Prosjektrapport

Uavhengig bankberedskap

Utarbeidet av prosjektet for uavhengig bankberedskap

30. september 2026

Innholdsfortegnelse

1 Innledning 4

1.1 Oppdraget 4

1.2 Sammendrag 6

1.3 Begrepsbruk 8

2 Beredskapsansvaret og etablerte beredskapsløsninger 9

2.1 Hvorfor bankenes data og systemer er viktige 9

2.2 Myndighetenes og bankenes ansvar for beredskap 9

2.3 Bankenes systemer er utformet for å opprettholde høy tilgjengelighet 10

2.4 Viktige beredskapsløsninger for kortbetalinger 11

2.5 Hvordan en operasjonell hendelse også kan bli en finansiell hendelse 11

3 Gjeldende rett 13

3.1 EØS-retten 13

3.2 Forordning om digital operasjonell motstandsdyktighet (DORA) 14

3.3 Håndtering av banker i krise 16

3.4 Innskuddsgarantiordningen 17

4 Tilsvarende arbeid i andre land 19

4.1 Innledning 19

4.2 Danmark 19

4.3 Finland 20

4.4 Storbritannia 20

4.5 Sverige 21

4.6 Ukraina 22

4.7 USA 23

5 Prosjektets vurderinger 24

5.1 Innledning 24

5.2 Målbilde 24

5.3 Nærmere beskrivelse av relevante tilnærminger 25

5.4 Prosjektets anbefaling 28

6 Rapportering til Bankenes sikringsfond 32

6.1 Nærmere om rapporteringen til Bankenes sikringsfond 32

6.2 EØS-regelverk og hvem som kan omfattes av rapporteringsplikt 33

6.3 Generelt om taushetsplikt og personvern ved et uavhengig datalager i regi av Bankenes sikringsfond 33

6.4 Vurdering av uavhengig datalagring og personvernhensyn 35
7 Nordiske fellesløsninger 38
8 Administrative og økonomiske konsekvenser 39
8.1 Innledning 39
8.2 Konsekvenser for bankene 39
8.3 Konsekvenser for myndighetene 39
8.4 Konsekvenser for kundene 39
9 Forslag til endringer i lov og forskrift 41

Figurer

Figur 1: Bankenes systemer er en sentral brikke i betalingssystemet 9

1 Innledning

1.1 Oppdraget

Finansdepartementet fastsatte i november 2023 mandatet til en arbeidsgruppe som skulle vurdere beredskapen i det digitale betalingssystemet.[1] Arbeidsgruppen leverte tre rapporter, den siste i februar 2025, og anbefalte i alt 18 tiltak som hadde som formål å gjøre betalingssystemet mer motstandsdyktig mot alvorlige krisescenarioer.[2] To av disse tiltakene innebar en styrking av motstandsdyktigheten mot situasjoner som kan føre til at en bank mister tilgangen til egne data og over tid ikke kan levere tjenester til sine kunder.

Det ene anbefalte tiltaket innebærer rapportering av informasjon om blant annet kundeinnskudd til et uavhengig datalager. Arbeidsgruppen omtalte dette som tiltak T055. Det andre tiltaket innebærer etablering av løsninger som er uavhengige av bankenes primære løsninger, og som gjør banken i stand til å levere kritiske betalingstjenester til kundene i alvorlige scenarioer der de primære løsningene blir utilgjengelige. Arbeidsgruppen omtalte dette som tiltak T083.

Arbeidsgruppen identifiserte flere alternativer for etablering av slike løsninger, og foreslo en videre utredning av tiltakene for å identifisere den mest hensiktsmessige måten å implementere disse på. Arbeidsgruppen mente det var viktig at bankene deltok direkte i en slik utredning.

Finansdepartementet ga 6. juni 2025 mandat til et prosjekt som skulle vurdere de to tiltakene.[3,4] Mandatet sier følgende:

> *Prosjektgruppen skal, på bakgrunn av delrapport I, II og III fra arbeidsgruppen for beredskap i det digitale betalingssystemet, utrede mulige løsninger for hvordan følgende tiltak kan konkretiseres:*
>
> - *Rapportering av kontoinformasjon til uavhengig datalager (tiltak T055 i delrapport II og III), og*
> - *Uavhengig beredskap for kort- og kontoadministrasjon (tiltak T083 i delrapport II og III)*
>
> *Prosjektgruppen skal belyse fordeler og ulemper ved ulike løsninger, herunder gjennom tallfesting av kostnader for etablering og drift, samt alternative tiltak som ev. kan svare på utfordringene nevnt i de relevante scenarioene i delrapport I. Det skal belyses i hvilken grad ulike løsninger muliggjør deltakelse fra utenlandske banker som opererer i Norge, og i hvilken grad det kan være grunnlag for å etablere nordiske fellesløsninger. Prosjektgruppen skal også utrede nødvendige regelverksendringer, og gi sin vurdering av hvilken løsning som vil gi størst nytteverdi i en norsk kontekst. Prosjektets vurderinger og anbefalinger, sammen med tilhørende utkast til*

[1] Se https://www.regjeringen.no/contentassets/cf6817157feb4e01b95cf40924300fb5/2023-11-13-vedlegg-mandat.pdf

[2] De tre rapportene er unntatt offentlighet. En oppsummerende rapport fra arbeidsgruppen er tilgjengelig her: https://www.regjeringen.no/contentassets/8658a4d2247940e086d2a3067d08c73f/sammendragsrapport-for-publisering.pdf

[3] Se https://www.regjeringen.no/contentassets/556dcd2c54a74296b1fa7691df81a698/mandat-prosjekt-om-uavhengig-bankberedskap.pdf

[4] Prosjektgruppen skulle opprinnelig levere sin rapport til Finansdepartementet innen 30. januar 2026, men fikk utsatt leveringsfristen etter avtale med departementet.

regelverksendringer, skal inngå i en rapport som kan sendes på offentlig høring. Rapporten skal utarbeides i tråd med utredningsinstruksen.

Oppdraget har en klar forankring i den nasjonale sikkerhetsstrategien for Norge, hvor regjeringen slår fast at samfunnet må bli mer motstandsdyktig og at evnen til å håndtere mer alvorlige hendelser må styrkes. I strategien pekes det blant annet på viktigheten av at grunnleggende tjenester, som kraft, telekommunikasjon og finansielle tjenester, er mulig å gjenopprette.

Prosjektet har hatt en styringsgruppe som har gitt innspill og tilbakemeldinger til prosjektets vurderinger. Styringsgruppen anser at mandatet er oppfylt. Anbefalingene og konklusjonene i rapporten er prosjektets egne. At institusjoner har hatt deltakere i prosjektgruppen eller i styringsgruppen er ikke til hinder for at institusjonene kan avgi eventuelle høringsinnspill.

Styringsgruppen har hatt 11 møter og har bestått av følgende medlemmer:

- Torbjørn Hægeland (Norges Bank, leder av styringsgruppen),
- Eivind Gjemdal (Bits),
- Anna Grinaker (Norges Bank),
- Knut Haugan (Finanstilsynet),
- Olav Johannessen (Finanstilsynet), og
- Marius Østli (Finansdepartementet).

Prosjektet har bestått av følgende deltakere:[5]

- Mats Bay Fevolden (Norges Bank, leder for prosjektgruppen),
- Maren Børslien (Finansdepartementet),
- Atle Dingsør (Finanstilsynet),
- Tor Runshaug Foss (Bankenes sikringsfond),
- Mathias Furevik (Sparebanken Norge),
- Espen Green (Norges Bank),
- Finn Robert Gynnild (SpareBank 1),
- Marta Stensheim Haugen (Nordea),
- Kristin Holberg (Finanstilsynet),
- Morten Krøgenes (Bits),
- Kristian Kyvik (Storebrand),
- Snorre Vik Sanfelt (Finanstilsynet) (frem til 15. mars 2026),
- Tormod Skjærpe (Bankenes sikringsfond),
- Torger Sollie (Eika),
- Nina Strandvik (Finanstilsynet),
- Peer Theien (DNB) (frem til 30. mai 2026), og
- Per Atle Thomassen (DNB) (fra 1. Juni 2026).

Prosjektrapporten er inndelt som følger. Kapittel 1 beskriver bakgrunnen for prosjektet, prosjektets forståelse av begrepene uavhengig datalager og uavhengig beredskap for kort- og kontoadministrasjon og oppsummerer prosjektets vurderinger og anbefalinger. Kapittel 2 beskriver

[5] Prosjektets vurderinger er deltakernes egne og gir ikke nødvendigvis uttrykk for synspunktene til deltakernes arbeidsgivere.

beredskapsansvaret og bankenes etablerte kontinuitets- og beredskapsløsninger. Kapittel 3 beskriver gjeldende rett. Kapittel 4 beskriver tilsvarende arbeid i andre land. Kapittel 5 redegjør for prosjektets vurderinger og anbefalinger. Kapittel 6 diskuterer regelverkskonsekvenser av prosjektets anbefaling. Kapittel 7 gir en vurdering av muligheten for nordiske fellesløsninger. Kapittel 8 beskriver administrative og økonomiske konsekvenser. I kapittel 9 gis forslag til endringer i lov om Bankenes sikringsfond og finansforetaksloven.

1.2 Sammendrag

Mandatet til prosjektet er å konkretisere innrettingen på to foreslåtte tiltak som kan bidra til at bankkunder får levert kritiske betalingstjenester også i mer alvorlige situasjoner, samt at kunders kontoinformasjon er sikret selv om en banks løsninger og sikkerhetskopier gjøres utilgjengelig.

Myndighetene har i lang tid vurdert det norske betalingssystemet som sikkert og effektivt. Bankenes etablerte kontinuitets- og beredskapsløsninger har bidratt til rask håndtering av avvik. Det er flere tiår siden en bank i Norge sist opplevde et avbrudd i sitt tjenestetilbud som pågikk over flere dager.

Samtidig ble disse løsningene etablert i en annen sikkerhetspolitisk virkelighet enn vi har i dag. Trusselbildet har de siste årene blitt mer alvorlig, og Nasjonal sikkerhetsmyndighet uttaler at *«Det sikkerhetspolitiske bildet skjerper kravene til beredskap og forebyggende sikkerhet i totalforsvaret.»*[6] I mer alvorlige scenarioer, som avanserte cyberangrep eller hybride angrep, kan en banks tjenester bli utilgjengelige. Bankens kunder kan da miste muligheten til å betale for eller få oppgjør for solgte varer og tjenester, motta betalinger eller ha oversikt over egen økonomi. En slik hendelse kan også ha konsekvenser for tilliten til bank- og betalingssystemet og for økonomisk aktivitet.

Det er et mål at kritiske banktjenester, som å motta og sende betalinger, kan opprettholdes også i mer alvorlige scenarioer. Dagens trusselbilde aktualiserer behovet for beredskapsløsninger som er mer uavhengige av de løsningene som benyttes i det daglige.

Prosjektet har vurdert tre ulike måter å konkretisere innretningen av de to foreslåtte tiltakene. Det ene er en løpende rapportering av kundeinnskudd fra bankene til et felles datalager uavhengig av de enkelte bankers systemer. Det andre er en styrking av bankenes egne beredskapsløsninger, som vil redusere risikoen for at banken blir utilgjengelig. Det tredje er etablering av en felles myndighetsløsning for drift av kritiske banktjenester, som kan aktiveres i situasjoner der en eller flere banker er utilgjengelige. Det første alternativet knytter seg til tiltak T055 fra arbeidsgruppen for betalingsberedskap, mens de to siste knytter seg til tiltak T083.

Prosjektgruppen anbefaler at det etableres et felles offentlig datalager med informasjon om kunders innskudd og at medlemmene av den norske innskuddsgarantiordningen får en plikt til regelmessig å rapportere informasjon om kundeinnskudd til dette datalageret. Formålet med datalageret er å være en beredskap for at innskuddsgarantien kan virke i situasjoner der en bank har mistet oversikt over hva kundene eier, og ikke innen rimelig tid kan gjenskape en slik oversikt. Prosjektgruppen mener at samfunnets motstandsdyktighet mot mer alvorlige scenarioer kan styrkes dersom informasjon om norske kunders innskudd for alle banker som deltar i innskuddsgarantiordningen finnes i et uavhengig datalager som er utenfor bankenes primære datasystemer. Prosjektet anslår at kostnadene ved å etablere og vedlikeholde et slikt datalager er forholdsvis lave sammenlignet med andre vurderte

[6] Se NSM (2026), Risiko 2026.

alternativer og trekker også frem at myndighetene med en slik løsning har et handlingsrom i en krise som de ellers ikke ville hatt. Et slikt felles datalager kan bygge på en felles rapporteringsstandard, for eksempel den som Bankenes sikringsfond allerede har etablert for innskuddsgarantiordningen og som i dag testes periodevis med deltagerne i innskuddsgarantiordningen. Det tilsier at datalageret etableres og driftes av Bankenes sikringsfond og kobles til forvaltningen av innskuddsgarantiordningen. Prosjektet foreslår i første omgang at datalageret etableres med informasjon om kundeinnskudd. På et senere tidspunkt kan det vurderes å utvide rapporteringen til også å gjelde annen type informasjon, som mer detaljert utlånsinformasjon.

Det eksisterende rammeverket for håndtering av kriser i banker legger til grunn at bankens systemer fungerer tilfredsstillende og at en krise kan løses gjennom bruk av finansielle krisehåndteringsverktøy eller at banken kan avvikles. I en situasjon der bankens krise skyldes operasjonelle problemer som innebærer at innskudd blir utilgjengelige, er det mindre klart om, og i så fall hvordan rammeverket skal anvendes. Dette er forhold som det kan være behov for å avklare nærmere, men prosjektet vurderer at en slik avklaring ligger utenfor prosjektets mandat.

Lov om digital operasjonell motstandsdyktighet i finanssektoren trådte i kraft i Norge 1. juli 2025 og gjennomfører forordning (EU) 2022/2554 om digital operasjonell motstandsdyktighet i finanssektoren (DORA) i norsk rett. DORA er et felleseuropeisk regelverk for å styrke den digitale operasjonelle motstandskraften til foretak i finanssektoren. DORA stiller blant annet krav til at bankene skal ha løsninger for å ivareta kontinuitet i kritiske tjenester i ulike scenarioer. Bankene arbeider løpende med å etterleve kravene i DORA, og prosjektet legger til grunn at dette bidrar til å styrke bankenes egne beredskapsløsninger. Det eksisterer dermed allerede et regelverk som bidrar til å styrke bankenes beredskapsløsninger.[7]

Prosjektet anbefaler ikke å etablere en felles myndighetsløsning for kort- og kontoadministrasjon. Finske myndigheter etablerte en offentlig beredskapsløsning i 2022. En viktig begrunnelse var at kritisk infrastruktur lå utenfor landet, noe som gjorde Finland særlig sårbart ved brudd i kommunikasjonslinjer til utlandet. I Norge er denne sårbarheten mindre, fordi infrastrukturen i større grad er nasjonal. Prosjektet vurderer at i Norge er den enkelte bank nærmest til å ha ansvaret for beredskapsløsninger som er tilpasset bankens kundegruppe og måten banken tilbyr betalingstjenester på i en normalsituasjon. Løsninger i regi av den enkelte bank kan også ivareta kritiske funksjoner i bankene som er nødvendig for å kunne gjennomføre både kundenes og egne betalinger, som likviditetsstyring, utenlandsbetalinger, oppgjør på vegne av internasjonale kunder og tilgang til valuta- og verdipapirmarkeder. Prosjektet legger videre til grunn at gjenoppretting av tjenester normalt vil håndteres raskere gjennom beredskapsløsninger i regi av den enkelte bank enn gjennom en felles myndighetsløsning, hvor terskelen for aktivering vil være høyere.

