Gjennomgang av svikt i tekniske løsninger for elektronisk bekymringsmelding til barnevernet

Svar på oppdrag 4 A
tillegg 7 til tildelingsbrevet for 2023

Bufdir

Innhold

Sammendrag **3**

1. Innledning **12**
1.1 Oppdraget 12
1.2 Aktørene som har bidratt i utforming av rapporten 14

2. Kartlegging av feilens omfang **17**
2.1 Antallet kommuner og andel av barnebefolkning som er berørt 17
2.2 Antallet meldinger som ikke har kommet frem 20

3. Oppdagelse og retting av feilen **23**
3.1 Hvordan feilen ble oppdaget, varslet om og rettet? 23
3.2 Vurdering av arbeidet med rettingen 28
3.3 Kompenserende tiltak for meldinger som hadde gått tapt 29

4. Konsekvenser av feilen **31**
4.1 Vurdering av feilens langsiktige konsekvenser for berørte barn 31
4.2 Sammenheng mellom feilen og trenden med færre bekymringsmeldinger? 34
4.3 Økonomiske og administrative konsekvenser for kommunene 35

5. Årsaksforhold og forebygging av fremtidige feil **37**
5.1 Årsaker til feilen 37
5.2 Hvorfor tok det tid før feilen ble varslet om? 38
5.3 Hendelsesforløpets og tidligere risikovurderinger 40
5.4 Forebyggende tiltak 44
5.5 Sannsynlighet for at feilen kan gjenta seg 45

6. Læring av feilen **48**
6.1 Læringspunkter for kommunesektoren 48
6.2 Offentlige myndigheters rolle 50
6.3 Læringspunkter for systemleverandørene 54
6.4 Risiko- og sårbarhetsanalyser 56

7. Avsluttende refleksjoner fra Bufdir **59**

Vedlegg 1: Hvordan har kommunene blitt fulgt opp? Status på del B av oppdraget

Vedlegg 2: Oppsummering av spørreundersøkelse om kommunenes respons på teknisk feil i overføring av bekymringsmeldinger

Tabeller

Tabell 1. Antall bekymringsmeldinger sendt gjennom NPB per kvartal (fra oppstart 2020 til og med september 2023) 19
Tabell 2. Oversikt over avvik, basert på tilbakemeldinger fra kommunene 20
Tabell 3. Antall gjennomgåtte bekymringsmeldinger for utvalgte kommuner i løpet av siste halvår 2017-2022 35

Figurer

Figur 1. Tidsløp fra oppdagelse til retting 5
Figur 2. Konkrete spørsmål som besvares i rapporten, iht. oppdrag i tillegg 7 til tildelingsbrevet til Bufdir for 2023 om å granske feilens årsaker, omfang og konsekvenser 13
Figur 3. Forsendelser gjennom KS sine løsninger 18

Sammendrag

I mai 2023 ble det avdekket en teknisk feil som førte til at bekymringsmeldinger som ble sendt gjennom Nasjonal portal for bekymringsmelding (NPB) i noen tilfeller ikke ble registrert i fagsystemet Visma Familia, og dermed ikke fanget opp av den kommunale barnevernstjenesten. Feilkilden var i integrasjonen mellom fagsystemet Visma Familia, som driftes av den enkelte kommune, og Nasjonal portal for bekymringsmelding, som driftes av KS. Integrasjonen mellom Visma Familia og NPB har vært tilgjengelig for kommunene siden 25.09.20. Det varierer når den enkelte kommune har tatt integrasjonen i bruk, og lengden på perioden den enkelte kommune har vært sårbar for feilen vil derfor variere.

Denne rapporten gir en beskrivelse av feilens årsaker, omfang og konsekvenser. Rapporten er utarbeidet av Bufdir i samarbeid med KS, Visma, Statens helsetilsyn, Datatilsynet og Digitaliseringsdirektoratet. Hver aktør har bidratt med tekster under de temaene som er relevante for deres ansvarsområder, og hver aktør står ansvarlig for sine respektive bidrag. Bufdir står ansvarlig for sammendraget og avsluttende refleksjoner.

Omfang av feilen

Hovedpunkter

- En teknisk feil oppdaget i mai 2023 førte til at bekymringsmeldinger som ble sendt gjennom Nasjonal portal for bekymringsmelding i noen tilfeller ikke ble fanget opp av den kommunale barnevernstjenesten. Feilen har eksistert siden september 2020.
- 22 kommuner er berørt av feilen
- 63 bekymringsmeldinger er registrert tapt. Berørte kommuner har lyktes med å gjenfinne informasjon fra flere av meldingene, men ikke alle. Det totale omfanget av hendelsen (antall meldinger som er tapt uten at man har klart å gjenfinne informasjon) er ikke kjent.

22 kommuner (18 barnevernstjenester) har rapportert til Visma at de har blitt påvirket av feilen.[1] Omfanget samsvarer med funn i en spørreundersøkelse Bufdir sendte ut juni 2023.[2] 63 bekymringsmeldinger er registrert tapt.[3] Med tap mener vi at meldingen ikke ble lagret i fagsystemet Visma Familia som forventet. De fleste av tjenestene som er berørt har tapt én

[1] Alver, Asker, Bergen, Drammen, Fredrikstad, Kristiansand, Birkenes, Lillesand, Larvik, Modum, Moss, Nærøysund, Narvik, Nordre Follo, Oslo, Sandnes, Sarpsborg, Tromsø, Vestnes, Volda, Øvre Eiker og Åmli.

[2] Bufdir gjennomførte en spørreundersøkelse til kommunenes barnevernstjenester for å kartlegge hvor mange bekymringsmeldinger som manglet, hvordan kommunene eventuelt ellers var påvirket av feilen og hva kommunene var i ferd med å gjøre for å rette opp i eller forhindre feil. 166 barnevernstjenester svarte, noe som utgjør 68 prosent av landets tjenester. Se vedlegg 2.

[3] Innrapportering fra kommunene til Visma.

bekymringsmelding. Enkelte kommuner har tapt to eller tre bekymringsmeldinger. Barnevernstjenesten i Kristiansandregionen og i Bergen skiller seg ut med henholdsvis 12 og 24 bekymringsmeldinger som ikke ble lagret i fagsystemet.[4]

Berørte kommuner, Visma og KS har i samarbeid gjennomført tiltak for å gjenfinne informasjon fra tapte meldinger. Kommunene har lyktes i å gjenfinne informasjon fra flere meldinger, men ikke alle. Aktørene har ikke oversikt over hvor mange av de tapte meldingene kommunene har klart å gjenfinne informasjon om. Det er svært alvorlig at det finnes potensielt viktig informasjon om barn som lever under omsorgssvikt, som fortsatt ikke er kjent for barnevernstjenestene.

Oppdagelse og retting av feilen

Hovedpunkter

- Mai 2023 mottok Visma en supportsak fra Bergen kommune om at en bekymringsmelding ikke var kommet frem i fagsystemet Familia. Senere samme måned ble klart at feilen gjaldt flere saker, både i Bergen og andre kommuner.
- Visma bistod kommuner med installering av programvarerettelse og til gjennomgang av logger for å avdekke avvik.
- Kommunene har lyktes med å gjenfinne informasjon fra meldinger som var tapt, i hovedsak gjennom oppfordring til meldere om å ta kontakt for å sjekke at innsendte meldinger var mottatt.
- KS vurderer at avvikshåndteringen i kommuner har hatt effekt, men at det ikke har vært mulig å gjenfinne informasjon fra flesteparten av meldingene som ikke kom frem.

En ansatt i Bergen kommune tok kontakt med barnevernstjenesten i kommunen for å etterlyse svar på bekymringsmelding sendt 01.02.23 den 10.03.23. Visma mottok en supportsak fra Bergen kommune 08.05.23 om at en bekymringsmelding ikke var kommet frem i Familia. Det ble klart fra logger fra kommunen at lagring til databasen hadde feilet, selv om KS hadde fått melding fra systemet om at mottak av melding var vellykket.

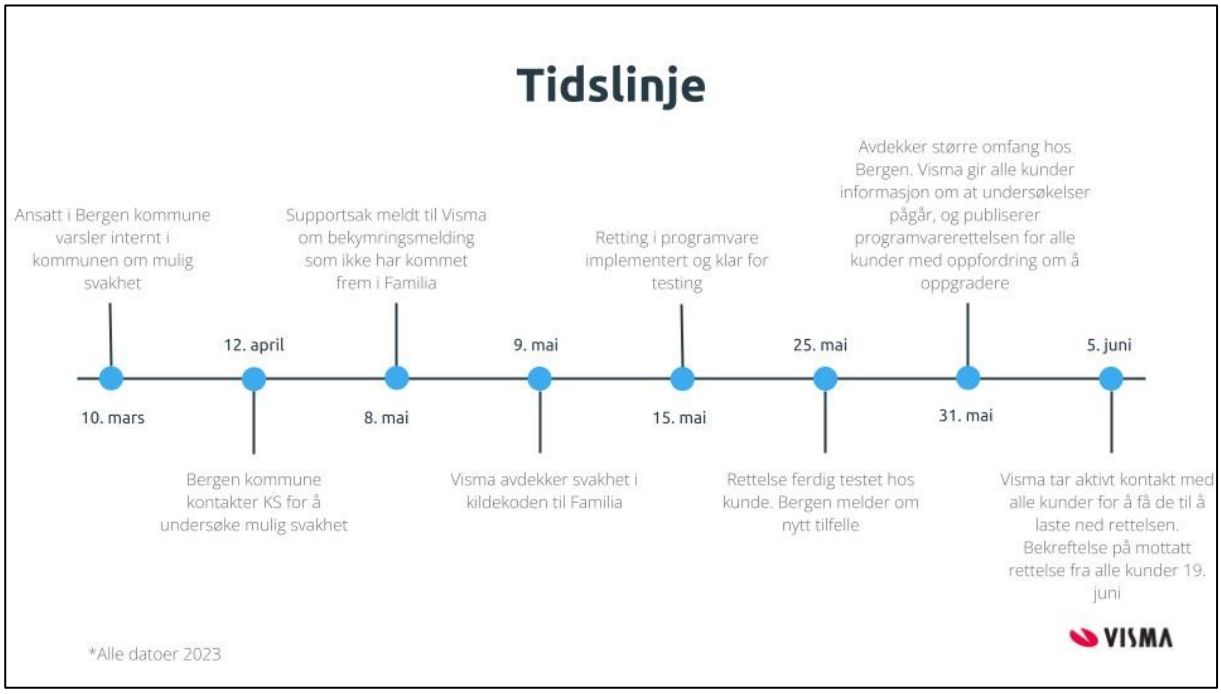
Avvikene har et sammensatt årsaksbilde. Visma beskriver at avvikene er utløst ved at lagring til kommunens database feilet, noe som har sammenheng med belastning på kommunens lokale infrastruktur i samspillet med Familia som applikasjon. Videre har mekanismen som skulle fange opp slike tilfeller i Familia ikke fungert som den skal grunnet en logisk brist i kildekoden i Familia. Dette medførte at i de tilfeller der lagring til databasen sviktet, ble ikke avsender gjort oppmerksom på at meldingen ikke var kommet frem til mottaker. Visma utviklet en programvarerettelse som sikrer at tilbakemelding om mottatt melding først blir sendt når lagring til databasen hos kommunen er vellykket. Meldinger som er sendt via NPB til fagsystemet blir

[4] Bufdirs spørreundersøkelse til kommunenes barneverntjenester i juni 2023. Se vedlegg 2.

mellomlagret i NPB i 14 dager før de blir slettet (senere utvidet til 30 dager når omfanget av feilen ble kjent). Dette medførte at tapte bekymringsmeldinger ikke kunne gjenopprettes etter at det hadde gått 14 dager fra avsendt melding.

Innledningsvis i saken jobbet aktørene ut fra en hypotese om at det sannsynligvis ikke fantes flere feil av samme art. I løpet av mai ble det klart at det var flere avvik i Bergen kommune. Visma gikk ut med programvarerettelse til alle kunder av Familia, for å forebygge at feil skulle oppstå i andre kommuner. Visma gjorde stikkprøver hos et utvalg kommuner som delte sine logger med Visma, og kontaktet senere alle kommuner på kundelisten for å informere om feil og avdekke omfang, etter at stikkprøvene viste forekomst av feil hos andre kommuner. Det ble da klart at feilen hadde et større omfang.

I starten av juni gikk Visma ut med informasjon til alle kommuner om at de kunne være berørt av feilen og at de derfor måtte iverksette tiltak for å forhindre mulige avvik og kartlegge omfang. Det har vært løpende dialog mellom Bufdir, Visma, KS og Datatilsynet for å sørge for tilstrekkelig og lik informasjonsdeling overfor kommunene.



Figur 1. Tidsløp fra oppdagelse til retting

Visma stilte personell til disposisjon for kommunene, både til bistand med installering av programvarerettelse og til gjennomgang av logger for å avdekke avvik, det vil si for å finne ut om bekymringsmeldinger var sendt til barnevernstjenesten, men ikke lagret i fagsystemet. Ved å gjennomgå logger for bekymringsmeldinger som ble sendt gjennom NPB, fikk barnevernstjenesten informasjon om dato og tidspunkt for meldingen, i tillegg til om melder hadde brukt skjema for offentlig eller privat melder.

Det er kun et fåtall av de tapte bekymringsmeldingene det har vært mulig å *gjenopprette*. Dette skyldes at bekymringsmeldinger ble slettet fra KS sin database 14 dager etter at fagsystemet hadde bekreftet mottak av meldingen.[5] KS er kjent med at 4 meldinger er gjenopprettet.

Kommunene har gjennomført tiltak for å *gjenfinne informasjon* fra bekymringsmeldinger som har gått tapt, som det ikke var mulig å gjenopprette. Kommunene har oppfordret offentlige og private meldere om å ta kontakt for å kontrollere om bekymringsmeldinger de har sendt i det aktuelle tidspunktet var blitt mottatt eller slettet. Dette var mulig å kontrollere ved å sammenligne tidspunkt for innsendte meldinger mot kommunens logger. Kommunene har oppfordret offentlige og private meldere om å sende inn bekymringsmeldinger på nytt dersom det er grunn til å tro at de ikke ble mottatt. Kommunene har forsøkt å nå ut både gjennom media og direkte kontakt med de offentlige virksomhetene som oftest sender bekymringsmeldinger.

KS vurderer at tiltakene for å gjenfinne informasjon fra tapte meldinger har hatt effekt, da det finnes eksempler på at meldere har sendt bekymringsmelding på nytt. For flesteparten av meldingene som har gått tapt har det likevel ikke vært mulig å gjenfinne informasjon. Det er ikke ensbetydende med at barna som det er meldt bekymring for er ukjente for barnevernet, men innebærer at man ikke har informasjon som gjør det mulig å avgjøre det.

Konsekvenser av feilen

Hovedpunkter

- Risikoen for langsiktige konsekvenser er stor for barna det gjelder. Saken omhandler få barn, og på samfunnsnivå er risikoen for langsiktige negative konsekvenser mer begrenset.
- Statsforvalterne vurderer at kommunene tidlig gjorde det de kunne for å få nødvendig oversikt over svikten og at de er i gang med egnede oppfølgingsaktiviteter.
- Den tekniske feilen er ikke medvirkende årsak til trenden med færre bekymringsmeldinger til barnevernet de senere årene.
- Feilen har økonomiske og administrative konsekvenser for kommunene, i hovedsak knyttet til tiltak for å hindre at tilsvarende feil oppstår igjen.
- Feilen fører til risiko for omdømmetap. Kommunene melder om svekket tillit til meldingsløsningene i barnevernet.

Vi mangler kunnskap om innholdet i bekymringsmeldingene som har gått tapt. Vurdering av risiko for langsiktige negative konsekvenser er derfor basert på generell kunnskap om bekymringsmeldinger og den aktuelle hendelsen. Det er sannsynlig at flere av de slettede

[5] Lagringsperioden ble utvidet til 30 dager i forbindelse med håndtering av denne hendelsen.

meldingene omhandler barn barnevernet kjenner til, enten fordi det allerede pågikk undersøkelse eller tiltak, eller fordi andre meldere har meldt bekymring for samme barn senere.

Bufdir og KS trekker frem at sakens omfang er begrenset, sammenlignet med hva man fryktet i den tidligere fasen etter at feilen ble kjent. Risikoen for langsiktige negative konsekvenser av hendelsen *på samfunnsnivå* er derfor begrenset.

Risikoen for langsiktige konsekvenser er likevel stor *for de barna det gjelder*, avhengig av hvorvidt barnevernstjenesten klarte å gjenopprette, eller gjenfinne informasjon fra, den tapte meldingen, og hvor lang tid det tok. Dette trekkes frem av både Bufdir, KS og Helsetilsynet.

Helsetilsynet har innhentet informasjon fra statsforvalterne om hvordan de har fulgt opp denne saken. Statsforvalterne har rapportert til Helsetilsynet at de så langt vurderer at kommunene tidlig gjorde det de kunne for å få nødvendig oversikt over svikten, og at de gikk tidlig i gang med egnede oppfølgingsaktiviteter. For å redusere konsekvenser for barn vurderer Helsetilsynet at tilsyn kan være egnet til å bidra til å styrke sikkerhet og kvalitet i tjenestene fremover i tid slik at lignende svikt ikke gjentar seg.

Da feilen ble kjent oppsto en hypotese om en sammenheng mellom hendelsen og trenden med færre bekymringsmeldinger til barnevernet de senere årene. Bufdir konkluderer tydelig med at nedgangen i antall bekymringsmeldinger skyldes andre forhold enn teknisk svikt. Sakens omfang er for begrenset til å ha en betydning for nasjonale utviklingstrekk. En gjennomgang viser dessuten at nedgangen er like tydelig i kommuner som ikke er rammet av feilen, som i kommuner hvor feilen er identifisert.

Omfang av økonomiske og administrative konsekvenser varierer mellom kommuner, men ressursbruken var vesentlig i perioden rett etter at avviket ble kjent. KS melder at den største ressursbruken for kommunene er knyttet til tiltak for å hindre at tilsvarende feil oppstår igjen, som økte ressurser til manuelle kontroller av digitale systemer.

KS antar også at svikten har gitt *indirekte* administrative og økonomiske konsekvenser. Dersom barn med behov ikke fanges opp tidlig kan det gi behov for tyngre og mer kostbare tiltak siden. Kommunenes tilbakemelding er at feilhendelsen kan ha bidratt til å svekke tilliten til barnevernet og meldingsløsningene. Bufdir trekker også frem at tilliten til meldingsløsningene kan være svekket. Kommunene melder at konsekvensene av svekket tillit synes å være at både meldere og mottakere kontrollerer om meldinger har kommet fram; ikke at de lar være å melde.

Årsaksforhold og forebygging av fremtidige feil

Hovedpunkter

- Avvikene har et sammensatt årsaksbilde: Vismas rotårsaksanalyser indikerer at avvikene ble utløst ved at lagring til kommunens database feilet, på grunn av overbelastning på kommunens lokale infrastruktur. Mekanismen som skulle fange opp slike tilfeller i Familia fungerte ikke som den skulle grunnet en logisk brist i kildekoden; dette førte til at i de tilfeller der lagring til databasen sviktet, ble ikke avsender gjort oppmerksom på at meldingen ikke var kommet frem til mottaker.
- Risiko for at fagsystemet sendte kvittering på mottatt melding uten at meldingen ble lagret var ikke identifisert som en egen risiko ved NPB.
- Vismas programvare kan ikke utbedre rotårsaken til hendelsen, at lagring i databasen feiler. Dersom det ikke gjøres utbedringer hos den enkelte kommune på de forhold som utløste at lagring feilet, kan lagring til databasen feile igjen.
- Svakheten i kildekoden i Familia, som førte til feilen, er rettet gjennom programvareoppdatering. De fleste kommuner viser til at de har iverksatt regelmessige kontroller av at det er samsvar mellom bekymringsmeldinger som blir registrert i NPB og meldinger som blir lagret i fagsystemet. Det er derfor lite sannsynlig at samme feil vil oppstå igjen.
- Manglende systematisk arbeid med informasjonssikkerhet kan utgjøre en risiko for at lignende feil vil kunne inntreffe igjen. Det er viktig med godt samspill mellom nasjonale fellesløsninger og sektorløsninger.

Tre faktorer forklarer hvorfor enkelte bekymringsmeldinger som ble sendt fra NPB har gått tapt og ikke kan gjenopprettes:

1. Enkelte bekymringsmeldinger som er sendt fra NPB har ikke blitt lagret i Familia, fordi lagring til kommunens database feilet. Vismas gjennomgang av logger fra et utvalg berørte kommuner indikerer at årsaken til at lagring feilet var at kommunens infrastruktur var overbelastet. Dette anses å være rotårsaken til feilen.
2. Mekanismen som skulle sende en feilmelding i tilfeller der en bekymringsmelding ikke er lagret i Familia har ikke fungert som den skal grunnet en logisk brist i kildekoden i Familia. Til tross for at meldingen ikke ble lagret i Familia, sendte Familia tilbakemelding til NPB om at bekymringsmeldingen var kommet frem. Derfor ble heller ikke bekymringsmeldingen skrevet ut og sendt i posten, slik den skal når systemet får en feilmelding.
3. Fordi KS ikke har selvstendig behandlingsgrunnlag for å oppbevare bekymringsmeldingene over tid, sletter de bekymringsmeldinger fra sin database 14 dager etter at fagsystemet har bekreftet mottak av meldingen.

Risiko for at fagsystemet sendte kvittering på mottatt melding uten at meldingen ble lagret var ikke identifisert som en egen risiko ved NPB. Det er i juni 2023 tatt inn i ROS-malene som KS Digitale fellestjenester gjør tilgjengelig for kommuner som bruker tjenesten.

Svakheten i kildekoden fra Visma er rettet gjennom programvareoppgradering. Dette bidrar til å hindre at samme feil vil skje igjen. Vismas analyser indikerer imidlertid at rotårsaken til feilen er at lagring til databasen feiler, på grunn av svært høy belastning på infrastrukturen i det øyeblikket Familia har mottatt og skal prosessere en bekymringsmelding fra KS.[6] Dette kan ikke utbedres gjennom oppdatering av Vismas programvare. Det er en feil som må utbedres i den enkelte kommune. Dersom det ikke gjøres utbedringer hos den enkelte kommune på de forhold som utløste at lagring feilet, kan lagring til databasen feile igjen.

