed og anvendelige for betalingstjenestebrugere. |
| Fortrolighed | Den egenskab, at oplysninger ikke gøres tilgængelige eller afsløres for uautoriserede personer, virksomheder eller processer. |
| Ægthed | Den egenskab ved en kilde, at den er, hvad den hævder at være. |
| Kontinuitet | Den egenskab, at de af en organisations processer, opgaver og aktiver, der er nødvendige for levering af betalingsrelaterede tjenester, er fuldt tilgængelige og arbejder på acceptable og prædefinerede niveauer. |
| Betalingsrelaterede tjenester | Forretningsaktiviteter i den i artikel 4, stk. 3, i PSD2 anvendte forstand og alle de tekniske støttefunktioner, der er nødvendige for den korrekte levering af betalingstjenester. |

# 3. Gennemførelse

## Ikrafttrædelsesdato

15. Disse retningslinjer finder anvendelse fra den 13. januar 2018.

# 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 skal klassificere drifts- eller sikkerhedshændelser som større, hvis de opfylder

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

b. tre eller flere kriterier på "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 underlæggende indikatorer:

*i. Berørte transaktioner*

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

*iii. Tjenestens nedetid*

Betalingstjenesteudbydere bør fastlægge den periode, hvor tjenesten må formodes at være utilgængelig for betalingstjenestebrugeren, eller hvor betalingsordren i den i PSD2 artikel 4, stk. 13, anvendte forstand ikke kan udføres af betalingstjenesteudbyderen.

*iv. Økonomisk indvirkning*

Betalingstjenesteudbydere bør fastlægge de samlede omkostninger, der er forbundet med hændelsen, og heri medregne både det absolutte beløb og i givet fald omkostningernes

relative størrelse i forhold til betalingstjenesteudbyderens størrelse (dvs. betalingstjenesteudbyderens kernekapital).

*v. Højt niveau af intern udbredelse*

Betalingstjenesteudbydere bør fastlægge, om denne hændelse er eller vil blive indberettet til deres øverste ledelse.

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

Betalingstjenesteudbydere bør fastlægge de konsekvenser for systemet, som hændelsen må formodes at ville afføde, dvs. dens potentiale for at brede sig fra den indledningsvis berørte betalingstjenesteudbyder til andre betalingstjenesteudbydere, finansielle markedsinfrastrukturer og/eller kortbetalingsordninger.

*vii. Indvirkning på omdømmet*

Betalingsudbydere bør fastlægge, 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 blevet berørt eller må formodes direkte eller indirekte at ville blive berørt af hændelsen, især dem, der ikke har kunnet initieres eller behandles, dem, for hvilke betalingsmeddelelsens indhold er ændret, og dem, der er bestilt i svigagtigt øjemed (uanset om midlerne er blevet tilbagebetalt eller ej).

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 blevet berørt af hændelsen, idet referenceperioden for beregningen er det foregående år. Hvis betalingstjenesteudbyderen ikke anser dette tal for repræsentativt (f.eks. på grund af sæsonbetingede svingninger), bør den i stedet anvende en anden, mere repræsentativ målemetode, og overfor den kompetente myndighed angive rationalet for denne tilgang i det tilhørende felt i skabelonen (se bilag 1).

*ii. Berørte betalingstjenestebrugere*

Betalingstjenesteudbydere bør ved "berørte betalingstjenestebrugere" forstå alle kunder (indenlandske eller udenlandske, forbrugere eller virksomheder), som med den berørte betalingstjenesteudbyder har en kontrakt om adgang til den berørte betalingstjeneste, og som er blevet udsat for følgerne af hændelsen eller må formodes at ville blive det. Betalingstjenesteudbydere bør forlade sig på skøn baseret på tidligere aktivitet til at bestemme det antal betalingstjenestebrugere, der kan have brugt betalingstjenesten i løbet af hændelsens levetid.

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

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 eller om de regnes som aktive eller passive betalingstjenestebrugere.

*iii. Tjenestens nedetid*

Betalingstjenesteudbydere bør medregne det tidsrum, hvori en opgave, proces eller kanal, der er knyttet til leveringen af betalingstjenester, er nede eller må formodes at være det 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 behøver have åbent for at kunne udføre betalingstjenester, og perioder, hvor de har lukket, samt vedligeholdelsesperioder, når dette er relevant og muligt. Hvis betalingstjenesteudbydere ikke kan fastslå, hvornår nedetiden for tjenesten begyndte, bør de undtagelsesvis beregne tjenestens nedetid fra det øjeblik, hvor nedetiden registreres.

*iv. Økonomisk indvirkning*

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

v. *Højt niveau af intern udbredelse*

Betalingstjenesteudbydere bør tage hensyn til, om den informationsansvarlige (eller tilsvarende) som følge af hændelsens indvirkning på betalingsrelaterede tjenester er informeret eller formodes at ville blive informeret om hændelsen uden om en eventuel regelmæssig indberetningsprocedure og løbende i hele hændelsens levetid. Desuden bør betalingstjenesteudbydere tage stilling til, om der er udløst en krisesituation, eller dette må forventes som følge af hændelsens indvirkning på betalingsrelaterede tjenester.

vi. *Andre betalingstjenesteudbydere eller relevante infrastrukturer, der kan være blevet berørt*

Betalingstjenesteudbydere bør vurdere hændelsens indvirkning på det finansielle marked, forstået som det finansielle markeds infrastrukturer og/eller kortbetalingsordninger, der

understøtter dem og andre betalingstjenesteudbydere. Betalingstjenesteudbydere bør navnlig vurdere, hvorvidt hændelsen har gentaget sig eller må forventes at gøre det hos andre betalingstjenesteudbydere, hvorvidt den har påvirket den gnidningsfrie funktion af det finansielle markeds infrastrukturer eller forventes at gøre det, og hvorvidt den har berørt det finansielle systems funktion som helhed eller forventes at gøre det. 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 internt eller eksternt, og hvorvidt betalingstjenesteudbyderen er ophørt eller må forventes at ophøre udførelsen af sine forpligtelser i det finansielle markeds infrastrukturer, hvori den indgår.

vii. *Indvirkning på omdømmet*

Betalingstjenesteudbydere bør medregne den synlighed, som hændelsen efter deres bedste vidende har opnået eller må forventes at opnå på markedet. Navnlig bør betalingstjenesteudbydere tage hensyn til sandsynligheden for, at hændelsen vil være samfundsskadelig, som en indikator for dens potentiale til at påvirke deres omdømme. Betalingstjenesteudbydere bør tage i betragtning, om (i) hændelsen har berørt en synlig proces og derfor må forventes at få mediedækning eller allerede har fået det (herunder ikke kun traditionelle medier som aviser, men også blogs, sociale netværk osv.), ii) forskriftsmæssige forpligtelser er blevet tilsidesat eller må forventes at blive det, iii) sanktioner har været overtrådt eller må forventes at blive det, eller (iv) samme type hændelse er indtruffet før.

1.4. Betalingstjenesteudbydere bør vurdere en hændelse ved, at de for hvert enkelt kriterium konstaterer, om de pågældende tærskler i tabel 1 er nået eller må forventes at blive nået før hændelsen er afhjulpet.

Tabel 1: Tærskler

| Kriterier | Lavere indvirkningsniveau | Højere indvirkningsniveau |
|---|---|---|
| Berørte transaktioner | > 10 % af betalingstjenesteyderens normale transaktionsniveau (i antal transaktioner)<br>**og**<br>> 100 000 EUR | > 25 % af betalingstjenesteyderens normale transaktionsniveau (i antal transaktioner)<br>**eller**<br>> 5 mio. EUR |
| Berørte betalingstjenestebrugere | > 5 000<br>**og**<br>> 10 % af betalingstjenesteudbyderens betalingstjenestebrugere | > 50 000<br>**eller**<br>> 25 % af betalingstjenesteudbyderens betalingstjenestebrugere |
| Tjenestens nedetid | > 2 timer | Ikke relevant |
| Økonomisk indvirkning | Ikke relevant | > Maks. (0,1 % af hovedkapital, * 200 000 EUR)<br>**eller**<br>> 5 mio. EUR |
| Højt niveau af intern udbredelse | Ja | Ja, og der forventes en krisesituation (eller tilsvarende) |

| | | |
|---|---|---|
| Andre betalingstjenesteudbydere eller relevante infrastrukturer, der kan være blevet berørt | Ja | Ikke relevant |
| Indvirkning på omdømmet | Ja | Ikke relevant |

*Hovedkapital 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 benytte skøn, hvis de ikke har faktiske data som grundlag for deres vurdering af, om en given tærskel er nået eller forventes nået, før hændelsen er afhjulpet (dette kan f.eks. tænkes at ske i den indledende undersøgelsesfase).