[7] DORA trådte i kraft etter at mandatet for dette prosjektet ble gitt. Selv om det var kjent at DORA ville innføres, har det gjennom dette prosjektet blitt tydeligere hvilke rammer DORA setter for uavhengig bankberedskap og myndighetenes mulighet til å supplere DORA med særnorske krav. Arbeidsgruppen for betalingsberedskap som foreslo utredningen, vurderte ikke hvorvidt DORAs krav til beredskapsløsninger for ulike scenarioer kunne ha betydning for forslaget om uavhengig bankberedskap.

1.3 Begrepsbruk

1.3.1 Uavhengig datalagring

Bankenes data kan bli utilgjengelige eller miste integritet av ulike grunner, for eksempel som følge av menneskelige eller tekniske feil som fører til at data overskrives og slettes. Angrep mot fysisk infrastruktur eller programvare kan også medføre at data blir misvisende eller slettes. I sofistikerte cyberangrep, som for eksempel løsepengevirusangrep, har angripere ofte som mål å ramme sikkerhetskopier i tillegg til produksjons- og reserveinfrastruktur.

Uavhengig datalagring er en måte å beskytte data, ved å lagre kopier av data i systemer som ikke har bindinger til hverandre. Et eksempel er at de mest kritiske dataene lagres i isolerte datalagre. Slik datalagring kommer gjerne i tillegg til foretakets sikkerhetskopier og gir et ekstra lag med redundans. Slike isolerte datalagre kan etableres med uavhengighet til foretakets andre systemer langs flere dimensjoner, som leverandør, geografi, personell eller teknologi.

1.3.2 Uavhengig beredskap for kort- og kontoadministrasjon

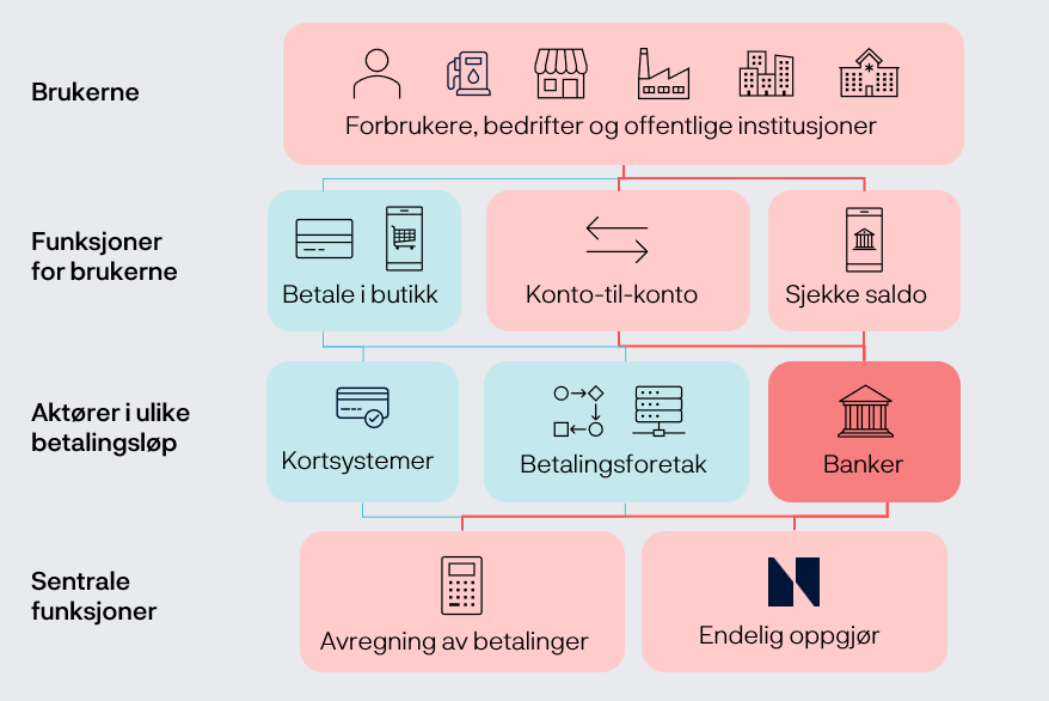
Med uavhengig beredskap for kort- og kontoadministrasjon menes tekniske beredskapsløsninger som kan levere tjenester, om enn med forenklet funksjonalitet, dersom de primære løsningene ikke er tilgjengelige og må gjenoppbygges. Med slike løsninger kan bank- og betalingstjenester tilbys med utgangspunkt i data fra uavhengige datalagre. Løsningene kan driftes av banken selv for sitt tjenestetilbud, eller myndighetene kan etablere slike løsninger for banksystemet i stort.

2 Beredskapsansvaret og etablerte beredskapsløsninger

2.1 Hvorfor bankenes data og systemer er viktige

Finansielle tjenester, herunder betalingsformidling, er sentrale funksjoner i samfunnet. Kort- og kontobetalinger (betalinger på utsalgssteder, netthandel, regninger, lønninger med mer) innebærer bruk av befolkningens og bedrifters bankinnskudd. Robustheten i bankenes data og systemer, herunder hos bankenes leverandører, er derfor avgjørende for at bankenes kunder kan gjøre opp for seg, motta betalinger og ha oversikt over hva de til enhver tid har av innskudd og lån.

Figur 1 illustrerer bankenes betalingstjenester i et samfunnsperspektiv.



Figur 1: Bankenes systemer er en sentral brikke i betalingssystemet

Selv kortere avbrudd i bankenes tjenestetilbud kan få store konsekvenser for bankens kunder, for samfunnet og for tilliten til bank- og betalingssystemet. Økonomisk aktivitet stopper opp om betalingsformidlingen ikke fungerer over tid.

2.2 Myndighetenes og bankenes ansvar for beredskap

Myndighetene skal fastsette regelverk for innretningen og driften av den finansielle infrastrukturen, påse at foretak i finanssektoren, herunder bankene, følger regelverket og overvåke risikoen i systemene. Finansdepartementet forvalter lov- og forskriftsverket for finanssektoren og har det overordnede ansvaret for å fremme finansiell stabilitet og bidra til forsvarlig drift i den finansielle infrastrukturen. I tråd med krav i samfunnssikkerhetsinstruksen gjennomfører departementet jevnlige risiko- og sårbarhetsanalyser (ROS-analyser) av både interne forhold og av forhold i sektoren, i tillegg til det løpende arbeidet med å vedlikeholde og oppdatere regelverket.

Finanstilsynet og Norges Bank overvåker det finansielle systemet for å avdekke forhold som kan true finansiell stabilitet. Finanstilsynet har etter finanstilsynsloven ansvar for tilsyn med konsesjonspliktig virksomhet, herunder banker.[8] Norges Bank har konsesjons- og tilsynsansvar for interbanksystemer etter lov om betalingssystemer. Bankenes sikringsfond skal gjennom innskuddsgarantiordningen bidra til finansiell stabilitet.

Ansvaret for systemene i den finansielle infrastrukturen ligger i hovedsak hos banker og andre foretak i finanssektoren. Den som har tillatelse til å yte betalingstjenester er ansvarlig for tjenestene og systemene. En stor del av de driftsmessige og tekniske leveransene til systemene er i dag satt bort til leverandører, men dette endrer ikke på ansvarsforholdene.

2.3 Bankenes systemer er utformet for å opprettholde høy tilgjengelighet

Bankenes drifts- og beredskapsløsninger har vært i kontinuerlig utvikling i takt med endringer i trusselbildet og regulatoriske krav. Bankenes kritiske løsninger er gjennomgående etablert for å opprettholde høy tilgjengelighet. Det innebærer blant annet redundans i komponenter og i kommunikasjon, samt rutiner for å håndtere ulike typer driftsavvik.

Etablerte kontinuitets- og beredskapsløsninger har bidratt til at bankene har hatt stabil drift i mange tiår. Det har vært få hendelser med potensial til å true finansiell stabilitet. Den kanskje mest alvorlige hendelsen skjedde i august 2001, da bankene som benyttet tjenester fra leverandøren Fellesdata opplevde at tjenestene var utilgjengelige i nesten to døgn. Hendelsen rammet rundt halvparten av norske bankkunder, og var forårsaket av at data utilsiktet ble slettet. Sikkerhetskopier og alle transaksjonsdata var tilgjengelig, men det tok over en uke å oppdatere alle kontoer til riktig saldo.[9]

Utviklingen i trusselbildet har aktualisert scenarioer som kan utfordre bankenes og deres leverandørers eksisterende beredskapsplaner og -løsninger og kan lede til situasjoner der en bank blir utilgjengelig i lengre tid. Angrep kan skje både gjennom logiske angrep mot programvare og data eller som en kombinasjon av logiske og fysiske angrep.

Store banker i Norden og Norge har lenge arbeidet med beredskapsløsninger for å opprettholde kritiske forretningsfunksjoner ved alvorlige cyberangrep. Disse løsningene innebærer uavhengighet til eksisterende driftsløsninger. Konseptene går under ulike navn, som «Minimum viable bank (MVB)», «Minimum viable services» eller «Minimum viable operations». Felles for tilnærmingene er at de typisk inkluderer uavhengig lagring av data (både kundedata og annen nødvendig metadata for å gjenopprette sine tjenester) og løsninger for å kunne gjenopprette bankens mest sentrale tjenester etter et alvorlig cyberangrep.

[8] Finanstilsynsloven § 1-2

[9] https://web.archive.org/web/20030406044941/http://www.edb.fellesdata.no/edb/nyheter/2001/08_08_Kredittilsynet.pdf

2.4 Viktige beredskapsløsninger for kortbetalinger

Det er viktig at befolkningen kan handle varer og tjenester, og særlig nødvendighetsvarer, også i situasjoner med feil hos banker eller i andre deler av betalingssystemet. Nødvendighetsvarer selges i stor grad på fysiske utsalgssteder der kundene hovedsakelig betaler med bankkort. Ved hendelser hvor norske banker har opplevd nedetid på sine tjenester, har kontinuitets- og beredskapsløsningene for betalingskort sørget for at bankenes kunder i stor grad har kunnet bruke betalingskort tilnærmet som normalt.

Det eksisterer primært to ulike kontinuitets-/beredskapsløsninger for kortbetalinger som skal gi trygghet for at befolkningen kan betale på brukersteder. Én løsning er STIP, forkortet fra Stand-in Processing, mens den andre løsningen er offline-løsninger, som BankAxept reserveløsning.

STIP kommer til anvendelse i situasjoner hvor et brukersted (butikk) får kommunisert med den bakenforliggende betalingsinfrastrukturen, men hvor banken/kortutstederen er utilgjengelig. Da kan blant annet kortordningene autorisere betalingen på vegne av banken, men innenfor beløps- og risikogrenser fastsatt av banken. STIP er etablert for de kortordningene som benyttes av norske kunder. Løsningen er tilgjengelig både for fysiske og digitale kort. Hvordan STIP-løsningen er satt opp til å fungere for det enkelte kort kan variere, blant annet med hensyn til beløpsgrenser og varighet. STIP kan primært betraktes som en kontinuitetsløsning som automatisk trer inn ved kortere avbrudd eller forsinkelser. STIP brukes derfor daglig i ulike situasjoner og vanligvis uten at kortbrukerne legger merke til det. Det er i tillegg etablert muligheter for å øke løsningens varighet hvis en eller flere banker har problemer mens resten av infrastrukturen fungerer.

En annen beredskapsløsning er offline-løsninger som trer inn dersom butikken ikke får kommunisert med den bakenforliggende betalingsinfrastrukturen. Det kan skyldes problemer hos butikken, i kommunikasjonslinjer, eller i den bakenforliggende betalingsinfrastrukturen. BankAxept har etablert en reserveløsning som i dag fungerer i opptil én uke for handel med nødvendighetsvarer. Det finnes også offline-funksjonalitet knyttet til internasjonale kortordninger som Visa og Mastercard. Dersom et problem skyldes feil kun hos banken, vil offline-løsninger ikke bli aktivert, men betalinger vil kunne autoriseres med STIP.

Arbeidsgruppen som vurderte beredskapen i betalingssystemet, foreslo flere tiltak for å styrke kontinuitets-/beredskapsløsningene for BankAxept-kortbetalinger. Finansnæringen er i gang med å følge opp tiltakene, jamfør Meld. St. 9 (2025-2026) Finansmarkedsmeldingen 2026.

Finansdepartementet har i brev 17. juni 2026 bedt Finanstilsynet om å blant annet gjøre en samlet vurdering av hvordan norske myndigheter best kan sikre tilstrekkelig beredskap for digitale betalinger på brukersteder, innen 18. desember 2026.

2.5 Hvordan en operasjonell hendelse også kan bli en finansiell hendelse

Ved betaling mellom kunder i ulike banker oppstår det et tilsvarende krav mellom avsender- og mottakerbank. Dette gjøres i mange tilfeller opp ved bruk av bankenes innestående i Norges Bank. En bank er avhengig av tilgjengelig likviditet (innskudd og/eller låneadgang) på sin konto hos Norges Bank (eller en annen privat bank) for å finansiere slike krav. Fordringer mellom banker kan også

oppstå på grunn av bankenes egne handler i penge- og kredittmarkedene. Summen av betalinger som bankene hver dag gjør opp på vegne av kunder og gjennom egenhandel, er svært stor.

Banker som er aktive i ulike valutaer må sikre at de har dekning for sine utgående betalinger i alle disse valutaene. Større banker bruker aktivt penge- og kredittmarkedene til å styre sin balanse, valutarisiko, og ha dekning for forventede betalinger i de ulike valutaene der banken er aktiv. Evnen til å styre egen likviditet innebærer blant annet muligheten til å overvåke inngående og utgående betalinger, lage prognoser over hvordan saldoen i ulike valutaer utvikler seg, holde oversikt over forventede oppgjør og forfall i handler bankene imellom og inngå handler med andre banker. Mindre banker styrer sin likviditet for eksempel gjennom avtaler om kreditt hos sin bankforbindelse (korrespondentbank).