De fleste kommuner som opplevde avvik på grunn av feilen har iverksatt regelmessige kontroller av at det er samsvar mellom bekymringsmeldinger som blir registrert i NPB og meldinger som blir lagret i fagsystemet. Det er tiltak som er ment å oppdage meldinger som ikke kommer fram slik at meldingene kan gjenopprettes. Det er derfor lite sannsynlig at samme avvik vil oppstå igjen.

Digitaliseringsdirektoratet påpeker at manglende systematisk arbeid med informasjonssikkerhet vil utgjøre en risiko for at lignende feil vil kunne inntreffe igjen. De vurderer at et fåtall av fylkeskommuner og kommuner gjennomfører risikovurderinger systematisk og periodisk. Risiko reduseres ved at man har et godt samspill mellom nasjonale fellesløsninger og sektorløsninger.

Læring av feilen

Når det gjelder læringspunkter for kommunesektoren

- påpeker Digitaliseringsdirektoratet at det stilles krav til at kommuner skal ha internkontroll for informasjonssikkerhet, og dette bør integreres som en del av virksomhetens helhetlige internkontroll. Virksomheten må identifisere, analysere og håndtere risikoer jevnlig, ikke bare når en hendelse inntreffer.
- påpeker KS at hendelsen avdekket at man ikke har hatt nødvendig kontroll i alle ledd ved digital meldingsflyt. De påpeker viktigheten av gode avviksrutiner i kommunene og en kultur som oppmuntrer til å melde avvik. KS mener det i mange kommuner er behov for å forbedre ROS- og DPIA-ene og tilhørende arbeid med internkontroll knyttet til barnevern og digitale løsninger. Flere kommuner vil trenge veiledning i dette arbeidet.
- anbefaler Visma at kommuner som drifter on-premise-løsninger i eget datasenter etablerer rutiner for å overvåke logger, oppdage og følge opp feilsituasjoner. Kommuner bør gjennomføre risikovurderinger for totalbildet av IT-systemer og integrasjoner i kommunen, slik at man kan agere raskt og forstår risikoen dersom alvorlige hendelser inntreffer. Visma oppfordrer kommunene til å vurdere om det er behov for kompetanseheving hos offentlige instanser om bekymringsmeldinger og barnevernets tilbakemeldingsplikt og -praksis.

[6] Lagringen til SQL-databasen har derfor ikke vært vellykket, og løsningen har dermed forkastet data grunnet utilgjengelig SQL-database.

- peker Helsetilsynet på behovet for risikoreduserende tiltak ved innføring av nye digitale løsninger, herunder testregimer og kontrolltiltak.

Når det gjelder hvordan offentlige myndigheter kan bidra til å redusere risikoen for alvorlige feil i barnevernets fagsystemer

- etterlyser KS tydeligere forventninger fra offentlige myndigheter om bruk av NPB for alle meldere med meldeplikt. Kommunene peker på NPB som den foretrukne kanalen å motta meldinger gjennom.
- etterlyser Digitaliseringsdirektoratet integrasjon mellom NPB og digitale fellesløsninger, som eFormidling eller Altinn, slik at statlige aktører kan sende bekymringsmeldinger til NPB direkte fra sine fagsystemer, uten behov for IT-utvikling i egen virksomhet.
- gir Visma flere eksempler på hvordan offentlige myndigheter kan bidra til å rådgi om og standardisere bruken av programvare/IT i kommunesektoren.
- peker Helsetilsynet på at digitale løsninger bør inngå i kommunens risikovurderinger for å sikre en effektiv internkontroll som bidrar til at tjenestene forblir trygge og forsvarlige.
- påpeker Bufdir at bruk av felleskomponenter i offentlig sektor gir forutsigbarhet og enhetlig praksis. Ved utvikling av tjenester mot kommunene er det sentralt at man benytter den felleskomponenten som er tilpasset kommunen og ikke velger sine egne løsninger. Her spiller KS en viktig rolle.
- trekker Bufdir frem at det nylig er iverksatt en endring i veiledning i NPB for offentlige meldere om at de kan forvente tilbakemelding fra barnevernstjenesten om mottak av melding og eventuell åpning av undersøkelse. Melder oppfordres i NPB til å etterspørre informasjon hvis de *ikke* mottar tilbakemelding. Dette reduserer ikke risikoen for alvorlige feil, men bidrar til å redusere negative konsekvenser av eventuelle feil.

Når det gjelder spørsmålet om det er læringspunkter for systemleverandørene som Bufdir eller andre offentlige aktører bør adressere

- påpeker KS at offentlige aktører kan bidra til å fjerne hindre for at NPB kan integreres med systemer som benyttes av ansatte med meldeplikt, samt stille tydelige forventninger om at alle offentlige meldere sender bekymringsmeldinger gjennom NPB.
- foreslår Visma at det etableres gode samarbeidsarenaer slik at leverandørene i større grad kan være med og påvirke utviklingen av felleskomponentene i nasjonale fellestjenester.

Når det gjelder risiko- og sårbarhetsanalyser

- beskriver KS faren for at risiko- og sårbarhetsanalyser begrenses til den delen av verdikjeden man har ansvar for eller kontroll over. Når det gjelder bekymringsmeldinger, og det digitale økosystemet ellers, vil risikohendelse og relevante tiltak ikke nødvendigvis ligge i samme virksomhet. I tilfeller det ikke er akseptabelt å forutsette at risiko er håndtert av andre aktører, må økosystemet være rigget slik at den enkelte aktør kan følge risikohåndteringen gjennom hele verdikjeden.
- påpeker Bufdir at alle aktører i verdikjeden har et ansvar for å foreta risikovurderinger av egne arbeidsprosesser og rutiner og sørge for ivaretakelse av sin del av verdikjeden. Bufdir

understreker at risiko for svikt i systemer alltid vil være til stede, både når det gjelder digitale og manuelle systemer. Rutiner for oppfølging, etterlevelse og internkontroll må derfor være på plass.

1. Innledning

1.1 Oppdraget

I oppdrag 4 A, tillegg 7 til tildelingsbrevet for 2023 fikk Bufdir i oppdrag å:

a) Granske feilens årsaker, omfang og konsekvenser (frist 31.10.22)
b) Følge opp berørte kommuners arbeid med å håndtere konsekvensene av feilen og veilede kommunesektoren i å forebygge at lignende feil skjer (løpende frist).

Denne rapporten gir et svar på del A av oppdraget.

Barne- og familiedepartementet (BFD) skriver at granskingen ikke skal gå lenger inn i teknologiske årsaksforhold enn det som er nødvendig for å kunne trekke nødvendig lærdom fra hendelsen og forebygge at lignende feil skjer i fremtiden.

Statens helsetilsyn er bedt om å bistå direktoratet med oppdrag A ut fra den kompetanse og det ansvar Helsetilsynet har. Oppdrag A skal løses ut fra den kompetanse og det ansvar Bufdir har som direktorat for kommunalt barnevern og forutsetter bidrag fra andre aktører og kompetansemiljøer. BFD har bedt Visma, KS, Datatilsynet og Digitaliseringsdirektoratet om å bidra inn i Bufdirs arbeid med oppdraget ut fra deres kompetanse og ansvarsområder.

Rapporten er utarbeidet av Bufdir i samarbeid med de ovennevnte aktørene. Hver aktør har bidratt med tekster under de temaene som er relevante for deres ansvarsområder, og hver aktør står ansvarlig for sine respektive bidrag. Bufdir står ansvarlig for sammendraget og avsluttende refleksjoner.

Spørsmålene som skal besvares gjennom oppdrag A er gjengitt i figur 1. Rapporten er strukturert etter spørsmålene, og enkelte steder har Bufdir ytterligere operasjonalisert spørsmålet i mer spesifikke underspørsmål. Dette fremgår tydelig der det gjelder.

I vedlegg 1 gis en status for arbeidet med del B av oppdraget per oktober 2023.

A. Kartlegging av feilens omfang

1. Hvor mange kommuner, og hvor stor del av landets barnebefolkning, var omfattet av feilen, og i hvilket tidsrom?
2. Hvor mange meldinger er det grunn til å frykte ikke er kommet frem?

B. Oppdagelse og retting av feilen

1. Hvordan ble feilen oppdaget, varslet om og rettet?
2. Hvordan vurderes arbeidet med rettingen, herunder informasjonen til berørte kommuner og tidsløpet fra oppdagelse til retting?
3. Hvilke tiltak ble satt i verk for å kompensere for meldinger som en må anta har gått tapt?

C. Konsekvenser av feilen

1. Hvordan vurderes risikoen for at feilen, etter at kompenserende tiltak som er satt i verk, kan ha langsiktige konsekvenser som følge av at omsorgssvikt grunnet denne feilen ikke blir oppdaget eller oppdages først etter så lang tid at barn har lidd et signifikant velferdstap?
2. Kan det være en sammenheng mellom feilen og trenden med færre bekymringsmeldinger til barnevernet?
3. Hvordan vurderes de økonomiske og administrative konsekvensene av feilen for kommunene?

D. Årsaksforhold og forebygging av fremtidige feil

1. Hva var årsaken til feilene?
2. Hva var årsakene til tiden som gikk fra feilen først ble oppdaget til brukerne og andre berørte aktører ble varslet?
3. Omfattes hendelsesforløpet av eventuelle risikovurderinger som er gjort tidligere?
4. Hvilke tiltak er satt i verk for å forebygge lignende feil, herunder at feil ikke blir oppdaget og rettet uten unødig opphold?
5. Hvordan vurderes risikoen for at feilene vi har sett i denne saken vil kunne skje i fremtiden?

E. Læring av feilen

1. Er det læringspunkter for kommunesektoren med tanke på deres internkontroll med systemet for mottak og formidling av bekymringsmelding?
2. Hvordan kan andre offentlige myndigheter bidra for å redusere risikoen for alvorlige feil i barnevernets fagsystemer?
3. Er det læringspunkter for systemleverandørene som det er naturlig at Bufdir eller andre offentlige aktører adresserer?
4. Hvordan bør risiko- og sårbarhetsanalyser ved bruk av IKT til innlevering og mottak av bekymringsmelding utvikles som følge av feilen, og hvordan bør feilen påvirke de vurderinger av risiko og sårbarhet ved svikt som gjøres for barna det meldes bekymring for?

Figur 2. Konkrete spørsmål som besvares i rapporten, iht. oppdrag i tillegg 7 til tildelingsbrevet til Bufdir for 2023 om å granske feilens årsaker, omfang og konsekvenser

1.2 Aktørene som har bidratt i utforming av rapporten

1.2.1 KS

KS er kommunesektorens organisasjon, med alle kommuner og fylkeskommuner som medlemmer. I tillegg til å være en interesseorganisasjon, har KS utviklet, drifter og forvalter Nasjonal portal for bekymringsmelding (NPB), og tilbyr den til kommunene. Ansvaret for NPB er fra 1. september overført til det KS-eide selskapet KS Digitale Fellestjenester AS. Når KS nevnes i denne gjennomgangen inkluderes imidlertid rollen og oppgavene som følger med drift og forvaltning av NPB.

I egenskap av interesseorganisasjon svarer KS i flere spørsmål på vegne av kommunene. Vi har i hele prosessen vært i kontakt med våre medlemmer i ulike arenaer, og vi har fått innsikt i brukernes behov gjennom brukerstøtte, brukerråd og annen kundedialog i KS Digitale fellestjenester. Den 13. juni arrangerte KS et åpent erfaringsdelingsmøte, der kommunene delte erfaringer i håndtering av feilsituasjonen. Møtet hadde mer enn 250 eksterne deltakere. I forbindelse med spørsmålene som blir stilt i denne gjennomgangen inviterte vi alle berørte kommuner til innspillsmøte 8. september. Der møtte representanter fra seks barnevernstjenester. Vi har også gjennomført et eget innspillsmøte med Bergen kommune. For oversikt over berørte kommuner og antall meldinger/barn har vi brukt kartleggingen Bufdir gjennomførte i kommunene i juni, som publisert på Bufdir sine nettsider.

Gjennom disse kontaktpunktene og dialogene med kommunene mener vi å ha fått et dekkende bilde av situasjonen – særlig i de berørte kommunene. Det er imidlertid ikke en komplett kartlegging, og det vil i mange tilfeller ikke være mulig å gi et entydig svar som favner alle kommuner. I vår besvarelse har vi valgt å i liten grad gå inn på enkeltkommuner, men fokusere på det som er felles samtidig som vi belyser variasjonene der det vurderes som relevant.

1.2.2 Visma

Visma leverer programvare tilpasset kommunemarkedet, herunder ulike administrasjonssystemer innen fagområder som for eksempel barnevern. Visma leverer fagsystemet Visma Familia (nærmere beskrevet i punkt 3.1.1.), som var mottakersystemet for bekymringsmeldinger i sakene omtalt i denne rapporten.

Gjennom rollen som programvareleverandør har Visma i denne saken bistått kommunene med informasjon, feilsøking, programvarerettelse og installasjon av programvarerettelse. Visma har også samlet tilbakemeldinger fra sine kunder om hvorvidt og i hvilket omfang de har avdekket avvik, samt støttet utredning og avvikshåndtering hos BufDir og Datatilsynet ved å tilgjengeliggjøre relevant informasjon om programvaren og hendelsen.

1.2.3 Digitaliseringsdirektoratet

«Digitaliseringsdirektoratet (Digdir) er et statlig direktorat underlagt Kommunal- og distriksdepartementet (KDD). Digdir er regjeringens fremste verktøy for raskere og mer samordnet digitalisering av samfunnet – i tett samarbeid med mange andre aktører både i offentlig og privat

sektor. Digdir har gitt innspill til denne rapporten ut fra sine roller som premissgiver for offentlig sektors arbeid med forebyggende informasjonssikkerhet, og leverandør av fellesløsninger.»

1.2.4 Helsetilsynet

Statens helsetilsyn (Helsetilsynet) er overordnet tilsynsmyndighet for sosiale tjenester i Nav, barnevern-, helse- og omsorgstjenester og folkehelsearbeid. Ansvaret på barnevernsområdet innebærer et overordnet faglig ansvar for tilsynet med barneverntjenester, formidling av tilsynsinnsikt og områdeovervåking. Det er statsforvalterne som utfører tilsyn.

Formålet med tilsyn er å bidra til å styrke sikkerhet og kvalitet. I dette oppdraget handler Helsetilsynets innretning om hvordan tilsyn kan være egnet til å bidra til å understøtte forbedringsarbeid i tjenestene fremover i tid.

Helsetilsynet har innhentet informasjon fra alle statsforvalterne i forbindelse med dette oppdraget. Statsforvalterne har så langt fulgt opp med dialog med kommunene. Tilsynsmyndighetene vil vurdere videre egnet oppfølging i etterkant av at denne rapporten foreligger.

1.2.5 Datatilsynet

Datatilsynet er tilsynsmyndighet på personvernregelverket. Tilsynets myndighet og oppgaver er regulert gjennom personopplysningsloven og personvernforordningen.

Etter personvernforordningen artikkel 33 skal brudd på personopplysningssikkerheten av en viss karakter meldes til Datatilsynet. De aktuelle hendelsene ble sendt oss i tråd med artikkel 33.

I tillegg driver Datatilsynet med informasjons- og veiledningsarbeid om saker som berører personvernet, blant annet i forbindelse med sikkerhetshendelser.

Datatilsynet la raskt ut informasjon på våre hjemmesider i forbindelse med hendelsen. Vi hadde i tillegg møter med involverte aktører i ledd av vår undersøkelse av sakene som ble meldt oss i tråd med personvernforordningen artikkel 33.

1.2.6 Bufdir

Barne-, ungdoms- og familiedirektoratet (Bufdir) er underlagt Barne- og familiedepartementet (BFD), og har ansvar for områdene barnevern, barn, ungdom og oppvekst, adopsjon, familievern, likestilling og ikke-diskriminering og vold og overgrep i nære relasjoner. Bufdir styrer også Barne-, ungdoms- og familieetaten (Bufetat) som har ansvar for det statlige barne- og familievernet. I utviklingen av digitale løsninger, tar Bufdir sikte på å utnytte nasjonale strategier og felleskomponenter til det beste for tjenestene og samfunnsutviklingen innenfor sektoren. Bufdir tar del i flere digitaliseringsinitiativ med nasjonalt nedslagsfelt, hvor formålet er å utvikle samordnede tjenester som gir gevinster for innbyggere. To eksempler på dette, er *DigiUng-samarbeidet* og *DigiBarnevern*.

DigiUng-samarbeidet er et tverrsektorielt samarbeid bestående av Helsedirektoratet, Bufdir og Direktoratet for e-helse, som jobber for å lage digitale løsninger for ungdom på tvers av sektorer. Målet er å kunne tilby målgruppen et helhetlig digitalt forløp, som inkluderer både informasjonstjenester med lav terskel, og fullverdige digitale hjelpetjenester som åpner for personlig oppfølging på tvers av sektorer.

DigiBarnevern ble etablert som et nasjonalt samarbeidsprosjekt mellom stat og kommune. Prosjektet har som mål å øke kvaliteten og effektiviteten i det kommunale barnevernet, blant annet ved å sørge for bedre IT-løsninger. Bufdir har vært prosjekteier på statlig side og har levert et digitalt barnevernfaglig kvalitetssystem som styrer prosesser og tilgang til oppdatert informasjon og støtte i de kommunale fagsystemene. KS har tatt ansvar for nasjonal portal for bekymringsmelding, og SSB har levert et nytt barnevernregister og system for automatisk innrapportering av data fra kommunalt barnevern. Trondheim kommune har ledet sammenslutningen av åtte kommuner som har anskaffet nytt fagsystem og ledet arbeidet med å styre utvikling og implementering. DigiBarnevern-prosjektet ble avsluttet ved årsskiftet 2022-23, men samarbeidet mellom Bufdir og KS fortsetter for å bidra til en helhetlig videreutvikling og forvaltning av løsningene.

2. Kartlegging av feilens omfang

2.1 Antallet kommuner og andel av barnebefolkning som er berørt

Spørsmål som besvares i delkapittelet

A1. Hvor mange kommuner, og hvor stor del av landets barnebefolkning, var omfattet av feilen, og i hvilket tidsrom?

2.1.1 Vismas beskrivelse av omfang og tidsrom

Integrasjonen mellom Visma Familia og Nasjonal portal for bekymringsmelding ble etter tilbakemelding om vellykket pilotprosjekt tilgjengeliggjort for alle kunder 25.09.20. Visma har mottatt oversikt over kommuner som har aktivert Nasjonal portal for bekymringsmelding hos KS, som viser at 242 kommuner hadde tatt i bruk integrasjonen da Visma ble kjent med avvik i integrasjonen. Oppsettet av integrasjonen mellom Familia og Nasjonal portal for bekymringsmelding har vært håndtert av den enkelte kunde selv, og Visma har derfor ikke oversikt over hvor lang tid integrasjonen har vært i bruk hos den enkelte kunde. Da Visma tok kontakt med kommunene for å følge opp det avdekkede avviket, meldte en håndfull kommuner tilbake at integrasjonen ikke enda var tatt i bruk, så i realiteten har det vært færre enn 242 kommuner som var eksponert i det aktuelle tidsrommet.

Gjennom dialog med kommunene fra 05.06.23 og påfølgende uke, fikk Visma tilbakemeldinger om at totalt 22 kommuner faktisk var blitt påvirket av feilen (se også totaloversikt inntatt i kap. 2.2.1).

2.1.2 Bufdirs vurdering av hvor stor andel av landets barnebefolkning som er påvirket

I de 22 kommunene som har rapportert tap av bekymringsmeldinger til Visma, utgjør barnebefolkningen i underkant av 380 000 barn.[7] Dette tilsvarer 34 prosent av Norges barnebefolkning, som potensielt kunne ha blitt berørt av den tekniske feilen. Ettersom ett barn kan være registrert med flere meldinger, og bekymringsmeldinger kan gjelde både «nye» barn og barn som barnevernet allerede er i kontakt med, er det ikke mulig å regne ut antall barn som faktisk er berørt.

2.1.3 KS' beskrivelse av omfang

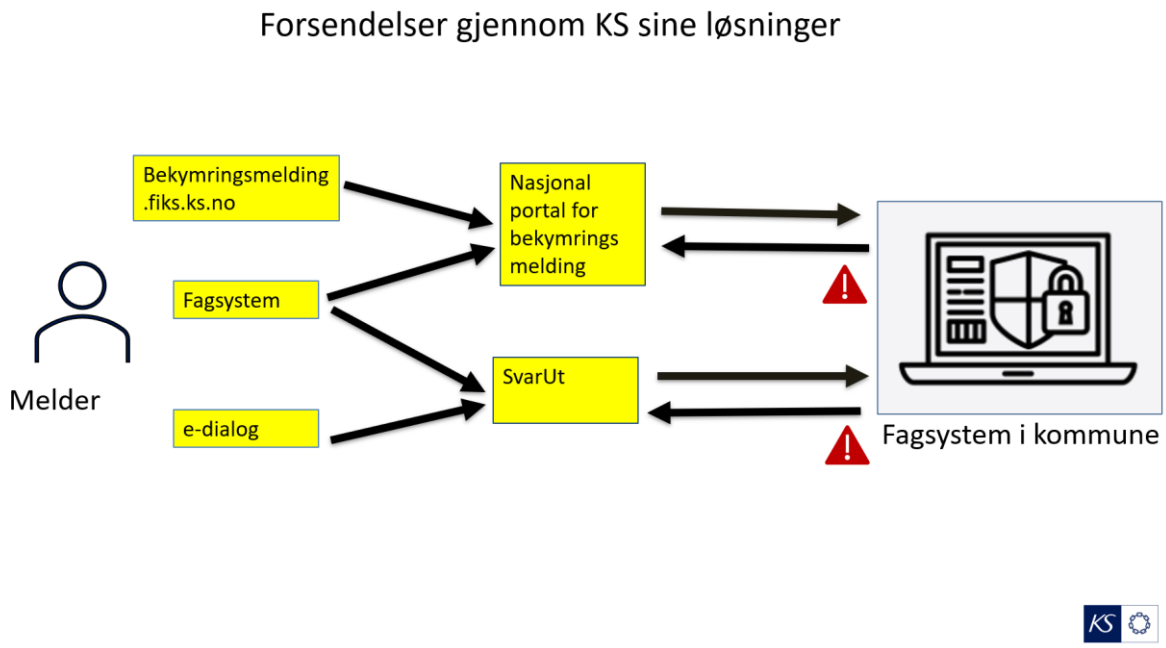
Om løsningen

[7] Statistisk sentralbyrå (2023a). Tabell 07459: Alders- og kjønnsfordeling i kommuner, fylker og hele landets befolkning (K) 1986 - 2023. Statistikkbanken (ssb.no)

Meldinger sendt gjennom NPB mottas av kommuner på to forskjellige måter: de mottas direkte i fagsystem, eller de lastes ned av barneverntjenesten direkte fra KS' forvaltningssider for tjenesteadministratorer gjennom et brukergrensesnitt. Dersom et fagsystem avviser en melding, sendes meldingen til print og deretter til barnevernet i posten. Meldinger lagres kun i begrenset tid hos NPB, nemlig 14 dager, basert på risikovurdering som ble gjort når portalen ble utviklet: KS skal ikke ha disse dataene lengre enn nødvendig; de skal lagres hos barneverntjenesten, ikke i forsendelseskanalen. Perioden ble endret til 30 dager etter oppdagelsen av feilen som risikoreduserende tiltak mens feilsøking og nå gransking pågår.