1.6. Betalingsudbydere bør løbende foretage denne vurdering i hændelsens levetid for at identificere enhver mulig statusændring, enten opad (fra ikke-større til større) eller nedad (fra større til ikke-større).

## Retningslinje 2: Anmeldelsesproces

2.1. Betalingstjenesteudbydere bør samle alle relevante oplysninger, udarbejde en hændelsesrapport med brug af skabelonen i bilag 1, og indsende den til den kompetente myndighed i hjemlandet. Betalingstjenesteudbydere bør udfylde skabelonen efter anvisningerne i bilag 1.

2.2. Betalingstjenesteudbydere bør anvende den samme skabelon til underretning af den kompetente myndighed i hele hændelsens levetid (dvs. til indledende, foreløbige og endelige rapporter som beskrevet i afsnit 2.7 til 2.21). Betalingstjenesteudbydere bør udfylde skabelonen trinvis på den bedst mulige måde, efterhånden som flere oplysninger bliver tilgængelige i løbet af deres interne undersøgelser.

2.3. Betalingstjenesteudbydere bør, hvis relevant, desuden forelægge den kompetente myndighed i deres hjemland en kopi af de oplysninger, der er udleveret (eller vil blive udleveret) til deres brugere, som fastsat i artikel 96, stk. 1, andet afsnit, af PSD2, så snart de foreligger.

2.4. Betalingstjenesteudbydere bør forelægge eventuelle supplerende oplysninger for den kompetente myndighed i hjemlandet, hvis oplysningerne foreligger og anses for relevante for den kompetente myndighed, ved at vedhæfte supplerende dokumentation til standardskabelonen som et eller flere bilag.

2.5. Betalingstjenesteudbydere bør følge op på alle anmodninger fra den kompetente myndighed i hjemlandet ved at udlevere supplerende oplysninger eller præciseringer vedrørende allerede indsendt dokumentation.

2.6. Betalingstjenesteudbydere bør til enhver tid bevare fortroligheden og integriteten af de oplysninger, der udveksles med den kompetente myndighed i deres hjemland, og også autentificere sig selv tilbørligt over for den kompetente myndighed i deres hjemland.

## Indledende rapport

2.7. Betalingstjenesteudbydere bør indsende en indledende rapport til den kompetente myndighed i hjemlandet, når en større drifts- eller sikkerhedshændelse første gang konstateres.

2.8. Betalingstjenesteudbydere bør sende den indledende rapport til den kompetente myndighed inden for 4 timer fra det tidspunkt, hvor den større drifts- eller sikkerhedshændelse første gang opdages, eller – hvis den kompetente myndigheds rapporteringskanaler på dette tidspunkt ikke er tilgængelige eller operationelle – så snart de bliver tilgængelige/operationelle igen.

2.9. Betalingsudbydere bør endvidere indsende en indledende rapport til den kompetente myndighed i hjemlandet, når en tidligere ikke-større drifts- eller sikkerhedshændelse bliver 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 ikke er tilgængelige eller operationelle – så snart de er tilgængelige/operationelle igen.

2.10. Betalingstjenesteudbydere bør i deres indledende rapporter medtage oplysninger på overskriftsniveau (dvs. afsnit A i skabelonen), så de derved medtager nogle grundlæggende karakteristika ved hændelsen og dens forventede konsekvenser på grundlag af de oplysninger, der foreligger straks efter, at den er konstateret eller omklassificeret. Betalingstjenesteudbydere bør anvende skøn, når der ikke foreligger faktiske data. Betalingstjenesteudbydere bør desuden i deres indledende rapport anføre datoen for næste ajourføring, som bør finde sted snarest muligt og under ingen omstændigheder efter mere end 3 arbejdsdage.

## Foreløbig rapport

2.11. Betalingstjenesteudbydere bør indsende foreløbige rapporter hver gang de mener, at der er en relevant ajourføring af status, og som minimum på datoen for næste ajourføring som angivet i den foregående rapport (enten den indledende rapport eller den foregående foreløbige rapport).

2.12. Betalingstjenesteudbydere bør indsende en første foreløbig rapport til den kompetente myndighed med en mere detaljeret beskrivelse af hændelsen og dens konsekvenser (skabelonens afsnit B). Betalingstjenesteudbydere bør desuden udarbejde yderligere foreløbige rapporter ved at ajourføre de oplysninger, der allerede er givet i skabelonens afsnit A og B, i det mindste når de får kendskab til nye relevante oplysninger eller væsentlige

ændringer siden den foregående underretning (f.eks. om hændelsen er tiltaget eller aftaget, og om der er konstateret nye årsager eller truffet tiltag til at løse problemet). Under alle omstændigheder bør betalingstjenesteudbydere udarbejde en foreløbig rapport på anmodning af den kompetente myndighed i hjemlandet.

2.13. Ligesom for indledende rapporter bør betalingstjenesteudbydere benytte skøn, når der ikke foreligger faktiske data.

2.14. Betalingstjenesteudbydere bør desuden i hver rapport anføre datoen for næste ajourføring, som bør finde sted snarest muligt og under ingen omstændigheder efter mere end 3 arbejdsdage. Hvis betalingstjenesteudbyderen ikke kan overholde den skønnede dato for næste ajourføring, bør denne kontakte den kompetente myndighed for at forklare årsagerne til forsinkelsen, foreslå en ny sandsynlig frist for indsendelse (højst 3 arbejdsdage) og indsende en ny foreløbig rapport, der udelukkende ajourfører oplysningerne om den skønnede dato for næste ajourføring.

2.15. Når de normale aktiviteter er genoptaget og driften igen er normal, bør betalingstjenesteudbydere indsende den seneste foreløbige rapport og underrette den kompetente myndighed om dette. Betalingstjenesteudbydere bør betragte driften som normal igen, når aktiviteten/operationerne er bragt tilbage på det niveau af service/betingelser, som er fastlagt af betalingstjenesteudbyderen eller fastlagt eksternt gennem en serviceniveauaftale (Service Level Agreement - SLA) om behandlingstider, kapacitet, sikkerhedskrav mv., og der ikke længere er beredskabsforanstaltninger i kraft.

2.16. Såfremt driften igen er normal inden 4 timer efter konstatering af hændelsen, bør betalingstjenesteudbyderen bestræbe sig på at indsende både den indledende og den seneste foreløbige rapport samtidig (dvs. med udfyldelse af skabelonens afsnit A og B) inden for 4-timers fristen.

### Endelig rapport

2.17. Betalingstjenesteudbydere bør indsende en endelig rapport, når den tilgrundliggende årsag er analyseret (uanset om der allerede er truffet afbødende foranstaltninger, eller om den endelige tilgrundliggende årsag er påvist) og der foreligger faktiske tal i stedet for skøn.

2.18. Betalingstjenesteudbydere bør indsende den endelige rapport til den kompetente myndighed højst 2 uger efter, at driften anses for igen at være normal. Betalingstjenesteudbydere, der behøver forlængelse af denne frist (f.eks. hvis der endnu ikke foreligger faktiske tal om indvirkningen), bør inden fristens udløb kontakte den kompetente myndighed og give en fyldestgørende begrundelse for forsinkelsen og en ny forventet dato for den endelige rapport.

2.19. Hvis betalingstjenesteudbyderen kan levere alle de oplysninger, der kræves i den endelige rapport (dvs. skabelonens afsnit C) inden for 4-timers tidsrummet efter konstatering af

hændelsen, bør den bestræbe sig på i den indledende rapport at indsende oplysninger svarende til den indledende, den seneste foreløbige og den endelige rapport.