Likviditetsstyringsfunksjonen, både teknisk, operasjonelt og i form av menneskelige ressurser, er helt avgjørende for at en bank skal kunne tilby sine kunder betalingstjenester. For å kunne gjøre opp betalinger på vegne av egne kunder, må en bank både være teknisk i stand til å gjøre opp for seg og ha dekning for kundenes betalinger. En bank som ikke får gjort opp for seg vil også skape problemer for andre banker, som forventer innkommende betalinger fra banken for å dekke egne forpliktelser. En bank som ikke evner å oppfylle sine forpliktelser kan miste tilgang til viktige markeder og motparter, både i Norge og utlandet, fordi motpartene ikke får oppgjør som avtalt, eller mangler tillit til at de får det. På denne måten kan et operasjonelt og teknisk problem gi opphav til en finansiell krise for den rammede banken. Feilen kan også få ringvirkninger og skape utfordringer for andre banker, og i ytterste konsekvens true finansiell stabilitet.

3 Gjeldende rett

3.1 EØS-retten

Finansielle tjenester er omfattet av EØS-avtalen. En konsekvens av dette er at norske regler på bank- og betalingsområdet i stor grad er gjennomføring av EØS-rett.

De mest sentrale EØS-rettsaktene for banker er kapitalkravsdirektivet (CRD) og kapitalkravsforordningen (CRR) med tilhørende delegerte kommisjonsforordninger. Dette bankregelverket omhandler organisatoriske forhold for bankvirksomhet.

Digital operasjonell motstandsdyktighet i finanssektoren reguleres av Digital Operational Resilience Act (DORA) med tilhørende delegerte kommisjonsforordninger, samlet omtalt som DORA i det videre. DORA stiller krav til bankers motstandsevne overfor digitale trusler og spesifiserer scenarioer (ikke uttømmende) bankene skal kunne håndtere for å sikre kontinuitet i sine tjenester.

Håndtering av en finansielt kriserammet bank følger av krisehåndteringsdirektivet (BRRD). Det skilles mellom krisehåndtering for å videreføre bankens virksomhet og avvikling under nasjonale insolvensregler. Regler om blant annet avvikling av kredittinstitusjoner fremgår av direktiv 2001/24/EF (winding up-direktivet). I tillegg stiller innskuddsgarantidirektivet (Deposit Guarantee Schemes Directive (DGSD)) krav til nasjonale innskuddsgarantiordninger.

EØS-reglene på bank- og betalingsområdet er blant annet gjennomført i finansforetaksloven, og foretak må oppfylle kravene som stilles for å kunne drive bankvirksomhet i Norge.

Banker må ha konsesjon fra norske myndigheter for å drive bankvirksomhet. Slik tillatelse gir blant annet adgang til å motta innskudd fra allmennheten. Bankene er underlagt tilsyn av norske myndigheter. Utenlandskeide banker som har bankkonsesjon fra norske myndigheter (datterselskaper) er i denne sammenheng å betrakte som norske banker. Krav for å få tillatelse til å etablere og drive virksomhet som finansforetak følger av finansforetaksloven kapittel 2.

I tillegg kan utenlandske banker drive bankvirksomhet i Norge. Dette kan gjøres gjennom etablering av filial i Norge eller gjennom grensekryssende virksomhet direkte fra hjemlandet. Bankene har i slike tilfeller tillatelse fra hjemlandsmyndigheten til å drive bankvirksomhet og er underlagt tilsyn i hjemlandet. For filialer er likevel noe tilsynsvirksomhet underlagt norske myndigheter, som for eksempel hvitvaskingstilsyn, markedsatferd, herunder forbrukerbeskyttelse og finansavtaleloven med videre. Alle banker som driver virksomhet (herunder filialer og banker som driver grensekryssende virksomhet) må følge norsk lovgivning som regulerer forholdet til kundene. Kravene som stilles for at utenlandske finansforetak skal kunne drive virksomhet i Norge fremgår av finansforetaksloven kapittel 5.

3.2 Forordning om digital operasjonell motstandsdyktighet (DORA)

3.2.1 Kort om DORA og gjennomføring i norsk rett

Forordning om digital operasjonell motstandsdyktighet (DORA) (EU) 2022/2554[10] er et harmonisert rammeverk for å styrke den finansielle sektorens evne til å forebygge, motstå, håndtere og gjenopprette etter IKT-relaterte hendelser og forstyrrelser. Forordningen pålegger finansforetak å etablere et helhetlig rammeverk for håndtering av IKT-risiko, som omfatter styring og kontroll, oversikt over IKT-aktiva, identifisering av risiko, beskyttelse, deteksjon, respons, gjenoppretting og kontinuerlig forbedring. Dette skal bidra til at sårbarheter og robusthet i systemer og prosesser håndteres på en proaktiv måte.

Digital operasjonell motstandsdyktighet er definert i DORA artikkel 3 nr. 1:

> "*«digital operasjonell motstandsdyktighet» en finansiell enhets evne til å bygge opp, sikre og gjennomgå sin operasjonelle integritet og pålitelighet gjennom å sikre, enten direkte eller indirekte gjennom bruk av tjenester levert av tredjepartsleverandører av IKT-tjenester, hele spekteret av IKT-relatert kapasitet som er nødvendig for å håndtere sikkerheten i de nettverks- og informasjonssystemene som en finansiell enhet bruker, og som støtter fortløpende levering av finansielle tjenester og deres kvalitet, herunder i forbindelse med forstyrrelser*".

DORA-forordningen er i norsk rett gjennomført i lov om digital operasjonell motstandsdyktighet (DORA-loven) som trådte i kraft 1. juli 2025. De fleste foretakene i finanssektoren omfattes av DORA.[11] I Norge tilsvarer dette i hovedsak foretak under tilsyn, jamfør finanstilsynsloven § 1-2. Tilsynsansvaret etter DORA er tillagt hjemstatsmyndigheten, og det er Finanstilsynet som har tilsynsansvaret for norske foretaks overholdelse av DORA.

Gjennom DORA stilles det omfattende krav til at foretakene skal være forberedt på ulike scenarioer og ha retningslinjer for å sikre kontinuitet for kritiske og viktige funksjoner dersom scenarioene skulle inntreffe. I tillegg skal foretakene raskt, hensiktsmessig og effektivt reagere og løse alle IKT-relaterte hendelser på en måte som begrenser skadevirkningene og prioriterer gjenoppretting av virksomheten.

I DORA gis eksempler på scenarioer (ikke uttømmende) som bankene skal ha beredskap for:

- Cyberangrep.
- Scenarioer der kvaliteten på leveringen av en kritisk eller viktig funksjon forverres til et uakseptabelt nivå eller mislykkes.
- Delvis eller fullstendig svikt i lokaler, herunder kontor- og forretningslokaler, og i datasentre.
- Vesentlig svikt i IKT-ressurser eller i kommunikasjonsinfrastrukturen.
- Manglende tilgjengelighet av et kritisk antall ansatte eller medarbeidere med ansvar for å garantere kontinuiteten i driften.
- Virkningene av klimaendringer og miljøødeleggelser, naturkatastrofer, pandemier og fysiske angrep, herunder inntrenging og terrorangrep.
- Innsideangrep.

[10] https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:32022R2554
[11] Hvilke foretak som omfattes framgår av DORA artikkel 2 og DORA-forskriften § 4

- Politisk og sosial ustabilitet, herunder, dersom det er relevant, i jurisdiksjonen til tredjepartsleverandøren av IKT-tjenester og stedet der dataene lagres og behandles.
- Omfattende strømbrudd.

DORA artikkel 4 inneholder en proporsjonalitetsbestemmelse som både foretakene og tilsynsmyndighetene skal ta hensyn til ved overholdelse og ved tilsynsmessig oppfølging av bestemmelsene i DORA. Proporsjonalitet innebærer at det skal tas hensyn til foretakets størrelse, samlet risikoprofil samt karakteren, omfanget og kompleksiteten av foretakets tjenester, aktiviteter og drift.

DORA etablerer også et rammeverk for myndighetsovervåking på europeisk nivå av kritiske IKT-leverandører og legger til rette for tettere samarbeid på tvers av land og myndigheter. Siden tilsynsansvaret etter DORA er tillagt hjemstatsmyndighetene i det enkelte land, kan det være forskjeller i krav og forventninger som stilles til bankfilialer og grensekryssende virksomhet som driver virksomhet i Norge, sammenlignet med forventninger som stilles av norske myndigheter til norske banker.

3.2.2 Myndighetenes handlingsrom

DORA stiller harmoniserte krav til IKT-sikkerhet for alle foretak innenfor EØS-området som er omfattet av forordningen. Forordningen kommer direkte til anvendelse i Norge, og den gir ikke norske myndigheter handlingsrom med hensyn til hvordan regelverket skal gjennomføres i norsk rett. Forordninger benyttes ofte når det er særlig behov for identiske regler i EØS-området. Myndighetene har som hovedregel ikke reguleringskompetanse innenfor forordningens virkeområde med mindre forordningen åpner for nasjonale valg. Denne begrensningen vil gjelde selv om forordningen er overordnet og på enkelte områder kan fremstå lite detaljert.

DORA inneholder ikke detaljerte krav om hvilke tjenester som anses viktige og kritiske for det enkelte foretak eller hvordan kravene skal etterleves. Etter DORA er det bankene selv som må identifisere viktige og kritiske funksjoner og påse at de pålagte oppgavene løses i samsvar med proporsjonalitetsprinsippet. Denne tilnærmingen må ses i sammenheng med at DORA gjelder for hele EØS-området og omfatter ulike foretakstyper, og foretak i samme kategori som er ulike.

Finanstilsynet har tilsyn med foretakenes etterlevelse av DORA. DORA stiller krav om beredskap for en rekke alvorlige scenarioer, og eksemplene som trekkes frem i DORA, er heller ikke uttømmende. Finanstilsynet har dermed et handlingsrom for å vurdere om alle relevante scenarioer er planlagt for, og om løsningene bankene etablerer er tilstrekkelige for å opprettholde kontinuitet i kritiske funksjoner. Finanstilsynet kan veilede om regelverket og stille krav til foretakene gjennom for eksempel å gi pålegg om retting.

Artikkel 1 nr. 3 i DORA fastsetter at forordningen ikke berører medlemsstatenes ansvar for vesentlige statlige funksjoner knyttet til offentlig sikkerhet, forsvar og nasjonal sikkerhet, i samsvar med EU-retten. Bestemmelsen viser til kompetansefordelingen mellom EU og medlemslandene og er ment å sikre at DORA ikke undergraver medlemsstatenes mulighet til å ivareta nasjonale sikkerhetsinteresser. Lignende bestemmelser finnes også i Critical Entities Resilience Directive (CER-direktivet) og Network and Information Security 2 directive (NIS2-direktivet), men disse er ikke gjennomført i norsk rett enda. Prosjektet legger til grunn at bestemmelsen åpner for at medlemsstatene i noe grad kan ha regulering i tillegg til DORA hvis dette er nødvendig ut fra nasjonal sikkerhet. Prosjektet har ikke

vurdert i hvilken grad denne bestemmelsen eventuelt åpner for at myndighetene av hensyn til nasjonal sikkerhet kan supplere DORA med nasjonale krav til bankenes beredskapsløsninger.

Private foretak som er kritiske for grunnleggende nasjonale funksjoner, kan også underlegges sikkerhetsloven. Sikkerhetsloven stiller krav om et forsvarlig sikkerhetsnivå. Prosjektet har ikke vurdert hvorvidt et forsvarlig sikkerhetsnivå etter sikkerhetsloven innebærer mer omfattende beredskapsløsninger enn beredskapsløsningene som er i tråd med DORA.

3.3 Håndtering av banker i krise

Erfaringene fra finanskrisen i 2008 førte til at det ble utarbeidet et nytt regelverk, blant annet for å håndtere banker som blir rammet av en finansiell krise. Et viktig mål med reglene er å kunne opprettholde samfunnsviktige funksjoner i en bank, som for eksempel betalingstjenester, som har stor betydning for finansiell stabilitet. Andre viktige formål er å beskytte innskudd, klientmidler og offentlige midler og å unngå vesentlige negative virkninger i finanssystemet.

Dersom en bank er eller må ventes i nær fremtid å bli ute av stand til å betale gjeld og andre forpliktelser ved forfall eller vilkårene for tilbakekall av foretakets konsesjon på annen måte er eller må ventes å bli oppfylt i nær fremtid, herunder som følge av at tap i foretaket helt eller delvis kan uttømme den ansvarlige kapitalen,[12] kan myndighetene enten beslutte å avvikle virksomheten under offentlig administrasjon eller gjennomføre en krisehåndtering.[13] Det er kun i tilfeller der krisehåndtering av finansforetaket anses å tjene allmenne interesser, at krisehåndtering skal gjennomføres. Dette innebærer at hele eller deler av virksomheten i banken videreføres eller overføres til et annet foretak. Dersom det ikke tjener allmenne interesser å videreføre bankvirksomheten, vil banken bli avviklet. Finansielle tiltak for å videreføre virksomheten (herunder nedskrivning og konvertering av gjeld) eller overføring av virksomheten til et annet foretak, forutsetter imidlertid at det foreligger oppdatert informasjon om bankens finansielle stilling, herunder at kunde- og motpartsdata er intakt. Ved operasjonelle hendelser kan dette grunnlaget falle bort, slik at krisehåndteringstiltakene i begrenset grad vil kunne gjennomføres. En ordnet avvikling av banken vil også kunne bli krevende dersom bankens systemer ikke fungerer.

Ved avvikling av banken som følge av finansielle problemer skal administrasjonsstyret etter samråd med innskuddsgarantiordningen så vidt mulig sikre at garanterte innskudd blir overført til et annet medlemsforetak slik at de fortsatt er fullt tilgjengelig for innskyterne. Se nærmere detaljer om innskuddsgarantiordningen i kapittel 3.4.

For banker hjemmehørende i Norge er det Finansdepartementet som treffer endelig avgjørelse om et finansforetak skal krisehåndteres eller avvikles under offentlig administrasjon, etter tilrådning fra Finanstilsynet. For banker hjemmehørende i EØS-området som driver virksomhet i Norge gjennom filial eller grensekryssende virksomhet direkte fra hjemlandet, skal en eventuell avvikling skje etter hjemlandets regler. Myndighetene i hjemstaten har kompetanse til å beslutte at banken, inkludert filialer i andre land, skal avvikles. I slike tilfeller vil norske myndigheter kun orienteres om beslutninger tatt i hjemlandet. Dette følger av winding up-direktivet, som bygger på

[12] Se finansforetaksloven § 20-15 for når en bank anses kriserammet

[13] Krisehåndtering følger av EUs krisehåndteringsdirektiv, direktiv 2014/59/EU (BRRD), som ble endret blant annet ved direktiv 2019/879/EU (BRRD2). Krisehåndteringsdirektivet er gjennomført i norsk rett i finansforetaksloven kapittel 20, med utfyllende bestemmelser i finansforetaksforskriften kapittel 20.

hjemstatsprinsippet.[14] Finansforetaksloven § 20-49 gir likevel departementet adgang til å beslutte at filialer av utenlandske foretak etablert i Norge skal krisehåndteres eller avvikles under offentlig administrasjon når hensynet til finansiell stabilitet og andre hensyn som skal ivaretas etter finanslovgivningen tilsier det.