SvarUt er en annen tjeneste som leveres av KS. Gjennom SvarUt-tjenesten kan offentlige virksomheter sende og motta forsendelser digitalt. Kommuner kan koble SvarUt mot sitt fagsystem for å motta forsendelser direkte i fagsystemet. Flere barneverntjenester mottar forsendelser fra SvarUt i Visma Familia, herunder bekymringsmeldinger. Dette er altså bekymringsmeldinger som ikke er sendt gjennom NPB, men som er sendt som en postforsendelse på lik linje som andre forsendelser som sendes gjennom SvarUt. KS sletter ikke forsendelser som sendes via SvarUt.

Figur 3 nedenfor viser at feilen både gjaldt mottak av forsendelser gjennom SvarUt og gjennom NPB.



Figur 3. Forsendelser gjennom KS sine løsninger

Om omfanget
KS har ikke en egen oversikt over antall kommuner som var omfattet og i hvilket tidsrom. Gitt feilens karakter vil det ikke være noe i KS sine systemer som indikerer at meldingene ikke er levert og korrekt lagret. KS viser derfor til Visma, kommunene og kartleggingen fra Bufdir i juni i år.

KS kan likevel bidra med enkelte tall som kan hjelpe å få oversikten og sette tallene i sammenheng. For bekymringsmeldinger mottatt gjennom NPB, er følgende tall relevante:

- Per august 2023 har 284 kommuner signert avtale med KS Digitale fellestjenester for å bruke NPB.
- Disse dekker over 93 prosent av Norges befolkning, og ca. det samme av Norges befolkning under 18 år.
- I 2022 ble ca. 11 000 ut av over 80 000 bekymringsmeldinger sendt gjennom NPB, hvis vi legger tallene fra SSBs tabell 12189[8] til grunn som totalt antall meldinger. I tabellen vises antall meldinger sendt gjennom NPB siden lansering av portalen, fordelt på meldinger fra offentlige meldere og private:
  ..

Kvartal	OFFENTLIG	PRIVAT	Totalsum
2020	**769**	**763**	**1532**
Kv2	33	34	67
Kv3	121	175	296
Kv4	615	554	1169
2021	**4587**	**3299**	**7886**
Kv1	1019	764	1783
Kv2	1286	746	2032
Kv3	891	830	1721
Kv4	1391	959	2350
2022	**6796**	**4202**	**10998**
Kv1	1476	970	2446
Kv2	1813	1048	2861
Kv3	1273	1081	2354
Kv4	2234	1103	3337
2023	**7552**	**3791**	**11343**
Kv1	2756	1178	3934
Kv2	2763	1352	4115
Kv3	2033	1261	3294
Totalsum	**19704**	**12055**	**31759**

Tabell 1. Antall bekymringsmeldinger sendt gjennom NPB per kvartal (fra oppstart 2020 til og med september 2023)

For bekymringsmeldinger mottatt gjennom SvarUt gjelder følgende:

Alle kommuner i Norge bruker SvarUt. Det er ukjent hvor mange bekymringsmeldinger som er sendt til barneverntjenestene som forsendelser gjennom SvarUt. For å avgjøre om det er en bekymringsmelding må man lese forsendelsens innhold. Kommuner har selv sjekket forsendelser fra SvarUt som ikke ble lagret i Visma Familia, og har kunnet laste ned disse forsendelsene fra

[8] Statistisk sentralbyrå (2023b). Tabell 12189: Meldingar til barnevernet, etter konklusjon på meldinga og handsamingstid av meldinga (K) 2015-2022. Statistikkbanken (ssb.no)

SvarUts selvbetjeningsløsning. Disse meldingene har altså blitt gjenopprettet og kommet fram, men forsinket.

2.2 Antallet meldinger som ikke har kommet frem

Spørsmål som besvares i delkapittelet

A2. Hvor mange meldinger er det grunn til å frykte ikke er kommet frem?

Operasjonalisering av spørsmålet:

- *Hvor mange meldinger er det bekreftet at ikke har kommet frem? Hvor mange meldinger har blitt gjenopprettet?*
- *I hvilken grad har kommunene klart å gjenfinne informasjon fra meldinger som gikk tapt, og som ikke kunne gjenopprettes?*
- *Er det grunn til å tro at det er flere meldinger som ikke har kommet frem, og i så fall hvor mange og hvorfor?*

2.2.1 Visma om meldinger som ikke har kommet frem

Pr. 19.06.23 hadde alle kommunene besvart Vismas henvendelser knyttet til avvik, og hatt grundige gjennomganger av sine logger, enten internt i kommunen eller med bistand av Visma sine konsulenter. Visma har ikke selv hatt adgang til å innhente denne informasjonen eller etterprøve tallene (pga. on-premise-teknologi[9]), så oversikten under er basert på tilbakemeldinger fra kommunene (sammenstilt av Visma):

Antall kommuner som benytter løsningene (Familia med integrasjon mot Nasjonal portal for bekymringsmelding)	242
Antall kommuner som har meldt avvik (har tapt bekymringsmelding)	22
Antall kommuner bekreftet uten avvik (ingen bekymringsmeldinger tapt)	220
Antall kommuner ennå ikke besvart	0
Totalt antall meldinger registrert tapt	63

Tabell 2. Oversikt over avvik, basert på tilbakemeldinger fra kommunene

[9] On-premise-teknologi innebærer at programvaren utvikles og tilgjengeliggjøres av systemleverandør, og installeres og driftes av kundene selv i deres eget IT-miljø, eller gjennom en driftspartner kunden har avtale med.

Visma har ikke mottatt tilbakemeldinger om hvorvidt enkelte av meldingene har latt seg gjenfinne eller gjenskape i ettertid, men har fanget opp i media at det kan være tilfellet for noen av meldingene.

2.2.2 KS om meldinger som ikke har kommet frem

KS har ikke egen informasjon om hvor mange meldinger som ikke har blitt lagret i Visma Familia og må regnes som tapt. Her viser vi til øvrige aktører. Informasjonen i meldingene som ikke ble lagret i Visma Familia kan ha blitt formidlet på nytt til barneverntjenesten på flere ulike måter. Noen meldinger kunne gjenopprettes fordi de ennå ikke var slettet fra NPB, andre ble gjenfunnet med hjelp fra mulige meldere, mens andre meldinger kan ha blitt formidlet på nytt uten at verken melder eller barneverntjenesten vet at den opprinnelige meldingen er blant de tapte meldingene. For å illustrere kompleksiteten med å gi nøyaktige tall kan vi vise til fire scenarier vi vet har inntruffet:

A) Meldingen ble sendt gjennom NPB. Visma Familia kvitterte til NPB for mottak av meldingen. Meldingen ble likevel ikke lagret i Visma Familia. Meldingen ble rutinemessig slettet fra NPB før oppdagelse av feilen. Kun loggen med tidspunkt og om meldingen ble sendt med skjema for privatpersoner eller for offentlige ansatte med meldeplikt er tatt vare på.
B) Meldingen ble sendt gjennom NPB. Visma Familia kvitterte til NPB for mottak av meldingen. Meldingen ble likevel ikke lagret i Visma Familia. Feilen ble oppdaget før meldingen ble slettet fra NPB, og meldingen ble sendt på nytt til barnevernstjenesten (gjenopprettet), og mottatt.
C) Meldingen ble sendt gjennom SvarUt. Visma Familia kvitterte til SvarUt for mottak av meldingen. Meldingen ble likevel ikke lagret i Visma Familia. Feilen ble oppdaget. Meldingen kunne lastes ned manuelt fra SvarUt (gjenopprettet) – da den ikke var slettet.
D) Meldingen ble sendt av offentlig melder. Offentlig melder etterlyser hos barnevernstjenesten etter kort tid om meldingen ble mottatt, gjerne på telefon. Barnevernstjenesten kan ikke finne meldingen. Det er ikke sikkert om ansatt i barnevernet sjekker hvordan meldingen ble sendt (post, NPB, SvarUt, ev. annen kanal) og om ansatt har kjennskap eller tilgang til NPB-dashboard for administrator. Både melder og ansatt i barnevernstjenesten antar at det var en brukerfeil, eller i hvert fall ikke at dette kan være symptom av en systemfeil som er større enn dette enkelttilfellet. Offentlig melder sender meldingen på nytt og den meldingen ansees som mottatt.

Det er også andre scenarioer, som er mulige, men som vi ikke vet om har skjedd. For eksempel KAN en offentlig eller en privat melder etter oppmerksomheten i media, sendt melding på nytt, uten å opplyse om at meldingen faktisk hadde blitt sendt før.

KS har ikke gjort en egen kartlegging av hvor mange meldinger som er innenfor hver kategori, men kartleggingen av kommuner og Visma tilsier at det for Bergen kommune og Kristiansand kommune var flest meldinger innenfor kategori A eller B, mens totalt antall meldinger var 1-3 for hver av de andre kommunene som rapporterte til Bufdir at de hadde blitt berørt av feilen. Den foreløpige kartleggingen fra Bufdir differensierer, etter vår tolkning, ikke om meldinger fra kategori A og C også tilhørte kategori D. Dermed gir tallgrunnlaget fra den første kartleggingen muligens ikke totalbildet. For noen kommuner var det nok ikke så klart heller at noen av meldingene kunne

tilhøre kategori D, men de oppdaget mens de arbeidet med avvikshåndtering at dette har skjedd i noen tilfeller. Vi vet ikke hvor mange meldinger som kommer i kategori D, og hvor mange av disse som var inkludert i kartleggingen. Vi vet at noen kommuner *har* tatt den med i kartleggingen, men andre kommuner kan ha tolket det som én og samme melding og vurdert at den faktisk har kommet frem. Vi vet også at avvikshåndteringen i kommuner har hatt effekt. Kommuner har oppfordret ansatte med meldeplikt som hadde sendt meldinger å sjekke om meldingen hadde kommet fram, og i noen tilfeller ble det klart at meldingen faktisk hadde blitt sendt på nytt allerede etter kort tid, og/eller at situasjonen fra barnet eller barna allerede var kjent hos barnevernet.

Kommunikasjon med kommunene tyder på at det er en forholdsvis liten del av meldinger i kategori A som er gjenfunnet. Fra Bergen kommune vet vi at barnevernet er kjent med innholdet i til sammen 5 av de 24 meldingene som ikke kom frem. 3 av disse kommer i kategori B, mens 2 av disse ble gjenfunnet grunnet arbeidet som ble gjort i Bergen kommune etter oppdagelsen av feilen og oppfordringen til meldere å melde på nytt eller sjekke om meldingen hadde blitt mottatt. Fra Kristiansand kommune vet vi at barnevernet er kjent med innholdet i til sammen 3 ut av de 12 meldingene som ikke kom frem. 1 melding kom i kategori B, mens 2 kom i kategori D.

De fleste meldinger som ikke kom frem er altså verken gjenopprettet eller gjenfunnet, ifølge dialogen KS har hatt med kommunene som stilte på innspillsmøtet. Det er ikke ensbetydende med at barnevernet ikke kjenner til barnet. Årsaken til at meldingene ikke er gjenfunnet kan være at melder allerede har sendt meldingen på nytt før feilen ble oppdaget, eller at melder vet at barnet er ivaretatt.

KS har grunn til å tro at alle aktuelle kommuner har fulgt rutinene for å avdekke meldinger som ikke har kommet frem. Utover det som der fremkommer er det ikke grunn til å tro at flere meldinger ikke har kommet frem.

KS har heller ikke tall på antall meldinger i kategori C. Her er melding altså ikke slettet, men barn(a) kan ha blitt berørt av at meldingen kom fram for seint.

Med såpass mange uklarheter, såpass lave antall meldinger (for flertallet av kommuner som har meldt til Bufdir at de var berørt kun 1 melding), og flere meldinger som ikke ble gjenfunnet, kan ikke KS skaffe nøyaktige tall om totalt antall meldinger eller totalt antall barn omfattet av hendelsen.

3. Oppdagelse og retting av feilen

3.1 Hvordan feilen ble oppdaget, varslet om og rettet?

Spørsmål som besvares i delkapittelet

B1. Hvordan ble feilen oppdaget, varslet om og rettet?

3.1.1 Visma om hvordan feilen ble oppdaget, varslet om og rettet

Innledende bemerkninger
Avviket som har ført til at enkelte bekymringsmeldinger gikk tapt etter å ikke ha blitt korrekt lagret i Visma Familia har et sammensatt årsaksbilde, som er nærmere utdypet i punkt 5.2.1. I dette kapittelet beskrives Vismas håndtering av den ene komponenten i årsaksforholdet, en svakhet i logikken i Vismas kildekode, herunder hvordan denne svakheten ble oppdaget, varslet om og rettet.

Kort om Visma Familia
Familia er en programvare utviklet og distribuert av Visma som et fagsystem for barnevernstjenesten. Familia benyttes til å dokumentere og følge opp ulike saker barnevernet utreder og håndterer, herunder ta imot og vurdere om bekymringsmeldinger skal følges opp. Fagsystemet kan gjennom ulike integrasjoner settes opp slik at Familia utveksler informasjon med andre tjenester, for eksempel mottak av bekymringsmeldinger fra KS sin Nasjonale portal for bekymringsmeldinger.

Familia er bygget som en on-premise-teknologi, hvilket innebærer at programvaren utvikles og tilgjengeliggjøres av Visma, og installeres og driftes av kundene selv i deres eget IT-miljø, eller gjennom en driftspartner kunden har avtale med. For løsninger som er installert on-premise, har ikke Visma tilgang til logger, den installerte versjonen av programvaren hos kunden eller data kunden har lagret i løsningen, med mindre hver enkelt kunde gjør uttrekk eller aktivt gir Visma en tilgang. Visma får kun slik tilgang i forbindelse med konkrete og tidsavgrensede konsulentoppdrag eller i forbindelse med særskilte support-saker.

Den første feilmeldingen
Etter mottatt support-henvendelse fra Bergen kommune den 08.05.23, startet Visma feilsøking for å identifisere årsaken til den innmeldte hendelsen. Det ble klart fra logger at lagring til databasen hadde feilet, men KS hadde mottatt melding fra systemet om at levering hadde skjedd. Gjennom feilsøking ble Visma deretter kjent med en logisk brist i kildekoden i Familia, som førte til at tilbakemelding om vellykket lagring ble sendt når melding var registrert mottatt til Familia, men før lagring i databasen faktisk hadde skjedd. Saken ble eskalert til utviklingsteamet 09.05 for å starte arbeidet med å utvikle en programvarerettelse, for å sikre at tilbakemelding om mottatt melding først blir sendt når lagring til databasen er vellykket. Innledningsvis i saken jobbet Visma

ut fra en hypotese om at det sannsynligvis ikke fantes flere feil av samme art, hverken hos Bergen kommune eller hos andre kunder (nærmere om dette i 5.2.1).

Rettelsen til programvaren var ferdig utviklet og klar for testing internt i Visma 15.05, og ble etter vellykkede tester tilgjengeliggjort for Bergen kommune for videre testing dagen etter. Visma mottok 22.05 tilbakemelding om at testene av programvarerettelsen hos kommunen var vellykket, og at den senere samme dag ble satt i produksjon hos kommunen.

Det ble etter produksjonssetting meldt tilbake til Visma om behov for ytterligere justeringer i konfigurasjonsfilen og programvarerettelsen, og disse justeringene ble foretatt løpende av Visma. Bergen kommune installerte oppdatert versjon av programvarerettelsen, og bekreftet 25.05 overfor Visma at programvaren nå virker som den skal. Bergen kommune lukket deretter supportsaken.

Flere feilmeldinger
Senere 25.05 mottok Vismas support-team en ny henvendelse fra Bergen kommune med mistanke om at det var avdekket et nytt tilfelle der bekymringsmelding ikke var kommet frem til Familia. Bergen kommune og Visma startet umiddelbart en gjennomgang av logger fra Bergen kommune, for å undersøke om det kunne finnes flere hendelser. Visma tok kontakt med KS for å undersøke om lagringstiden for sendte meldinger kunne utvides frem til situasjonen var avklart. KS utvidet deretter lagringsperioden fra 14 til 30 dager.

31.05 hadde Bergen kommune og Visma i samarbeid avdekket totalt 24 logginnslag av den aktuelle typen avvik i perioden 01.01.21-31.05.23. To av disse logginnslagene var de to sakene som var blitt meldt inn til support hhv. 08.05 og 25.05, og ett tilfelle var inntruffet innen de siste 14 dagene, slik at bekymringsmeldingen kunne hentes ut fra KS og sendes til barnevernstjenesten på nytt. Det forelå dermed 21 tilfeller der bekymringsmeldinger ikke hadde nådd frem til barnevernet hos Bergen kommune og innholdet var tapt.

Basert på omfanget av avvik som ble avdekket den 31.05, besluttet Visma umiddelbart å gå ut med programvarerettelsen til alle kunder av Familia, som et preventivt tiltak frem til Visma kunne verifisere om det hadde forekommet tilsvarende avvik hos flere kunder.

På bakgrunn av det økte omfanget av avvik som ble avdekket hos Bergen kommune den 31.05, iverksatte Visma samme dag en innsats med å fremskaffe logger fra andre kunder for å kunne gjennomføre stikkprøver med formål om å undersøke hvorvidt flere kunder hadde avvik. Fordi Familia er en lokalt installert programvare som den enkelte kommune drifter selv, har Visma som utgangspunkt ikke tilgang til logger.

Gjennomgang av logger ble påbegynt 01.06. De første undersøkelsene ble gjort i loggene til Kommune B og Kommune C og viste ingen avvik.

I løpet av perioden 02.-04.06 foretok Visma undersøkelser av logger fra Kommune D, Kommune E, Kommune F og Kommune G. Visma fant ingen avvik tilknyttet bekymringsmeldinger hos Kommune D, tre avvik hos Kommune E og ett avvik hver hos henholdsvis Kommune F og Kommune G.

Pr. 04.06 var det totalt avdekket 29 bekymringsmeldinger som ikke var kommet frem, fordelt på kommunene Bergen kommune (24), Kommune E (3), Kommune F (1) og Kommune G (1). Basert på disse funnene besluttet Visma å gå ut med ytterligere informasjon til alle Familia-kunder som har aktivert Nasjonal portal for bekymringsmelding.

Basert på funnene av avvik 04.06, besluttet Visma å gå ut med ytterligere informasjon til alle kunder påfølgende mandag, 05.06, om at de kunne være berørt av avviket som ble informert om 31.05 og derfor måtte iverksette tiltak for å forhindre nye avvik og kartlegge omfang. Søndag 04.06 ble benyttet til å

- Ha dialog og statusmøter med Bergen kommune om videre oppfølging av saken
- Utforme og kvalitetssikre informasjon til kunder om avviket, tiltak og viktigheten av å gjennomføre tiltak
- Sammenstille en fullstendig oversikt over hvilke kunder som potensielt kunne være eksponert for feilen, herunder få oversikt fra KS over hvilke kommuner som hadde aktivert Nasjonal portal for bekymringsmelding (Visma var som utgangspunkt ikke involvert i oppsettet hos den enkelte kunde)
- Skaffe en liste over hensiktsmessige kontaktpersoner hos de aktuelle kundene
- Kontakte Datatilsynet for å få oversikt over kommunenes personvernombud slik at Visma kunne kontakte disse direkte
- Omdisponere ressurspersoner internt slik at alle de 242 kommunene på oversikten kunne ringes fortløpende fra og med påfølgende mandag

Varsling til alle kunder
Kunder som kunne være berørt ble informert pr. mandag 05.06.23 via Visma Community, pr. telefon, samt pr. e-post til personvernombudene (i henhold til informasjon mottatt fra Datatilsynet). Visma publiserte også en pressemelding med informasjon om hendelsen på visma.no, med bred distribusjon til norske lokal-, regional-, og riksmedier. Vismas mål med å benytte flere kommunikasjonskanaler var å sikre at noen hos hver kommune ville motta budskapet i løpet av mandag 05.06, slik at kommunene kunne agere raskt på informasjonen og forhindre nye avvik.

Informasjonen som ble delt med Vismas kunder inneholdt en oppfordring om å installere programvareoppdatering umiddelbart, samt sjekke logger for forekomst av avvik. Det ble også delt en beskrivelse av fremgangsmåte for hvordan logger kan sjekkes, da dette måtte gjøres av kundene selv fordi løsningen er driftet lokalt hos kundene (on-premise) og Visma ikke har tilgang til logger hos kunden uten at dette spesifikt deles med Visma.

Visma delte samtidig en artikkel på Visma Community til kunder av Visma Flyt Barnevern med to formål: Orientere om feilen i Familia, slik at tidligere Familia-kunder kunne undersøke om de hadde avvik før de migrerte til Visma Flyt Barnevern, samt orientere om at Visma Flyt Barnevern ikke er berørt av samme svakhet i kildekoden.

Gjennom kontakten med kunder 05.06 og påfølgende dager, kommuniserte Visma viktigheten av å installere programvarerettelsen, samt skaffe oversikt over hvorvidt og i hvilket omfang den enkelte kommune var berørt. Visma ba kunder om tilbakemeldinger angående omfang gjennom et skjema som ble publisert i artikkelen på Community. For kunder som hadde behov for bistand har

Visma stilt support- og konsulentpersonell til disposisjon, både til bistand med installering av programvarerettelsen og til gjennomgang av logger. Slik bistand har blitt gitt fortløpende. Pr. 14.06 hadde alle kommunene som har aktivert portalen bekreftet at de har installert programvarerettelsen.