2.20. Betalingstjenesteudbydere bør bestræbe sig på i deres endelige rapport at medtage fuldstændige oplysninger, dvs. (i) faktiske tal om indvirkningen i stedet for skøn (samt enhver anden ajourføring, der er nødvendig i afsnit A og B i skabelonen), og (ii) skabelonens afsnit C, som omfatter den tilgrundliggende årsag, hvis denne allerede kendes, og en sammenfatning af de foranstaltninger, der er vedtaget eller planlægges vedtaget for at eliminere problemet og forhindre, at det gentager sig i fremtiden.

2.21. Betalingstjenesteudbydere bør desuden indsende en endelig rapport, når 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 opklaret. I så fald bør betalingstjenesteudbydere indsende den endelige rapport, så snart denne omstændighed konstateres, og under alle omstændigheder senest på den forventede dato for næste rapport. I denne særlige situation bør betalingstjenesteudbyderen i stedet for at udfylde afsnit C i skabelonen afkrydse feltet "hændelse omklassificeret til ikke-større" og redegøre for årsagerne til denne nedgradering.

## Retningslinje 3: Delegeret og konsolideret indberetning

3.1. Hvis den kompetente myndighed tillader det, bør betalingstjenesteudbydere, der ønsker at uddelegere 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 i givet fald en koncerns eksisterende interne ordninger, der er grundlag for delegeret indberetning mellem betalingstjenesteudbyderen og tredjeparten, fastlægger entydigt ansvarsfordelingen mellem alle parter. Det fremgår navnlig klart af kontrakten, at den berørte betalingstjenesteudbyder – uafhængigt af den eventuelle uddelegering 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. Uddelegeringen 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 (EMD), eller

   ii. CEBS' retningslinjer for outsourcing i relation til kreditinstitutter.

c. Oplysningerne forelægges på forhånd for den kompetente myndighed i hjemlandet og under alle omstændigheder i henhold til 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 sikret.

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

a. Medtag denne bestemmelse i kontrakten, der er grundlag for uddelegeret indberetning.

b. Gør den konsoliderede underretning betinget af, at hændelsen skyldes en afbrydelse af de ydelser, der leveres af tredjeparten.

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

d. Sørg for, at tredjeparten vurderer hændelsens betydning for hver berørt betalingstjenesteudbyder, og at tredjeparten i den konsoliderede indberetning kun medtager de betalingstjenesteudbydere, for hvem hændelsen klassificeres som større. Sørg desuden for, at betalingstjenesteudbyderen i tvivlstilfælde medtages i den konsoliderede indberetning, så længe der ikke er bevis for, at betalingstjenesteudbyderen ikke bør medtages.

e. Sørg for, når der er felter i skabelonen, hvor det ikke er muligt at give et fælles svar (f.eks. afsnit B 2, B 4 eller C 3), at tredjeparten enten (i) udfylder dem for hver enkelt berørt betalingstjenesteudbyder og specificerer identiteten af hver betalingstjenesteudbyder, der omfattes af oplysningerne, eller (ii) i de felter, hvor det er muligt, angiver intervaller svarende til de laveste og højeste værdier, der er iagttaget eller skønnet for de forskellige betalingstjenesteudbydere.

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

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

3.4. Betalingstjenesteudbydere, der ønsker at trække uddelegeringen af deres indberetningsforpligtelser tilbage, bør underrette den kompetente myndighed i hjemlandet om denne beslutning i overensstemmelse med 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 opfylde deres indberetningsforpligtelser uden brug af ekstern bistand, når 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 desuden sikre, at en hændelse ikke indberettes to gange, dels af den nævnte betalingstjenesteudbyder, dels igen af tredjeparten.

## 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 implementeres for at opfylde kravene i nærværende retningslinjer.

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

## Retningslinje 5: Vurdering af hændelsens relevans

5.1. De kompetente myndigheder i hjemlandet bør vurdere en større drifts- eller sikkerhedshændelses relevans for andre indenlandske myndigheder på grundlag af deres egen ekspertudtalelse og med følgende kriterier som primære indikatorer for hændelsens vigtighed:

a. Årsagerne til hændelsen hører under den anden nationale regulerende myndigheds kompetenceområde.
b. Hændelsens konsekvenser har indvirkning på en anden indenlandsk myndigheds målsætninger (f.eks. varetagelse af finansiel stabilitet).
c. Hændelsen berører i vid udstrækning betalingstjenestebrugerne eller kan tænkes at gøre det.
d. Hændelsen må forventes at få bred mediedækning eller har fået det.

5.2. De kompetente myndigheder i hjemlandet bør foretage denne vurdering løbende i hændelsens levetid, så de kan identificere enhver mulig ændring, der kan gøre en hændelse relevant, selv om den ikke tidligere er blevet anset for at være det.

## Retningslinje 6: Oplysninger, der skal deles

6.1. Uanset eventuelle andre lovbestemte krav om at dele hændelsesrelaterede oplysninger med andre indenlandske myndigheder bør de kompetente myndigheder give oplysninger om væsentlige drifts- eller sikkerhedshændelser til de indenlandske myndigheder, som er identificeret efter retningslinje 5.1 (dvs. "andre relevante nationale myndigheder") i det mindste på tidspunktet for modtagelse af den indledende rapport (eller alternativt den rapport, der førte til udveksling af oplysninger) og når de underrettes om, at driften igen er normal (dvs. seneste foreløbige rapport).

6.2. De kompetente myndigheder bør forelægge andre relevante nationale myndigheder de oplysninger, der er nødvendige for at give et klart billede af, hvad der er sket, og de mulige konsekvenser heraf. Dertil bør de som minimum give de oplysninger, der er anført af

betalingstjenesteudbyderen i følgende af skabelonens felter (enten i den indledende eller foreløbige rapport):

- dato og klokkeslæt for konstatering af hændelsen
- dato og klokkeslæt for hændelsens indtræden
- dato og klokkeslæt, hvor hændelsen blev afhjulpet eller forventes afhjulpet
- en kort beskrivelse af hændelsen (herunder ikkefølsomme dele af den detaljerede beskrivelse)
- en kort beskrivelse af trufne eller planlagte foranstaltninger til afhjælpning af hændelsen
- en beskrivelse af, hvordan hændelsen kan tænkes at berøre andre betalingstjenesteudbydere og/eller infrastrukturer
- en beskrivelse af eventuel mediedækning
- årsagen til hændelsen.

6.3. De kompetente myndigheder bør sikre tilbørlig anonymisering i det omfang, det er nødvendigt, og udelade oplysninger, der kan tænkes at være omfattet af begrænsninger vedrørende fortrolighed eller intellektuel ejendomsret, før de deler hændelsesrelaterede oplysninger med andre relevante nationale myndigheder. De kompetente myndigheder bør dog oplyse den indberettende betalingstjenesteudbyders navn og adresse til andre relevante nationale myndigheder, forudsat at disse kan garantere, at oplysningerne behandles fortroligt.

6.4. De kompetente myndigheder bør til stadighed opretholde fortroligheden og integriteten af de oplysninger, de opbevarer og udveksler med andre relevante nationale myndigheder, og også autentificere sig tilbørligt over for andre relevante nationale myndigheder. Navnlig bør de kompetente myndigheder behandle alle oplysninger, de modtager i henhold til disse retningslinjer, i overensstemmelse med tavshedspligten fastlagt i PSD2, med forbehold af gældende EU-lovgivning og nationale krav.

# 6. Retningslinjer for kompetente myndigheder om kriterierne for vurderingen af de relevante oplysninger i hændelsesrapporterne, der skal deles med EBA og ECB, og om formatet af deres kommunikation og procedurerne herfor.

## Retningslinje 7: Oplysninger, der skal deles

7.1. De kompetente myndigheder bør altid til EBA og ECB fremsende alle rapporter, der er modtaget fra (eller på vegne af) betalingstjenesteudbydere, som berøres af en større drifts- eller sikkerhedshændelse (dvs. indledende, foreløbige og endelige rapporter).