For finanskonsern som driver virksomhet i flere land, fastsetter krisehåndteringsdirektivet regler for samarbeid mellom de ulike landenes myndigheter. Dette gjøres i relevante kriseutvalg. Det er ikke krav om at det skal etableres formelle samarbeidsformer etter winding up-direktivet. Finansforetaksloven regulerer imidlertid samarbeid med garantiordninger i andre EØS-stater. Regjeringen har satt ned et utvalg[15] som skal utrede behovet for endringer i regelverket om bankkrisehåndtering og innskuddsgaranti, blant annet for å gjennomføre endringer i krisehåndteringsdirektivet og innskuddsgarantidirektivet («CMDI»). Utvalget skal også vurdere behovet for endringer i organiseringen og eventuelt finansieringen av myndighets- og forvaltningsoppgaver, herunder også eventuelle endringer i Bankenes sikringsfonds forvaltningsrettslige organisering. Utvalgets vurderinger og oppfølgingen av dette kan få implikasjoner for Bankenes sikringsfonds rolle og forvaltningsrettslige status.

3.4 Innskuddsgarantiordningen

Bankenes sikringsfond administrerer den norske innskuddsgarantiordningen. Den norske innskuddsgarantiordningen bygger på EUs innskuddsgarantidirektiv.[16] Innskuddsgarantidirektivet stiller krav til nasjonalstatene om å ha en innskuddsgarantiordning samt setter nærmere krav til ordningen.

Innskuddsgarantiordningen gir kundene trygghet for at innskudd i bank er sikre, ved at kundenes innskudd dekkes inntil visse beløp dersom banken skulle bli kriserammet. Ordningen reduserer samtidig faren for at mange kunder tar ut pengene dersom det oppstår tvil om en banks tilstand. [17] Rammes én bank av slike uttak, kan det spre seg til flere. I en slik situasjon kan bankene få problemer med å fylle rollen sin i det finansielle systemet og den økonomiske aktiviteten i Norge kan bli skadelidende. Det overordnede formålet med innskuddsgarantien er derfor å bidra til finansiell stabilitet. Innskuddsgarantiordninger ble for sparebanker lovfestet i 1924 og for forretningsbanker i 1961.

Medlemmer i den norske innskuddsgarantiordningen er norske banker samt filialer av EØS-banker som har frivillig «topping-up» medlemskap i den norske ordningen. Topping-up medlemskap for filialer dekker differansen mellom hjemlandets innskuddsgarantidekning på 100.000 euro og to

[14] Winding up-direktivet, direktiv 2001/24/EF, regulerer reorganisering og avvikling av kredittinstitusjoner. Direktivets lovvalgsbestemmelser er gjennomført i finansforetaksforskriftens kapittel 21A.
[15] https://www.regjeringen.no/no/aktuelt/utvalg-skal-utrede-endringer-i-regelverket-om-bankkrisehandtering-og-innskuddsgaranti/id3153151/
[16] Directive 2014/49/EU of the European Parliament and of the Council of 16 April 2014 on deposit guarantee schemes
[17] Den alminnelige innskuddsgarantidekningen er etter finansforetaksloven § 19-4 1.ledd to millioner kroner. For innskudd mottatt gjennom filial eller ved grensekryssende virksomhet er beløpsgrensen et beløp i norske kroner som tilsvarer EUR 100.000, jf. finansforetaksloven § 19-4 3.ledd. For innskudd knyttet til salg eller kjøp av fast eiendom og hendelser knyttet til særskilte livshendelser («THB») gis en ubegrenset innskuddsgarantidekning på inntil 12 måneder, jf. finansforetaksloven § 19-4 2.ledd.

millioner norske kroner. På nåværende tidspunkt har den norske innskuddsgarantiordningen 12 topping-up medlemmer. Det inkluderer Nordea, Handelsbanken, Danske Bank, Swedbank og SEB.[18]

Innskuddsgarantien utløses når bankinnskudd er vurdert å være utilgjengelig for kundene. Det følger av finansforetaksloven § 19-5 at innskudd skal regnes som utilgjengelig når departementet har truffet vedtak om avvikling av foretaket under offentlig administrasjon eller Finanstilsynet har truffet vedtak om at foretaket ikke kan foreta utbetaling til innskytere eller det er truffet en annen tilsvarende beslutning som medfører at innskyterens rett til utbetaling suspenderes. Innskudd skal også regnes som utilgjengelig «når Finanstilsynet har besluttet at et medlemsforetak ikke har tilbakebetalt innskudd som er forfalt til betaling, og at det ut fra foretakets økonomiske stilling må antas at foretaket verken er eller vil bli i stand til å foreta tilbakebetaling». Prosjektet har ikke vurdert hvordan bestemmelsen kan anvendes i en situasjon med operasjonell svikt.

Innskuddsgarantiordningen skal gjøre garanterte innskudd tilgjengelig for innskyterne i norske kroner innen syv arbeidsdager etter at innskuddet ble utilgjengelig.

Det følger av finansforetaksloven at Bankenes sikringsfond skal treffe administrative tiltak for å forberede utbetaling av garanterte innskudd og for å sørge for at medlemsforetakene elektronisk stiller til disposisjon og jevnlig holder oppdatert den informasjonen om innskytere og kvalifiserte innskudd som trengs. Opplysningene skal gis elektronisk i en form som er overførbar og tilpasset garantiordningens systemer. De nærmere operasjonelle kravene til dette fremkommer i innskuddsgarantiforskriften.

Bankenes sikringsfonds eksisterende løsning for rapportering av garanterte innskudd baserer seg på at en bank gjennom en portalløsning leverer informasjon om kundenes innskudd innen en definert frist i samsvar med kravene i innskuddsgarantiforskriften. Dersom det fattes vedtak om avvikling av en bank under offentlig administrasjon, er fristen for administrasjonsstyret til å levere kundeinformasjon tre dager fra vedtaket er fattet. Det er en forutsetning for en effektiv innskuddsgarantiordning at bankene kan levere oppdaterte datasett i samsvar med innskuddsgarantiforskriften. Dersom informasjon om kundeinnskudd er utilgjengelige, vil ikke Bankenes sikringsfond kunne utbetale garanterte innskudd.

Finansforetaksloven stiller krav til stresstesting av innskuddsgarantiordningene. Det stilles krav til jevnlig gjennomføring av stresstester (situasjonstesting) av de administrative systemene, minimum hvert tredje år.

[18] Register over medlemmer i innskuddsgarantiordningen https://www.bankenessikringsfond.no/om-oss/medlemmer/

4 Tilsvarende arbeid i andre land

4.1 Innledning

Som beskrevet i kapittel 3 er finansielle foretak i EU underlagt DORA, som stiller felleseuropeiske krav til bankenes digitale motstandsdyktighet. Flere europeiske land har etablert krav og ordninger for å styrke beredskapen i bank- og betalingssystemet for mer alvorlige scenarioer. Disse kravene inkluderer etablering av planverk for koordinering, deltakelse i felles responsgrupper, samt deltakelse i felles øvelser.

Under gis en mer inngående beskrivelse av tiltak for å styrke beredskapen i seks land i og utenfor EU.

4.2 Danmark

Sentralbanken i Danmark, Nationalbanken, etablerte i 2016 «Finansielt sektorforum for operasjonell robusthet» (FSOR), som er et offentlig-privat samarbeid med formål om å øke motstandsdyktigheten i finansiell sektor mot blant annet cyberhendelser. Deltakelse i FSOR er frivillig, men samfunnsviktige aktører deltar. Deltakerne i FSOR er systemisk viktige banker og realkreditinstitutter, avregnings- og oppgjørssystemer, datasentraler, eiere og leverandører av infrastruktur, bransjeorganisasjoner, NFCERT og representanter fra forsikrings- og pensjonssektoren. Fra myndighetssiden deltar Styrelsen for Samfundsikkerhet, senter for cybersikkerhet, Finanstilsynet, Skatte- og vækstministeriet og Nationalbanken.

Nationalbanken ivaretar formannskapet og sekretariat for FSOR. Arbeidet i FSOR inkluderer felles risikoanalyser, kriseberedskap, informasjonsdeling og øvelser.

Nationalbanken igangsatte i 2023 en analyse av avhengigheter mellom aktører på sektornivå og en kartlegging av eksisterende kontinuitets- og beredskapsløsninger. Med utgangspunkt i arbeidet i FSOR identifiserte Nationalbanken en rekke tiltak. Tiltakene anbefales fulgt opp av finanssektoren i Danmark og vil bidra til å gjøre sektoren mer motstandsdyktig.[19] For bankene anbefaler Nationalbanken at myndighetene etablerer et sentralt datalager basert på felles rapporteringsstandarder og at bankene hver for seg etablerer infrastruktur/nødløsninger som er uavhengig av deres primære infrastruktur som kan videreføre kritiske tjenester som samfunnet er avhengig av (det inkluderer kundenære tjenester som tilgang til konto og betalinger, herunder bruk av betalingskort, mottak av lønn og overføring av penger).

Nationalbanken peker videre på at en sentral datainnsamling sikrer at kritiske kundedata er tilgjengelige og ensartede, og at det alltid eksisterer korrekte data om kundenes innestående, selv dersom data i en bank er blitt kompromittert. De sentrale nødløsningene understøtter rask aktivering ved at ansvar for drift, aktivering og kundehåndtering forblir hos den enkelte bank. Felles rapporteringsstandarder gir fleksibilitet ved at data i siste instans kan overføres mellom banker dersom en banks egen nødløsning feiler. Scenarioene slike løsninger skal være et svar på er omfattende systemsvikt, kompromittering av data eller ved fysisk ødeleggelse av ordinær

[19] Se Nationalbanken(2025) https://www.nationalbanken.dk/en/news-and-knowledge/publications-and-speeches/analysis/2025/emergency-preparedness-for-critical-financial-sector-activities-in-extreme-scenarios

infrastruktur. Krigsscenarioer er i analysen holdt utenfor. Nationalbanken understreker at slike løsninger vil kreve tett samarbeid mellom banksektoren og myndighetene fremover og at det må gjennomføres nødvendige regelverksendringer.

4.3 Finland

Russlands angrep på Ukraina og den endrede sikkerhetspolitiske situasjonen i Europa førte til økt oppmerksomhet om cyber- og hybridtrusler mot kritisk finansiell infrastruktur og var bakgrunnen for etableringen av nye beredskapsløsninger for daglige betalinger i Finland.[20]

8. juli 2022 vedtok det finske parlamentet «Loven om visse ordninger for å sørge for forsyningssikkerhet i finanssektoren».[21] Loven gir myndigheten for finansiell stabilitet ansvar for å ivareta en beredskapsløsning for kontohold og kortbetaling. Myndigheten for finansiell stabilitet[22] kan kreve den informasjonen den trenger fra kredittinstitusjoner for å opprettholde løsningene. Myndigheten for finansiell stabilitet er ansvarlig for personopplysningene som rapporteres.

Loven gir regjeringen fullmakt til å iverksette løsningen dersom en kredittinstitusjon er ute av stand til å opprettholde og delta i de systemene som er nødvendige for å sikre forsyningssikkerhet, både i normale og ekstraordinære omstendigheter. Beslutningen om å ikke lenger benytte beredskapssystemene fattes også av regjeringen.

Løsningen ble etablert som en beredskap for langvarig avbrudd hos en enkeltbank og bortfall av kommunikasjon fra Finland til det europeiske fastlandet.

4.4 Storbritannia

Arbeidet med å gjøre finansiell sektor i Storbritannia motstandsdyktig følges opp gjennom regelverk og i samarbeidsfora der myndighetene og finansnæringen er representert.

Britiske institusjoner omfattet av kapitaldekningsregelverket har siden mars 2022 vært underlagt krav til operasjonell motstandskraft.[23] Kravene til operasjonell motstandskraft for britiske banker er sammenlignbare med kravene som stilles til europeiske banker etter DORA.

The Cross Market Operational Resilience Group (CMORG) er et privat-offentlig samarbeid i britisk finanssektor bestående av banker, forsikringsselskaper, interbanksystemer og finansmyndigheter. CMORG har tre formål:

- identifisere risikoer for finanssektoren,
- utarbeide løsninger for å styrke motstandskraften for finanssektoren, og
- dele kunnskap.

CMORG har publisert veiledere, rammeverk og verktøy. CMORG har blant annet utarbeidet en veileder for operasjonell motstandskraft, som ble oppdatert i 2025 for å hensynta

[20] Se tale av Tuomas Välimäki, styremedlem i Suomenpankki: https://www.bis.org/review/r231017e.pdf
[21] https://www.finlex.fi/sv/lagstiftning/forfattningssamling/2022/666#OT1
[22] Ansvarlig for krisehåndtering av banker og innskuddsgarantiordningen
[23] Se regelverk gitt av den britiske tilsynsmyndigheten, Prudential Regulation Authority (PRA), PRA Rulebook: https://www.prarulebook.co.uk/pra-rules/operational-resilience/

tilsynsmyndighetenes krav til operasjonell motstandskraft. Bruken av veilederne er frivillig for medlemmene.

CMORG publiserte i januar 2025 en veileder for lagring av data i skybasert datahvelv, "Cloud-Hosted Data Vaulting Good Practice Guidance"[24]. Rapportering av kritisk data til uavhengige datahvelv bidrar til at et foretak har tilgang til data og kan gjenopprette infrastruktur og integritet som igjen kan være avgjørende for å holde kritiske tjenester tilgjengelige i møte med enkelte alvorlige scenarioer. Veilederen peker på fire scenarioer der dataene fra et uavhengig datalager kan komme til nytte, hvorav det mest aktuelle er løsepengevirusangrep. Veilederen lister videre opp 17 prinsipper for utforming av datahvelv.

4.5 Sverige

Det sivile beredskapssystemet i Sverige er på nasjonalt nivå inndelt i tolv beredskapssektorer. Hver beredskapssektor består av en eller flere beredskapsmyndigheter, og arbeidet i hver sektor ledes av en sektoransvarlig myndighet. I tråd med den svenske forordning (2022:524) om statlige myndigheters beredskap (beredskapsförordningen) skal beredskapsmyndighetene bidra til å nå det overgripende målet for totalforsvaret som Riksdagen har besluttet.

Beredskapsmyndighetene er ansvarlige for å redusere samfunnets sårbarhet og utvikle en god evne til å håndtere sine oppgaver ved krisesituasjoner i fredstid og ved forhøyet beredskap.

Den sektoransvarlige myndigheten skal lede arbeidet med å samordne tiltak både i forkant av og under krisesituasjoner. Den skal drive arbeidet framover innenfor sin beredskapssektor, støtte beredskapsmyndighetene og bidra til at samordning skjer med andre aktører.

