

Bekendtgørelse om indberetning af drifts- og sikkerhedshændelser ~~m.v.~~ for udbydere af betalingstjenester¹⁾

I medfør af § 127, stk. 4, og § 152, stk. 7, i lov om betalinger, jf. lovbekendtgørelse nr. 2710 af 7. december 2021, som ændret ved lov nr. ...[...], fastsættes:~~I medfør af § 127, stk. 4, og § 152, stk. 7, i lov nr. 652 af 8. juni 2017 om betalinger fastsættes:~~

Kapitel 1

Anvendelsesområde og definitioner

§ 1. Denne bekendtgørelse finder anvendelse på følgende virksomheder ved udbud af betalingstjenester:

- 1) Pengeinstitutter, der udsteder elektroniske penge eller udbyder betalingstjenester, jf. §§ 2 og 3 i lov om betalinger.
- 2) Offentlige myndigheder og Danmarks Nationalbank, hvis disse udsteder elektroniske penge eller udbyder betalingstjenester, jf. §§ 2 og 3 i lov om betalinger.
- 3) Virksomheder, der er meddelt tilladelse som e-pengeinstitut i medfør af § 8 i lov om betalinger, og som udbyder betalingstjenester, jf. bilag 1 i lov om betalinger.
- 4) Virksomheder, der er meddelt tilladelse som betalingsinstitut i medfør af § 9 i lov om betalinger.
- 5) Virksomheder, der er meddelt begrænset tilladelse til at udstede elektroniske penge i medfør af § 50 i lov om betalinger.
- 6) Virksomheder, der er meddelt begrænset tilladelse til at udbyde betalingstjenester i medfør af § 51 i lov om betalinger.
- 7) Virksomheder, der er meddelt tilladelse til at udbyde kontooplysningstjenester i medfør af, ~~jf.~~ § 60, stk. 1, i lov om betalinger.

§ 2. I denne bekendtgørelse forstås ved:

- 1) Drifts- og sikkerhedshændelse: En enkeltstående eller en række af hændelser, der ikke er planlagt af en virksomhed omfattet af § 1, og som har fået eller formodes at få negativ indvirkning på betalingsrelaterede tjenesters integritet, tilgængelighed, fortrolighed, eller ægthed ~~eller kontinuitet~~.
- 2) Betalingsrelaterede tjenester: Betalingstjenester omfattet af bilag 1 i lov om betalinger og alle de tekniske støttefunktioner, der er nødvendige for den korrekte levering af betalingstjenester.

Kapitel 2

Indberetning af større hændelser

§ 3. En virksomhed omfattet af § 1 skal snarest muligt ~~underrette indberette Finanstilsynet om~~ større drifts- og sikkerhedshændelser til Finanstilsynet.

Stk. 2. Virksomheden skal vurdere ~~o~~ Omfanget af en drifts- og sikkerhedshændelse ~~skal vurderes~~ ud fra kriterierne angivet i bilag 1. Virksomheden skal for de enkelte kriterier fastslå, om tærskelværdierne som nævnt i bilag 1 er eller sandsynligvis vil blive nået, før hændelsen er afhjulpet. Der vil være tale om en større drifts- og sikkerhedshændelse, når hændelsen opfylder eller forventes at opfylde

- 1) ét eller flere af kriterierne på højere indvirkningsniveau, jf. bilag 1, eller
- 2) tre eller flere af kriterierne på lavere indvirkningsniveau, jf. bilag 1.

Stk. 3. Virksomheden skal klassificere hændelsen snarest muligt efter, at hændelsen er konstateret, dog senest 24 timer herefter, og snarest muligt efter virksomheden er i besiddelse af de oplysninger, der er nødvendige for at klassificere hændelsen, jf. dog stk. 4.

Stk. 4. Har virksomheden behov for længere tid til at klassificere hændelsen, jf. stk. 3, skal den redegøre for årsagen hertil i den indledende rapport, jf. § 4, stk. 1.

Stk. ~~5~~3. UnderIndberetningen efter stk. 1 skal bestå af:

- 1) En indledende rapport, jf. § 4.
- 2) Foreløbige rapporter om ~~løbende orientering af~~ status på hændelsen, jf. § 5.
- 3) En endelig rapport, jf. § 6.

Stk. 64. ~~Under~~Indberetning ~~efter stk. 1 af hændelser~~ skal ske gennem den fælles digitale løsning for indberetning af hændelser til offentlige myndigheder på www.virk.dk.