## Retningslinje 8: Kommunikation

8.1. De kompetente myndigheder bør til stadighed opretholde fortroligheden og integriteten af de oplysninger, de opbevarer og udveksler med EBA og ECB, og bør desuden autentificere sig tilbørligt over for EBA og ECB. Navnlig bør de kompetente myndigheder behandle alle oplysninger, de modtager i henhold til disse retningslinjer, i overensstemmelse med tavshedspligten fastlagt 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 minimere risikoen for driftsforstyrrelser bør de kompetente myndigheder være i besiddelse af passende kommunikationsmidler.

# Bilag 1 - Indberetningsskabeloner til betalingstjenesteudbydere

CLASSIFICATION: RESTRICTED

## Major Incident Report

| | |
|---|---|
| ☐ Initial report | within 4 hours after detection |
| ☐ Intermediate report | maximum of 3 business days from previous report |
| ☐ Last intermediate report | |
| ☐ Final report | within 2 weeks after closing the incident |
| ☐ Incident reclassified as non-major — Please explain: | |

| | | | |
|---|---|---|---|
| Report date | DD/MM/YYYY | Time | HH:MM |
| Incident identification number, if applicable (for interim and final reports) | | | |

### A - Initial report

| A 1 - GENERAL DETAILS | | | | | |
|---|---|---|---|---|---|
| **Type of report** | | | | | |
| Type of report | ☐ Individual | ☐ Consolidated | | | |
| **Affected payment service provider (PSP)** | | | | | |
| PSP name | | | | | |
| PSP unique identification number, if relevant | | | | | |
| PSP authorisation number | | | | | |
| Head of group, if applicable | | | | | |
| Home country | | | | | |
| Country/countries affected by the incident | | | | | |
| Primary contact person | | Email | | Telephone | |
| Secondary contact person | | Email | | Telephone | |
| **Reporting entity (complete this section if the reporting entity is not the affected PSP in case of delegated reporting)** | | | | | |
| Name of the reporting entity | | | | | |
| Unique identification number, if relevant | | | | | |
| Authorisation number, if applicable | | | | | |
| Primary contact person | | Email | | Telephone | |
| Secondary contact person | | Email | | Telephone | |

| A 2 - INCIDENT DETECTION and INITIAL CLASSIFICATION | | | |
|---|---|---|---|
| Date and time of detection of the incident | DD/MM/YYYY, HH:MM | | |
| The incident was detected by (1) | | If Other, please explain: | |
| Please provide a short and general description of the incident (should you deem the incident to have an impact in other EU Member States(s), and if feasible within the applicable reporting deadlines, please provide a translation in English) | | | |
| What is the estimated time for the next update? | DD/MM/YYYY, HH:MM | | |

## B - Intermediate report

### B 1 - GENERAL DETAILS

| | |
|---|---|
| Please provide a more DETAILED description of the incident. e.g. information on:<br>- What is the specific issue?<br>- How it happened<br>- How did it develop<br>- Was it related to a previous incident?<br>- Consequences (in particular for payment service users)<br>- Background of the incident detection<br>- Areas affected<br>- Actions taken so far<br>- Service providers/ third party affected or involved<br>- Crisis management started (internal and/or external (Central Bank Crisis management))<br>- PSP internal classification of the incident | |
| Date and time of beginning of the incident (if already identified) | DD/MM/YYYY, HH:MM |
| Incident status | ☐ Diagnostics ☐ Recovery<br>☐ Repair ☐ Restoration |
| Date and time when the incident was restored or is expected to be restored | DD/MM/YYYY, HH:MM |

### B 2 - INCIDENT CLASSIFICATION & INFORMATION ON THE INCIDENT

| | |
|---|---|
| Overall impact | ☐ Integrity ☐ Confidentiality ☐ Continuity<br>☐ Availability ☐ Authenticity |
| Transactions affected [2] | Number of transactions affected — ☐ Actual figure ☐ Estimation<br>As a % of regular number of transactions — ☐ Actual figure ☐ Estimation<br>Value of transactions affected in EUR — ☐ Actual figure ☐ Estimation<br>Comments: |
| Payment service users affected [3] | Number of payment service users affected — ☐ Actual figure ☐ Estimation<br>As a %-of total payment service users — ☐ Actual figure ☐ Estimation |
| Service downtime[4] | Total service downtime: DD:HH:MM — ☐ Actual figure ☐ Estimation |
| Economic impact [5] | Direct costs in EUR — ☐ Actual figure ☐ Estimation<br>Indirect costs in EUR — ☐ Actual figure ☐ Estimation |
| High level of internal escalation | ☐ YES ☐ YES, AND CRISIS MODE (OR EQUIVALENT) IS LIKELY TO BE CALLED UPON ☐ NO<br>Describe the level of internal escalation of the incident, indicating if it has triggered or is likely to trigger a crisis mode (or equivalent) and if so, please describe |
| Other PSPs or relevant infrastructures potentially affected | ☐ YES ☐ NO<br>Describe how this incident could affect other PSPs and/or infrastructures |
| Reputational impact | ☐ YES ☐ NO<br>Describe how the incident could affect the reputation of the PSP (e.g. media coverage, potential legal or regulatory infringement, etc.) |

### B 3 - INCIDENT DESCRIPTION

| | |
|---|---|
| Type of Incident | ☐ Operational ☐ Security |
| Cause of incident | ☐ Under investigation<br>☐ External attack<br>☐ Internal attack<br>Type of attack:<br>☐ Distributed/Denial of Service (D/DoS)<br>☐ Infection of internal systems<br>☐ Targeted intrusion<br>☐ Other<br>If Other, specify<br>☐ External events<br>☐ Human error<br>☐ Process failure<br>☐ System failure<br>☐ Other<br>If Other, specify |
| Was the incident affecting you directly, or indirectly through a service provider? | ☐ Directly ☐ Indirectly<br>If indirectly, please provide the service provider's name |

### B 4 - INCIDENT IMPACT

| | |
|---|---|
| Building(s) affected (Address), if applicable | |
| Commercial channels affected | ☐ Branches ☐ Telephone banking ☐ Point of sale<br>☐ E-banking ☐ Mobile banking ☐ Other<br>☐ ATMs<br>If Other, specify: |
| Payment services affected | ☐ Cash placement on a payment account ☐ Credit transfers ☐ Money remittance<br>☐ Cash withdrawal from a payment account ☐ Direct debits ☐ Payment initiation services<br>☐ Operations required for operating a payment account ☐ Card payments ☐ Account information services<br>☐ Acquiring of payment instruments ☐ Issuing of payment instruments ☐ Other<br>If Other, specify: |
| Functional areas affected | ☐ Authentication/authorisation ☐ Clearing ☐ Indirect settlement<br>☐ Communication ☐ Direct settlement ☐ Other<br>If Other, specify: |
| Systems and components affected | ☐ Application/software ☐ Hardware<br>☐ Database ☐ Network/infrastructure<br>☐ Other<br>If Other, specify: |
| Staff affected | ☐ YES ☐ NO<br>Describe how the incident could affect the staff of the PSP/service provider (e.g. staff not being able to reach the office to support customers, etc.) |

### B 5 - INCIDENT MITIGATION

| | |
|---|---|
| Which actions/measures have been taken so far or are planned to recover from the incident? | |
| Has the Business Continuity Plan and/or Disaster Recovery Plan been activated?<br>If so, when?<br>If so, please describe | ☐ YES ☐ NO<br>DD/MM/YYYY, HH:MM |
| Has the PSP cancelled or weakened some controls because of the incident?<br>If so, please explain | ☐ YES ☐ NO |

| C - Final report | |
|---|---|
| *If no intermediate report has been sent, please also complete section B* | |
| **C 1 - GENERAL DETAILS** | |
| Please update the information from the intermediate report (summary):<br>- additional actions/measures taken to recover from the incident<br>- final remediation actions taken<br>- root cause analysis<br>- lessons learnt<br>- addittional actions<br>- any other relevant information | |
| Date and time of closing the incident | DD/MM/YYYY, HH:MM |
| If the PSP had to cancel or weaken some controls because of the incident, are the original controls back in place? | ☐ YES ☐ NO |
| If so, please explain | |
| **C 2 - ROOT CAUSE ANALYSIS AND FOLLOW-UP** | |
| What was the root cause (if already known)?<br>(possible to attach a file with detailed information) | |
| Main corrective actions/measures taken or planned to prevent the incident from happening again in the future, if already known | |
| **C 3 - ADDITIONAL INFORMATION** | |
| Has the incident been shared with other PSPs for information purposes? | ☐ YES ☐ NO |
| If so, please provide details | |
| Has any legal action been taken against the PSP? | ☐ YES ☐ NO |
| If so, please provide details | |