Finansinspektionen er sektoransvarlig myndighet for beredskapssektoren *Finansielle tjenester*.

Finansinspektionen har identifisert følgende viktige samfunnsfunksjoner i sektoren:

- Betalingsformidling
- Sikring av finansiell stabilitet
- Forsikring
- Sparing, finansiering og finansiell risikohåndtering

Finansinspektionen har utarbeidet et støtteverktøy til virksomhetenes arbeid med beredskap.[25] Det er ikke rettslig bindende. Finansinspektionen inndeler finansielle foretak i tre kategorier etter hvor viktig aktørene er i en totalforsvarssammenheng. Den første kategorien inneholder *alle finansielle foretak*, den andre kategorien *samfunnsviktige foretak*, og den tredje kategorien *totalforsvarsviktige foretak*. Finansinspektionen gir ulike anbefalinger til de tre kategoriene av finansinstitusjoner og stiller størst forventinger til kategorien totalforsvarviktige foretak. I alt 20 aktører er per i dag utpekt under kategori tre. Til disse aktørene anbefaler Finansinspektionen en rekke tiltak. Foretakene bør blant annet etablere en krigsorganisasjon, dele situasjonsbilde med myndighetene, etablere løsninger for kommunikasjon med myndighetene og egne kunder, etablere redundans for virksomhetskritiske prosesser, ha lager av viktige fysiske innsatsfaktorer ved brudd i leveransekjeder og kunne håndtere

[24] https://www.cmorg.org.uk/artefact/cloud-hosted-data-vaulting-good-practice
[25] https://www.fi.se/globalassets/media/dokument/diverse/2025/planeringsinriktning-finansiella-foretag.pdf

ulike geografiske risikoer. Med redundans for virksomhetskritiske prosesser menes blant annet redundans for data og kommunikasjon og redundans for å kunne drive virksomhetskritiske prosesser.

Riksbanken har et særskilt beredskapsansvar for betalinger i henhold til kapittel 5 i lov (2022:1568) om Sveriges riksbank. Riksbanken har ansvar for at allmennheten skal kunne gjennomføre betalinger under krisesituasjoner i fredstid og ved hevet beredskap.

Riksbanken har fastsatt forskrifter (RBFS 2023:3) som utpeker virksomheter av særlig betydning for gjennomføringen av betalinger, og som stiller krav til virksomhetenes planlegging og forberedelser for krisesituasjoner i fredstid og ved hevet beredskap. Dette omfatter blant annet krav om opplæring og deltakelse i øvelser.

Ettersom Riksbanken etter riksbanksloven har et ansvar knyttet til betalinger, samtidig som Finansinspektionen er sektoransvarlig myndighet for Finansielle tjenester, foreligger det et overlappende ansvarsområde. Det er derfor inngått en avtale mellom myndighetene som regulerer ansvaret knyttet til betalinger.

4.6 Ukraina

Etter Russlands annektering av Krimhalvøya i 2014 etablerte ukrainske myndigheter og banker beredskapsplaner for å kunne opprettholde banktjenester under mer alvorlige scenarioer.[26]

I månedene før Russlands fullskalainvasjon 24. februar 2022 og like etter krigen begynte, gjennomførte bankene og myndighetene flere tiltak for å beskytte kundedata og opprettholde betalingstjenester. I mars 2022 åpnet myndighetene for at bankene kunne benytte sky-tjenester utenfor Ukrainas grenser. Målet var å unngå at fysiske angrep mot sentral IT-infrastruktur i Ukraina gjorde kundedata eller tjenester utilgjengelig. Flere banker benyttet muligheten som en beredskap til den infrastrukturen de hadde i Ukraina. En slik migrering tar gjerne flere år, men ble i den alvorlige situasjonen gjennomført i løpet av kort tid.

Med krigen har cyberangrep mot bankene økt. Bankene har styrket sin motstandskraft mot cyberangrep slik at kritiske banktjenester holdes tilgjengelig.

Sammen med blant annet sentralbanken opprettet bankene et konsept kalt «Power Banking»[27], der kunder av alle banker kan benytte et stort antall utpekte bankkontorer over hele landet til å få utført blant annet betalingstjenester, uavhengig av hvilken bankforbindelse kunden har. De utpekte bankkontorene har forsterket beredskap blant annet for strøm, kommunikasjon, kontanter og personell. Gjennom den forsterkede beredskapen for strøm og kommunikasjon som disse bankkontorene leverer, har dette også blitt samlingspunkter for befolkningen for blant annet å få ladet mobiltelefoner når strømmen er borte. Power Banking inkluderer per i dag rundt 2400 bankkontorer spredt over hele Ukraina.

[26] Se for eksempel https://nordicfintechmagazine.com/unbreakable-the-financial-frontline-of-a-nation-at-war/ og https://www.europeanpaymentscouncil.eu/news-insights/insight/payments-wartime-story-national-bank-ukraine

[27] Se https://power.bank.gov.ua/

4.7 USA

Sheltered Harbor ble stiftet i 2015 av en rekke virksomheter i finansiell sektor i USA og tilbød sertifisering av uavhengige datalagre og gjenopprettingsløsninger. Bakgrunnen for etableringen av Sheltered Harbor var erfaringene fra offentlige-private cybersikkerhetsøvelser (Hamilton Series), hvor det ble konkludert med at finanssektoren og den amerikanske økonomien er sårbar for at en eller flere finansinstitusjoner opplever et alvorlig cyberangrep der institusjonenes data eller systemer blir utilgjengelige. En slik hendelse kan få ringvirkninger også for institusjoner som ikke er direkte berørt av et angrep, ved at tilliten til sektoren som helhet utfordres.

Sheltered Harbor var en ikke-kommersiell organisasjon bestående av 30 medlemmer, som banker, meglerhus og leverandører. Sheltered Harbor hører organisatorisk til under Financial Services Information Sharing and Analysis Center (FS-ISAC). Selv om det var frivillig for amerikanske finansinstitusjoner å få en Sheltered Harbor sertifisering, befant likevel en betydelig del av bankinnskudd i USA seg i en institusjon med en slik sertifisering. I 2026 ble Sheltered Harbor lagt ned og alle dens eiendeler, inkludert dokumentasjon, ble overført til moder-organisasjonen FS-ISAC og vedlikeholdes av FS-ISACs Resilience Congress. Etter overføringen er rammeverket blitt gjort tilgjengelig for alle FS-ISAC sine medlemmer.

Sheltered Harbor består grunnleggende av tre elementer:

- **Datahvelv.** Data lagres i et sikkert datahvelv, der de beskyttes mot endring eller sletting, slik at data kan gjenskapes etter et angrep. Data skal være kryptert, uforanderlig og helt avskåret fra virksomhetens øvrige infrastruktur, inklusive back-up-systemer.
- **Gjenopprettingsplattform og -plan.** Virksomheten skal utarbeide forretningsmessige og tekniske prosesser som kan aktiveres, hvis virksomhetens kritiske systemer, inkludert back-up, feiler. Det skal være en alternativ midlertidig gjenopprettingsplattform, hvor data fra datahvelvet og tilhørende tjenester hurtigst mulig kan gjøres tilgjengelig for kunder.
- **Sertifisering.** Virksomhetene implementerer kontroller og løsninger som så underlegges uavhengig revisjon for å vurdere etterlevelse av Sheltered Harbor-standardene. Virksomhetene kan deretter bli tildelt en Sheltered Harbor-sertifisering. Validering av løsninger opp mot Sheltered Harbors standarder skjer minimum årlig.

I arbeidet med å etablere datalagring og gjenopprettingsløsninger må finansinstitusjonene identifisere kritiske forretningsfunksjoner for virksomheten (såkalte «minimum viable operations»). Beredskap som inngår i Sheltered Harbor-sertifiseringene er de funksjonene som foretakene har identifisert som mest kritiske. Tilnærmingen i Sheltered Harbor har likhetstrekk med tilnærmingen til europeiske myndigheter som kommer til uttrykk i DORA. I kjølvannet av dialog med en rekke finansinstitusjoner i EU, publiserte Sheltered Harbor i oktober 2025 en oppfordring til bruk av Sheltered Harbor-standardene for å oppfylle DORA. Her beskriver Sheltered Harbor også forskjellene mellom kravene og tilnærmingen i DORA og sertifiseringsstandardene til Sheltered Harbor.

5 Prosjektets vurderinger

5.1 Innledning

Mandatet til prosjektet er å konkretisere innrettingen på to tiltak foreslått av arbeidsgruppen for betalingsberedskap som kan bidra til at bankkunder får levert kritiske betalingstjenester også i mer alvorlige situasjoner, samt at kundenes kontoinformasjon er sikret selv om en banks løsninger og sikkerhetskopier gjøres utilgjengelig.[28] De to tiltakene prosjektet har vurdert er etablering av et felles uavhengig datalager og etablering av uavhengige beredskapsløsninger for kort- og kontoadministrasjon (henholdsvis tiltak T055 og T083 fra arbeidsgruppen for betalingsberedskap).

Prosjektets utredning må sees i sammenheng med de andre forslagene fra arbeidsgruppen for betalingsberedskap, hvor målet er at hele betalingssystemet skal bli mer motstandsdyktig. Bankenes systemer er en viktig komponent som må virke for at betalingsformidling skal fungere.

Prosjektet anbefaler å etablere et felles uavhengig datalager med informasjon om kunders innskudd. Formålet med datalageret er å være en beredskap for at innskuddsgarantien kan fungere også når en bank er teknisk utilgjengelig. Av den grunn foreslår prosjektet at datalageret forvaltes av Bankenes sikringsfond.

Etablering av uavhengig beredskapsløsninger for kort- og kontoadministrasjon kan i hovedsak gjøres enten i regi av bankene eller i regi av myndighetene. DORA stiller krav til at bankene skal identifisere hvilke tjenester de leverer som er kritiske og ha beredskap for at disse tjenestene kan leveres i ulike alvorlige scenarioer, som cyberangrep og fysiske angrep. Etterlevelse av DORA kan innebære etablering av uavhengige beredskapsløsninger for kort- og kontoadministrasjon. Prosjektet vurderer at det allerede eksisterer et regelverk for beredskap for kort- og kontoadministrasjon som bidrar til kontinuitet i bankers kritiske tjenester.

Prosjektet anbefaler ikke etablering av en felles uavhengig myndighetsløsning for kort- og kontoadministrasjon.

I dette kapitlet følger en nærmere beskrivelse av hovedalternativene for uavhengig datalager og uavhengige beredskapsløsninger for kort- og kontoadministrasjon, fordeler og ulemper ved de ulike tilnærmingene, samt en begrunnelse for prosjektets anbefalinger.

5.2 Målbilde

Beredskapsløsninger for betalingstjenester bør som minimum tilby en basis funksjonalitet som kundene er avhengig av for å kunne gjennomføre og motta betalinger. Eksempler på basisfunksjonalitet kan være:

- Kortbetalinger.
- Konto-til-konto betalinger med og uten KID (kontooverføringer).

[28] I betalingssystemet er det andre aktører enn banker som også må fungere for at betalinger skal kunne gjennomføres. Det inkluderer avregning- og oppgjør, samt autorisering av kortbetalinger. Denne rapporten konsentrerer seg utelukkende om bankenes løsninger, og det er andre initiativer som vil styrke beredskapen i andre deler av betalingssystemet.

- Enkelt nettbank- og/eller mobilapp-grensesnitt med oversikt over oppdaterte kontobeholdninger og lån.
- Kortinnløsning (for å gi brukersteder oppgjør for solgte varer og tjenester).
- Filbaserte betalings- og rapporteringsløsninger for virksomheter (private og/ eller offentlige).

Målet er at kritiske betalingstjenester kan holdes tilgjengelige også i svært alvorlige situasjoner, som ved avanserte cyberangrep, angrep ved bruk av innsidere eller fysiske angrep.

5.3 Nærmere beskrivelse av relevante tilnærminger

5.3.1 Felles datalager med kundeinformasjon og rapporteringsplikt

Etablering av et felles datalager med tilhørende rapporteringsplikt for berørte banker innebærer at bankene jevnlig rapporterer relevant informasjon til et datalager hvor myndighetene eller en annen sentral aktør står som eier og operatør av datalageret.[29] Et slikt datalager kan innrettes helt uavhengig av bankenes systemer, personell og leverandørkjede.

Hva som er relevant informasjon avhenger av hva formålet med lagringen er, og jo mer komplekse tjenester datalageret skal være beredskap for, desto mer kompleks vil rapporteringen til og bruken av datalageret være.

Dersom formålet for eksempel er å sikre at en rammet bank kan bruke informasjonen i datalageret til å *gjenopprette* sine tjenester, må datalageret inneholde all nødvendig informasjon som gjør banken i stand til å tilby betalingstjenester i en situasjon der bankens systemer og data er utilgjengelige. Det inkluderer informasjon om bankens kunder (som saldo), bankens egne innskudd/investeringer og gjeld, sikkerhetskopier av nødvendige applikasjoner og beskrivelser av hvordan bankenes logiske infrastruktur og tjenester er konfigurert. Et slikt datalager vil ha unik rapportering fra ulike banker, da bankenes systemer er forskjellige, med blant annet ulike formater, informasjonsstrukturer, -elementer og applikasjoner. I et alvorlig angrep der bankenes data- og betalingstjenester er utilgjengelige, kan også underliggende applikasjoner og infrastruktur som bruker dataene være det. Datalageret må derfor inneholde informasjon og applikasjonskopier, som gjør at banken kan gjenopprette kritiske tjenester. Rapportering av kun saldoinformasjon er i en slik situasjon utilstrekkelig for å gjenopprette en banks tjenester.

Dersom formålet er å legge til rette for at kunder kan få levert banktjenester av *en annen bank,* kan det at bankene regelmessig rapporterer kunde- og innskuddsinformasjon til datalageret forenkle et slikt bankbytte. Verdien av et slikt datalager vil først og fremst være bedre beredskap for at innskuddsgarantiordningen kan fylle sin funksjon også i situasjoner der en bank for eksempel har tapt nødvendige data om kundenes innskudd og ikke får gjenopprettet egne tjenester, til tross for at banken har etablert løsninger i tråd med DORA. Et slikt datalager kan bygge på en felles rapporteringsstandard, for eksempel den som Bankenes sikringsfond allerede har etablert for innskuddsgarantiordningen. Det kan tilsi at datalageret kobles til forvaltningen av innskuddsgarantiordningen.

[29] Som omtalt i kapittel 2.3 innebærer forsterkede beredskapsløsninger i regi av den enkelte bank også uavhengig datalagring, men da skjer dette hos den enkelte bank. En forskjell er altså at det i et felles datalager rapporteres informasjon til et samlet sted for alle bankene.