Mulighet for gjenoppretting fra andre Visma-systemer
Der bekymringsmeldinger er sendt fra andre Visma-fagsystemer er det en mulighet for at kopi av meldingen kan ligge i avsender-systemet. Visma gjorde derfor et arbeid med å identifisere hvilke kunder som hadde sendt bekymringsmelding fra et annet Visma-fagsystem og i tillegg meldt inn avvik på mottakersiden. Visma tok et uttrekk med oversikt over meta-data om bekymringsmeldinger opprinnelig sendt fra det andre Visma-fagsystem til portalen for bekymringsmeldinger, og sendte dette som vedlegg til kunden som opprinnelig skulle mottatt meldingen. Informasjonen ble sendt 08.06 direkte til de åtte mottaker-kommunene dette gjaldt. I vedlegget fremgikk dato, klokkeslett og avsender av meldingen oppnevnt (gjeldende tjeneste), samt klient internID fra avsendersystem. Dersom dato for en innsendt bekymringsmelding i listen samsvarer med en melding som ikke har blitt mottatt i Visma Familia, så vil det være en mulighet for at avsender kan finne meldingen i fagsystemet meldingen ble sendt fra. Visma delte en beskrivelse av hvordan avsender-tjeneste kunne finne tapt melding og sende dem inn til aktuell barnevernstjeneste på nytt.

Søk etter rotårsak
Visma har iverksatt et arbeid for å få klarhet i hvorfor lagring til databasen i enkelte tilfeller feilet etter at melding var mottatt i Familia. Det faktum at det er svært skjev fordeling i hvilke kommuner som har avvik tilsier at lokale forhold kan være en del av svaret. Det kan også være at det er ulike forhold som fører til manglende lagring i ulike tilfeller.

Visma tok i løpet av den første uken etter mandag 05.06 kontakt med de kundene som har rapportert inn høyest antall avvik og ba om å få tilgang til et større utvalg logger, både logger fra applikasjonen og logger fra infrastruktur og database. Visma fant gjennom loggene tilfeller der avvik i Familia oppstod på samme tidspunkt som logger fra kommunens database viste at databasen var overbelastet. Det bemerkes at ikke alle kundene Visma har vært i kontakt med hadde logger for infrastruktur og database fra tidspunktene avvik inntraff, og Vismas analyser er derfor basert på et svært begrenset utvalg av logger.

I den oppdaterte versjonen av Familia, er det sammen med programvarerettelsen også inntatt utvidet funksjonalitet for logging i applikasjonen når lagring feiler. Disse endringene gir mer detaljer fra applikasjonen, men er ikke en erstatning for logger fra infrastruktur eller database (se nærmere om dette i punkt 6.2.1 og 6.3.5). Fredag 23.06 tok KS kontakt og gjorde Visma oppmerksom på at en bekymringsmelding var gått til print på grunn av at lagring feilet. Visma fikk tillatelse av den berørte kunden til å hente ut logger. Disse indikerer at serveren på samme tidspunkt som lagringen feilet, gjorde en større jobb med å ta backup av et annet system. Også dette tilfellet indikerer at overbelastning av kundens lokale infrastruktur var årsaken til at lagring feilet.

3.1.2 KS om hvordan feilen ble oppdaget, varslet om og rettet

Bergen kommune har i juni delt informasjon om tidslinjen for oppdagelse av feilen: 10.03.23 tok en ansatt i Bergen kommune kontakt med barnevernet for å etterlyse svar på bekymringsmelding sendt 01.02.23. Barnevernet opplyste at meldingen ikke var mottatt. Den ansatte registrerte avvik i kommunens kvalitetssystem, og barneverntjenesten avklarte den aktuelle bekymringen. Fra dette tidspunktet var barnet ivaretatt, og det var ingen indikasjoner på at omfanget var større enn denne ene saken. Behandlingen av avviket startet seinere i mars. I forbindelse med avvikshåndtering sendte Bergen kommune 12.04.23 spørsmål til KS om en melding som ble sendt gjennom NPB men ikke gjenfunnet i fagsystemet. Gjennom flere runder med undersøkelse av logger både hos KS og Bergen kommune ble det 08.05.23 konkludert med at meldingen hadde blitt sendt gjennom portalen, men ikke lagret i Visma Familia. Bergen kommune sendte melding til Datatilsynet om dette 16.05.23. KS henviste Bergen kommune til Visma for videre håndtering, da alt så bra ut i våre logger, og ingen andre kommuner hadde meldt om lignende problemer. I løpet av mai pågikk det en dialog om meldingen hvor KS veiledet i bruk av dashboard i NPB til kontroll på antall meldinger. Ved disse kontrollene oppdaget Bergen kommune at en annen melding, sendt 23.05.23, ikke hadde blitt lagret heller, til tross for at loggene i NPB viste at den var mottatt av Visma Familia. Denne meldingen ble sendt på nytt fra NPB, da den ble oppdaget før fristen for sletting i NPB.

KS hadde dialog både med Bergen kommune og Visma, og ga veiledning og bistand. Feilsøkingen måtte, grunnet feilens art, gjøres i fagsystemet, men KS ba om å bli oppdatert om feilens omfang. Bergen kommune hadde varslet personvernombud og Datatilsynet, noe som KS ellers hadde gitt anbefaling om. Så snart Bergen kommune visste at feilen berørte flere meldinger, og Visma sin feilsøking viste at feilen kunne gjelde flere kommuner, sendte Visma informasjon til alle kommuner som potensielt var berørt. 31.05.23 ble saken eskalert internt i KS, men KS var avhengig av informasjon fra Visma for å vite om flere enn Bergen var berørt. Når Bergen kommune og Visma samtidig gikk ut med informasjon om at flere kommuner kunne være berørt, samkjørte KS informasjon ut til kunder sammen med Visma, og orienterte Bufdir. I videre informasjonsarbeid samarbeidet Visma med begge parter, og henviste også til informasjon fra Datatilsynet.

Rettelse av feilen skjedde hos Visma og kommuner. KS bisto aktivt med informasjon og veiledning ved behov, både gjennom brukerstøtte, dialog med Visma og Bufdir, informasjon på ks.no og andre kanaler og organisering av et erfaringsdelingsmøte.

3.1.3 Datatilsynet om hvordan feilen ble varslet om

Datatilsynets kontaktperson for personvernombud ble kontaktet av Visma søndag 04.06.23. Visma ønsket bistand til å finne kontaktopplysninger til kommunenes personvernombud for å sikre at informasjonen om hendelsen kom frem til rett mottaker. Denne informasjonen ble delt med Visma.

Datatilsynet har mottatt avviksmeldinger om hendelsen fra 28 kommuner. Meldingene er sendt inn i tråd med kravene i personvernforordningen artikkel 33. Enkelte av disse var foreløpige meldinger om mulige brudd på personopplysningssikkerheten, og enkelte av disse kommunene kan gjennom undersøkelser ha kommet til at de ikke er berørt. Behandlingen av avviksmeldingene

er ikke avsluttet på rapporttidspunktet. Datatilsynet la ut informasjon om hendelsen med råd til kommunene på vår nettside den 05.06.23.

Som ledd i informasjonsinnhenting, hadde Datatilsynet et møte med Visma og et møte med KS og Bufdir den 06.06.23. Datatilsynet har også hatt et oppfølgingsmøte med Visma, og mottatt en rapport med beskrivelse av hendelsen og deres håndtering internt og overfor kommunene.

3.2 Vurdering av arbeidet med rettingen

Spørsmål som besvares i delkapittelet

B2. Hvordan vurderes arbeidet med rettingen, herunder informasjonen til berørte kommuner og tidsløpet fra oppdagelse til retting?

Operasjonalisering av spørsmålet:

- *Beskrive hvilken informasjon som ble gitt og når*
- *Beskrive arbeidet med selve rettingen av feilen (tidsløpet fra oppdagelse til retting), inkludert oppsummering av erfaringer fra berørte kommuner, hvis mulig*
- *Aktørene vurderer eget arbeid med rettingen, inkludert forbedringsmuligheter for fremtiden*

3.2.1 Vismas vurdering av arbeidet med rettingen

Se redegjørelse i 3.1.1. for tidslinje og saksforhold.

Visma har gjennom håndtering av saken erfart at dialogen med kommunene har vært god og effektiv. Videre er det Vismas oppfatning at samarbeid og informasjonsutveksling med KS, Bufdir og Datatilsynet har vært løsningsorientert, og bidratt til at saken ble håndtert på en konstruktiv måte.

3.2.2 KS' vurdering av arbeidet med rettingen

KS hadde brukeroppfølging direkte med kommuner, samt dialog med Visma, og direkte dialog med Bufdir om samkjøring, samt sjekk i dialog med Bergen kommune om at Datatilsynet og personvernombud var varslet.

KS publiserte og oppdaterte artikkel på ks.no og samkjørte informasjon med Datatilsynet og Bufdir. I tillegg ble det lagt ut nyhet og oppdatert spørsmål-og-svar-siden på https://portal.fiks.ks.no/sporsmal-og-svar-om-mottak-av-bekymringsmeldinger-juni-2023/ .

Fra dialog med kommuner så er det viktig å fremheve at kommunene syntes det var positivt at offentlige aktører og KS og Visma samkjørte informasjon ut. De gir Visma ros for kundedialogen, både skriftlig informasjon og kundeoppfølging gjennom flere kanaler, herunder telefon. Eneste

merknad som ble gitt var at det kunne være litt ineffektivt at informasjonsutveksling med Visma skjedde mye på Visma Community. Da det var mange berørte i kommuner, var det av og til litt tungvint å dele informasjon derfra til andre som jobbet med avvikshåndtering. Visma delte også direkte med KS hvilken informasjon som ble sendt, men KS opplevde også at det var mye informasjonsutveksling i Visma Community som kundene satt på, og baserte spørsmål til KS på, men som KS ikke hadde direkte tilgang til. Det er likevel bare en liten problemstilling hvor det ikke fantes en effektiv løsning for, og den store linjen er at kommunene har uttrykt at de opplevde all hjelp og informasjon fra Visma som meget bra.

3.2.3 Bufdirs vurdering av arbeidet med rettingen

Det viktigste formålet med den tidlige oppfølgingen var å rette svikten for å hindre at liknende feil skjer igjen, og å forsøke å finne ut hvilke barn eventuelle manglende meldinger gjelder.

05.06.23 publiserte Bufdir informasjon til norske kommuner på sine nettsider. I saken ble kommunene som benytter seg av Visma Familia oppfordret til å kontakte Visma for å finne ut om feilen gjelder egen kommune, og for å få bistand fra Visma i det tekniske arbeidet for å forsikre om at de har riktig og oppdatert programvare, samt få oversikt over antall- og hvilke meldinger som eventuelt var borte.

07.06.23 sendte Bufdir ut et brev i samarbeid med KS til norske kommuner med informasjon og anbefalinger om hvordan kommunene burde følge opp saken. I brevet ba også Bufdir kommunenes barnevernstjenester om å besvare en spørreundersøkelse for å kartlegge hvor mange bekymringsmeldinger som manglet, hvordan kommunene eventuelt ellers var påvirket av feilen og hva kommunene var i ferd med å gjøre for å rette opp i eller forhindre feil. Spørreundersøkelsen kom i tillegg til Vismas egen kartlegging over hvilke kommuner som var rammet av feilen. Det kom 166 svar på spørreundersøkelsen, som utgjør 68 prosent av landets 244 barnevernstjenester.

3.3 Kompenserende tiltak for meldinger som hadde gått tapt

Spørsmål som besvares i delkapittelet

B3. Hvilke tiltak ble satt i verk for å kompensere for meldinger som en må anta har gått tapt?

3.3.1 Vismas iverksatte tiltak for å kompensere for feilen

Tiltakene Visma satte i verk for å kompensere for feilen var å

- Rette den logiske bristen i kildekoden gjennom programvareoppdateringen tilgjengeliggjort 31.05.23
- Utvide loggfunksjonalitet gjennom programvareoppdateringen tilgjengeliggjort 31.05.23 for å forsøke å skaffe bedre innsikt i hvorfor lagring i kundes database feiler

- Kontakte KS for å undersøke om lagringstiden for bekymringsmeldinger sendt i portalen kunne utvides fra 14 dager. Lagringstiden ble deretter økt til 30 dager
- Kontakte alle kunder for å sikre installasjon av programvareoppdateringen
- Tilgjengeliggjøre informasjon om hvordan kunde/kommunen kan undersøke omfang ved å søke i sine logger
- Bistå kunder som har hatt behov for det med installasjon av programvarerettelse og søk i logger
- Ha løpende dialog med KS, Datatilsynet og Bufdir for å samkjøre informasjon. Brukt Visma Community som kanal for å bistå i å spre informasjon og tips fra KS, Datatilsynet og Bufdir
- Gi ytterligere informasjon til Familia-kunder som også har andre Visma-fagsystemer som kan melde saker til Familia via Nasjonal portal for bekymringsmelding om hvordan man kan forsøke å finne tilbake til meldingen i avsender-systemet
- Innhente tilbakemeldinger fra kunder for å få oversikt over omfanget av avvik
- Arbeid for å analysere hvorfor lagring til databasen i enkelte tilfeller hos enkelte kommuner feiler

3.3.2 KS om tiltak ble satt i verk for å kompensere for tapte meldinger

Visma har bistått kommuner med å finne ut hvilke meldinger som ikke har blitt lagret i fagsystemet. Noen kommuner har innhentet ekstra teknisk støtte. Hva man visste om meldingene var avhengig av hvilken kanal som var benyttet: SvarUt eller NPB. Meldinger (og andre forsendelser) som ble sendt gjennom SvarUt kunne gjenfinnes i sin helhet. For bekymringsmeldinger som ble sendt gjennom NPB var kun tidspunkt kjent, i tillegg til om melder hadde brukt skjema for offentlig eller privat melder. Tiltakene som ble iverksatt dreide seg primært om å få melderne til å ta kontakt med barnevernstjenesten for å sjekke at meldingene de har sendt er mottatt.

KS vet at kommuner har oppfordret bredt om å melde på nytt eller sjekke om meldingen ble mottatt. Både gjennom media og ved direkte kontakt med samarbeidspartnere har kommunene forsøkt å nå ut til så mange som mulig. Flere kommuner har, basert på hvilke offentlige virksomheter som sender flest bekymringsmeldinger, tatt direkte kontakt og bedt dem å kontrollere deres meldinger med loggene fra kommunen. Dette gjaldt både kommunale virksomheter, som skoler og barnehager innenfor barnevernssamarbeid, og ikke-kommunale virksomheter som Politiet. Noen kommuner, som Bergen kommune, oppbemannet barnevernstjenestemottak for å kunne ta imot spørsmål og ekstra meldinger. I noen kommuner var det mange privatpersoner som hadde meldt bekymring til barnevernet, som ringte for å forsikre seg at meldingen hadde blitt mottatt (og barnevernet dermed hadde hatt mulighet å følge opp barn som trengte hjelp). Hos de kommunene KS har hatt kontakt med var ingen av disse private meldingene tapt.

4. Konsekvenser av feilen

4.1 Vurdering av feilens langsiktige konsekvenser for berørte barn

Spørsmål som besvares i delkapittelet

C1. Hvordan vurderes risikoen for at feilen, etter at kompenserende tiltak som er satt i verk, kan ha langsiktige konsekvenser som følge av at omsorgssvikt grunnet denne feilen ikke blir oppdaget eller oppdages først etter så lang tid at barn har lidd et signifikant velferdstap?

4.1.1 KS' vurdering av feilens langsiktige konsekvenser for berørte barn

Den største risikoen for langsiktige konsekvenser vurderes å være for barna som er omfattet av bekymringsmeldingene man ikke har lykkes med å spore opp, da man ikke vet om disse barna lever med omsorgssvikt. Alvorligheten i de enkelte av disse meldingene vil det ikke være mulig å si noe konkret om, nettopp fordi man ikke kjenner til meldingens innhold. At man ikke kan utelukke at én eller flere av disse meldingene omhandler svært alvorlige forhold gjør hendelsen kritisk.

I KS sin vurdering av risiko vil de se på muligheten for at barnevernstjenesten er kjent med barna, selv om de ikke har lykkes med å koble meldingene som har blitt borte til barna.

Med det vi vet nå må vi forutsette at det er tilfeldig hvilke meldinger som ble borte. Statistisk (Kostra, tall for 2022) omhandler 38 prosent av bekymringsmeldinger barn det allerede er undersøkelse eller aktive tiltak for, mens 47 prosent av meldingene går til undersøkelse. Øvrige meldinger blir henlagt. Samme statistikk viser at det for 37 prosent av undersøkelsene konkluderes med behov for videre oppfølging i en eller annen form.

Å bruke denne statistiske fordelingen på de 57 meldingene som er borte vil neppe gi et riktig bilde av omfanget eller alvorligheten. Men det gir grunn til å anta at flere av de slettede meldingene omhandler barn barnevernet kjenner til, enten fordi det allerede pågikk undersøkelse eller tiltak, eller fordi andre meldere har meldt bekymring for samme barn senere. At man antakelig kjenner til flere av barna underbygges av kommunenes tilbakemeldinger om at offentlige meldere med meldeplikt ofte følger opp meldingene de har sendt, eller sender på nytt dersom de ikke hører noe. Der bekymringen er særlig stor vil en slik oppfølging i større grad være tilfelle.

I hovedsak må man kunne konkludere med at det må ha sviktet flere steder enn i den tekniske løsningen, for at bekymringsmeldinger sendt av offentlige meldere med meldeplikt ikke er fanget opp av barnevernet på andre måter, etter de kompenserende tiltakene som er gjort. Selv om sannsynligheten kan vurderes som moderat, vil det for det enkelte barnet som er utsatt for omsorgssvikt være alvorlige konsekvenser. KS mener derfor at det ikke er grunn til å nedvurdere alvorligheten i situasjonen, men at omfanget antakelig er begrenset.

4.1.2 Helsetilsynets vurdering av feilens langsiktige konsekvenser for berørte barn

Helsetilsynet har innhentet informasjon fra statsforvalterne om hvordan de har fulgt opp denne saken. Statsforvalterne har sørget for at de er oppdaterte på tilstanden i sine kommuner. De har rapportert til Helsetilsynet at de så langt vurderer at kommunene tidlig gjorde det de kunne for å få nødvendig oversikt over svikten, og at de gikk tidlig i gang med egnede oppfølgingsaktiviteter.

Så vidt Helsetilsynet er kjent med, vil det trolig ikke være mulig å avdekke hvilke bekymringsmeldinger eller dokumenter som mangler, hva som er innholdet i dem eller hvem meldingene kommer fra. Undersøkelsene som er gjennomført så langt har derfor ikke klarlagt hvilke konkrete barn som er rammet av svikten.

Helsetilsynets vurdering av hvilke konsekvenser feilen har hatt for enkeltbarna som er rammet blir derfor generelle. Barnevernet er avhengig av informasjon fra personer og tjenester rundt barna for å settes i stand til å følge opp eventuell bekymring. Funn fra Helsetilsynets rapport «Det å reise vasker øynene – en gjennomgang av 106 barnevernssaker» viser at det kan få alvorlige konsekvenser for barna dersom bekymringsfull informasjon glipper. Alvorlig bekymring avdekkes ikke, eller det avdekkes først på et senere tidspunkt når barnas problemer har eskalert. Undersøkelser og tiltak tilpasses ikke barnets behov og situasjon, og dermed får ikke barna og familien den hjelpen de trenger.

Kommunene selv er de viktigste til å følge opp og gjøre det de kan for å finne barna svikten omhandler og sørge for at de får hjelp. For å redusere konsekvenser for barn vurderer Helsetilsynet at tilsyn kan være egnet til å bidra til å styrke sikkerhet og kvalitet i tjenestene fremover i tid slik at lignende svikt ikke gjentar seg.

4.1.3 Bufdirs vurdering av feilens langsiktige konsekvenser for berørte barn

Vi mangler kunnskap om innholdet i bekymringsmeldingene som har gått tapt. Vurderingen av risikoen for langsiktige negative konsekvenser er derfor basert på generell kunnskap om bekymringsmeldinger og den aktuelle hendelsen.

Det er kritisk og svært alvorlig at kommunene ikke har lyktes i å gjenfinne informasjon fra flere av de tapte bekymringsmeldingene. Det kan føre til at barn som lever under omsorgssvikt ikke blir oppdaget, eller oppdages for sent. Det er generelt forbundet høy risiko ved å leve under vedvarende omsorgssvikt. De langsiktige negative konsekvensene kan være knyttet til svakere skolegjennomføring, dårligere helse, svekket tilknytning til arbeidsmarkedet, dårligere livskvalitet og økte kostnader for samfunnet i form av økte trygdeytelser.

Sakens omfang er begrenset, sammenlignet med hva man fryktet i den tidlige fasen etter at feilen ble kjent. Risikoen for langsiktige negative konsekvenser av hendelsen *på samfunnsnivå* er derfor begrenset. Hadde saken hatt et vesentlig større omfang, ville risikoen for langsiktige negative konsekvenser være betydelig høyere.

Risikoen for langsiktige konsekvenser er likevel stor *for de barna det gjelder*, avhengig av hvorvidt barnevernstjenesten har klart å gjenfinne informasjon fra den tapte meldingen, og hvor lang tid det tok. Risikoen for negative konsekvenser vil være størst for de sakene hvor man ikke klarte å gjenfinne informasjon fra den tapte meldingen, mens risikoen vil være mindre der man klarte å gjenfinne informasjon. Risikoen vil øke avhengig av hvor lenge viktig informasjon ble forsinket til barnevernstjenesten, som følge av feilen.

Det faktum at en vesentlig andel av bekymringsmeldinger til barnevernet ikke er alvorlige (henlegges) kan bidra til å redusere risikoen for langsiktige konsekvenser av hendelsen. Det at noen av sakene sannsynligvis ville være kjent for barnevernet fra før, og/eller at det ville kommet en ny melding om barnet etter en viss tid, kan også bidra også til å redusere risikoen for langsiktige konsekvenser av hendelsen (se nærmere utdypning om faktorer som kan bidra til å øke eller moderere risiko under).