Notes:

(1) Pull-down menu: payment service user; internal organisation; external organisation; none of the above

(2) Pull-down menu: > 10% of regular level of transactions and > EUR 100,000; > 25% of regular level of transactions or > EUR 5 milion; none of the above

(3) Pull-down menu: > 5,000 and > 10% payment service users; > 50,000 or > 25% payment service users; none of the above

(4) Pull-down menu: > 2 hours; < 2 hours

(5) Pull-down menu: > Max (0,1% Tier 1 capital, EUR 200,000) or > EUR 5 million; none of the above

| CONSOLIDATED REPORT - LIST OF PSPs | | |
|---|---|---|
| **PSP Name** | **PSP Unique Identification Number** | **PSP Authorisation number** |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

## ANVISNINGER I, HVORDAN SKABELONERNE UDFYLDES

Betalingstjenesteudbydere bør udfylde det relevante afsnit af skabelonen afhængigt af den indberetningsfase, de er i: afsnit A for den indledende rapport, afsnit B for foreløbige rapporter, og afsnit C for den endelige rapport. Alle felter skal udfyldes, medmindre andet tydeligt er angivet.

### Overskrift

**Indledende rapport:** Denne indberetning er den første, som betalingstjenesteudbyderen indsender til den kompetente myndighed i hjemlandet.
**Foreløbig rapport:** Denne rapport er en ajourføring af en tidligere (indledende eller foreløbig) rapport om samme hændelse.
**Sidste foreløbige rapport:** Denne rapport underretter den kompetente myndighed i hjemlandet om, at de normale aktiviteter er genoptaget, og at driften igen er normal, så der ikke vil blive indsendt flere foreløbige rapporter.
**Endelig rapport:** Denne rapport er den sidste, som betalingstjenesteudbyderen sender om hændelsen, eftersom (i) der allerede er udført en analyse af tilgrundliggende årsager, og de skønnede tal kan erstattes med faktiske tal, eller (ii) hændelsen ikke længere betragtes som større.
**Hændelsen 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 angive begrundelsen for denne nedgradering.
**Rapportens dato og klokkeslæt:** Den nøjagtige dato og det nøjagtige klokkeslæt for indsendelse af rapporten til den kompetente myndighed.
**Eventuelt identifikationsnummer på hændelsen (for den foreløbige og endelige rapport):** Eventuelt referencenummer, som på tidspunktet for den indledende indberetning er udstedt af den kompetente myndighed for entydigt at identificere hændelsen (hvis et sådant referencenummer er udstedt af den kompetente myndighed).

## A – Indledende rapport

### A 1 – Generelle oplysninger

**Rapportens art:**

**Enkeltstående rapport:** Rapporten omfatter en enkelt betalingstjenesteudbyder.
**Konsolideret rapport:** Rapporten omfatter flere betalingstjenesteudbydere, som gør brug af muligheden for konsolideret indberetning. Felterne under "berørt betalingstjenesteudbyder" bør være tomme (med undtagelse af feltet "land(e), der berøres af hændelsen"), og der bør gives en liste over de betalingstjenesteudbydere, som rapporten omfatter, ved udfyldelse af den tilsvarende tabel "konsolideret rapport – liste over berørte betalingstjenesteudbydere".

**Berørt betalingstjenesteudbyder:** Henviser til den betalingstjenesteudbyder, som er udsat for hændelsen.

**Betalingstjenesteudbyderens navn:** Det fulde navn på den betalingstjenesteudbyder, som indberetningen vedrører, således som det fremgår af det pågældende officielle nationale register over betalingstjenesteudbydere.
**Betalingstjenesteudbyderens entydige identifikationsnummer, hvis relevant:** Hvis feltet "betalingstjenesteudbyderens autorisationsnummer" ikke er udfyldt, bør betalingstjenesteudbyderen angive det unikke identifikationsnummer, der anvendes i hver medlemsstat til identifikation af betalingstjenesteudbyderen.
**Betalingstjenesteudbyderens autorisationsnummer:** Hjemlandets autorisationsnummer.

**Leder af koncernen:** Angiv navnet på den ledende virksomhed i en eventuel koncern af virksomheder som defineret i artikel 4, stk. 40, 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) 1093/2010 og om ophævelse af direktiv 2007/64/EF.

**Hjemland:** Medlemsstat, hvor betalingstjenesteudbyderens hjemsted er beliggende, eller, hvis betalingstjenesteudbyderen ifølge sin nationale lovgivning ikke har noget vedtægtsmæssigt hjemsted, den medlemsstat, hvor hovedkontoret er beliggende.

**Land(e), der berøres af hændelsen:** Land(e), hvor virkningen af hændelsen har vist sig (som f.eks., hvis hændelsen berører flere af betalingstjenesteudbyderens afdelinger, der er beliggende i forskellige lande). Dette kan være samme land som hjemlandet, men behøver ikke være det.

**Primære kontaktperson:** For- og efternavn på den person, der er ansvarlig for indberetningen af hændelsen, eller, hvis en tredjepart indberetter på vegne af den berørte betalingstjenesteudbyder, for- og efternavn på den ansvarlige for forvaltning af hændelser/risikoafdelingen eller tilsvarende hos den berørte betalingstjenesteudbyder.

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

**Telefon:** Telefonnummer til brug ved eventuelle anmodninger om yderligere præciseringer. 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, når den primære kontaktperson ikke træffes. Hvis en tredjepart indberetter på vegne af den berørte betalingstjenesteudbyder, anføres for- og efternavn på en anden person i afdelingen med administrativt ansvar for hændelser/risikoafdelingen eller tilsvarende hos den berørte betalingstjenesteudbyder.

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

**Telefon:** Telefonnummeret på den anden kontaktperson, som kan besvare eventuelle anmodninger om yderligere præciseringer. Dette kan være en persons eller en virksomheds telefonnummer.

**Indberettende virksomhed:** Dette afsnit bør udfyldes, hvis en tredjepart opfylder indberetningsforpligtelserne på vegne af den berørte betalingstjenesteudbyder.

**Navnet på den indberettende virksomhed:** Det fulde navn på den virksomhed, der indberetter hændelsen, således som dette fremgår af det pågældende officielle nationale selskabsregister.

**Betalingstjenesteudbyderens entydige identifikationsnummer, hvis det er relevant:** Det pågældende unikke identifikationsnummer, der i tredjepartens hjemland anvendes til identifikation af den virksomhed, som indberetter hændelsen. Skal angives af den indberettende virksomhed, hvis feltet "autorisationsnummer" ikke er udfyldt.

**Eventuelt autorisationsnummer:** Tredjepartens eventuelle autorisationsnummer i det land, hvor den er hjemmehørende.

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

**E-mail:** Den e-mailadresse, hvortil eventuelle anmodninger om yderligere præciseringer kan rettes. Dette kan være en personlig e-mail eller virksomhedens e-mail.

**Telefon:** Telefonnummer til brug ved eventuelle anmodninger om yderligere præciseringer. Dette kan være en persons eller en virksomheds telefonnummer.

**Sekundær kontaktperson:** For- og efternavn på en anden person i den virksomhed, der indberetter hændelsen, og som kan kontaktes af den kompetente myndighed, når den primære kontaktperson ikke kan træffes.
**E-mail:** E-mailadresse på den anden kontaktperson, som eventuelle anmodninger om yderligere præciseringer kan rettes til. Dette kan være en personlig e-mailadresse eller virksomhedens e-mailadresse.
**Telefon:** Telefonnummer på den anden kontaktperson, som kan besvare eventuelle anmodninger om yderligere præciseringer. Dette kan være en persons eller en virksomheds telefonnummer.