Et datalager med rapportering av kunde- og innskuddsdata som er ensartet for alle rapporteringspliktige banker, vil være forholdsvis ukomplisert å håndtere både for bankene og for den som skal eie og drifte løsningen. Dersom informasjonen i datalageret må anvendes til å overføre kundenes innskudd, forutsetter det at kunden har konto i en annen fungerende bank, eller at andre fungerende banker har kapasitet til å ta imot kunder fra en eller flere banker med alvorlige driftsproblemer. I normalsituasjoner har banker i dag kapasitet til å drifte sine tjenester selv med en betydelig økning i antall kunder. Det finnes likevel tjenester som bankene vil ha utfordringer med å skalere opp på kort sikt, særlig hvis en større kundegruppe må etablere kundeforhold i nye banker. For eksempel er ikke en banks kundesentre bemannet for å håndtere en sterk økning i antall kunder, og banker har heller ikke store lagre av fysiske plastkort for å produsere betalingskort til en større gruppe nye kunder. Det vil være et problem spesielt for ikke-digitale kunder at det vil ta tid å lage nye fysiske kort som så skal fraktes med posten. Digitale kort kan derimot utstedes raskt.

Bruken av data i datalageret vil kreve en opprydningsjobb i etterkant. Midlene som utbetales til kundene gjennom innskuddsgarantiordningen vil trolig basere seg på eldre saldoinformasjon som ikke hensyntar betalinger autorisert gjennom STIP eller betalinger gjennomført etter data er levert til Bankenes sikringsfond og før banken ble utilgjengelig.

5.3.2 Uavhengig beredskapsløsning og datalagring i regi av den enkelte bank

Uavhengige beredskapsløsninger for kort- og kontoadministrasjon skal sikre at en bank har alternative systemer som ikke er avhengige av bankens primære IT-løsninger, og som kan tilby bank- og betalingstjenester til bankens kunder dersom ordinære systemløsninger blir utilgjengelige og det tar tid å gjenopprette normal drift. De uavhengige beredskapsløsningene skal tilby de viktigste tjenestene bankens kunder er avhengig av, mens banken parallelt arbeider med en full gjenoppretting av alle sine tjenester.

Uavhengige beredskapsløsninger i regi av den enkelte bank gjør banken også i stand til å styre egen likviditet. Likviditetsstyring er nødvendig for at banken kan gjøre opp både sine kunders betalinger og egne handler med for eksempel andre banker.

Beredskapsløsningene kan være uavhengige fra de ordinære løsningene langs ulike dimensjoner. De kan være fysisk og logisk atskilt fra bankens øvrige infrastruktur. Det kan for eksempel gjelde systemer, personell eller leverandørkjeder. Hvor stor grad av uavhengighet en bank velger for eventuelle uavhengige beredskapsløsninger, må vurderes i henhold til bankens risikovurdering.

Beredskapsløsningene kan driftes på bankens allerede etablerte datasentre, eller de kan driftes på en fysisk infrastruktur som ikke er en del av bankens ordinære systemløsninger (verken primære eller sekundære datasentre). En løsning som bygger på en uavhengig fysisk infrastruktur vil gi et ytterligere vern mot fysiske hendelser, men vil også være vesentlig dyrere å etablere.

Et sentralt element i slike løsninger er graden av uavhengighet i datalagring. Typiske egenskaper ved datalagring er at dataene som lagres ikke kan endres, at datalageret er helt isolert fra infrastrukturen som banken benytter i det daglige, og at det er frakoblet all kommunikasjon. Hvilke bank- og betalingsfunksjoner som skal opprettholdes gjennom beredskapsløsningene, danner grunnlag for hvilke data bankene lagrer i uavhengige datalagre. Slik datalagring vil typisk inkludere både kundedata og nødvendig metadata om hvordan funksjonene og underliggende infrastruktur skal gjenoppbygges.

En beredskapsløsning i regi av enkeltbanker må kunne gjenopprette kritiske tjenester etter svært alvorlige hendelser i løpet av relativt kort tid. Forventningene i for eksempel Sheltered Harbor er 24-36 timer.

5.3.3 Felles offentlig beredskapsløsning og datalager

En offentlig eid og forvaltet beredskapsløsning for kort- og kontoadministrasjon innebærer at myndighetene har en løsning som kan tilby grunnleggende bank- og betalingstjenester dersom en eller flere banker over tid ikke evner å gjenopprette tjenestene til egne kunder. En myndighetsløsning vil bestå av et uavhengig datalager med informasjon om blant annet kunders innskudd, samt inneholde systemer som gjør myndighetene i stand til å levere betalingstjenester. Prosjektet vurderer at en slik løsning sannsynligvis ikke vil komme i konflikt med DORA fordi myndighetene påtar seg å etablere beredskapsløsningen.

En uavhengig beredskapsløsning bygger på data rapportert av bankene til et offentlig uavhengig datalager. Grunnen til at det er mest hensiktsmessig at datalageret for bruk i en slik beredskapsløsning er eid av det offentlige, er at rapporteringen til datalageret må være kompatibelt med bruk i den offentlige uavhengige beredskapsløsningen. En slik rapportering vil bygge på en felles rapporteringsstandard. Rapporteringen bør skje ofte nok til at informasjonen er mest mulig oppdatert dersom løsningen må aktiveres, som for eksempel hver virkedag. De rapporterte innskuddssaldoene vil være utgangspunktet for videre kreditering og debitering av kundenes kontoer ved aktivering av løsningen. Prosjektet antar at myndighetene vil måtte være ansvarlig for føringene som gjøres på kundenes kontoer mens løsningen er i bruk.

En offentlig beredskapsløsning kan etableres enten ved at myndighetene bygger videre på eksisterende løsninger for kontoadministrasjon og betalingsformidling som brukes av banker i det norske markedet i dag, eller baseres på en helt annen programvare (for eksempel åpen kildekode). Begge alternativene er teknisk krevende og vil medføre betydelige utviklings- og driftskostnader. For eksempel vil en løsning basert på åpen kildekode kreve omfattende tilpasninger til det norske betalingssystemet for å fungere. En beredskapsløsning som bygger videre på eksisterende programvare er trolig rimeligere å etablere og vedlikeholde, men en slik løsning kan være eksponert for den samme hendelsen som gjør en banks tjenester utilgjengelig.

Uansett hvordan løsningen etableres, må den vedlikeholdes og tilpasses løpende endringer i resten av betalingsinfrastrukturen, slik som nye standarder eller formater for betalinger eller omlegginger og moderniseringer i resten av infrastrukturen.

En offentlig beredskapsløsning må betjene både privatkunder og bedriftskunder for at befolkningen skal kunne handle varer og tjenester, betale regninger, få utbetalt lønn og for at bedrifter skal få oppgjør for varer og tjenester de selger. Kompleksiteten i betalingsformidling, særlig for bedriftsmarkedet og statlige virksomheter er et argument mot etablering av en offentlig beredskapsløsning. Å legge til rette for betalingsformidling for bedriftskunder krever omfattende rapportering. Det må blant annet eksistere oppdaterte oversikter over fullmakter og rettigheter til å disponere en bedrifts konto. Fordi bedrifter har store inn- og utbetalinger, vil feilføringer for bedrifter kunne få store konsekvenser for myndighetene som operatør.

En bank som over tid ikke har IT-systemer tilgjengelig, vil trolig være ute av stand til å styre egen likviditet. Det er rimelig å anta at det vil gå noe tid fra en hendelse rammer en bank før myndighetene

vil beslutte å ta i bruk en offentlig beredskapsløsning. Det er derfor en reell risiko for at banken ikke lenger er likvid når den offentlige løsningen skal tas i bruk, eller at banken mister sin likviditet etter at løsningen tas i bruk, for eksempel ved at kundene benytter muligheten til å flytte sine innskudd til en annen bank. Hvis en myndighetsløsning skal sikre betalingstjenester til bankens kunder på vegne av banken, må løsningen også inneholde en mulighet for at den enkelte bank kan drive likviditetsstyring og ha dekning for egne og kunders betalinger. Dette vil øke kompleksiteten i løsningen ytterligere og utvide hvilke data som vil måtte rapporteres til datalageret. Et alternativ til en slik funksjon er at myndighetene tilfører banken nødvendig likviditet.

En utfordring med å bokføre betalinger på vegne av bankens kunder i et myndighetssystem er at den berørte banken i etterkant må oppdatere egne systemer med betalinger gjennomført i myndighetenes beredskapsløsning. Prosjektet vurderer at langvarig bruk av en myndighetsbasert løsning for betalingstjenester kan ha konsekvenser for bankens evne til å gjenoppta normal drift. Overgangen tilbake til ordinære banktjenester bør derfor vurderes nøye som en del av beredskaps- og robusthetsplanleggingen i en eventuell myndighetsbasert løsning.

5.4 Prosjektets anbefaling

5.4.1 Rapportering til myndighetseiet datalager

Prosjektet anbefaler at banker som er medlem i den norske innskuddsgarantiordningen får plikt til å rapportere kundeinnskudd til et felles datalager som eies av myndighetene. Et slikt datalager vil ikke gjøre den enkelte bank i stand til å tilby bank- og betalingstjenester, men kan gi en trygghet for at informasjon om kundenes innskudd ikke går tapt selv om den enkelte bank skulle oppleve en hendelse som medfører at tjenester og data gjøres utilgjengelig eller integriteten i data er brutt.

Rapportering til et slikt datalager innebærer en beredskap for at innskuddsgarantien kan virke i situasjoner der den ikke vil fungere i dag på grunn av manglende data for tilgjengeliggjøring. Det eksisterende rammeverket for håndtering av kriser i banker legger til grunn at bankens systemer fungerer tilfredsstillende og at en krise kan løses gjennom bruk av finansielle verktøy eller at banken kan avvikles.

Uavhengig av om banken er planlagt krisehåndtert eller avviklet, bør informasjonen om kunders innskudd være rapporteringspliktig for banken. Også innskudd i banker som planlegges krisehåndtert er dekket av innskuddsgarantien, og også disse bankene kan, dersom forholdene tilsier det, bli avviklet under offentlig administrasjon.

Gjennom eksistensen av et felles datalager vil myndighetene og bankene kunne kommunisere til kundene at innskuddene er trygge også i en situasjon der banken har mistet tilgang til eller kontroll på data. En slik rapportering vil bare være en beredskap for kunder i banker som er omfattet av den norske innskuddsgarantiordningen (som forvaltes av Bankenes sikringsfond). Dette er alle norske banker, samt bankfilialer fra EØS som er frivillige medlemmer. Kunder som har innskudd i utenlandske bankfilialer som ikke er frivillige medlemmer i den norske innskuddsgarantiordningen eller som har innskudd i bank som driver grensekryssende virksomhet i Norge, vil falle utenfor.

Fordi prosjektet foreslår å knytte datalageret til innskuddsgarantien foreslår prosjektet å legge ansvaret for datalageret til Bankenes sikringsfond. Det vil være kostnadseffektivt at Bankenes sikringsfond får det ansvaret, siden de allerede har etablert et felles format for rapportering av denne

type informasjon og en teknisk løsning som testes jevnlig med bankene (se omtale i kapittel 3.4). Det er denne rapporteringen som foreslås innført med en regelmessig rapporteringsfrekvens.

Norske innskytere har betydelig innskudd i nordiske filialer. Norske innskytere i filialer av utenlandske EU/EØS-banker som er medlem av den norske innskuddsgarantiordningen, er dekket av beløp opp til 100.000 euro av innskuddsgarantiordningen i hjemlandet til banken. Utbetaling av denne dekningen skal etter finansforetaksloven § 19-8 andre ledd foretas av Bankenes sikringsfond på vegne av hjemlandets ordning i samsvar med instrukser og finansiering derfra.

Det er bare beløp over 100.000 euro som dekkes av filialmedlemsskapet i den norske innskuddsgarantiordningen. Dersom et filialmedlem opplever en situasjon der informasjon om innskudd blir utilgjengelig, vil det i utgangspunktet være hjemlandets myndigheter som eventuelt må beslutte at kunder skal få tilgjengeliggjort garanterte innskudd. Adgangen til å beslutte at en filial etablert i Norge av utenlandsk foretak skal krisehåndteres eller avvikles under offentlig administrasjon, er begrenset til tilfeller hvor hensynet til finansiell stabilitet og andre hensyn som skal ivaretas etter finanslovgivningen tilsier det. I slike ekstraordinære situasjoner vil innskuddene anses utilgjengelige som følge av norske myndigheters beslutning, jamfør finansforetaksloven § 20-49. Det er videre gitt enkelte bestemmelser om administrasjons – eller konkurssituasjon hos filialmedlemmet i finansforetaksforskriften § 19-6. Gjennomføring av en løsning som også omfatter en filial, forutsetter antagelig involvering av filialenes hjemstatsmyndigheter. Prosjektet har ikke vurdert dette nærmere.

Data som rapporteres til et datalager kan være manipulert før de blir rapportert. For å gi økt trygghet for at kunder får utbetalt et korrekt beløp, kan det være nødvendig å lagre data i en viss periode. Samtidig er ikke formålet med det foreslåtte datalageret å være et arkiv for å sikre korrekthet i bankenes data. Retting av feil i data kan videre komme i konflikt med at kunder nokså raskt får tilgjengeliggjort betalingsmidler. Lagring av data i en viss periode skal ikke overta ansvaret bankene har til å sikre korrekthet i kundedata. Integritetskontroller er en del av bankenes løpende ansvar og ansvaret med å påse at den rapporterte informasjonen er korrekt bør ligge hos bankene.

Prosjektet legger til grunn at et datalager i regi av Bankenes sikringsfond for å ivareta innskuddsgarantien ikke vil komme i konflikt med DORA, siden et slikt datalager skal ivareta et annet formål enn DORA.

Etablering av et datalager i regi av Bankenes sikringsfond innebærer en konsentrasjonsrisiko og innføring av en ny sårbarhet. Databrudd vil kunne ramme alle som er kunder i banker som er medlem i innskuddsgarantiordningen dersom innsamlede data kommer på avveie. På den andre siden vil samfunnet kunne bli mer motstandsdyktig mot ekstreme scenarioer som gjør banker utilgjengelig over en lengre periode. Kostnadene ved å etablere og vedlikeholde et slikt datalager er videre lavere enn andre vurderte alternativer. Prosjektet vurderer at gevinstene ved styrket beredskap veier tyngre enn risikoen ved å samle informasjonen om kundeinnskudd i ett og samme datalager og kostnadene ved å etablere og vedlikeholde datalageret.

Dersom Bankenes sikringsfond får ansvaret med å forvalte et slikt datalager, bør det arbeides videre med praktiske problemstillinger for at overføring av samlede kundeinnskudd fra en bank til en annen skal kunne skje så sømløst som mulig i en ekstremsituasjon, jamfør beskrivelsene i kapittel 5.3.1. Blant annet bør myndighetene arbeide videre med å legge planer for koordinering samt for kommunikasjon mot publikum, samt sammen med banker legge planer for hvordan slike mer omfattende situasjoner kan håndteres.