Det er risiko for at *omdømmetap* som følge av feilen kan ha hatt skadevirkning. Medieoppmerksomheten rundt saken kan ha svekket tilliten til barnevernet generelt og systemene for å melde til barnevernet. Dette kan igjen føre til at færre melder inn bekymring. I følge KS erfarer kommunene at feilhendelsen kan ha bidratt til å svekke tilliten til barnevernet og meldingsløsningene, men konsekvensen synes å være at meldere og mottakere i økende grad kontrollerer om meldinger har kommet fram, ikke at de lar være å melde (jf. pkt. 4.3.1).

<u>Nærmere om faktorer som kan bidra til å øke eller moderere risiko:</u>

En av fem bekymringsmeldinger er så alvorlige at de leder til undersøkelse og videre til tiltak
Bekymringsmeldinger har varierende alvorlighetsgrad. Mens noen bekymringsmeldinger er svært alvorlige og kan føre til akuttiltak, er andre bekymringsmeldinger mindre eller ikke alvorlige. I 2022 gjaldt 38 prosent av bekymringsmeldingene barn som allerede var kjent for barnevernet, enten ved at det allerede var pågående tiltak eller en pågående undersøkelse. 15 prosent av alle bekymringsmeldinger ble henlagt. Det vil si at over halvparten av meldingene gjaldt barn som var kjent for barnevernstjenesten fra før eller barn der det ble vurdert at det ikke var behov for å starte undersøkelse. Av de resterende 47 prosent av meldingene som gikk til undersøkelse, ble i underkant av to tredjedeler henlagt, mens 36 prosent førte til tiltak. Vi kjenner ikke innholdet i bekymringsmeldingene som har gått tapt, men ut fra statistikken kan vi estimere at i underkant av en av fem ville ha ledet til undersøkelse og derfra videre til tiltak. Dette er forhold som bidrar til å redusere risikoen for langsiktige konsekvenser av hendelsen.

Det kan komme inn flere bekymringsmeldinger om samme sak
Det kan komme inn flere bekymringsmeldinger i samme sak. Når en tapt bekymringsmelding var den første bekymringsmeldingen på barnet, er dette potentielt svært alvorlig, spesielt dersom barnet befinner seg i en skadelig omsorgssituasjon som er godt skjult.

I 2022 fikk 49 400 barn til sammen rundt 80 000 meldinger. Siden en melding kan omhandle flere barn, er det ikke mulig å beregne antall meldinger sendt per barn for et gitt år. Tallene viser likevel at noen barn får mer enn en bekymringsmelding per år. Det kan også komme flere bekymringsmeldinger om samme sak over en lengre periode. Det er derfor en viss sannsynlighet for at noen av de tapte meldingene omhandlet saker som var kjent for barnevernstjenesten fra

før. Det er også en viss sannsynlighet for at det ville kommet en ny melding om barnet etter en tid. Dette er forhold som bidrar til å redusere risikoen for langsiktige konsekvenser av hendelsen.

Samtidig kan nye bekymringsmeldinger om barn som barnevernstjenesten kjenner til fra før tilføye viktige opplysninger som bidrar til å belyse saken bedre og hjelpe barnet på en bedre måte. Tap av «supplerende» bekymringsmeldinger kan dermed føre til tap av relevante opplysninger som kunne vært viktig for videre oppfølging av saken.

Videre vil en forsinkelse i mottak av melding (i tilfeller hvor en melding gikk tapt, men det kom en ny melding etter noe tid) kunne bidra til å forsterke de mulige negative virkningene for barnet. Det finnes ikke oversikt over hvor lang tid det går mellom én og eventuell neste bekymringsmelding på samme barn, men vi må anta at det kan ta lang tid før noen andre enn den opprinnelige melderen også oppdager situasjonen og sender en egen bekymringsmelding, eller før den opprinnelige senderen sender en melding til. Dette er verdifull tid hvor barnet lever lenger enn "nødvendig" under omsorgssvikt, og kan lide et potensielt signifikant velferdstap. I 2022 ble de fleste meldingene sendt fra politi/lensmann, barnevernstjenesten, mor/far/foresatte, skole og lege/sykehus/tannlege. Til sammen utgjorde disse meldere nesten 60 prosent av alle sende meldinger. Dette er aktører som er tett på mange barn på ulike arenaer og det er derfor et håp om at en av disse ville oppdage barnet og sende en bekymringsmelding etter hvert.

4.2 Sammenheng mellom feilen og trenden med færre bekymringsmeldinger?

Spørsmål som besvares i delkapittelet

C2. Kan det være en sammenheng mellom feilen og trenden med færre bekymringsmeldinger til barnevernet?

4.2.1 Bufdirs vurdering av sammenhengen mellom feilen og trenden med færre bekymringsmeldinger

Da feilen om teknisk svikt ble kjent oppsto raskt en hypotese om at det kunne være en mulig sammenheng mellom den tekniske svikten og trenden med færre bekymringsmeldinger til barnevernet. Tallene på nasjonalt nivå viser at det overordnet har vært en nedadgående trend i antall meldinger og antall barn med melding helt siden 2017. Nedgangen har likevel vært særlig sterk de to siste årene, med 7000 færre meldinger fra i 2022 enn i 2020. Denne sterke nedgangen sammenfaller både med perioden med feil i systemet, Covid19-pandemi og innføring av barnevernsreform.

Når vi nå vet at feilen gjelder 22 kommuner som har identifisert et begrenset antall tapte meldinger, kan vi med større sikkerhet enn da svikten ble oppdaget konkludere med at nedgangen i antall bekymringsmeldinger de siste årene skyldes andre forhold enn teknisk svikt. Vi ser også at

nedgangen er like tydelig i kommuner som ikke er rammet av feilen, som i kommuner hvor feilen er identifisert.

Nasjonale tall er lite egnet til å belyse om nedgangen i antall bekymringsmeldinger de siste årene kan skyldes at meldinger ikke har nådd frem, ettersom de tilslører forskjeller mellom kommuner. Bufdir har derfor sammenlignet trenden i antall bekymringsmeldinger for utvalgte kommuner som vi vet var berørt av svikt i den nasjonale løsningen for elektronisk bekymringsmelding og som benytter fagsystemet Familia, med kommuner som ikke var berørt av svikt, og som benytter fagsystemet Dipsbarnevern. Tallene viser at den nedadgående trenden også finnes i kommuner som ikke er berørt av feilen, slik som for eksempel Trondheim og Bærum. I tillegg ser vi at den nedadgående trenden for kommuner vi vet er rammet, slik som Oslo og Bergen, startet før andre halvår 2020.

Bufdir konkluderer med at nedgangen i antall bekymringsmeldinger de siste årene skyldes andre forhold enn teknisk svikt.

	2017	2018	2019	2020	2021	2022	Prosentvis endring fra 2019 til 2022
OSLO	3312	3112	3075	3135	2720	2596	-15,6
BERGEN	1333	1213	1115	1121	1028	996	-10,7
DRAMMEN	730	594	521	628	471	489	-6,1
TROMSØ	389	334	393	433	395	376	-4,3
STAVANGER	580	660	616	643	649	618	0,3
TRONDHEIM	713	746	701	805	705	642	-8,4
BÆRUM	437	347	391	422	366	324	-17,1

Kilde: Kommunenes halvårsrapportering

Kommuner markert oransje benytter fagsystemet Familia, mens kommuner i blått benytter fagsystemet Dips Barnevern.

Tabell 3. Antall gjennomgåtte bekymringsmeldinger for utvalgte kommuner i løpet av siste halvår 2017-2022

4.3 Økonomiske og administrative konsekvenser for kommunene

Spørsmål som besvares i delkapittelet

C3. Hvordan vurderes de økonomiske og administrative konsekvensene av feilen for kommunene?

4.3.1 KS om økonomiske og administrative konsekvensene av feilen for kommunene

Direkte økonomiske og administrative konsekvenser for kommunene er i hovedsak knyttet til tiltak for å hindre at tilsvarende feil oppstår igjen. Selv om tiltakene varierer fra kommune til kommune, synes økte ressurser til manuelle kontroller av de digitale systemene å være en gjennomgående konsekvens. Her melder noen kommuner at det krever betydelige ressurser, som har den konsekvensen at man må stramme inn på andre områder eller bemanne opp. Andre beskriver langt mindre konsekvenser, der en ansatt ved barnevernskontoret kan gjøre en forholdsvis hurtig ukentlig sjekk. Samlet omfang av dette er det for tidlig å si noe om, og flere melder at de ikke er sikre på at de har landet på de riktige tiltakene. Det er også usikkert om disse tiltakene vil bli permanente, eller er midlertidige for å forsikre seg om at retting av den aktuelle feilen har ønsket effekt. Kommunene har tilgang på et dashboard på forvaltningssidene til KS, hvor kommuner kan følge med på antall mottatte meldinger gjennom NPB og sjekke logg per melding. Dette brukes nå mer aktivt i kommunene enn før avviket. Noen kommuner meldte på erfaringsdelingsmøte i regi av KS at de allerede hadde laget egne løsninger hvor antall fra NPB sammenlignes med antall mottatt i fagsystem.

Ressursbruken var vesentlig i perioden rett etter at avviket ble kjent. Flere kommuner satt krisestab. Både barnevernsfaglige, tekniske og lederressurser brukte mye tid på mediehåndtering, informasjonsarbeid ut mot potensielle meldere hvis melding ikke hadde kommet fram, jobbet med feilsøking og tekniske avklaringer.

Feilen har gitt økt oppmerksomhet også på bruk av andre fellesløsninger, som Altinn og SvarUt. Det har i minst ett tilfelle gjort at man iverksetter større og bredere gjennomganger av kommunens bruk av digitale forsendelser, og også har satt av betydelige midler til interne og eksterne gjennomganger av den totale digitale informasjonsflyten.

KS har først og fremst hatt dialog om denne saken med kommunene som avdekket meldinger som ble borte. Den økte ressursbruken de beskriver vurderes som like aktuell for alle kommuner, uavhengig av om de var berørt av feilen. Det er likevel usikkert om øvrige kommune i like stor grad har økt sin ressursbruk på dette området.

Indirekte administrative og økonomiske konsekvenser kan i noen grad sannsynliggjøres. Dersom barn med behov ikke fanges opp tidlig kan det gi behov for tyngre og mer kostbare tiltak siden – enten i barnevernstjenesten eller andre deler av tjeneste- eller hjelpeapparatet. Kommunenes tilbakemelding er at feilhendelsen kan ha bidratt til å svekke tilliten til barnevernet og meldingsløsningene. Dersom en slik svekket tillit fører til senere bekymringsmeldinger eller dårligere samarbeid rundt barn med behov, vil også det kunne bidra til økt ressursbruk, dyrere tiltak eller fordeling av oppgaver som ikke er ønskelig. Kommunene melder likevel at svekket tillit i større grad kan antas å ha hatt som konsekvens at både meldere og mottakere kontrollerer om meldinger har kommet fram; ikke at de lar være å melde.

5. Årsaksforhold og forebygging av fremtidige feil

5.1 Årsaker til feilen

Spørsmål som besvares i delkapittelet

D1. Hva var årsaken til feilene?

5.1.1 Visma om årsakene til feilen

Det er tre ulike faktorer som spiller inn i hvorfor enkelte bekymringsmeldinger som er sendt fra Nasjonal portal for bekymringsmelding er gått tapt og ikke kan gjenopprettes:

1. Enkelte bekymringsmeldinger som er sendt fra Nasjonal portal for bekymringsmelding har ikke blitt lagret korrekt i fagsystemet Familia. Årsaken er at lagring til kommunens database feilet. Vismas rotårsaksanalyser viser at for de kundene Visma har mottatt logger fra har det vært høy belastning på infrastrukturen hos kommunen i det øyeblikket Familia har mottatt og skal prosessere melding fra KS. Lagringen til SQL-databasen har derfor ikke vært vellykket, og løsningen har dermed forkastet data grunnet utilgjengelig SQL-database.
2. Mekanismen som skulle sende en feilmelding i tilfeller der en bekymringsmelding ikke er lagret i Familia har ikke fungert som den skal grunnet en logisk brist i kildekoden i Familia. Til tross for at meldingen ikke ble lagret i Familia, sendte Familia tilbakemelding til Nasjonal portal for bekymringsmelding om at bekymringsmeldingen var mottatt. Dette skyldes en svakhet i koden som gjorde at en slik bekreftelsesmelding ble trigget i det Familia mottok meldingen og ikke på det tidspunktet meldingen var lagret i Familia. Svakheten i koden har dermed medført at det i tilfeller der lagringen feilet (ref. punkt 1 over), ikke ble generert en feilmelding til KS eller innsender av saken. En slik feilmelding ville medført at dokumentet gikk til print og ble sendt i post i stedet for digitalt mottak, som er KS sin standard B-løsning for dokumenter som ikke kommer frem digitalt gjennom Nasjonal portal for bekymringsmelding.
3. Fordi KS ikke har selvstendig behandlingsgrunnlag for å oppbevare bekymringsmeldingene over tid, sletter de bekymringsmeldinger fra sin database 14 dager etter at fagsystemet har bekreftet mottak av meldingen. Dermed kan ikke bekymringsmeldinger som ikke ble korrekt lagret gjenopprettes lenger tilbake i tid enn 14 dager.

For at en bekymringsmelding skal gå tapt, må årsak 1 og 2 opptre samtidig, og avviket ikke bli oppdaget før etter 14 dager.

5.1.2 KS om årsakene til feilen

En programfeil i fagsystemet Visma Familia gjorde at meldinger som ikke ble lagret i fagsystemet likevel ble bekreftet som vellykket håndtert av fagsystemet til fellesløsningene fra KS. Feilen gikk ut på at Visma Familia ga beskjed til fellesløsningene fra KS (SvarUt og NPB) at meldingen hadde blitt mottatt, før disse faktisk ble lagret i fagsystemet. I de fleste tilfellene ble meldingen lagret i fagsystemet, mens det viser seg nå at noen av meldingene ikke ble lagret. Da KS sine løsninger fikk kvitteringer, er det ikke mulig å se i KS sine logger hvilke meldinger dette gjaldt.

NPB
Ved utvikling av NPB ble det vurdert, av KS og Bufdir, at KS ikke hadde databehandlingsgrunnlag for å lagre bekymringsmeldinger sendt gjennom NPB lenger enn 14 dager. Grunnet overvåkingsrutiner og andre risikoreduserende tiltak (som å sende meldinger i post dersom de ble avvist av fagsystem), ble 14 dager vurdert som tilstrekkelig lagringstid for at alle meldinger skulle komme frem. Dermed ble de aktuelle meldingene rutinemessig slettet fra KS sine servere, uten at de var lagret noe annet sted. NPB sender meldinger som blir avvist av fagsystemet videre til print og postforsendelse. Meldingene i hendelsen ble kvittert ut som mottatt, og dermed ble ikke disse sendt videre.

SvarUt
Forsendelser gjennom SvarUt som ikke ble lagret i Visma Familia hadde blitt lagret hos KS. Her er lagringstid ikke begrenset til 14 dager. Vurderingen om 14 dagers lagringstid ble gjort spesifikt for NPB, siden NPB er spesifikk for bekymringsmeldinger til barnevernet.

5.2 Hvorfor tok det tid før feilen ble varslet om?

Spørsmål som besvares i delkapittelet

D2. Hva var årsakene til tiden som gikk fra feilen først ble oppdaget til brukerne og andre berørte aktører ble varslet?

5.2.1 Visma om tidsløpet fra feilen ble oppdaget til berørte aktører ble varslet

Da den første saken ble meldt til Visma 08.05.23, arbeidet de ut fra en hypotese om at det kun var én feil, og at feilen kun berørte én kunde. Hypotesen ved mottak av den første support-saken var basert på kombinasjonen av følgende momenter:

1. Visma er kjent med at det er spesielle kjennetegn ved Bergen kommune sin infrastruktur og konfigurasjoner av programvaren som skiller seg fra andre kunder, og at det derfor var sannsynlig at feilen kunne ha sammenheng med lokale forhold.
2. Det ble i tillegg kun meldt fra om ett enkeltstående tilfelle av manglende melding. Visma hadde ingen indikasjon på at hendelsen skulle gjelde flere meldinger, dels på grunn av tiden som har forløpt uten innmelding av lignende hendelser i lys av kjennskap til at

Nasjonal portal for bekymringsmelding i stor grad benyttes av offentlige aktører, som er kjent med svarplikt og behandlingstider hos barnevernet (for eksempel plikt til tilbakemelding innen 3 uker, jf. barnevernsloven § 13-3), og dels på grunn av at lokalt installert programvare kan virke ulikt i ulike miljøer.

Da Visma fikk sikker kunnskap om et større omfang av avvik i loggen hos kunden som meldte den første saken, gikk Visma ut med informasjon til alle kunder samme dag. Parallelt startet Visma et arbeid med å fremskaffe logger fra andre kunder for å kunne undersøke om flere var rammet. Hos de første tre kundene Visma undersøkte, fantes ingen avvik. Det ble i løpet av helgen 02.-04.06.23. påvist avvik i logg hos tre kunder, og Visma startet dermed forberedelser for å gi korrekt, rask og hensiktsmessig informasjon til alle kunder fra og med mandag 05.06.23. Se nærmere beskrivelse i punkt 3.1.1.

5.2.2 KS om tidsløpet fra feilen ble oppdaget til berørte aktører ble varslet

Viser til 5.2.1. KS har overvåkingsrutiner, og følger blant annet med på om meldinger som blir avvist av fagsystem faktisk sendes til print og post. KS hadde ingen informasjon om mulige feil i loggene, da meldingene ble kvittert som mottatt av fagsystem. Da Bergen kommune tok kontakt med KS første gang om en melding som muligens ikke hadde kommet fram til barnevernstjenesten, henviste KS' brukerstøtte til Visma som leverandør og ga informasjon om meldingen basert på loggen i NPB. Det har ikke kommet inn lignende henvendelser med mistanke om feil fra andre kommuner, og overvåking av NPB og SvarUt ga ingen tegn på avvik. Da det viste seg at meldingen faktisk ikke hadde blitt lagret, ga KS bistand med veiledning til feilsøking. Dialog med Visma ble også opprettet. Det var i disse første dagene ikke grunn for KS å anta at flere meldinger eller kommuner var berørt, men KS ba Visma å oppdatere dem kontinuerlig om kartlegging av feilen.

I KS sin oppfølging av feilen har de vært i dialog med kommuner som forteller om enkeltstående eksempler på at samarbeidsparter hadde tatt kontakt om bekymringsmeldinger de hadde sendt, men som barnevernstjenesten ikke hadde mottatt. Som en sa det: «Den digitale selvtilliten er så lav, at man stoler mindre på sin egen kompetanse enn på de digitale systemene». Så når noe ikke går som forventet forklares det ofte med brukerfeil, og det meldes ikke avvik som kan følges opp. Denne type mekanismer, i tillegg at det for flere kommuner kun gjaldt én melding, kan være en forklaring på at det tok tid fra symptomene på feilen først ble merket i en kommune (ikke nødvendigvis Bergen) til den ble identifisert og varslet som en teknisk feil.

At det var snakk om en teknisk feil, ble avdekket av Bergen kommune i samarbeid med Visma og KS. Da barnevernstjenesten ikke fant en melding som ble etterlyst av melder sendte de henvendelse til KS. Det tok 33 dager fra avviket ble registrert til Bergen kontaktet KS om saken, og 26 dager fra KS ble kontaktet til det ble identifisert at avviket skyldes en teknisk feil i Familia. Barnevernstjenesten var, helt fra avviket ble registrert, kjent med den aktuelle meldingen, og det var ingen indikasjon på at det var et generelt problem som lå bak. Avviket ble håndtert deretter. Bergen kommune var avhengig av både KS og Visma for å kunne eliminere og identifisere feilkilder, og alt dette bidro til at det tok tid.

Da feilen var identifisert var det fortsatt ingen indikasjoner på at dette gjaldt andre meldinger eller andre kommuner. Da Bergen kommune den 25.05.23 avdekket en ny melding som ble borte 23.05.23 ble det iverksatt ytterligere tiltak for å avdekke avvik. 31.05.23 ble det klart for Bergen kommune at det totalt dreide seg om 24 meldinger i Bergen som var borte. Kommunen begynte umiddelbart å varsle berørte aktører i takt med at man fikk oversikt over situasjonen. 5 dager etter omfanget var kjent, ble allmennheten orientert gjennom media.

Da den enkelte kommune også utenfor Bergen ble kjent med at meldinger var borte i deres kommune, er det KS sin oppfatning at informasjon om dette ble gitt umiddelbart.

5.3 Hendelsesforløpets og tidligere risikovurderinger

Spørsmål som besvares i delkapittelet

D3. Omfattes hendelsesforløpet av eventuelle risikovurderinger som er gjort tidligere?

5.3.1 Visma om tidligere risikovurderinger

Visma har risikovurderinger som dekker både Familia som produkt, og den generelle risikoen for at et av selskapets produkter kan rammes av et personvernbrudd. Risikovurderingene dekker i hovedsak

- Produktsikkerhet
- Personvern og privacy by design
- Leverandørvalg

Risiko for at personopplysninger kan gå tapt er dekket, og risiko for at feil kan oppstå i integrasjoner, men dette spesifikke scenarioet er ikke beskrevet.

5.3.2 KS om tidligere risikovurderinger gjort av KS og kommunene

Kommunene
KS antar, basert på brukerdialog, at de fleste kommunene har tatt med i egne risikovurderinger at personopplysninger kan gå tapt. I tillegg har kommuner egne barnevernsfaglige risikovurderinger som kan omfatte hendelsesforløpet. KS vet også at flere offentlige meldere har rutiner for å ta kontakt med barnevernet for å forsikre seg om at meldingen er mottatt.

For SvarUt, og mer generelt alle fellesløsninger fra KS Digitale fellestjenester, gjøres det tilgjengelig ROS- og DPIA-mal som kommuner kan bruke for å ferdigstille egne risikoanalyser og personvernvurderinger. Akkurat denne hendelsen er ikke konkret beskrevet som en risiko, men flere punkter er aktuelle for hendelsen, som tidlig varsling og god testing med fagsystemleverandør.

KS

Når det gjelder NPB, så var risikoen ved at fagsystemet sendte kvittering på mottatt melding uten at meldingen ble lagret ikke identifisert som en egen risiko. Det er i juni 2023 tatt inn i ROS-malene som KS Digitale fellestjenester gjør tilgjengelig for kommuner som bruker tjenesten.