### A 2 – Konstatering og indledende klassificering af hændelsen

**Dato og klokkeslæt for konstatering af hændelsen:** Dato og klokkeslæt, hvor hændelsen første gang blev identificeret.
**Hændelsen konstateret af:** Angiv, om hændelsen blev registreret af en betalingstjenestebruger, en anden instans hos betalingstjenesteudbyderen (f.eks. den interne revisionsfunktion) eller en ekstern part (f.eks. en ekstern tjenesteudbyder). Hvis det ikke var nogen af disse, gives en redegørelse i det tilhørende felt.
**Kortfattet, generel beskrivelse af hændelsen:** Redegør kort for de mest relevante problemer ved hændelsen, herunder dens mulige årsager, umiddelbare konsekvenser osv.
**Hvad er det skønnede tidspunkt for næste ajourføring?** Angiv forventet dato og klokkeslæt for indsendelse af næste ajourføring (foreløbig eller endelig rapport).

## B – Foreløbig rapport

### B 1 – Generelle oplysninger

**Mere detaljeret beskrivelse af hændelsen:** Beskriv hændelsens hovedindhold i det mindste svarende til punkterne i spørgeskemaet (hvilket konkret problem står betalingstjenesteudbyderen over for, hvordan begyndte hændelsen, hvordan udviklede den sig, dens eventuelle sammenhæng med en tidligere hændelse, og dens konsekvenser, navnlig for betalingstjenestebrugere, osv.).
**Dato og klokkeslæt for hændelsens begyndelse:** Dato og klokkeslæt, hvor hændelsen begyndte, hvis det kendes.
**Hændelsens status:**

**Fejlfinding:** Hændelsens kendetegn er netop blevet fastlagt.
**Udbedring:** De angrebne punkter er under rekonfigurering.
**Genopretning:** De fejlbehæftede punkter er under genopretning til deres seneste genoprettelige tilstand.
**Retablering:** Den betalingsrelaterede tjeneste leveres igen.

**Dato og klokkeslæt, hvor hændelsen blev genoprettet eller forventes genoprettet:** Angiv dato og klokkeslæt, hvor hændelsen kom under kontrol eller forventedes at være det, og driften vendte tilbage til det normale eller forventes at gøre det.

### B 2 – Klassificering af hændelsen/oplysninger om hændelsen

**Samlet indvirkning:** Angiv, hvilke egenskaber der er blevet påvirket af hændelsen. Der kan afkrydses flere felter.

**Integritet:** Den egenskab, at korrektheden og fuldstændigheden af aktiver (herunder data) opretholdes.
**Tilgængelighed:** Den egenskab ved betalingsrelaterede tjenester, at de er tilgængelige og anvendelige for betalingstjenestebrugere.

**Fortrolighed:** Den egenskab, at oplysninger ikke gøres tilgængelige eller afsløres over for uautoriserede personer, virksomheder eller processer.

**Ægthed:** Den egenskab ved en kilde, at den er, hvad den hævder at være.

**Kontinuitet:** Den egenskab ved en organisations processer, opgaver og aktiver, som er nødvendige for, at de betalingsrelaterede tjenester, den leverer, er fuldt tilgængelige og fungerer på acceptable prædefinerede niveauer.

**Berørte transaktioner:** Betalingstjenesteudbydere bør angive, hvilke tærskler der er nået eller forventes nået af hændelsen, og de tilhørende tal: antal berørte transaktioner, procentdel berørte transaktioner i forhold til det antal betalingstransaktioner, der udføres med de betalingstjenester, som er blevet berørt af hændelsen, og transaktionernes samlede værdi. Betalingstjenesteudbydere bør angive konkrete værdier for disse variabler, som enten kan være faktiske tal eller skøn. Virksomheder, der indberetter på vegne af flere betalingstjenesteudbydere (dvs. konsolideret indberetning) kan i stedet angive værdier for de laveste og højeste iagttagne eller skønnede værdier inden for den koncern af betalingstjenesteudbydere, som rapporten omfatter, adskilt af en bindestreg. Som hovedregel bør betalingstjenesteudbydere som "berørte transaktioner" betragte alle indenlandske og grænseoverskridende transaktioner, der direkte eller indirekte er blevet berørt af hændelsen eller må forventes at blive det, navnlig de transaktioner, der ikke har kunnet indledes eller behandles, dem, for hvilke betalingsmeddelelsens indhold er ændret, og dem, der er bestilt i svigagtigt øjemed (uanset om midlerne er betalt tilbage 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 betalingstjenesteudbyderen ikke dette tal for at være repræsentativt (f.eks. på grund af sæsonbetingede svingninger), bør han i stedet anvende en anden, mere repræsentativ, målemetode og over for den kompetente myndighed angive rationalet for denne tilgang i feltet "Kommentarer".

**Betalingstjenestebrugere, der berøres:** Betalingstjenesteudbydere bør angive, hvilke eventuelle tærskler der er nået eller forventes nået af hændelsen, og de tilhørende tal: det samlede antal betalingstjenestebrugere, der er blevet berørt, og procentdelen af berørte betalingstjenestebrugere i forhold til det samlede antal betalingstjenestebrugere. Betalingstjenesteudbydere bør angive konkrete værdier for disse variable, enten som faktiske tal eller skøn. Virksomheder, der indberetter på vegne af flere betalingstjenesteudbydere (dvs. konsolideret indberetning) kan i stedet angive værdier for de laveste og højeste iagttagne eller skønnede værdier inden for den koncern af betalingstjenesteudbydere, som rapporten omfatter, adskilt af en bindestreg. Betalingstjenesteudbydere bør ved "berørte betalingstjenestebrugere" forstå alle kunder (indenlandske eller udenlandske, forbrugere eller virksomheder), der har en kontrakt med den berørte betalingstjenesteudbyder og derved har adgang til den berørte betalingstjeneste, og som er blevet udsat for følgerne af hændelsen eller må formodes at blive det. Betalingstjenesteudbydere bør forlade sig på skøn baseret på tidligere aktivitet til at bestemme det antal betalingstjenestebrugere, der kan have brugt betalingstjenesten i løbet af hændelsens levetid. For koncerner bør hver betalingstjenesteudbyder kun medregne sine egne betalingstjenestebrugere. Hvis en betalingstjenesteudbyder tilbyder driftstjenester til andre, bør denne betalingstjenesteudbyder kun medregne sine eventuelle egne betalingstjenestebrugere, og ligeledes bør betalingstjenesteudbydere, der modtager disse driftstjenester, 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 uanset om de anses for aktive eller passive betalingstjenestebrugere.

**Tjenestens nedetid:** Betalingstjenesteudbydere bør angive, om tærskelværdien er nået eller må forventes nået af hændelsen, og det tilhørende tal: den totale nedetid for tjenesten. Betalingstjenesteudbydere bør for denne variabel angive konkrete værdier, som enten kan være faktiske tal eller skøn. Virksomheder, der indberetter på vegne af flere betalingstjenesteudbydere (dvs. konsolideret indberetning) kan i stedet angive et interval svarende til de laveste og højeste værdier, der er iagttaget eller skønnes for den koncern af betalingstjenesteudbydere, som indberetningen omfatter, adskilt af en bindestreg. Betalingstjenesteudbydere bør medregne det tidsrum, hvori en opgave, proces eller kanal, der er knyttet til leveringen af betalingstjenester, er eller må formodes at være nede og derved forhindrer (i) igangsættelse 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 hensyn til både de perioder, hvor de skal have åbent med henblik på udførelse af betalingstjenester, og de perioder, hvor de har lukket, og vedligeholdelsesperioder, når det er relevant og gennemførligt. Hvis betalingstjenesteudbydere ikke kan fastslå, hvornår nedetiden for tjenesten begyndte, bør de undtagelsesvis beregne tjenestens nedetid fra det øjeblik, hvor nedetiden registreres.