Et felles datalager ivaretar behovet for oppdatert oversikt over kundeinnskudd, slik at de kan gjøres tilgjengelige og at kunder dermed kan betale for seg i en situasjon hvor banken er operasjonelt utilgjengelig. I første omgang foreslår prosjektet at rapporteringen gjelder saldo på kundeinnskudd for både bedrifter og husholdninger. På et senere tidspunkt etter at datalageret er etablert, kan det vurderes om det er behov for å rapportere også annen informasjon, som mer detaljert utlånsinformasjon.

5.4.2 Bankenes ansvar for beredskapsløsninger

Prosjektet mener det må være et mål at bankene har tilstrekkelig motstandskraft til å kunne opprettholde kritiske kundetjenester også i mer alvorlige scenarioer.

DORA stiller krav til at bankene skal kunne forebygge, motstå, håndtere og gjenopprette tjenester også for mer alvorlige scenarioer som digitale og fysiske angrep. Etter DORA er det bankene som er ansvarlige for å identifisere hvilke tjenester de tilbyr som er kritiske og etablere løsninger som gir kontinuitet i disse tjenestene. Finanstilsynet har i sin tilsynspraksis lagt til grunn at det å sørge for at kunder kan gjennomføre betalinger er en viktig/kritisk tjeneste, blant annet basert på DSBs oversikt over samfunnets kritiske funksjoner. Det eksisterer derfor allerede et harmonisert regelverk som skal sørge for at bankene har løsninger som skal gi et høyt beskyttelsesnivå for bankens kunder når det gjelder gjennomføring av betalinger.

Bankene kan selv velge å etablere uavhengige datalagre eller uavhengige beredskapsløsninger for kort- og kontoadministrasjon, slik noen banker arbeider med, eller bankene kan etablere andre løsninger for å oppfylle kravene om kontinuitet i tjenestene etter DORA.

Finanstilsynet gir foretakene veiledning om DORA[30]. Finanstilsynet kan videre gi pålegg om retting hvis bankenes løsninger ikke er tilstrekkelige for å oppfylle kravene i DORA. I tillegg kan myndighetene kommunisere forventninger om egenskaper ved bankenes beredskapsløsninger, slik Finanstilsynet har gjort i *Risiko-og sårbarhetsanalyse 2026*. Bankene og myndighetene bør opprettholde samarbeid om beredskapsspørsmål gjennom etablerte fora som for eksempel Beredskapsutvalget for finansiell infrastruktur (BFI) og Beredskapsrådet for finansielle tjenester. Bankene kan også alene eller sammen med myndighetene etablere beste praksiser eller standarder for beredskapsløsninger, slik at målet om å opprettholde kundebetalinger i mer alvorlige scenarioer, blir ivaretatt.

Det er hjemstatsmyndighetene som har tilsynsansvaret for å følge opp bankfilialer og banker som driver grensekryssende virksomhet i Norge.

5.4.3 Myndighetsløsning for kort- og kontoadministrasjon

Prosjektet anbefaler ikke etablering av en myndighetsløsning for kort- og kontoadministrasjon.

En myndighetsløsning har den fordelen at den vil være helt uavhengig av bankenes systemer og personell.

Prosjektet har likevel kommet til at det ikke er hensiktsmessig å etablere en slik beredskapsløsning i regi av myndighetene i Norge fordi det er flere ulemper med en slik løsning. En felles beredskapsløsning i regi av myndighetene for drift av bankers tjenester som potensielt skal kunne betjene enhver banks kunder vil være både kostbar og kompleks å etablere og vedlikeholde. I tillegg

[30] Jf. https://www.finanstilsynet.no/tema/dora/

vil en slik løsning ha en senere aktivering og dermed gjenoppretting av kritiske tjenester enn beredskapsløsninger i bankenes regi og vil innebære en krevende synkronisering av betalinger mellom myndighetens og bankens systemer i etterkant. Ved en myndighetsløsning antar prosjektet at ansvaret for å levere banktjenester til bankens kunder vil overføres fra banken til myndighetene, som dermed også må bære risikoen for eventuelle feilføringer. Etter prosjektets vurdering er løsninger i regi av enkeltbanker eller en sammenslutning av banker en mer hensiktsmessig måte å skape trygghet for at kritiske banktjenester kan fungere i alvorlige scenarioer. Erfaringene fra Ukraina viser i tillegg at slike myndighetsløsninger ikke er nødvendig for at betalinger skal fungere, selv i en situasjon med fullskala krig.

Valget om å etablere en offentlig beredskapsløsning i Finland, som omtalt i kapittel 4.3, ble delvis begrunnet i at sentral infrastruktur som banker i Finland var avhengige av, lå utenfor landet. Dette gjorde Finland særlig sårbare for eksempel ved brudd i kommunikasjonslinjer til utlandet. I Norge er dette i mindre grad en sårbarhet, fordi man i større grad har infrastruktur nasjonalt.

En myndighetsløsning vil heller ikke ivareta nærhetsprinsippet, altså at den som har ansvar i normalsituasjonen også er den som har ansvaret i en krisesituasjon. Hvis beredskapen for de mest alvorlige scenarioene er en del av det generelle arbeidet med beredskap, er det også større sjanse for at hendelsene effektivt blir håndtert, enn om slike scenarioer skal håndteres av løsninger som ikke brukes i det daglige.

6 Rapportering til Bankenes sikringsfond

6.1 Nærmere om rapporteringen til Bankenes sikringsfond

Prosjektet anbefaler en plikt for bankene til regelmessig å rapportere kundedata til Bankenes sikringsfond.

Etablering og drift av et datalager bør basere seg på Bankenes sikringsfonds eksisterende rapporteringsløsning for garanterte innskudd, som Bankenes sikringsfond i dag benytter til å innhente kundelister både for testing og analyse samt for tilgjengeliggjøring av garanterte innskudd dersom en bank blir avviklet under offentlig administrasjon.

Anbefalingen innebærer at medlemmene av Bankenes sikringsfond[31] skal rapportere kundedata regelmessig til Bankenes sikringsfond, og at rapporterte data blir lagret i Bankenes sikringsfond over en viss tid. En slik bruk stiller strengere krav til sikkerheten til datalageret hos Bankenes sikringsfond enn dagens løsning.

Etablering av et datalager med denne plikten forutsetter endring av finansforetaksloven, lov om Bankenes sikringsfond, samt en forskriftshjemmel for Finansdepartementet til nærmere bestemmelser om datalageret og forvaltningen av dette.

Hvor ofte det bør rapporteres data til Bankenes sikringsfond og hvor lenge de rapporterte dataene bør være lagret, vil være en avveining mellom hensynet til å ha tilgjengelig oppdaterte data og en viss historikk i rapporterte data for det tilfelle at rapporterte filer er korrupte, og hensynet til personvern og kostnader for bankene og Bankenes sikringsfond. Det er en fordel at dataene er mest mulig oppdaterte dersom de må tas i bruk i en krisesituasjon hvor banken er utilgjengelig. Det tilsier en hyppig rapportering som for eksempel hver virkedag. Rapporterte data kan slettes automatisk etter et fastsatt tidsintervall som for eksempel 14 dager, med mindre det foreligger særskilte forhold som tilsier at dataene bør lagres i en lengre periode. Slik prosjektet vurderer det, vil det være naturlig å vurdere dette og andre utestående spørsmål nærmere i et forskriftsarbeid.

Forslaget innebærer at omfattende mengder persondata vil lagres i datalageret. Lov om Bankenes sikringsfond § 1 fjerde ledd stiller krav til at virksomheten i Bankenes sikringsfond skal organiseres og drives på en forsvarlig måte. Dette knytter seg til både styrings- og kontrollsystemer og kvalifikasjoner og erfaring blant de ansatte. Forretningsføreren i Bankenes sikringsfond (nå administrerende direktør) skal sørge for at det blir fastsatt instrukser som angir de ansattes arbeidsoppgaver og ansvarsforhold, samt rapporterings- og saksbehandlingsregler.

Etableringen av et datalager som foreslått innebærer samtidig en konsentrasjonsrisiko som kan medføre at datalageret bør være underlagt strenge krav til sikkerhet. Det kan derfor være behov for å stille supplerende krav til datalageret og forvaltningen av det, herunder om sikkerhet. Prosjektet foreslår derfor en forskriftshjemmel for departementet til å fastsette nærmere regler, blant annet om dette.

[31] Liste over medlemmer og filialmedlemmer finnes på https://www.bankenessikringsfond.no/om-oss/medlemmer/

Regjeringen har satt ned et utvalg som skal utrede behovet for endringer i regelverket om bankkrisehåndtering og innskuddsgaranti, blant annet for å gjennomføre CMDI-regelverket.[32] Utvalget skal vurdere behovet for endringer i organiseringen og eventuelt finansieringen av myndighets- og forvaltningsoppgaver, herunder også eventuelle endringer i Bankenes sikringsfonds forvaltningsrettslige organisering. Utvalgets vurderinger kan få konsekvenser for prosjektets forslag om å legge forvaltningen av et datalager til Bankenes sikringsfond.

6.2 EØS-regelverk og hvem som kan omfattes av rapporteringsplikt

Innskuddsgarantidirektivet inneholder verken et krav til eller et forbud mot at innskuddsgarantiordningen på regelmessig basis samler inn og tar vare på informasjon om innskuddene fra bankens kunder. Løpende rapportering til Bankenes sikringsfond vil kunne bidra til å oppfylle innskuddsgarantiordningens lovpålagte mandat på en mer effektiv måte. Dette for eksempel dersom en bank avvikles under offentlig administrasjon som følge av en alvorlig cyberhendelse.

Banker som er hjemmehørende i Norge er etter innskuddsgarantidirektivet pålagt å være medlem i den norske innskuddsgarantiordningen. Innskuddsgarantidirektivet stiller ikke krav til medlemskap i den norske innskuddsgarantiordningen for filialer av utenlandske banker som opererer i Norge. Norge tilbyr imidlertid frivillig medlemskap (såkalt topping-up) for EØS-filialer for å dekke differansen mellom hjemlandets dekning på 100.000 euro og to millioner norske kroner. På det nåværende tidspunkt har den norske innskuddsgarantiordningen 12 topping-up medlemmer.

Banker som er frivillige medlemmer i den norske innskuddsgarantiordningen har allerede i dag en plikt til på forespørsel å rapportere kundedata til Bankenes sikringsfond etter finansforetaksloven § 19-14, jamfør § 19-2. Disse bankfilialene har allerede etablert prosesser for å kunne levere kundedata til Bankenes sikringsfond, jamfør innskuddsgarantiforskriften § 3.

Slik prosjektet vurderer det, vil det ikke være i strid med EØS-avtalen artikkel 31 om etableringshindringer å pålegge topping-up-medlemmer i innskuddsgarantiordningen en rapporteringsplikt til datalageret. Dette skyldes at det er frivillig for en filial av en EØS-kredittinstitusjon å være topping-up-medlem i den norske innskuddsgarantiordningen. Dersom dekningsnivået til den norske innskuddsgarantiordningen i fremtiden skulle bli harmonisert med det som gjelder i EU, vil det ikke lenger være behov for topping-up-medlemskap, og det bør da i tilfelle vurderes å etablere andre løsninger for rapporteringsplikt for norske filialer av EØS-kredittinstitusjoner.

6.3 Generelt om taushetsplikt og personvern ved et uavhengig datalager i regi av Bankenes sikringsfond

Prosjektets anbefaling om et datalager administrert av Bankenes sikringsfond for de banker det gjelder, vil innebære at store mengder kundedata vil bli lagret hos Bankenes sikringsfond. Dette kan reise spørsmål om taushetsplikt og personvern.

[32] https://www.regjeringen.no/no/aktuelt/utvalg-skal-utrede-endringer-i-regelverket-om-bankkrisehandtering-og-innskuddsgaranti/id3153151/

Finansforetakene har taushetsplikt om kunders og andres forhold som de får kjennskap til i forbindelse med utførelsen av virksomheten. Unntak fra taushetsplikten krever enten samtykke eller rettsgrunnlag. Et slikt rettsgrunnlag kan være lovbestemt opplysningsplikt.

Norske banker og filialer av utenlandske banker som har frivillig medlemskap i innskuddsgarantiordningen har opplysningsplikt overfor Bankenes sikringsfond etter finansforetaksloven § 19-14, og taushetspliktbestemmelsene er således ikke til hinder for rapportering til et uavhengig datalager forvaltet av Bankenes sikringsfond.

Behandling av personopplysninger, slik som innsamling, registrering og lagring av personopplysninger, må oppfylle kravene i EUs personvernforordning (GDPR). Forordningen er gjennomført i norsk rett i personopplysningsloven.

Etter personvernforordningen art. 4 nr. 1 er personopplysninger definert som *«enhver opplysning om en identifisert eller identifiserbar fysisk person («den registrerte»)»*. Kundedata fra en bank er å anse som personopplysninger.

Behandlingen av personopplysningene er bare lovlig dersom behandlingen er i tråd med minst ett av personvernforordningens behandlingsgrunnlag. De mest relevante behandlingsgrunnlagene ved eventuell rapportering til et uavhengig datalager er artikkel 6 nr. 1 bokstav c og e.

Etter bokstav c må behandlingen være nødvendig for å oppfylle en rettslig forpliktelse som påhviler den behandlingsansvarlige. Etter bokstav e kreves det at behandlingen er nødvendig for å utføre en oppgave i allmennhetens interesse eller utøve offentlig myndighet som den behandlingsansvarlige er pålagt. Det følger av begge artiklene at det kreves et rettsgrunnlag fastsatt i lov eller med hjemmel i lov, som pålegger behandlingen av opplysningene for å oppnå et bestemt formål. Dette fremgår også av artikkel 6 nr. 3.

Prinsippene for behandling av personopplysninger følger av artikkel 5, som blant annet innebærer at behandlingen skal være adekvat, relevant og begrenset til nødvendige opplysninger for å oppnå formålene opplysningene behandles for ("dataminimering"), jamfør artikkel 5 nr. 1 bokstav c.

Behandling av personopplysninger må utøves i samsvar med rettighetene som følger av den europeiske menneskerettighetskonvensjonen («EMK») artikkel 8 og Grunnloven § 102, som begge beskytter retten til et privatliv. Myndighetenes inngrep i denne retten krever lovhjemmel, og at inngrepet må være *"nødvendig i et demokratisk samfunn av hensyn til den nasjonale sikkerhet, offentlige trygghet eller landets økonomiske velferd, for å forebygge uorden eller kriminalitet, for å beskytte helse eller moral, eller for å beskytte andres rettigheter og friheter"*, jamfør. EMK artikkel 8 nr. 2. Inngrep må også være forholdsmessig.