Under utviklingen av NPB i samarbeid med Bufdir identifiserte KS risikoen for at fagsystemet ikke kvitterer for mottak av bekymringsmeldinger som er sendt gjennom portalen. Kompenserende tiltak var å bygge funksjonalitet for sending via ordinær post i de tilfellene. Dette skjedde før implementering av NPB. For bekymringsmeldinger sendt gjennom NPB ble i tillegg meldinger lagret i 14 dager i NPB, og ikke umiddelbart slettet etter mottak av fagsystem, manuell nedlastning eller forsendelse i post. Forsendelser sendt gjennom SvarUt blir ikke slettet.

Kommunene meldte i august 2021 om en risiko for menneskelige feil i registrering av post, og at bekymringsmeldinger fra portalen av den grunn ikke ble fanget opp. Kompenserende tiltak ble iverksatt juni 2022, ved at det ble gjort tilgjengelig et dashbord der kommunene kunne hente ut oversikt over innkomne bekymringsmeldinger til bruk i egen internkontroll. En slik internkontroll, med sammenligning av registreringer i fagsystemet med opplysninger på dette dashbordet, kunne potensielt avdekke avvik som skyldtes den aktuelle feilen i Familia. KS vet fra brukerdialog at flere kommuner eller IKT-samarbeid allerede hadde innført (delvis) automatiserte kontrollrutiner basert på egne ROS-vurderinger før avviket ble kjent i juni 2023.

5.3.3 Bufdir om tidligere risikovurderinger

Prosjektet Nasjonal portal for bekymringsmelding var et av delprosjektene i DigiBarnevern, som blant annet har utviklet nye og forbedret digitale løsninger for statlig og kommunalt barnevern. Prosjektet DigiBarnevern hadde store ambisjoner om å levere på regjeringens IKT-politikk, og særlig målsetningene om «brukeren i sentrum» og at «staten tar en stor rolle i løsninger som dekker stat og kommune».

Delprosjektet NPB hadde som ambisjon å levere én felles løsning for å levere bekymringsmelding - til alle landets barnevernstjenester. KS sin FIKS-plattform, som er den samme teknologien og plattform som brukes for andre digitale brev til og fra landets kommuner, ble i konsept- og planleggingsfasen vurdert av prosjektet[10] til å være den beste felleskomponenten for å realisere portalen. Med denne løsningen kunne man:

1. Levere bekymringsmelding som digital post til kommuner som er forberedt for dette.
2. Sørge for automatisk utskrift, konvoluttering og forsendelse i fysisk post til kommuner som ennå ikke er forberedt.
3. Når kommunale fagsystemer er på plass kan bekymringsmelding sendes direkte inn i til kommunenes løsning(er) - uten at postmottak og andre instanser er involvert.

I 2019 var det planlagt at portalen skulle utvikles, driftes og forvaltes av Bufdir, i statlig regi.

Når det gjelder risikovurderinger ble det i denne perioden lagt særlig lagt vekt på to punkter:

[10] Prosjektet DigiBarnevern (Bufdir, DigiBarnevernkommunene, KS)

1) At løsningen hadde en "fallback-løsning" dersom kommunene ikke hadde lastet ned meldingen innen en gitt tidsperiode. Det ble derfor besluttet at meldinger som ikke ble lastet ned i løpet av denne tidsperioden skulle sendes via ordinær post.
2) Bekymringsmeldingen skulle ikke lagres på portalen lengre enn strengt tatt nødvendig. Dette var et informasjonssikkerhetstiltak. Dette medførte bl.a. at innsenderen av meldingen ikke skulle kunne mellomlagre kladder av meldingen og at meldingen skulle bli fjernet fra serveren så raskt portalen mottar en kvittering/bekreftelse fra mottakende kommune om at overføringen til kommunen var vellykket.

Gjennomføringsfasen for NPB startet 01.01.19 som et statlig prosjekt. Under gjennomføringsfasen ble det raskt klart at målsetningen om en nasjonal portal var vanskelig å realisere med Bufdir som eier. Dette skyldes at det er kommunene som sitter på lovhjemlene for å behandle bekymringsmeldinger etter Barnevernsloven, noe som blant annet medfører at det må opprettes avtaler[11] med kommunene. I praksis betydde dette at det blir frivillig for kommunene om de vil motta bekymringsmelding via portalen.

Videre var konsekvensen at det måtte opprettes en driftsorganisasjon som må forvalte avtalene og drive «markedsføring» mot kommunene. Det ble vurdert at det er lite hensiktsmessig på sikt at denne forvaltningsorganisasjonen etableres hos Bufdir, siden dette er oppgaver som også må gjøres i delprosjektet «innbyggertjenester» i DigiBarnevern, [12] men også i andre tjenester som benytter FIKS-plattformen (f.eks. Digisos[13]).

Begrensningene mht. lovhjemmel og mulige synergier mot andre prosjekt tilsa at det var nødvendig å se etter en bedre og mer effektiv måte å realisere portalen. I denne sammenhengen ble det vurdert at FIKS-plattformen fortsatt var det naturlige valget. FIKS-rammeverket har allerede stor utbredelse i kommunene og hadde allerede etablert en organisasjon for å forvalte plattformen med tilhørende databehandleravtaler og samarbeidsavtaler. Det ble derfor besluttet at Nasjonal portal for bekymringsmelding overføres til KS for utvikling og forvaltning.

Den nye tilnærmingen ga flere synergier sammenlignet med opprinnelig tiltenkt organisering.

- Felles forvaltningsorganisasjon med innbyggertjenester (og andre tjenester i FIKS)
- Felles plattform med delprosjektet innbyggertjenester
- Felles strategi for «markedsføring» av tjenestene mot kommuner og brukere
- Utbredelse av FIKS-plattformen
- Felles opplæring, brukerstøtte og drift
- Synergier mot andre digitaliseringsprosjekter (f.eks. Digisos)

---

[11] Databehandleravtaler etter personvernlovgivningen og samarbeidsavtaler som regulerer rettigheter og plikter i forbindelse med bruk av tjenesten.

[12] Delprosjektet "digitale innbyggertjenester» i Digibarnevern vil gi barn, unge og foresatte innsyn i egne dokumenter i en barnevernssak og gjøre det enklere å kommunisere digitalt med ansatte i barnevernet. Les mer på KS sine nettsider: https://www.ks.no/fagomrader/digitalisering/felleslosninger/digibarnevern/digitale-innbyggertjenester-barnevern

[13] Digitale sosialtjenester (Digisos) er et samarbeid mellom stat og kommune, som har utviklet digitale tjenester for sosialhjelpsområdet på NAV.no. Les mer på KS sine nettsider: https://www.ks.no/fagomrader/digitalisering/felleslosninger/digitale-sosialtjenester-digisos/

Arbeidet med personvern og sikkerhet (DPIA, ROS-analyser, databehandleravtaler, etc.) skulle ifølge tilskuddsbrevet[14] gjennomføres av utviklingsprosjektet (KS). Dette arbeidet ble i hovedsakelig utført våren 2020. I dette arbeidet ble det lagt til grunn at KS behandler personopplysninger i løsningen som databehandler, på vegne av de kommunene som har tatt løsningen i bruk. Behandling av bekymringsmeldinger etter barnevernsloven er en kommunal oppgave.[15] Det er derfor hver enkelt kommune som er behandlingsansvarlig for behandling av personopplysninger i forbindelse med mottak av bekymringsmeldinger. Av dette følger det også at det er den enkelte kommune som er ansvarlig for at det blir gjennomført personkonsekvensvurderinger og ROS-analyser etter personvernregelverket.

I denne sammenhengen ble det utarbeidet en produktbeskrivelse, ROS- og DPIA-mal. Disse dokumentene må sees i sammenheng.

I produktbeskrivelsen beskrives:

- bakgrunn og formål med tjenesten
- funksjonalitet, hvilken informasjon som sendes og meldingsflyt
- hvem som er den registrerte
- behandlingens omfang

Prosjektet i KS utarbeidet maler som kommuner kan ta utgangspunkt i når de skal gjennomføre egne risiko- og sårbarhetsanalyser (ROS) og vurderer personvernkonsekvenser (DPIA). Målet for malene var at de skulle være til hjelp når den enkelte kommune selv skal gjøre deres egne vurderinger og tilpasse innholdet til kommunens situasjon. I arbeidet med å utarbeide malene deltok representanter fra kommuner i DigiBarnevern. Dette var et viktig tiltak for å fremme kommunenes perspektiv og ansvar.

Produktbeskrivelsen, ROS-analysen og DPIA-analysen er dynamiske dokumenter som må oppdateres når eventuelle nye risikosituasjoner blir identifisert eller det skjer endringer i tjenesten. KS har mekanismer i forvaltningen av tjenesten for å revidere dokumentene. KS har også etablert mekanismer for innsyn i logger av kommunens bruk av portalen.[16]

[14] Overføringen fra Bufdir til KS ble formelt forankret i revidert nasjonalbudsjett for 2019 og oppdraget ble gitt til KS i form av et tilskuddsbrev.
[15] Barnevernsloven (2021) § 15-3 tredje ledd bokstav a), jf. bestemmelsens første ledd.
[16] Siste versjon av DPIA og ROS-analyserer tilgjengelig i Fiks-portalen (KS digitale fellestjenester): https://portal.fiks.ks.no/fiks-bekymringsmelding-nasjonal-portal-for-bekymringsmelding/fiks-bekymringsmelding-produktbeskrivelse-ros-og-dpia-mal/

5.4 Forebyggende tiltak

Spørsmål som besvares i delkapittelet

D4. Hvilke tiltak er satt i verk for å forebygge lignende feil, herunder at feil ikke blir oppdaget og rettet uten unødig opphold?

5.4.1 Visma om iverksetting av forebyggende tiltak

Svakheten i kildekoden fra Visma, som førte til at Familia genererer tilbakemelding om at melding er mottatt før bekymringsmelding er korrekt lagret i kundens database, er rettet gjennom programvareoppgraderingen som ble tilgjengeliggjort 31.05.23 på Visma Community. Pr. 14.05.23 hadde alle kommunene som har aktivert portalen bekreftet at de har installert programvarerettelsen.

Det viktigste tiltaket kommunene har gjort for å forhindre nye avvik er å installere programvarerettelsen som sikrer at B-løsning vil trigges dersom lagring feiler. Det er også nedlagt en betydelig innsats i å undersøke om og i hvilket omfang den enkelte kunde har vært berørt. Visma har utarbeidet og tilgjengeliggjort en guide for hvordan kunder kan feilsøke i sine logger, samt bistått i feilsøkingen ved behov. Visma har pr. 19.06.23 mottatt tilbakemelding fra alle kunder om de har registrert avvik eller ikke. Videre har Visma gjennomført nærmere undersøkelser for å identifisere rotårsaken til at lagring til databasen feilet.

Som en videre oppfølging av saken gjennomfører Visma en internrevisjon av prosessene knyttet til feilen i Familia. I internrevisjonen arbeider Visma med å gå systematisk gjennom prosessene for utvikling og test av programvare, support av programvare og prosessen for håndtering av personvernavvik, med mål om å identifisere forbedringspunkter i prosessene eller tilhørende støtteverktøy.

5.4.2 KS om iverksetting av forebyggende tiltak

Årsaken til den aktuelle feilen er beskrevet i 5.2. De fleste kommuner viser til at de har iverksatt regelmessige kontroller av at det er samsvar mellom bekymringsmeldinger som blir registrert i «Nasjonal portal for bekymringsmelding» og meldinger som blir lagret i fagsystemet. Det er tiltak som er ment å oppdage meldinger som ikke kommer fram slik at meldingene kan gjenopprettes. Med slike tiltak ville den aktuelle feilen blitt oppdaget, og ingen meldinger gått tapt. Måten kontrollene gjennomføres varierer. Noen kommuner baserer seg på manuelle kontroller, mens andre i tillegg bruker egne digitale verktøy for å gjennomgå logger.

De tekniske løsningene på akkurat dette området har nå blitt gjennomgått grundig. Risikoen for at samme feil oppstår igjen er redusert og må vurderes som liten. En ny feil vil ikke nødvendigvis gi samme konsekvenser eller vise seg på samme måte, og kan skje på et helt annet sted i verdikjeden. Å gjennomgå hele denne kjeden med tanke på forebyggende tiltak er en større jobb, og kan resultere i bredere tiltak. Noen kommuner har begynt på det arbeidet. Økt innsats overfor

offentlige meldere med meldeplikt, og praksis rundt tilbakemeldinger, er aktuelle tiltak som nevnes.

KS opplever høy bevissthet rundt dette hos kommunene som ble berørt av feilen. KS vet også at flere andre kommuner har iverksatt eller videreført tilsvarende tiltak. Det er ikke mulig å si om tiltak i de berørte kommunenes er representative for sektoren som helhet.

5.5 Sannsynlighet for at feilen kan gjenta seg

Spørsmål som besvares i delkapittelet

D5. Hvordan vurderes risikoen for at feilene vi har sett i denne saken vil kunne skje i fremtiden?

5.5.1 Visma om sannsynlighet for at feilen kan gjenta seg

I programvarerettelsen er den konkrete sikkerhetsmekanismen i Vismas programvare utbedret, og det er i senere versjoner av programvaren også foretatt andre forbedringsmekanismer, som bidrar til å hindre at samme feil vil skje igjen. Det er dog verdt å bemerke at Vismas programvare ikke kan utbedre rotårsaken til hendelsen, at lagring i databasen feiler. For de kommunene som drifter Vismas programvare lokalt i kommunen må kommunene selv sørge for å loggføre og overvåke databasene for å identifisere feil tidlig nok til at de kan rettes. Dersom det ikke gjøres utbedringer hos den enkelte kommune på de forhold som utløste at lagring feilet, kan lagring til databasen feile igjen. I eventuelt nye tilfeller av feilet lagring, vil Familia i ny versjon forsøke å lagre flere ganger. Dersom lagringen fortsatt ikke er vellykket, vil tilbakemelding til KS-portalen om dette trigge B-løsning, og bekymringsmeldingen vil sendes pr. post. Det er dermed usannsynlig at samme avvik vil oppstå igjen.

Så lenge det er mennesker som lager teknologi, vil teknologien aldri kunne bli fullstendig feilfri. Det er derfor viktig at alle som benytter teknologi til å behandle viktige data, også har gode interne rutiner, for eksempel for å følge opp manglende svar på henvendelser, slik at eventuelle feilsituasjoner fanges opp og utbedres raskt (se punkt 6.1.2 og 6.3.5). Visma undersøker også som en del av sitt pågående revisjonsarbeid om utvidet bruk av teknologiske løsninger kan bidra til å minimere risikoen for feil i utvikling, testing og leveranse av sine tjenester.

5.5.2 KS om sannsynlighet for at feilen kan gjenta seg

Som nevnt tidligere er de tekniske løsningene på akkurat dette området nå blitt gjennomgått grundig. Risikoen for at samme feil oppstår igjen er redusert, og må på generelt grunnlag vurderes som liten. Det er også økt sannsynlighet for at en tilsvarende feil blir oppdaget raskere, og dermed får mindre konsekvenser.

I KS sin oppfølging av hendelsen er det imidlertid bruken av de nasjonale fellesløsningene og de prinsipielle spørsmålene om datautveksling, digital samhandling og samspill mellom ulike systemer som står i sentrum. I det større bildet ser KS at de ulike aktørene tar et ansvar for sin del av

verdikjeden, men at ansvaret for helheten forsvinner. Utfordringen er ikke nødvendigvis å plassere ansvaret rent juridisk, men at de ansvarlige ikke er fullt klar over hva ansvaret innebærer og heller ikke er i stand til å ivareta det. Her er det fortsatt uavklarte forhold som bidrar til forhøyet risiko ved bruk av nasjonale fellesløsninger og prosesser som krever samspill med flere aktører og systemer. Tar vi utgangspunkt i en slik generell forståelse av utfordringene er det ikke et spørsmål *om* feil vil oppstå, men *når* og *hvordan* de vil oppstå, og med hvilke konsekvenser. Selv om det isolert sett er lav risiko for at svikten skjer for bekymringsmeldinger neste gang, så er også den verdikjeden omfattet av det samme generelle problemkomplekset.

5.5.3 Datatilsynet om sannsynlighet for at feilen kan gjenta seg

Det er et naturlig ledd i behandlingen av avviksmeldingene Datatilsynet har mottatt at de vurderer om håndteringen av hendelsene skjer i tråd med kravene i personvernregelverket. Avvikshåndteringen hos de enkelte kommunene skal inneholde dokumentasjon av de faktiske forholdene rundt hendelsen, virkningen av den og hvilke tiltak som er truffet for å utbedre.

Håndteringen av brudd på personopplysningssikkerheten har blant annet som formål å sikre at lignende hendelser ikke oppstår på nytt senere. Måten denne hendelsen har blitt håndtert av blant annet kommunene og Visma tilsier at det er gjort relevante tiltak for å redusere risikoen for gjentakelser.

5.5.4 Digitaliseringsdirektoratet om sannsynlighet for at feilen kan gjenta seg

Digdir tolker spørsmålet i den forstand at «feilene vi har sett i denne saken» ikke kun er avgrenset til en teknisk kodefeil driftet av en systemleverandør. Selv om rotårsaken i dette tilfelle oppstod hos Visma, så kan det foreligge andre feil, f.eks. i manuelle rutiner, manglende risikostyring og mangelfulle vurderinger. Digdir forstår «risikoen» til å innebære en vurdering av en kombinasjon av sannsynlighet og konsekvens. På et generelt grunnlag vil manglende systematisk arbeid med informasjonssikkerhet utgjøre en risiko for at feil vil kunne skje i framtiden.

Statistikk fra 2023[17] viser at et fåtall av fylkeskommuner og kommuner gjennomfører risikovurderinger systematisk og periodisk. I tillegg er det flere som ikke har iverksatt nødvendig risikohåndtering.

Totalt sett vil manglende systematisk arbeid med informasjonssikkerhet øke sannsynligheten for at lignende hendelser slik som denne kan inntreffe igjen.

For å redusere en slik sannsynlighet vil det, i tillegg til vurdering og håndtering av risiko, også være viktig med leverandøroppfølging, og god overvåking og hendelseshåndtering. Digdir tilbyr veiledning om generell styring og kontroll/internkontroll på informasjonssikkerhetsområdet, inkludert etablering av et system for hendelseshåndtering.

[17] SSB (2023c). Tabell 12041: Tiltak/rutiner ved administrasjon av IKT-sikkerheten (prosent), etter forvaltningsnivå, antall innbyggere, statistikkvariabel og år. Statistikkbanken (ssb.no).

For å redusere sannsynligheten vil det være viktig å se det tekniske systemet i sammenheng med virksomhetens organisasjon og arbeidsprosesser for å avdekke hvilke tekniske og manuelle rutiner som er på plass, og hvor det må etableres sikkerhetstiltak for å sikre god meldingsformidling.

Videre vil Digdir også påpeke at risiko reduseres ved at man har et godt samspill mellom nasjonale fellesløsninger og sektorløsninger, slik det legges opp til i de føringer som er gitt i Digitaliseringsrundskrivet og gjeldende strategier. Framover bør det derfor vurderes å etablere støtte for innsending via de statlige fellesløsningene eFormidling eller Altinn mot Bekymringsmeldingsportalen. Dette er videre et fokusområde som adresseres både i Digdir sitt arbeid med videreutvikling av fellesløsninger, i strategiprosesser for produktgruppe meldingsutveksling, og i arbeidet med ny nasjonal digitaliseringsstrategi.

6. Læring av feilen

6.1 Læringspunkter for kommunesektoren

Spørsmål som besvares i delkapittelet

E1. Er det læringspunkter for kommunesektoren med tanke på deres internkontroll med systemet for mottak og formidling av bekymringsmelding?

6.1.1 KS om læringspunkter for kommunesektoren

Hvilke læringspunkter den enkelte kommune har gjort vil variere, blant annet på bakgrunn av hvilke rutiner, systemer og internkontroll de hadde fra før. Generelt har hendelsen avdekket at man ikke har hatt nødvendig kontroll i alle ledd ved digital meldingsflyt. Det har igjen gitt ny erkjennelse av kompleksiteten i digitale verdikjeder, og nødvendigheten av større bevissthet rundt kommunens ansvar og ikke minst vurderinger av risiko og sårbarhet.

Et annet punkt som noen kommuner peker på, er praksis og kultur rundt avviksmeldinger. Når de går tilbake og ser på tidligere hendelser, finner de at det har vært tilfeller der digitale bekymringsmeldinger ble borte som burde vært meldt som avvik av melder og/eller kommunen, men som i stedet har blitt forklart med menneskelig feil (brukerfeil), og rettet opp ved å sende bekymringsmeldingen på nytt. At både kommunen, men også offentlige ansatte som bruker digitale løsninger i sitt arbeid i større grad forstår betydningen av gode avviksrutiner, inkludert en kultur som oppmuntrer til å melde avvik, er noe som blir trukket frem. Hendelsen har økt bevissthet på at feil som oppdages faktisk kan være systemfeil med konsekvenser for flere.

Et siste punkt som kan nevnes er kommunenes behov for gode rutiner i håndteringen av slike hendelser, og å forbedre vurderinger av risiko og personvern (ROS- og DPIA-ene) knyttet til barnevern og digitale løsninger kontinuerlig. For flere kommuner var dette første gang de måtte vurdere melding til Datatilsynet, håndtere media, koble på personvernombud, sikre god intern og ekstern kommunikasjon.

Ingen KS har vært i kontakt med ønsker at alternativer til NPB, som post, skal brukes. Tvert imot, så ansees portalen som den foretrukne kanalen å motta meldinger på, og de ønsker i høyere grad at NPB brukes av alle meldere. Å motta bekymringsmeldinger gjennom én kanal gir en høyere trygghet ved bedre kontrollmulighet.

6.1.2 Visma om læringspunkter for kommunesektoren

Visma har i vår dialog med kommunene erfart at det er svært varierende praksis mellom kommunene knyttet til lagring og overvåking/oppfølging av logger og avvikende logginnslag. Visma vil anbefale at kommuner som drifter on-premise-løsninger i eget datasenter etablerer rutiner for å overvåke logger, oppdage og følge opp feilsituasjoner. Dette kan være både tid- og

ressurskrevende, og det kan derfor være hensiktsmessig for kommunene å undersøke om de kan kjøpe seg disse tjenestene, for eksempel kjøpe en driftstjeneste eller migrere til en skyløsning der leverandør har ansvar og risiko for å monitorere driften.