§ 4. En virksomhed omfattet af § 1 skal indsende en indledende rapport til Finanstilsynet, ~~snarest muligt og senest 4 timer efter, at~~ drifts- og sikkerhedshændelsen ~~er klassificeret som større konstateres og om muligt indenfor 4 timer~~. Konstateres drifts- og sikkerhedshændelsen uden for normal arbejdstid, skal den indledende rapport sendes til Finanstilsynet senest 4 timer efter, at normal arbejdstid er påbegyndt den efterfølgende arbejdsdag. Omklassificerer virksomheden en hændelse til en større drifts- og sikkerhedshændelse, skal virksomheden indsende en indledende rapport til Finanstilsynet straks efter omklassificeringen.

Stk. 2. Er alle oplysninger til brug for ~~indberetningen~~~~underretningen~~ ikke tilgængelige for virksomheden på tidspunktet, hvor ~~indberetning~~~~underretning~~ skal foretages, jf. stk. 1, skal virksomheden indsende en indberetning afgive en underretning baseret på skøn.

§ 5. En virksomhed omfattet af § 1 skal ~~løbende~~ indsende en foreløbige rapporter til Finanstilsynet, ~~når driften igen er normal, dog senest 3 arbejdsdage efter indsendelsen af den indledende rapport og første gang indenfor 3 arbejdsdage fra, at drifts- og sikkerhedshændelsen konstateres~~. Den foreløbige rapporter skal løbende ~~ajourføres~~opdateres overfor Finanstilsynet, når virksomheden får kendskab til ~~nye relevante oplysninger eller væsentlige ændringer siden den forudgående indberetning~~~~underretning~~, ~~dog ikke med større interval end 3 arbejdsdage, og indtil hændelsens ophør~~.

Stk. 2. Er alle oplysninger til brug for ~~indberetningen~~~~underretningen~~ ikke tilgængelige for virksomheden på tidspunktet, hvor ~~indberetning~~~~underretning~~ skal foretages, jf. stk. 1, skal virksomheden afgive en ~~indberetning~~~~underretning~~ baseret på skøn.

§ 6. En virksomhed omfattet af § 1 skal indsende en endelig rapport til Finanstilsynet senest 20 arbejdsdage~~to uger~~ efter, at drifts- og sikkerhedshændelsen er ophørt, og normal driften ~~er genoptaget kan anses for at være tilbage til normal~~.

Stk. 2. En virksomhed omfattet af § 1 skal indsende en endelig rapport, såfremt det konstateres, at en indberettet hændelse ikke længere opfylder kriterierne for at være en større hændelse.

Stk. 3. Den endelige rapport skal være baseret på faktiske oplysninger.

Outsourcing og konsolideret indberetning

§ 7. En virksomhed omfattet af § 1 kan outsource indberetningen af større drifts- og sikkerhedshændelser efter § 3, jf. §§ 4-6, til en tredjepart, når følgende betingelser er opfyldt, jf. dog stk. 2:

- 1) Virksomheden underretter forinden Finanstilsynet om outsourcingen af indberetningen.
- 2) Den formelle kontrakt mellem virksomheden og tredjeparten, der er grundlaget for outsourcingen af indberetningen, fastlægger entydigt opgavefordelingen mellem parterne.
- 3) Fortroligheden af følsomme data samt kvaliteten, sammenhængen, integriteten og pålideligheden af de oplysninger, der gives til Finanstilsynet, er forsvarligt sikret.

Stk. 2. Virksomheder omfattet af § 1, nr. 3 og 4, skal foruden stk. 1 opfylde de krav til outsourcing af væsentlige driftsmæssige funktioner, som er fastlagt i §§ 39 og 40 i lov om betalinger.

Stk. 3. Den virksomhed, der efter stk. 1 outsourcer indberetningen efter § 3§ 4-6, har fortsat ansvaret for opfyldelsen af de ~~kravene~~ til indberetningen-, der følger af §§ 4-6, samt for de oplysninger, der afgives til Finanstilsynet.

Stk. 4. Virksomheden skal underrette Finanstilsynet, hvis virksomheden trækker outsourcing efter stk. 1~~en af indberetningen~~ tilbage. Virksomheden skal desuden underrette Finanstilsynet om enhver væsentlig ændring, der berører tredjeparten og dennes evne til at opfylde indberetningsforpligtelsen.