Etter lov om Bankenes sikringsfond § 7 gjelder forvaltningsloven, herunder denne lovens bestemmelser om taushetsplikt, for Bankenes sikringsfond. Det fremkommer i tillegg i forskrift om Bankens sikringsfond § 2 andre ledd supplerende bestemmelser om taushetsplikt for styremedlemmer og ansatte i Bankens sikringsfond samt for sakkyndige som utfører oppdrag på vegne av Bankenes sikringsfond.

6.4 Vurdering av uavhengig datalagring og personvernhensyn

Etter prosjektets anbefaling skal banker rapportere kundedata, herunder kunders innskudd til Bankenes sikringsfond, på regelmessig basis. Bankenes sikringsfond skal oppbevare de rapporterte opplysningene i et datalager. Det legges i utgangspunktet opp til at dataene lagres i to uker og deretter slettes, men at dataene kan lagres lengre dersom det foreligger særlige forhold. Særlige forhold kan for eksempel være at en bank ikke har tilgang til sine kundedata på grunn av cyberangrep.

Formålet med rapporteringen er å ivareta innskuddsgarantiordningens lovbestemte oppgaver, herunder å sikre at informasjon om innskyternes beholdninger eksisterer og er tilgjengelig utenfor bankenes primære systemer i situasjoner der bankenes egne systemer over tid er utilgjengelige, for eksempel som følge av en alvorlig operasjonell hendelse.

Norske banker og frivillige filialmedlemmer i innskuddsgarantiordningen har allerede i dag plikt til å rapportere informasjon til Bankenes sikringsfond og innskuddsgarantiordningen etter finansforetaksloven og innskuddsgarantiforskriften. Dette omfatter innskuddsbeholdninger samt saldo utlån. Formålet med dagens rapportering er å teste kvaliteten i bankenes kundelister, herunder korrekthet, fullstendighet og struktur, slik at listene kan benyttes effektivt til å realisere innskuddsgarantiordningens formål, herunder ved en eventuell utbetaling av garanterte innskudd. Som et ledd i gjennomgangen av listene gjøres det også vurderinger av innskuddssammensetningen i opp mot operasjonalisering av utbetaling av garanterte innskudd. Dette kan for eksempel omfatte andel innskytere som er ikke-digitale og som må håndteres i mer manuelle løp.

Rapporteringen skjer i dag på forespørsel overfor den enkelte bank. Bankenes sikringsfond er lovpålagt å teste samtlige banker minst hvert tredje år. De innrapporterte kundelistene slettes etter testingen så snart testen er avsluttet og resultatet er kommunisert tilbake til banken.

Prosjektets anbefaling vil innebære at svært store mengder kundeinformasjon vil være lagret hos Bankenes sikringsfond til enhver tid. Dette representerer en endring i omfang og hyppighet av rapportering, men ikke i hvilke typer personopplysninger som behandles.

De lagrede datasettene vil hovedsakelig ligge urørt, men kan for eksempel benyttes til testing av datakvaliteten, tilsvarende de testene Bankenes sikringsfond allerede gjennomfører i dag. Innskuddslistene vil også benyttes i forbindelse med tilgjengeliggjøring av garanterte innskudd i forbindelse med avvikling av en bank under offentlig administrasjon.

Bankenes sikringsfond er behandlingsansvarlig for de datapunktene som i dag innrapporteres etter innskuddsgarantiforskriften, jamfør Personvernforordningen artikkel 4 nr. 7, ettersom behandlingen skjer som ledd i Bankenes sikringsfonds lovpålagte oppgaver. Bankenes sikringsfond har utpekt et personvernombud som er registret hos Datatilsynet.

Prosjektets anbefaling innebærer at Bankenes sikringsfond fortsatt er behandlingsansvarlig for de rapporterte dataene. At Bankenes sikringsfond er behandlingsansvarlig, kombinert med en rapporteringsplikt i lovs form, innebærer også at bankene ikke har videre ansvar for de rapporterte dataene etter at de er avgitt.

Det kan reises personvernmessige spørsmål rundt at en stor mengde oppdaterte personopplysninger om nær alle bankkunder i Norge overføres og lagres i et sentralt lager kontrollert av én behandlingsansvarlig. Prosjektet har drøftet andre mulige måter å håndtere denne behandlingen på,

herunder å juridisk definere overføringen og lagringen som en form for deponering, der bankene forblir behandlingsansvarlig for personopplysningene og Bankenes sikringsfond opptrer som databehandler på vegne av medlemmene inntil det eventuelt blir nødvendig å benytte opplysningene i registeret.

Den tekniske løsningen for rapporteringen vil i seg selv trolig ikke være særlig forskjellig enten Bankenes sikringsfond opptrer som behandlingsansvarlig eller databehandler. Fordi den anbefalte overføringen og lagringen av data i datalageret har et stort omfang og kan oppfattes å være av en annen karakter enn oppgavene Bankenes sikringsfond hittil har ivaretatt, vil prosjektet nevne dette som en mulighet dersom det av personvernmessige eller andre hensyn er ønskelig med en annen juridisk konstruksjon rundt datalageret.

Prosjektet har imidlertid vurdert at en eventuell konstruksjon med Bankenes sikringsfond som databehandler på vegne av bankene reiser en del spørsmål av prinsipiell, juridisk og praktisk art.

Den prinsipielle dimensjonen ligger i at en slik modell avviker fra den normale modellen ved lovpålagt rapportering til det offentlige og at modellen avviker fra grunnstrukturen i prosjektets anbefaling med å bygge videre på den eksisterende rapportering til Bankenes sikringsfond.

Fra et juridisk perspektiv vil alternativet innebære at Bankenes sikringsfond vil være en tjenesteleverandør og databehandler for medlemmer i innskuddsgarantiordningen, noe som ligger utenfor Bankenes sikringsfonds nåværende mandat. Dette alternativet vil også kunne reise spørsmål opp mot DORA ved at det i lovs form stilles nasjonale krav til hvorledes banken skal sikre overholdelse av krav i denne forordningen.

Fra en rent praktisk synsvinkel vil alternativet med at Bankenes sikringsfond er databehandler for de avgivende bankene bety at Bankenes sikringsfond må inngå og overholde krav i databehandleravtaler med hver enkelt bank, samtidig som den avgivende bank er ansvarlig for eventuelle sikkerhetsbrudd knyttet til dataene som håndteres hos Bankenes sikringsfond. Dette er trolig ikke en hensiktsmessig ordning.

Prosjektet anbefaler derfor at Bankenes sikringsfond skal være behandlingsansvarlig for de rapporterte dataene.

Gitt at rapporteringsplikten fremkommer i lovs form, vil Bankenes sikringsfonds behandlingsgrunnlag for de rapporterte opplysningene være personvernforordningen artikkel 6 nr. 1 bokstav c og e, siden behandlingen er nødvendig både for å oppfylle en rettslig forpliktelse som påhviler Bankenes sikringsfond og for å utføre en oppgave i allmennhetens interesse eller utøve offentlig myndighet.

Det fremkommer etter personvernforordningen kapittel III at registrerte har rett til innsyn (artikkel 15), rett til retting (artikkel 16) og rett til sletting (artikkel 17) av personopplysninger registrert om dem. Disse rettighetene er imidlertid ikke absolutte, og kan begrenses gjennom lovgivning i samsvar med artikkel 23.

I forslaget til ny § 2 fjerde ledd i lov om Bankenes sikringsfond er de registrertes rettigheter etter personvernforordningen artikkel 15, 16 og 17 begrenset i lovs form. Begrunnelsen er at datalageret i realiteten er en sikkerhetskopi utfra beredskapsformål av de data som allerede er lagret i bankens systemer. Dersom kunden ønsker å utøve sine rettigheter etter personvernforordningen artikkel 15, 16 og 17, er det naturlig at dette gjøres overfor og håndteres av banken. Dersom det kreves retting

eller sletting overfor banken, vil dette automatisk også hensyntas ved neste oversendelse av data til det uavhengige datalageret. At rettingen og/eller slettingen ikke skjer simultant i datalageret medfører ikke noe uforholdsmessig inngrep i den registrertes personvern.

Det vil bli lagret betydelige mengder persondata i datalageret, og det vil stilles relativt store krav til datasikkerhet knyttet til datalageret. Samtidig begrunnes anbefalingen i at grunnleggende nasjonale interesser ivaretas i samsvar med den nasjonale sikkerhetsstrategien for Norge hvor det blant annet legges vekt på å gjøre samfunnet mer motstandsdyktig. Anbefalingen om datalagring hos Bankenes sikringsfond er nødvendig og forholdsmessig, både i et individperspektiv og i et samfunnsperspektiv.

7 Nordiske fellesløsninger

Mandatet ber prosjektet vurdere *«.. i hvilken grad det kan være grunnlag for å etablere nordiske fellesløsninger»*. Nordiske finansmarkeder er tett integrerte, og flere store nordiske banker opererer på tvers av landegrensene. Hensynet til samordning og effektivitet kan i teorien tilsi at nordiske fellesløsninger vil være hensiktsmessig. Jamfør gjennomgangen i kapittel 4, har nordiske land valgt noe ulike tilnærminger til innretningen på beredskapsarbeidet og valg av løsninger for beredskap i betalingssystemet.

Prosjektet ser ikke at det per i dag er hensiktsmessig å for eksempel anbefale at det etableres et felles nordisk datalager med informasjon om kundeinnskudd. Et nasjonalt datalager gir myndighetene et handlingsrom og valgmuligheter man ikke nødvendigvis får gjennom overnasjonale løsninger. Samtidig er det en utfordring at banker som er filialer i Norge ikke rapporterer tilsvarende informasjon til hjemlandets myndighet.

Det er heller ikke grunnlag for å anbefale en fellesnordisk offentlig beredskapsløsning for drift av kundebetalinger jamfør at det kun er Finland som har valgt en slik løsning, og at dette prosjektet heller ikke tilrår å etablere en slik løsning.

Banker som har aktivitet i alle eller flere nordiske land kan selv velge å etablere beredskapsløsninger for hele sin virksomhet, eller etablere løsninger for tjenestene de tilbyr i de enkelte landene, ut fra hva som er hensiktsmessig for sin organisering.

Prosjektet mener imidlertid det vil være en fordel med et godt samarbeid mellom nordiske myndigheter om sentrale beredskapsspørsmål, herunder hvordan DORA følges opp, slik at kravene og beredskapen mellom banker blir likest mulig.

8 Administrative og økonomiske konsekvenser

8.1 Innledning

Formålet med anbefalingen om rapportering til et myndighetseiet datalager er å ha en beredskap for at innskuddsgarantien kan virke i situasjoner der den ikke vil fungere i dag på grunn av manglende data. Et slikt datalager gir myndighetene et utvidet handlingsrom i svært alvorlige situasjoner. I tillegg vil myndighetene og bankene gjennom eksistensen av en slik løsning kunne kommunisere til kundene at innskuddene er trygge også i en situasjon der banken har mistet tilgang på data.

I dette kapitlet presenteres kostnader for anbefalingene om å etablere et uavhengig datalager som forvaltes av Bankenes sikringsfond og en plikt for bankene til å rapportere informasjon til dette datalageret. Prosjektet har ikke beregnet kostnadene for de ulike alternativer av uavhengig beredskap for kort- og kontoadministrasjon, verken i regi av bankene eller i regi av myndighetene.

8.2 Konsekvenser for bankene

Anbefalingen om at bankene på regelmessig basis må rapportere kundedata til Bankenes sikringsfond medfører en mer utstrakt rapportering enn etter gjeldende regelverk der rapportering skjer på forespørsel og det gjennomføres en test av hver enkelt bank minimum hvert tredje år.

Rapportering på regelmessig basis vil medføre ekstra kostnader for bankene når det gjelder etablering av automatiske rapporteringssystemer og drift av systemene.

Prosjektet har ikke innhentet eksakte kostnadsanslag. Gitt at løsningen baseres på samme formater og regler for uttrekk av data som benyttes for rapportering til Bankenes sikringsfond i dag, anslår prosjektet at kostnadene for næringen kan være i størrelsesorden 50-80 millioner kroner i investeringsutgifter og 10-25 millioner kroner i årlige drifts- og forvaltningskostnader.

8.3 Konsekvenser for myndighetene

Bankenes sikringsfond vil, med krav om utvidet rapportering av kundeinformasjon til Bankenes sikringsfond, ha behov for å bygge ut dagens rapporteringsløsning, både med hensyn til kapasitet, sikkerhet med videre.

Bankenes sikringsfond anslår at kostnaden med å bygge videre på dagens rapporteringsløsning for å etablere et uavhengig datalager vil være om lag 20 millioner kroner og at en slik oppgave vil gi Bankenes sikringsfond rundt 2-5 millioner kroner i økte årlige driftsutgifter.

Gitt at administrasjon av et uavhengig datalager blir en lovpålagt oppgave for innskuddsgarantiordningen, og at de rapporterte dataene kan benyttes til å gjennomføre Bankenes sikringsfonds lovpålagte oppgaver, vurderer prosjektet at kostnadene til etablering og drift for Bankenes sikringsfond kan dekkes av innskuddsgarantiordningen.

8.4 Konsekvenser for kundene

Hvis bankene rapporterer kundedata til Bankenes sikringsfond, vil kundene ha en økt trygghet for at ordningen med innskuddsgarantien kan gjennomføres. Dette vil gjelde for kunder av norske banker og

for kunder av utenlandske filialer som er frivillige medlemmer i den norske innskuddsgarantiordningen.

Prosjektets anbefaling vil innebære at store mengder kundeinformasjon vil være lagret hos Bankenes sikringsfond til enhver tid. Se nærmere omtale i kapittel 6.4.

9 Forslag til endringer i lov og forskrift

I

I lov 10. april 2015 nr. 17 om finansforetak og finanskonsern (finansforetaksloven) gjøres følgende endringer.

Ny § 19-14 tredje ledd skal lyde:

(3) *Medlemmer i innskuddsgarantiordningen har plikt til jevnlig å rapportere kundedata til et datalager som skal forvaltes av Bankenes sikringsfond. Finansdepartementet kan i forskrift gi nærmere bestemmelser om datalageret og forvaltningen av dette, herunder hvor lenge data skal oppbevares og krav til sikkerhet.*

Nåværende tredje til femte ledd blir fjerde til sjette ledd.

II

I lov 23. mars 2018 nr. 3 om Bankens sikringsfond gjøres følgende endringer.

Ny § 2 fjerde ledd skal lyde:

(4) Bankenes sikringsfond skal administrere og forvalte et datalager for sikker oppbevaring av kundedata til bruk for innskuddsgarantiordningens lovpålagte oppgaver. Bankenes sikringsfonds kostnader ved datalageret skal bæres av innskuddsgarantiordningen.

Bankenes sikringsfond skal være behandlingsansvarlig for datalageret. For behandlingen gjelder ikke retten til innsyn etter personvernforordningen artikkel 15, retten til retting etter artikkel 16 eller retten til sletting etter artikkel 17.

Bankens rapporterte data kan tilgjengeliggjøres for den aktuelle banken ved behov.