Det er videre Vismas erfaring fra oppfølging av kommunene i Familia-saken, at det var stor variasjon i hvilken alvorlighetsgrad og prioritering kommunene mente at saken skulle ha. Visma mener derfor det kan være hensiktsmessig for kommuner som ikke allerede har gjort det, at det gjennomføres risikovurderinger som dekker totalbildet av IT-systemer og integrasjoner, samt vurderes hvilke konsekvenser ulike brudd kan ha, slik at man agerer raskt og forstår risikoen dersom alvorlige hendelser inntreffer. Videre kan slike risikovurderinger benyttes til å tilpasse manuelle rutiner og oppfølging for systemer som behandler sensitive data.

I lys av at det hos enkelte kunder er snakk om flere meldinger som ikke har kommet frem, over en lenger tidsperiode, mener Visma at det også kan være hensiktsmessig for kommunene å vurdere om det er behov for kompetanseheving hos ulike offentlige instanser om bekymringsmeldinger og barnevernets tilbakemeldingsplikt og -praksis. Dette vil kunne bidra til at eventuelt andre feilsituasjoner kan oppdages og utbedres raskt. Det samme gjelder eventuelt annen viktig kommunikasjon som utveksles mellom ulike aktører innad i kommunene.

6.1.3 Digitaliseringsdirektoratet om læringspunkter for kommunesektoren

Det stilles krav til at kommuner skal ha internkontroll for informasjonssikkerhet, og dette bør integreres som en del av virksomhetens helhetlige internkontroll. Digdirs veileder Internkontroll i praksis - Informasjonssikkerhet tar for seg syv anbefalte styringsaktiviteter for å styre risiko på informasjonssikkerhetsområdet.

Det er viktig at virksomheten vurderer risiko tilknyttet sine arbeidsoppgaver og tjenester. Man må ha tilstrekkelig oversikt over interne arbeidsprosesser og informasjonsbehandlingen som inngår i dette. Det er også viktig at det vurderes risiko etter hendelser, og ved anskaffelser. Før en IT-anskaffelse må virksomheten ha oversikt over hvilke sikkerhetsbehov IT-tjenestene må oppfylle. Det å stille sikkerhetskrav vil være en viktig måte å håndtere risiko på. Eksempler på generelle sikkerhetskrav kan være sikkerhetstesting, endringshåndtering og rutiner for å håndtere uønskede hendelser. [18]

Når man skal bruke tjenesteleveranser i oppgaveløsningen vil det alltid være behov for å vurdere hvordan det endrer på ting, og vurdere og håndtere risiko i den nye situasjonen, siden det innebærer at en annen virksomhet får et avtalefestet ansvar for informasjonsbehandlingen i en eller flere av virksomhetens oppgaver og tjenester.

[18] Anskaffelser.no (2023). *Krav om sikkerhet og personvern i anskaffelser av IT.* Direktoratet for forvaltning og økonomistyring (DFØ). https://anskaffelser.no/hva-skal-du-kjope/it/krav-om-sikkerhet-og-personvern-i-anskaffelser-av-it

Virksomheten må identifisere, analysere og håndtere risikoer jevnlig, ikke bare når en hendelse inntreffer. En viktig støtte er et godt utarbeidet system for hendelses- og avvikshåndtering. [19] Oppfølging av hendelser er viktig som videre grunnlag for læring.

6.2 Offentlige myndigheters rolle

Spørsmål som besvares i delkapittelet

E2. Hvordan kan andre offentlige myndigheter bidra for å redusere risikoen for alvorlige feil i barnevernets fagsystemer?

6.2.1 KS' vurdering om offentlige myndigheters rolle i å redusere risiko for feil

En utfordring kommunene har pekt på er kompleksiteten og mangfoldet i løsningene for digitale forsendelser. Ulike kanaler, ulike måter å bruke dem på, ulike måter å autorisere tilganger og ulik grad av integrering med fagsystemet gjør det utfordrende å ha den fulle oversikten. Dette er en generell utfordring. For bekymringsmeldinger finnes det imidlertid en nasjonal tjeneste som er ment å redusere kompleksiteten for kommunene og samtidig støtte melder i arbeidet med å formidle bekymringen. Effekten av denne tjenesten avhenger imidlertid av at den faktisk benyttes. Her mener KS det er på tide at man diskuterer føringer for bruk av NPB, som er en offentlig finansiert tjeneste utviklet for å forbedre sending av bekymringsmeldinger – også med tanke på sikkerhet. I hvilken grad kan man velge å (ikke) benytte tjenestene? Hvordan sikrer vi at tjenestene brukes i tråd med intensjonen? Vil det kreve noe annet av tjenesten og/eller KS som tilbyr den?

Knyttet til denne saken vil det være gunstig for kommunene om det var tydelige forventninger om bruk av Nasjonal portal for bekymringsmelding for alle meldere med meldeplikt. KS er klar over utfordringene det medfører for flere aktører, men nettopp å bidra til rammer som muliggjør bruk er noe kommunene trenger andre myndigheters hjelp til.

6.2.2 Datatilsynets vurdering om offentlige myndigheters rolle i å redusere risiko for feil

Datatilsynets anbefaling er at ulike offentlige aktører benytter tilgjengelig veiledning for å sikre at de har tilstrekkelige systemer for å fange opp mangler knyttet til informasjonssikkerhet. I dette tilfellet er det prinsippet om tilgjengelighet som er berørt.

[19] Digdir (2023). *Etableringsaktiviteter.* Digitaliseringsdirektoratet. https://www.digdir.no/informasjonssikkerhet/etableringsaktiviteter/3046#6_etablere_system_for_hendelses_og_avvikshndtering

6.2.3 Digitaliseringsdirektoratets vurdering om offentlige myndigheters rolle i å redusere risiko for feil

Digdir besvarer dette spørsmålet ut fra sitt mandat og myndighetsrolle med kort informasjon om hva dette innebærer, og hvilke ressurser som kan være relevante bidrag.

Digdir som offentlig myndighet har både en rolle som leverandør av nasjonale fellesløsninger for offentlig sektor, og som premissgiver på ulike områder som skal bidra til å styrke digitaliseringen i Norge. Ressurser Digdir har tilgjengelig som er relevante i denne sammenhengen er blant annet generell styring av informasjonssikkerhet, rammeverk for digital samhandling, og referansearkitekturer for datautveksling. I tilknytning til vår leverandørrolle så jobber Digdir kontinuerlig for bedre sammenheng og samhandling på tvers av fellesløsninger, sektorløsninger, og innbyggere og virksomheter.

Når det gjelder den konkrete bruken av fellesløsningene, tilbyr Digdir omfattende dokumentasjon, kurs, og informasjonsmateriell til kommuner som kan benyttes for å kunne utforme gode rutiner i tilknytning til forsendelse og mottak av meldinger. Vår erfaring er at det er stor variasjon i hvordan dette er innarbeidet i den enkelte kommune.

Bekymringsmeldingsportalen har i dag ikke integrasjoner med de statlige fellesløsningene eFormidling eller Altinn. En slik integrasjon ville tillatt en statlig aktør som politiet å sende bekymringsmeldinger til portalen direkte fra sine fagsystemer, uten behov for IT-utvikling på politiets side. Etter Digdirs vurdering, bør slike mottakskapabiliteter komme på plass i fremtiden. Dette vil sikre at statlige virksomheter benytter allerede etablerte grensesnitt som de har til fellesløsningene for sin formidling. Det er en vesentlig del av verdiforslaget til fellesløsningene at man kan oppnå effektiv og god tverrsektoriell samhandling ved å knytte seg opp mot disse.

Det er også verdt å nevne at Direktoratet for forvaltning og økonomistyring (DFØ) er fagorgan for anskaffelser i offentlig sektor. De har blant annet veiledning om informasjonssikkerhet og personvern i IKT-anskaffelser.

6.2.4 Bufdirs vurdering om offentlige myndigheters rolle i å redusere risiko for feil

Samarbeid og erfaringsdeling sentralt i offentlig sektor kan være med å avdekke risiko og dele erfaring rundt risikohåndtering. Det er etablert et tverrgående etatssamarbeid for utsatte barn og unge (KUBU). Bufdir foreslår at det vurderes om dette forumet kan benyttes som arena for informasjon- og læring for digitale løsninger som har konsekvenser for utsatte barn og unge og som vedrører forholdet mellom stat og kommune.

Offentlige myndigheters bruk av nasjonale felleskomponenter i utvikling av nye løsninger, er med på å bygge forutsigbarhet og mer enhetlig praksis. Bruk av felleskomponenter tilrettelegger for økt deling av informasjon og praktisering av god informasjonsforvaltning. På et overordnet nivå, kan klare digitale strategier, tydelig kommunikasjon av krav og anbefalinger, og tydelig oppfølging fra sentrale myndigheter på digitaliseringsområdet, for eksempel Digdir, hjelpe til med å finne de gode løsningene - som virker for alle parter.

Et sentralt krav i offentlige myndigheters tjenesteutvikling er at brukeren skal settes i sentrum. Dette prinsippet må også gjelde i samarbeid med kommunene, og når staten lager løsninger der brukeren er kommunene. Dette betyr at når det skal utvikles tjenester mot kommunene er det sentralt at man benytter den felleskomponenten som er tilpasset kommunen og ikke velger sine egne løsninger. Her spiller KS en viktig rolle som det sentrale organet for alle kommuner. Et bærende prinsipp bør således være at man baserer seg på KS sine anbefalinger når man skal utvikle tjenester til bruk i kommunene.

I tillegg er det viktig å sikre god informasjon og eierskap i de enkelte kommunene, slik at tjenesten kan bidra til å levere kvalitativt bedre tjenester, samt avklare hvilke effekter tjenesten vil ha organisatorisk og juridisk. Tidlig involvering vil kunne bidra til bedre forankring og kunnskap om løsningene, samt forbedre muligheten for å avdekke og håndtere risikoer i tjenesten.

Helt konkret i forvaltningen av Nasjonal portal for bekymringsmelding, har KS og Bufdir besluttet at det er FIKS IO som skal benyttes som felleskomponent. I tillegg er det iverksatt en endring i veiledning i NPB for offentlige meldere om at de kan forvente tilbakemelding fra barnevernstjenesten om mottak av melding og eventuell åpning av undersøkelse, og at melder oppfordres i NPB til å etterspørre tilbakemelding hvis denne ikke kommer. Disse tiltakene reduserer ikke feil som sådan, men forebygger uheldige konsekvenser av eventuelle feil: Hvis offentlige meldere etterspør tilbakemelding kan svikt oppdages tidligere.

6.2.5 Vismas vurdering om offentlige myndigheters rolle i å redusere risiko for feil

Vismas erfaring fra denne saken er at offentlige myndigheter kan bidra til å rådgi om og standardisere bruken av programvare/IT i kommunesektoren, for eksempel ved å

- Formulere beste-praksis og stille tydeligere krav til drift av egen, kommunal infrastruktur for IT-tjenester, for eksempel krav knyttet til lagring og oppfølging av logger, testing av trafikk og belastning av infrastrukturen, risikovurderinger og konsekvensanalyse, eventuelt krav til sertifisering av driften, osv.
- Allokere flere midler til kommunal drift av infrastruktur, slik at miljøene for eksempel kan ivareta behov for tilstrekkelig kapasitet i infrastruktur og rett kompetanse til å følge opp logger fra sine IT-systemer.
- Allokere midler slik at kommunene kan investere i mer moderne teknologi. Gjennom bruk av skytjenester kan kommunen kjøpe seg tjenester også tilknyttet drift, logger, oppgraderinger og sikkerhet, og leverandøren sitter på mer risiko og ansvar.
- Utarbeide tydeligere krav/protokoller til hvordan meldingsutveksling av sensitive data skal foregå i offentlig sektor. For eksempel kan man se til hvordan dette er løst i andre fagområder slik som retningslinjer fra NHN for helsesektoren.
- Tilrettelegge for, og ta initiativ til, større grad av samarbeid med leverandørene av fagsystemer som skal kobles mot de nasjonale fellestjenestene.

6.2.6 Helsetilsynets vurdering om offentlige myndigheters rolle i å redusere risiko for feil

I tråd med barnevernsloven § 1-7 har kommunen ansvaret for at saksbehandling, tjenester og tiltak skal være forsvarlige. Den viktigste jobben med å identifisere læringspunkter gjør tjenestenes selv, gjennom sin systematiske internkontroll med at tjenestene er forsvarlige i tråd med bvl § 15-2 og kommuneloven § 25-1.

Kommunene står nærmest til å identifisere læringspunkter og drive forbedringsarbeid. Helsetilsynet forventer at kommunene gjør det de kan for å få oversikt over hvilke barn og familier som kan være rammet av denne svikten og følger opp med nødvendige tiltak for å redusere negative konsekvenser for dem. Statsforvalterne rapporterer til Helsetilsynet at de vurderer at kommunene reagerte raskt da feilen ble oppdaget, undersøkte og fulgte opp det de trengte. Statsforvalternes vurdering er at kommuner med identifisert svikt er i gang med å gjennomgå egne systemer for håndtering av bekymringsmeldinger og digital håndtering av dokumenter.

Barnevernet tar i økende grad i bruk digitale løsninger i utførelsen av sitt samfunnsoppdrag. Digitale løsninger må inngå i kommunens risikovurderinger for å sikre en effektiv internkontroll som bidrar til at tjenestene forblir trygge og forsvarlige. Helsetilsynet forventer at kommunene nøye vurderer behovet for forbedring av sine internkontrolltiltak. Dette er avgjørende for å kunne forebygge, oppdage og redusere risikoen for at flere barn vil oppleve negative konsekvenser som følge av lignende svikt i fremtiden.

Selv om kommunen har et selvstendig ansvar for forsvarlige tjenester, mener Helsetilsynet at kommunene må kunne forvente at nasjonale tekniske og digitale løsninger fungerer som de må. Dette er også i tråd med Helsetilsynets vurdering etter tilsyn med innføring av Helseplattformen. Herunder at leverandør bidrar til at testing, implementering, oppdateringer, avvikshåndtering og retting gjennomføres. Leverandør må bidra til at erfaringer og fortløpende vurderinger etter testing deles, slik at kommunene settes i stand til å gjøre gode risikovurderinger når de tar i bruk nye digitale løsninger. Helsetilsynet vurderer at et sentralt læringspunkt i denne saken handler om hvordan det bør jobbes med risikoreduserende tiltak ved innføring av nye digitale løsninger.

Denne saken handler i hovedsak om svikt i tekniske løsninger. Helsetilsynet og statsforvalterne må bruke rapporten fra denne pågående gjennomgangen i risikovurderinger som grunnlag for mulige tilsynsaktiviteter. Helsetilsynet mener at svikten som er avdekket i denne saken, også kan ha sammenheng med svakheter i kommunens systematiske samhandling og informasjonsflyt i oppfølgingen av risikoutsatte barn og unge. Offentlige ansatte i andre kommunale velferdstjenester for barn og unge står for en betydelig andel av bekymringsmeldingene til barneverntjenesten. Det er derfor rimelig å anta at en del av de forsvunne bekymringsmeldingene kom fra disse tjenestene. Samhandling og koordinering i oppfølgingen av barn og unge er et kjent område med risiko for svikt fra tidligere. Helsetilsynet har gjennom prioritering av tilsynsaktiviteter for 2024, allerede pekt ut kommunens systemer for å fange opp barn i risiko, informasjonsflyt og samarbeid i kommunen som aktuelle risikotemaer for tilsyn.

I tråd med barnevernsloven (bvl) § 15-1 har kommunen et overordnet ansvar for å forebygge at barn utsettes for omsorgssvikt, og kommunen skal sørge for å samordne tjenestetilbudet til barn

og familier. Dette gjelder særlig tjenester i kommunen som jobber med barn og unge hver dag, som skole, barnehage og skolehelsetjenesten. Noe som gjør det særlig relevant for kommunen å innlemme disse tjenestene i kommunens forbedringsarbeid etter denne svikten. Kommunens plan for forebygging jf. bvl § 15-1, andre ledd vil være et egnet verktøy for systematisk samordning av arbeidet her.

Teknologiske fremskritt og digitalisering har en økende innvirkning på levering av velferdstjenester, inkludert barnevern. Denne saken illustrerer at feil og svikt kan forekomme både i teknologiske løsninger og i samhandlingen mellom mennesker. Det er derfor viktig at tilsyn også er i stand til å overvåke forsvarligheten av tjenester som benytter teknologi, samtidig som det ikke hindrer nødvendig teknologisk og digital innovasjon.

Helsetilsynet prioriterer å utvikle tilsyn som understøtter virksomhetenes ansvar for å redusere risikoen for alvorlige feil i de nåværende og fremtidige fagsystemene som brukes. Dette inkluderer å utvikle tilsynsmyndighetenes evne til å identifisere og påpeke uforsvarlige forhold knyttet til teknologisk og digital tjenesteleveranse. Helsetilsynet jobber også med metoder for å undersøke, evaluere og følge opp stadig mer avansert teknologisk tjenesteleveranse. Det er sentralt å samarbeide med andre relevante tilsynsorganer, som for eksempel Datatilsynet for å avklare ansvarsfordelingen for tilsyn med teknologi. Helsetilsynet er i gang med å bygge egen kompetanse for å effektivt møte utfordringene i den digitale utviklingen, og følger tett med på tilsynspraksis i andre land.

6.3 Læringspunkter for systemleverandørene

Spørsmål som besvares i delkapittelet

E3. Er det læringspunkter for systemleverandørene som det er naturlig at Bufdir eller andre offentlige aktører adresserer?

6.3.1 KS' vurdering om læringspunkter for systemleverandørene

Fra dialog med kommuner vet KS, spesielt også i lys av at mange meldinger ikke kom fram gjennom Altinn, at det kan være uoversiktlig at bekymringsmeldinger sendes gjennom forskjellige kanaler. Det er et klart ønske at alle offentlige meldere sender bekymringsmeldinger gjennom NPB. Kommuner har gode rutiner for håndtering og tilgangsstyring for meldinger som mottas gjennom NPB. At leverandørene av de ulike sektorspesifikke fagsystemene utvikler støtte for system-system-integrasjon med NPB er en suksessfaktor. Særlig aktuelt vil være systemer som benyttes av ansatte med meldeplikt; eksempelvis i helsesektoren, oppvekst, skole og politi. NPB tilbyr allerede i dag slik integrasjon. At aktuelle systemer ikke støtter dette har nok flere årsaker, men juridiske hindre og etterspørsel fra kundene må trekkes frem. Her kan offentlige aktører bidra til å fjerne de ulike hindrene og stille tydelige forventninger.

6.3.2 Datatilsynets vurdering om læringspunkter for systemleverandørene

Dersom partene har en databehandlerrelasjon, følger det av personvernforordningen artikkel 28 nr. 3, bokstav f) at databehandler har en plikt til å bidra til at den ansvarlige etterlever blant annet kravene til å sikre personopplysninger og å håndtere avvik. God kjennskap til disse pliktene vil kunne medføre at leverandører bidrar i den utstrekning det er forventet og hensiktsmessig.

Datatilsynets inntrykk er at Visma har tatt et stort ansvar for å bistå kommunene i å undersøke og rette opp i hendelsen.

6.3.3 Digitaliseringsdirektoratets vurdering om læringspunkter for systemleverandørene

Digdir forstår spørsmålet som at det handler om læringspunkter for systemleverandører generelt, og at spørsmålet ikke er avgrenset til den enkeltstående leverandøren i denne saken.

På generelt grunnlag må leverandører ivareta sine plikter ved avtale. For å sikre at oppdragsgivers behov knyttet til informasjonssikkerhet ivaretas på en god måte, bør leverandøren involvere denne når det gjennomføres risikovurderinger, og de må ha jevnlig dialog for å forsikre seg om felles forståelse for avtalens innhold.

Det er også spesielt viktig med fordeling av ansvar for sikkerhetstiltak:

- Hvilke sikkerhetstiltak har leverandøren ansvaret for at er etablert og fungerer etter hensikten?
- Hvilke sikkerhetstiltak er det delt ansvar for?
- Hvilke sikkerhetstiltak har virksomheten selv ansvar for at er etablert og fungerer etter hensikten?

Dersom en virksomhet velger å tjenesteutsette en oppgave helt eller delvis, så vil det uansett være virksomheten som har et selvstendig ansvar for styring og kontroll, og som må ha vurdert risiko ved anskaffelsen og stille sikkerhetskrav til IT-tjenesten basert på sine behov. Virksomheten må selv kontrollere eksterne prosesser, produkter og tjenester som er relevant for at de skal ha styring og kontroll på informasjonssikkerhetsområdet.[20]

6.3.4 Bufdirs vurdering om læringspunkter for systemleverandørene

Bufdir ser stor verdi i samordning, løpende dialog og erfaringsutvekslinger. Det kan være fordelaktig å jobbe for å standardisere arbeidet med risiko- og sårbarhetsanalyser, og slik danne et bedre felles grunnlag for vurderinger og tiltak. Det er hensiktsmessig å få til en samordning og god dialog rundt sentrale, generelle problemstillinger som gjelder flere, og unngå én-til-én dialog mellom kommunene og systemleverandører. Noe av bakgrunnen for DigiBarnevern som prosjekt, er nettopp en slik samordning. Prosjektet har sørget for en felles tilnærming til markedet og

[20] ISO/IEC 27001, Clause 8.1.

leverandørene. Dette er en mekanisme som bør gå begge veier, ikke bare ved utvikling og anskaffelse, men også i forvaltning og risikovurdering og -håndtering.

Det bør også tilrettelegges for jevnlig og god dialog, ikke bare i utviklingsprosess eller når hendelser inntreffer. Det finnes allerede gode arenaer for dialog hvor systemleverandørene kan komme med tilbakemeldinger til sentrale myndigheter på fagområdene. Ett eksempel på dette er Bufdirs leverandørkonferanser som avholdes jevnlig. KS har også hatt leverandørkonferanser for dialog med leverandørmarkedet innen kommunal IKT.

Det kan i tillegg være hensiktsmessig med større grad av erfaringsdeling på tvers, slik at kommuner som allerede har erfaring med systemene kan bidra til en smidigere overgang for de som skal kobles på. I tillegg kan det bidra til å fange opp felles utfordringer som gir et bedre grunnlag for generell dialog med systemleverandør. KS sine regionale digitaliseringsnettverk kan være et eksempel på en arena for slik erfaringsdeling.