**Økonomisk indvirkning:** Betalingstjenesteudbydere bør angive, om tærskelværdien er nået eller må forventes nået af hændelsen, og det tilhørende tal: direkte omkostninger og indirekte omkostninger. Betalingstjenesteudbydere bør angive konkrete værdier for disse variable, enten som faktiske tal eller skøn. Virksomheder, der indberetter på vegne af flere betalingstjenesteudbydere (dvs. konsolideret indberetning) kan i stedet angive et interval svarende til de laveste og højeste værdier, der er iagttaget eller skønnes for den koncern af betalingstjenesteudbydere, som indberetningen omfatter, adskilt af en bindestreg. Betalingstjenesteudbydere bør medregne både de omkostninger, der direkte kan forbindes med hændelsen, og dem, der er indirekte er relateret til hændelsen. Betalingstjenesteudbydere bør blandt andet medregne eksproprierede midler eller aktiver, omkostninger til udskiftning af hardware eller software, øvrige retlige eller afhjælpende omkostninger, gebyrer som følge af manglende overholdelse af kontraktlige forpligtelser, sanktioner, eksterne forpligtelser og tabte indtægter. Af indirekte omkostninger bør udbydere af betalingstjenester kun tage hensyn til dem, der allerede kendes eller højst sandsynligt vil påløbe.

> **Direkte omkostninger:** Omkostninger (i euro), der direkte skyldes hændelsen, herunder beløb 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. reklamationer fra kunder/erstatning til kunder, indtægtstab som følge af mistede forretningsmuligheder, potentielle sagsomkostninger).

**Højt niveau af intern udbredelse:** Betalingstjenesteudbydere bør overveje, om den informationsansvarlige (eller tilsvarende) som følge af hændelsens konsekvenser for betalingsrelaterede tjenester allerede er eller forventes at blive informeret om hændelsen uden for en eventuel regelmæssig underretningsprocedure og løbende i hele hændelsens levetid. I tilfælde af delegeret indberetning finder udbredelsen sted hos tredjeparten. Betalingstjenesteudbydere bør desuden tage hensyn til, om der er udløst en krisesituation, eller om dette må forventes, som følge af hændelsens indvirkning på betalingsrelaterede tjenester.

**Andre betalingstjenesteudbydere eller relevante infrastrukturer, der potentielt berøres:** Betalingstjenesteudbydere bør vurdere hændelsens indvirkning på det finansielle marked, forstået som det finansielle markeds infrastrukturer og/eller kortbetalingsordninger, der er grundlag for markedet og de øvrige betalingstjenesteudbydere. Betalingstjenesteudbydere bør navnlig vurdere, hvorvidt hændelsen har gentaget sig hos andre betalingstjenesteudbydere eller forventes at gøre det, om den har påvirket den gnidningsfrie funktion af det finansielle markeds infrastrukturer eller forventes at gøre det, og om den har berørt soliditeten af det finansielle system som helhed eller forventes at gøre det. 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 internt eller eksternt, og om betalingstjenesteudbyderen er ophørt med at opfylde sine forpligtelser i de finansielle markedsinfrastrukturer, han indgår i, eller om han må forventes at gøre det.

**Følger for omdømmet:** Betalingstjenesteudbydere bør tage det synlighedsniveau i betragtning, som hændelsen efter deres bedste overbevisning har fået eller må forventes at få på markedet. Navnlig bør betalingstjenesteudbydere overveje sandsynligheden for, at hændelsen vil være samfundsskadelig, som en indikator for dens potentiale til at påvirke deres omdømme. Betalingstjenesteudbydere bør tage i betragtning, (i) om hændelsen har påvirket en synlig proces og derfor må forventes at få mediedækning eller allerede har fået det (herunder ikke kun traditionelle medier som aviser, men også blogs, sociale netværk osv.), ii) om der er tilsidesat lovkrav eller der må forventes at blive det, iii) om der er overtrådt sanktioner eller der må forventes at blive det, eller (iv) om samme type hændelse er indtruffet tidligere.

### B 3 – Beskrivelse af hændelsen

**Hændelsens art:** Angiv, om der efter din bedste overbevisning er tale om en drifts- eller sikkerhedshændelse.

**Driftshændelse:** Hændelse, der skyldes ufyldestgørende processer eller fejl i processer, hos personer eller i systemer, eller tilfælde af force majeure, der berører betalingsrelaterede tjenesters integritet, tilgængelighed, fortrolighed, ægthed og/eller kontinuitet.

**Sikkerhedshændelse:** Uautoriseret adgang, anvendelse, offentliggørelse, afbrydelse, ændring eller ødelæggelse af betalingstjenesteudbyderens aktiver, som påvirker betalingsrelaterede tjenesters integritet, tilgængelighed, fortrolighed, ægthed og/eller kontinuitet. Dette kan ske, bl.a. når betalingstjenesteudbyderen kommer ud for cyberangreb, ufyldestgørende udformning eller implementering af sikkerhedspolitikker eller utilstrækkelig fysisk sikkerhed.

**Hændelsens årsag:** Angiv hændelsens årsag eller, hvis denne endnu ikke kendes, den mest sandsynlige årsag. Der kan afkrydses flere felter.

**Undersøgelse pågår:** Årsagen er endnu ikke fastlagt.

**Eksternt angreb:** Årsagen er ekstern og forsætligt rettet mod betalingstjenesteudbyderen (f.eks. malware-angreb).

**Internt angreb:** Årsagen er intern og forsætligt rettet mod betalingstjenesteudbyderen (f.eks. intern svig).

**Angrebets art:**

**Distributed/Denial of Service (D/DoS):** Forsøg på at gøre en onlinetjeneste utilgængelig ved at overbelaste den med trafik fra flere kilder.

**Infektion af interne systemer:** Skadelig aktivitet, der angriber computersystemer, forsøger at stjæle harddiskplads eller CPU-tid, få adgang til personlige oplysninger, korrumpere data, spam-kontakter osv.

**Målrettet indtrængen:** Uautoriseret spionage, snagen i og tyveri af oplysninger gennem cyberspace.

**Andet:** Enhver anden form for angreb, som betalingstjenesteudbyderen måtte være blevet udsat for, enten direkte eller gennem en tjenesteleverandør. Særligt hvis der har været rettet et angreb mod godkendelses- og autentifikationsprocessen, bør dette felt afkrydses. Detaljer tilføjes i fritekstfeltet.

**Eksterne hændelser:** Årsagen hænger sammen med begivenheder, der sædvanligvis er uden for organisationens kontrol (f.eks. naturkatastrofer, juridiske spørgsmål, forretningsproblemer og afhængighed af eksterne tjenester).

**Menneskelig fejl:** Hændelsen skyldtes en utilsigtet menneskelig fejl, hvad enten der var tale om en del af betalingsproceduren (f.eks. uploadning 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).

**Processvigt:** Årsagen til hændelsen var uhensigtsmæssig udformning eller udførelse af betalingsprocessen, proceskontrollerne og/eller de grundlæggende processer (for eksempel proces til ændring/migration, testning, konfigurering, kapacitet, overvågning).

**Systemsvigt:** Hændelsen hænger sammen med uhensigtsmæssig udformning, udførelse, komponenter, specifikationer, integration eller kompleksitet af de systemer, som betalingsaktiviteten er baseret på.

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

**Påvirkede hændelsen din virksomhed direkte eller indirekte via en tjenesteudbyder?** En hændelse kan ramme en betalingstjenesteudbyder direkte eller påvirke den indirekte gennem en tredjepart. For indirekte virkninger skal navnet på tjenesteudbyderen eller -udbyderne angives.

## B 4 – Hændelsens indvirkning

**Berørt(e) bygning(er) (adresse), hvis relevant:** Hvis en fysisk bygning er berørt, angives dens adresse.

**Berørte kommercielle relationer:** Angiv de(n) relation(er) med betalingstjenestebrugere, 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 regnes for én enkelt filial, når de er oprettet i samme medlemsstat af en betalingstjenesteudbyder med hovedsæde i en anden medlemsstat.