§ 8. En eller flere virksomheder omfattet af § 1, kan på konsolideret niveau outsource indberetning~~en~~ efter § 3§ 4-6 til en tredjepart, som er etableret i Danmark, i de tilfælde hvor en drifts- og sikkerhedshændelse skyldes en afbrydelse af den eller de ydelser, der leveres af den pågældende tredjepart.

Stk. 2. Virksomheden skal forinden underrette Finanstilsynet om outsourcingen af indberetningen efter stk. 1.

Stk. 3. Kontrakten mellem virksomheden og tredjeparten, der er grundlaget for outsourcingen af indberetningen, skal entydigt fastlægge opgavefordelingen mellem parterne, og det skal fremgå, at tredjeparten holder virksomheden løbende underrettet om alle relevante oplysninger om hændelsen, herunder den dialog, som tredjeparten har med Finanstilsynet, i det omfang det ikke udgør et brud på fortroligheden af oplysninger, som vedrører andre virksomheder.

Orientering til brugerne af betalingstjenesten

§ 9. En virksomhed omfattet af § 1 skal snarest muligt, efter konstatering af en drifts- og sikkerhedshændelse ~~n-konstateres~~, jf. § 2, nr. 1, vurdere, om drifts- og sikkerhedshændelsen direkte eller indirekte har eller kan få indvirkning på betalingstjenestens brugere og deres økonomiske interesser.

Stk. 2. Viser virksomhedens vurdering, jf. stk. 1, at drifts- og sikkerhedshændelsen direkte eller indirekte har eller kan få indvirkning på brugernes økonomiske interesser, skal virksomheden snarest muligt orientere brugerne om hændelsen og om de tilgængelige foranstaltninger, som de kan træffe for at begrænse hændelsens negative følger. Ved orienteringen til brugerne skal virksomheden tage hensyn til drifts- og sikkerhedshændelsens negative følger samt den måde, hvorpå virksomheden normalt kommunikerer med sine brugere på.

Kapitel 3

Straffebestemmelser

§ 10. Overtrædelse af § 3, stk. 1, stk. 2, 1. pkt., og stk. 3, §§ 43-6 og § 9 straffes med bøde.

Stk. 2. Der kan pålægges selskaber m.v. (juridiske personer) strafansvar efter reglerne i straffelovens 5. kapitel.

Ikrafttræden

§ 11. Bekendtgørelsen træder i kraft den 1. januar 2023~~2019~~.

Stk. 2. Bekendtgørelse nr. 1428 af 3. december 2018 om indberetning af drifts- og sikkerhedshændelser m.v. for udbydere af betalingstjenester ophæves.

Finanstilsynet, den

Jesper Berg

/ Tobias Thygesen

¹⁾ Bekendtgørelsen indeholder bestemmelser, der gennemfører dele af Europa-Parlamentets og Rådets direktiv 2015/2366/EU 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, EU-Tidende 2015, nr. L 337, side 35.

Bilag 1

Kriterier for vurdering af drifts- og sikkerhedshændelser

Omfanget af en drifts- og sikkerhedshændelse skal vurderes ud fra følgende kriterier og ud fra en vurdering af, om tærskelværdierne i tabellen er eller sandsynligvis vil blive nået, før hændelsen er afhjulpet:

| Kriterier | Beskrivelse af kriterier | Lavere indvirkningsniveau | Højere indvirkningsniveau |
|--|--|---|--|
| Berørte transaktioner | <p><u>Virksomheden skal fastslå den samlede værdi af alle transaktioner, der er eller formodes at være blevet eller sandsynligvis vil blive direkte eller indirekte berørt af hændelsen, samt antallet af berørte betalinger som en procentdel af det antal transaktioner, der normalt foretages med de berørte betalingstjenester.</u></p> <p>Ved det "normale niveau af betalingstransaktioner" forstås den daglige mængde, beregnet som årsgennemsnit af transaktioner, der udføres med de betalingstjenester, der er blevet berørt af hændelsen, idet referenceperioden er det forudgående år.</p> <p><u>For driftshændelser, der påvirker evnen til at initiere eller behandle transaktioner, skal virksomheden kun indberette hændelser, der har en varighed på mere end en time. Hændelsens varighed måles fra det øjeblik, hvor hændelsen opstår, til det øjeblik, hvor de almindelige aktiviteter og funktioner er genetableret på niveauet fra før hændelsen.</u></p> | <p>> 10 % af betalingstjenesteyderens normale transaktionsniveau (i antal transaktioner)</p> <p>og</p> <p><u>> 100.000 EUR hændelsens varighed > 1 time</u></p> <p>eller</p> <p><u>> 500.000 EUR</u></p> <p>og</p> <p><u>hændelsens varighed > 1 time</u></p> | <p>> 25 % af betalingstjenesteyderens normale transaktionsniveau (i antal transaktioner)</p> <p>eller</p> <p><u>> 5 mio. 15 000 000 EUR</u></p> |
| Berørte betalingstjenestebrugere | <p><u>Virksomheden skal fastslå det samlede antal af alle berørte betalingstjenestebrugere, både i absolutte tal og som procentdel af det samlede antal betalingstjenestebrugere. Der skal medregnes alle både aktive og passive betalingstjenestebrugere, der er kontraktligt bundet til virksomheden på tidspunktet for hændelsen og har adgang til den berørte betalingstjeneste.</u></p> <p><u>For driftshændelser, der påvirker evnen til at initiere eller behandle transaktioner, skal virksomheden kun indberette hændelser, der påvirker betalingstjenestebrugere og har en varighed på mere end en time. Hændelsens varighed måles fra det øjeblik, hvor hændelsen opstår, til det øjeblik, hvor de almindelige aktiviteter og funktioner er genetableret på niveauet fra før hændelsen.</u></p> | <p><u>> 5.000 5.000</u></p> <p>og</p> <p><u>hændelsens varighed > 1 time</u></p> <p>eller</p> <p>> 10 % af betalingstjenesteudbyderens betalingstjenestebrugere</p> <p>og</p> <p><u>hændelsens varighed > 1 time</u></p> | <p><u>> 50.000 500.000</u></p> <p>eller</p> <p>> 25 % af betalingstjenesteudbyderens betalingstjenestebrugere</p> |
| Tjenestens nedetid | <p><u>Virksomheden skal fastslå den periode, hvor tjenesten formodes at sandsynligvis vil være utilgængelig for betalingstjenestebrugeren, eller hvor betalingsordrer ikke kan udføres af virksomheden.</u></p> | > 2 timer | Ikke relevant |
| Brud på sikkerheden i netværks- eller informationssystemer | <p><u>Virksomheden skal fastslå, om en ondsindet handling har skadet sikkerheden i netværks- eller informationssystemer med relation til levering af betalingstjenester.</u></p> | Ja | Ikke relevant |

| | | | |
|---|--|---------------|--|
| Økonomisk indvirkning | Virksomheden skal <u>fastslå</u> fastlægge de samlede omkostninger, der direkte eller indirekte er relateret til hændelsen, herunder f.eks. omkostninger til udskiftning af hardware eller software, andre omkostninger af retlig eller afhjælpende art, eksterne forpligtelser og tabte indtægter. <u>Kernekapital er 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.</u> | Ikke relevant | > Maks. 10,1 % af kernekapitalen; 200 000 EUR }} eller > <u>5.000.000</u> 5 mio. EUR |
| Højt niveau af intern <u>udbredelse</u> se kalerin <u>g</u> | Virksomheden skal <u>fastslå</u> fastlægge, om bestyrelsen eller direktionen den informationsansvarlige er blevet eller <u>sandsynligvis vil formodes at ville</u> blive informeret om hændelsen uden om en eventuel regelmæssig indberetningsprocedure, herunder om hændelsen har eller vil udløse en krisesituation. | Ja | Ja, og der forventes en krisesituation (eller tilsvarende) <u>vil sandsynligvis blive udløst</u> |
| Andre betalingstjenesteudbydere eller relevante infrastrukturer, der kan være blevet berørt | Virksomheden skal <u>fastslå</u> vurdere hændelsens indvirkning på det finansielle markedes infrastrukturer og/eller kort betalingsordninger, navnlig om hændelsen har gentaget sig eller <u>sandsynligvis vil forventes at</u> gøre det hos andre virksomheder, der udbyder betalingstjenester, om hændelsen har påvirket den gnidningsløse funktion af det finansielle markedes infrastrukturer eller <u>sandsynligvis vil forventes at</u> gøre det, og om hændelsen har berørt det finansielle systems funktion som helhed eller <u>sandsynligvis vil forventes at</u> gøre det. | Ja | Ikke relevant |
| Indvirkning på om-dømmet | Virksomheder skal <u>fastslå</u> fastlægge, hvordan <u>om</u> hændelsen kan underminere brugernes tillid til virksomheden selv og generelt til den underliggende tjeneste og markedet som helhed, navnlig under hensyntagen til sandsynligheden for, at hændelsen vil være samfundsskadelig. | Ja | Ikke relevant |