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

**Telefonbank:** Finansielle transaktioner, der gennemføres pr. telefon.

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

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

**Salgssted:** Fysiske lokaler tilhørende den forretningsvirksomhed, hvor betalingstransaktionen er initieret.

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

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

**Kontant indbetaling på en betalingskonto:** Indbetaling af et kontant beløb til en betalingstjenesteudbyder for at indsætte det på en betalingskonto.

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

**Operationer, der er nødvendige for at føre en betalingskonto:** Procedurer, der er nødvendige til at aktivere, deaktivere og/eller føre en betalingskonto (f.eks. åbning eller spærring).

**Erhvervelse af betalingsinstrumenter:** En betalingstjeneste bestående i, at en betalingstjenesteudbyder indgår aftale med en betalingsmodtager om at tage imod og behandle betalingstransaktioner, hvilket medfører overførsel af midler til betalingsmodtageren.

**Pengeoverførsler:** En betalingstjeneste, der på grundlag af en instruktion fra betaleren foretages af betalingstjenesteudbyderen og krediterer en betalingsmodtagers betalingskonto gennem en eller flere betalinger fra betalerens betalingskonto, som forvaltes af betalingstjenesteudbyderen.

**Direkte debiteringer:** En betalingstjeneste til debitering af betalerens betalingskonto, hvor betalingsmodtageren initierer en betalingstransaktion på grundlag af betalerens samtykke enten til betalingsmodtageren, til betalingsmodtagerens betalingstjenesteudbyder eller til betalerens egen betalingstjenesteudbyder.

**Kortbetalinger:** En betalingstjeneste, der er baseret på en betalingskortordnings infrastruktur og forretningsregler 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 bestående i, at en betalingstjenesteudbyder indgår aftale med en betaler om at udlevere et betalingsinstrument til at initiere og behandle betalerens betalingstransaktioner.

**Betalingsformidling:** En betalingstjeneste, med hvilken der modtages midler fra en betaler, uden at der oprettes betalingskonti i betalerens eller betalingsmodtagerens navn, og som alene tjener til at overføre et tilsvarende beløb til en betalingsmodtager eller en anden betalingstjenesteudbyder, der handler på dennes vegne, og/eller med hvilken sådanne midler modtages på betalingsmodtagerens vegne og stilles til rådighed for denne.

**Betalingsinitieringstjenester:** Betalingstjenester til initiering af en betalingsordre på anmodning af betalingstjenestebrugeren vedrørende en betalingskonto hos en anden betalingstjenesteudbyder.

**Kontooplysningstjenester:** Online-betalingstjenester til levering af konsoliderede oplysninger om en eller flere betalingskonti, som indehaves af betalingstjenestebrugeren hos én eller flere andre betalingstjenesteudbydere.

**Andet:** Den berørte betalingstjeneste er ikke en af ovennævnte. Yderligere oplysninger tilføjes i fritekstfeltet.

**Berørte funktionsområder:** Angiv det eller de trin i betalingsprocessen, der er blevet berørt af hændelsen. Der kan afkrydses flere felter.

**Autentifikation/godkendelse:** Procedurer, hvorved betalingstjenesteudbyderen kan verificere betalingstjenestebrugerens identitet eller gyldigheden af brugen af et specifikt betalingsinstrument, herunder brugerens personlige sikkerhedsoplysninger og samtykket fra betalingstjenestebrugeren (eller en tredjepart, der handler på dennes vegne) til at overføre midler eller værdipapirer.

**Kommunikation:** Informationsstrøm til identifikation, autentificering, oplysning og information mellem den kontoforvaltende betalingstjenesteudbyder og betalingsinitieringsudbydere, kontooplysningstjenesteudbydere, betalere, betalingsmodtagere og andre betalingstjenesteudbydere.

**Clearing:** Proces til overførsel, afstemning og undertiden bekræftelse af overførselsordrer forud for afviklingen, eventuelt også modregning af ordrer og endelig stillingtagen 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.

**Berørte systemer og komponenter:** Angiv, hvilke(n) del(e) af betalingstjenesteudbyderens teknologiske infrastruktur der er blevet berørt af hændelsen. Der kan afkrydses flere felter.

**Applikation/software:** Programmer, operativsystemer mv., der understøtter betalingstjenesteudbyderens levering af betalingstjenester.

**Database:** Datastruktur, der opbevarer personlige oplysninger og betalingsoplysninger, som er nødvendige for at udføre betalingstransaktioner.

**Hardware:** Fysisk teknologisk udstyr, der kører de processer og/eller lagrer de data, som betalingstjenesteudbydere har brug for til at udøve deres betalingsrelaterede aktivitet.

**Netværk/infrastruktur:** Telekommunikationsnetværk, enten offentlige eller private, der muliggør udveksling af data og oplysninger under betalingsprocessen (f.eks. internettet).

**Andet:** Systemet og komponenten, der berøres, er ingen af ovennævnte. Yderligere oplysninger tilføjes i fritekstfeltet.

**Berørt personale:** Angiv, hvorvidt hændelsen har eller ikke har berørt betalingstjenesteudbyderens personale, og anfør i bekræftende fald oplysninger i fritekstfeltet.

### B 5 – Afbødning af hændelsen

**Hvilke tiltag/foranstaltninger er der hidtil truffet eller planlægges truffet til at afbøde hændelsen?** Oplys om tiltag, der er truffet eller planlægges truffet til midlertidig afhjælpning af hændelsen.

**Er virksomhedens driftskontinuitetsplaner og/eller katastrofegenoprettelsesplaner bragt i anvendelse?** Oplys, om dette er tilfældet eller ej, og angiv i bekræftende fald de mest relevante oplysninger om, hvad der skete (dvs. hvornår planerne blev bragt i anvendelse, og hvad de bestod af).

**Har betalingstjenesteudbyderen annulleret eller svækket nogen kontroller på grund af hændelsen?** Angiv, om betalingstjenesteudbyderen har været nødsaget til at tilsidesætte nogen kontroller (f.eks. ophør med brugen af fire øjne-princippet) for at afbøde hændelsen, og giv i så fald oplysninger om, hvorfor disse kontroller er blevet annulleret eller svækket.

## C – Endelig rapport

### C 1 – Generelle oplysninger

**Ajourføring af oplysningerne fra den foreløbige rapport (sammendrag):** Giv yderligere oplysninger om de foranstaltninger, der er truffet til afhjælpning af hændelsen og undgåelse af, at den gentager sig, analyse af den grundlæggende årsag, lærte erfaringer osv.

**Dato og klokkeslæt for lukning af hændelsen:** Angiv dato og klokkeslæt for, hvornår hændelsen blev betragtet som lukket.

**Er de oprindelige kontroller genindført?** Hvis betalingstjenesteudbyderen var nødt til at annullere eller svække visse kontroller på grund af hændelsen, angives det, hvorvidt disse kontroller er genindført, og eventuelle yderligere oplysninger gives i fritekstfeltet.

### C 2 - Analyse af grundlæggende årsager, og opfølgning

**Hvad var den grundlæggende årsag, hvis den allerede kendes?** Forklar, hvad der er den grundlæggende årsag til hændelsen eller, hvis den grundlæggende årsag endnu ikke kendes, de foreløbige konklusioner fra analysen af den. Betalingstjenesteudbyderen kan vedhæfte en fil med detaljerede oplysninger, hvis det vurderes nødvendigt.

**De vigtigste korrigerende handlinger/foranstaltninger, der er truffet eller er planlagt til forebyggelse af, at hændelsen gentager sig, hvis de allerede kendes:** Beskriv de vigtigste tiltag, der er gjort eller planlagt for at forhindre, at hændelsen gentager sig.

### C 3 – Supplerende oplysninger

**Er hændelsen blevet delt med andre betalingstjenesteudbydere til orientering?** Giv en oversigt over, hvilke betalingstjenesteudbydere der er blevet kontaktet formelt eller uformelt for at underrette dem om hændelsen, oplys, hvilke oplysninger der er blevet delt, og hvad begrundelsen var for at dele disse oplysninger.

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