6.3.5 Vismas vurdering om læringspunkter for systemleverandørene

Visma har gjennom håndtering av denne saken sett hvor verdifullt det er at det etableres og vedlikeholdes et godt samarbeid og åpen informasjonsutveksling mellom leverandør og offentlige myndigheter som KS, Bufdir og Datatilsynet. Aktørene har gitt gode innspill og veiledning som Visma mener har bidratt til en konstruktiv håndtering av saken.

Visma ser generelt stor verdi av at det etableres og vedlikeholdes nasjonale fellestjenester, for eksempel for meldingsutveksling mellom offentlige aktører, som private systemleverandører kan koble sine fagsystemer opp mot. For at dette samarbeidet skal fungere optimalt, mener Visma det kan være nyttig om det etableres gode samarbeidsarenaer utenom krisetilfeller, slik at leverandørene i større grad kan være med og påvirke utviklingen av felleskomponentene, for eksempel ved å delta i diskusjoner om digitaliseringsstrategi.

6.4 Risiko- og sårbarhetsanalyser

Spørsmål som besvares i delkapittelet

E4. Hvordan bør risiko- og sårbarhetsanalyser ved bruk av IKT til innlevering og mottak av bekymringsmelding utvikles som følge av feilen, og hvordan bør feilen påvirke de vurderinger av risiko og sårbarhet ved svikt som gjøres for barna det meldes bekymring for?

6.4.1 Vismas vurdering av hvordan ROS-analyser bør utvikles

Risiko- og sårbarhetsanalyser bør ha en kategorisering av løsninger/integrasjoner (hvis de ikke har gjort det slik tidligere). Analysene bør benyttes til å identifisere målrettede tiltak, herunder hvordan manuelle rutiner kan samspille med IT-løsninger for å sikre en sikker behandling.

Del to av spørsmålet er mer relevant for andre aktører å besvare, da Visma ikke har tilgang på informasjon om innholdet i de konkrete sakene som er berørt, eller hvorvidt innholdet faktisk har latt seg gjenskape eller gjenfinne

6.4.2 KS' vurdering av hvordan ROS-analyser bør utvikles

KS tilbyr maler for ROS og DPIA for alle digitale tjenester som KS tilbyr, og kommuner signerer en databehandleravtale med KS før tjenesten kan tas i bruk. Malene for ROS og DPIA lages typisk i samarbeid med kommuner som er aktiv i utviklings- og/eller piloteringsfase. Kommunen som tar tjenesten i bruk må likevel selv gjøre vurderinger ut fra egen situasjon. ROS- og DPIA-malene forenkler arbeidet, da det vil være en del overlapp fra kommune til kommune hvordan risiko vurderes, og gir en trygghet til kommunen at den får med seg relevante risikomomenter i egne vurderinger.

Utarbeidelse av risiko- og sårbarhetsanalyser resulterer ofte i et internt dokument med tiltak man kan følge opp i egen organisasjon. I en verdikjede der hvert ledd har ansvar for sin del er det en fare for at risikovurderingen også begrenses til den delen man har ansvar for eller reell kontroll over. Selve tanken om økosystem bygger langt på vei på en modell der hvert ledd har sitt definerte ansvar. Men når det gjelder bekymringsmeldinger, og det digitale økosystemet ellers, vil risikohendelse og relevante tiltak ikke nødvendigvis ligge i samme virksomhet. Derfor bør det ved utarbeidelse av risiko- og sårbarhetsanalyser være en bevissthet rundt hvilke risikoer man velger å ikke inkludere i sin egen analyse. Det må gjøres på bakgrunn av en vurdering av om det er akseptabelt for virksomheten å forutsette at risikoen er håndtert av en annen/andre aktører, uten videre kontroll/tiltak i egen organisasjon. Der det vurderes å ikke være akseptabelt, må økosystemet være rigget slik at den enkelte aktør kan følge håndteringen risikoen gjennom hele verdikjeden.

Integritet, tilgjengelighet, konfidensialitet er vanlige dimensjoner når man vurderer informasjonssikkerhet. Datatilsynet legger til robusthet som en fjerde, og overgripende, dimensjon når de beskriver styringssystem for informasjonssikkerhet. Å planlegge for å kunne håndtere situasjoner hvor integritet, tilgjengelighet eller konfidensialitet er truet eller brutt, er nødvendig. Noen kommuner etterlyser en slags «beredskapsplan» ved digitale hendelser. Utarbeidelse av risiko- og sårbarhetsanalyser kan identifisere slike behov, eller implementere det som en del av tilhørende tiltak.

6.4.3 Datatilsynets vurdering av hvordan ROS-analyser bør utvikles

Datatilsynet ønsker å påpeke at ROS-analyser for slike systemer må ha fokus på tilgjengelighetsperspektivet, det vil si at systemene sikrer at nødvendig data er tilgjengelig når det er behov for dem. Manglende tilgjengelighet kan ha store konsekvenser på et område hvor kritisk informasjon går tapt.

6.4.4 Digitaliseringsdirektoratets vurdering av hvordan ROS-analyser bør utvikles

Generelt sett er det viktig å lære av hendelser – det at informasjonssikkerhetsbruddet nå har skjedd må virksomhetene og systemleverandørene ha med i fremtidige vurderinger av risiko.

Når man vurderer risiko er det i tillegg viktig å se på hele arbeidsprosessen/informasjonsflyten, ikke utelukkende på systemet som sådan. Der man ser at det er kritisk meldingsutveksling må virksomheten vurdere behovet for kompenserende tiltak i tilfelle meldingen ikke kommer fram til rette vedkommende/instans, for eksempel en lesebekreftelse i form av beskjed om at det faktisk er lest av et menneske, ikke bare at det er mottatt av en maskin.

6.4.5 Bufdirs vurdering av hvordan ROS-analyser bør utvikles

I utarbeidelsen av risiko- og sårbarhetsanalyser er det sentralt at alle aktører er bevisste på at hele verdikjeden vurderes, ende til ende. Alle aktører i verdikjeden har et ansvar for å kvalitetssikre prosessene, samt identifisere og håndtere risikoer løpende. Avsender har et ansvar for at mottaker er i stand til å motta informasjon og tilsvarende ansvar ligger på mottaker. Ansvarlig for felleskomponent i midten har også et ansvar for informasjon kan gå begge veier. Her er det ikke bare et teknisk perspektiv, men også et organisatorisk perspektiv. Alle aktører i verdikjeden har et ansvar for å foreta risikovurderinger av egne arbeidsprosesser og rutiner og sørge for ivaretakelse av sin del av verdikjeden.

Det er viktig å bemerke at risikoen for svikt i systemer alltid vil være til stede, både når det gjelder digitale og manuelle systemer. Risikoen for svikt vil være like stor om avviket skyldes digitale eller manuelle systemer. Rutiner for oppfølging, etterlevelse og internkontroll må derfor være på plass uansett leveringsmekanisme.

7. Avsluttende refleksjoner fra Bufdir

Feil i IT-systemer kan forårsake svikt i offentlig tjenesteyting, og dette påvirker livene til enkeltpersoner. I barnevernet gjelder dette utsatte barn, unge og familier. Bufdir synes det er svært beklagelig at tekniske systemfeil i dette tilfellet har skapt konsekvenser vi ikke har klart å avdekke fullt ut.

Tekniske systemer er komplekse. Ingen IT-systemer er feilfrie, men kvalitetskontroll med utvikling, implementering og drift må kunne forventes. Når ulike IT-systemer knyttes sammen i digitale økosystemer øker kompleksiteten, og kravene til kontroll og oppfølging blir enda høyere. Denne gjennomgangen har vist at kritisk funksjonalitet for å motta meldinger i kommunenes fagsystem ikke har vært testet godt nok. Det har også vært ustabilitet knyttet til driften av kommunenes IT-løsninger. Når disse to feilene har skjedd samtidig har bekymringsmeldinger blitt borte. Selv om man kan forvente feil i IT-systemer, er det Bufdir sin vurdering at grunnleggende kvalitetskontroll hos leverandøren i dette tilfellet har vært mangelfull. Hendelsen viser at kommunenes internkontroll med IT-løsninger heller ikke har vært god nok. Det har ikke har vært utøvet tilstrekkelig kontroll med leveransekjedene i den daglige driften. Selv om det har vært tilgjengelige verktøy for overvåking av meldingstrafikken, har de kommunale barnevernstjenestene ikke brukt disse verktøyene på en slik måte at feil kunne oppdages raskt.

Gjennomgangen viser at organiseringen av, og kontrollen med, digitale tjenestekjeder spiller en rolle i systemsvikten. Bufdir vurderer det som bekymringsverdig at feilen har kunnet eksistere i over to år før den ble avdekket og rettet. En bedre oppfølging av dataflyten ville kunnet bidratt til å redusere konsekvensene av feilen betydelig eller helt. Offentlige meldere skal i henhold til barnevernsloven motta tilbakemelding om at en innsendt bekymringsmelding er mottatt og informasjon om hvordan den er fulgt opp. Denne hendelsen viser at offentlige meldere i liten grad har etterspurt informasjon, selv om tilbakemelding fra barneverntjenesten har uteblitt. KS viser til eksempler fra kommuner der digitale bekymringsmeldinger har blitt borte, hvor det burde vært meldt avvik av melder og/eller kommunen. I stedet har slike hendelser blitt forklart med menneskelig feil (brukerfeil), og rettet opp ved å sende bekymringsmeldingen på nytt. KS trekker frem følgende sitat fra en berørt kommune: «Den digitale selvtilliten er så lav, at man stoler mindre på sin egen kompetanse enn på de digitale systemene».

Bufdir vurderer at det ikke er stor risiko for langsiktige negative konsekvenser av hendelsen på samfunnsnivå, fordi sakens er omfang er begrenset, sammenlignet med hva man fryktet i den tidlige fasen. Hadde saken hatt et vesentlig større omfang, ville risikoen for langsiktige negative konsekvenser vært betydelig høyere. Men vi kjenner ikke konsekvensene for det enkelte barn og den enkelte familie som er berørt. Flere av familiene kan vi anta at barneverntjenesten kjenner til, men det er alvorlig hendelsen kan ha ført til at noen barn som lever under omsorgssvikt ikke blir oppdaget, eller oppdages for sent.

Det kan være grunn til å spørre seg om utvikling av offentlig digitale løsninger i for stor grad har vært preget av optimisme. Utviklingen av konsepter og store ambisjoner blir fremhevet i strategier, gjennom finansiering og på konferanser. Operasjonalisering, internkontroll, etterlevelse og løsninger i drift får ikke samme oppmerksomheten. Tjenestekjeder, informasjonsflyt,

datadeling, bruk av felleskomponenter og offentlig/privat samarbeid er viktige bærebjelker i nasjonale strategier. Den digitale tjenestekjeden som nå opplevde svikt, tilfredsstiller alle disse strategiske kravene og føringene. Det er drift og forvaltning av løsningen som har vært mangelfull og hvor det har vært svikt i flere deler av verdikjeden.

Brukerne har forventninger til at offentlige systemer virker, og til at det offentliges IT-systemer gjør det de skal, har trygg håndtering og kontroll på data – og at systemene sier fra om noe er feil. Bufdir mener at det må være rimelig å ha slike forventninger, og at robuste digitale løsninger er grunnleggende for å styrke tilliten til de offentlige tjenestene. Barnevernets håndtering av sensitiv informasjon og barnevernstjenestenes potensielt inngripende rolle i den enkeltes liv gjør dette særlig viktig. For å møte brukernes forventninger må digitale økosystemer og tjenestekjeder ha systemer for drift og internkontroll som er representative for den helheten brukerne forventer. Bufdir mener det er grunn til å ha en større oppmerksomhet omkring helheten når man etablerer digitale verdikjeder, særlig når dette omfatter flere aktører, på tvers av virksomheter og forvaltningsnivåer. Aktørene som har ansvar for de ulike delene av tjenestekjedene må snakke sammen og følge hverandre opp – gjennom avtaler, felles rutiner, møter og arbeidsgrupper. Spørsmålet "virker dette i hverdagen" bør stilles - og besvares - oftere. Dette gjelder spesielt ved oppgradering av eksisterende løsninger, hvor man er avhengig av at alle kommuner gjennomfører oppgraderingen for at løsningene skal være kvalitetssikret. Noe av svikten i denne saken er manglende kvalitetssikring av at dette faktisk er gjennomført. Dette er et ansvar som hviler på kommunene og systemleverandørene, samtidig som alle som deltar i arbeidet med å digitalisere offentlige tjenester må bidra til at dette arbeidet blir realistisk gjennomførbart.

En ny nasjonal digitaliseringsstrategi er på trappene, og skal lanseres i 2024. Denne bør ta inn over seg disse forholdene, og adressere krav til sikker implementering og oppfølging. En ny nasjonal digitaliseringsstrategi bør også stille krav til å redusere kompleksiteten og sikre transparens for de løsningene som tas i bruk. Digitale satsinger fra regjeringen bør ha krav til implementering og oppfølging i sektorene, slik at frivillighet ikke skaper unødig høy kompleksitet.

En OECD-rapport fra 2016 peker på at en sentral digitaliseringsmyndighet bør gis større makt og gjennomføringskraft i Norge.[21] I lys av de konkrete funnene i denne rapporten mener Bufdir det kan være grunn til å vurdere denne anbefalingen på nytt.

For den nasjonale bekymringsmeldingsportalen har det vært valgt én løsning for hele landet. KS melder at NPB er kommunenes foretrukne kanal for mottak av bekymringsmeldinger. Løsningen har også oppslutning blant systemleverandørene til sektoren. Løsningen er en del av prosjektet DigiBarnevern, som har hatt som målsetning å erstatte gammeldagse og uhensiktsmessige IT-systemer i kommunale barneverntjenester. Løsningene som er laget er gode, de er laget under ledelse av- og i samarbeid med kommunene - og de virker. Det er etablert systemer for drift, forvaltning og fortløpende kontroll med meldingsflyten. Et viktig læringspunkt er at teknologi og organisering må virke sammen - og at uten dette kan enkle, grunnleggende feil forårsake svikt. Bufdir vurderer at enhetlig bruk av nasjonale løsninger bør forsterkes i offentlige strategier, og at

[21] OECD (2016). *Digital Government Review of Norway. Boosting the digital transformation of the public sector. Assessment and recommendations.* https://www.oecd.org/gov/digital-government/digital-government-review-norway-recommendations.pdf

en felles oppslutning om den nasjonale bekymringsportalen vil gi kommunene enklere oversikt og oppfølging av sine digitale verdikjeder.

Bufdir vil i særlig grad takke Visma og KS som har gått i dialog med alle landets kommuner for å bidra med feilsøking og programvareoppdatering. Når feilen først var et faktum agerte Visma, KS og berørte kommuner raskt med relevante tiltak for å rette feilen og redusere negative konsekvenser. Kommunene gir også Visma ros for den dialogen og oppfølgingen de har hatt overfor sine kunder i denne saken.

Visma og KS har også vært sentrale i å tilby data og oversikt til Bufdir, slik at vi kunne få et bilde av helhetssituasjonen og kommunisere til våre overordnede myndigheter og media. Kommunene opplevde at offentlige aktører, KS og Visma var samkjørte i sin informasjonsformidling. Kommunene har vært raske til å implementere programvareoppdateringen fra Visma. Denne åpenheten og villigheten til å samarbeide har vært sentral for å redusere ytterligere konsekvenser av feilen. Arbeidet med oppfølging av kommunene som har opplevd å miste bekymringsmeldinger fortsetter, og Bufdir har bedt KS om å fortsatt ta en sentral rolle i dette.

Vi vil takke alle bidragsyterne for mobilisering, åpenhet og villighet til å gå inn arbeidet med gjennomgangen - med formål om å lære og bli bedre. Vi ser fram til framtidig samarbeid om tjenesteutvikling og digitalisering.

Vedlegg 1: Hvordan har kommunene blitt fulgt opp?

Oppsummering

I dette vedlegget gir Bufdir en status for hvordan relevante aktører per 24.10.23 har fulgt opp kommuners arbeid med å håndtere konsekvensene av feilen og veiledet kommunesektoren i å forebygge at lignende feil skjer, jf. del B av oppdraget.

Kommunenes installasjon av nødvendige rettelser fra systemleverandør

Visma

Visma har kontaktet alle potensielt berørte kommuner, samt tilrettelagt for dialog mellom kommunene om saken, gjennom vårt kundeforum Visma Community.

Alle kommuner som benytter Familia og integrasjonen mot Nasjonal portal for bekymringsmelding har installert programvarerettelsen Visma publiserte 31.05.23. Kommuner som har hatt behov for det har fått bistand av Visma til installasjonen. To senere versjoner med justeringer og forbedringer av programvarerettelsen har blitt tilgjengeliggjort for alle kunder. Visma har tatt kontakt med enkelte berørte kommuner, for å få tilgang til ulike typer logger, for å forsøke å få innsikt i rotårsaken til hendelsen.

Videre har Visma fulgt opp generelle forespørsler fra våre kunder på ordinær måte gjennom vårt supportapparat.

Datatilsynet

Datatilsynet la raskt ut informasjon i en nettartikkel om at kommunene måtte følge instruksjoner og anbefalinger fra Visma. Dette anså vi hensiktsmessig ut fra den informasjonen vi hadde fått fra Visma om hvordan de bistod kommunene i å undersøke og rette opp i avviket.

Kommunene som har sendt oss avviksmelding vil i det videre vil følges opp gjennom ordinær saksbehandling.

Manuelle rutiner for at bekymringsmeldinger når fram

Visma

Interne rutiner kan bidra til å sikre at bekymringsmeldinger sendt i ulike kanaler når frem til barnevernet. I hovedsak ser Visma følgende eksempler på rutiner som kan bidra til å sikre at tilsvarende hendelser ikke skjer igjen:

- Den enkelte kommune kan ha rutiner for å monitorere, eller i det minste ta stikkprøver av, logger når de drifter løsningen i egen infrastruktur, slik at feilsituasjoner raskere fanges opp.
- Barnevernstjenesten kan etablere rutiner for tilbakemelding som supplerer de automatiske rutinene i systemet, slik at melder får tilbakemeldinger i to steg
    1. Systemgenerert melding om at "vi har mottatt din bekymringsmelding"
    2. Manuell (eller systemgenerert på gitte kriterier) melding om at "En saksbehandler har fått tildelt din bekymringsmelding og vil følge den opp". Dersom melding to ikke sendes, vil meldere ha en oppfordring til å følge opp at meldingen faktisk har kommet frem.
- Offentlige meldere kan ha rutiner for å følge opp med barnevernet i sin kommune, dersom de ikke har mottatt tilbakemelding om at saken er mottatt og tatt til vurdering ihht. barnevernslovens bestemmelser om tilbakemelding

KS

Rutiner kan gjelde både den som sender meldinger og den som mottar meldinger.

Bekymringsmeldinger som sendes gjennom NPB sendes direkte fra fagsystem eller gjennom nettsiden. I samråd med Bufdir har KS på nettsiden lagt inn en ekstra oppfordring til offentlig melder, både før og etter innsendelse, å ta kontakt med barnevernet dersom tilbakemelding uteblir. I tillegg er det lagt inn en oppfordring til offentlig melder å lagre meldingen et trygt sted og ta vare på kvitteringen.

Bekymringsmeldinger skal komme fram i fagsystem eller ved manuell nedlasting. Selv om avviket gjaldt de meldingene som sendes til fagsystem, har KS gjort et grep for kommuner som laster ned meldinger manuelt fra NPB: barnevernstjenesten får varsel tre ganger i døgnet (istedenfor 1) om meldinger som ligger klar til nedlasting.

Vi vet fra dialog med kommuner at mange har innført eller skjerpet manuelle kontrollrutiner, der antall meldinger som mottas gjennom NPB og SvarUt sammenlignes med antall meldinger som registreres i fagsystem. For å hjelpe kommuner å gjennomføre kontrollen mest effektivt, forbedrer KS dashbordet som viser antall meldinger.

KS arrangerte 13. juni et erfaringsdelingsmøte, der kommunen kunne utveksle erfaringer og praksis rundt arbeidet med kontroll av digitale bekymringsmeldinger.

Aktiviteter for at tapte bekymringsmeldinger kan meldes på nytt

Visma

Vismas bidrag til at tapte bekymringsmeldinger kan meldes på nytt har vært å forsøke å sette kommunen i stand til å håndtere situasjonen ved å

- Informere kommunene om saken
- Legge til rette for samarbeid/ erfaringsutveksling mellom berørte kommuner
- Dele instruksjoner om hvordan man kan finne feilsituasjoner i logger
- Bistå kommuner som hadde behov for det med å finne feilsituasjoner i logger
- Tilgjengeliggjøre metadata for når meldinger er sendt fra andre Visma-fagsystemer, for å se om man kan finne tilbake til melding eller melder (kun for de kundene som benytter andre Visma-fagsystemer som også er integrert mot KS sine fellestjenester).

KS

KS Digitale fellestjenester har økt lagringstid fra meldinger som kommer gjennom NPB fra 14 dager til 30 dager. Avhengig av resultatene fra denne gjennomgangen, kan KS Digitale fellestjenester i samarbeid med kommuner, gjøre en ny vurdering om det er ønskelig at lagringstid beholdes.

Ellers viser vi til det som ble nevnt under 3.3.2.

Utvikling og implementering av rutiner for å forebygge lignende feil

Visma

Visma gjennomfører en internrevisjon av relevante prosesser for å kartlegge forbedringspunkter i prosessene eller tilhørende støtteverktøy. Revisjonen har særlig fokus på prosess for utvikling og testing av programvare. Revisjonen vil også gjennomgå prosessene for support og håndtering av personvernavvik, for å identifisere eventuelle forbedringspunkter.

Alle læringspunkter fra internrevisjonen vil deles internt i Visma, slik at flere fagområder og team kan lære av saken.

KS

KS Digitale fellestjenester tilbyr maler for ROS og DPIA som kommuner kan bruke som grunnlag når de tar tjenester i bruk. KS Digitale fellestjenester har tatt inn risikoen for at lignende feil kan skje inn i ny versjon av ROS-mal til kommuner.

KS Digitale fellestjenester har videreutviklet dashbord for kommuner for at kommuner kan gjennomføre manuelle kontroller hvor antall fra NPB sammenlignes med antall meldinger i fagsystem.

I dialogen med kommuner kommer det fram at kommunene vil bruke denne erfaringen for å forbedre både internkontroll og beredskapsplaner, herunder gode rutiner for varsling til personvernombud og Datatilsynet. Tanken er også at mer samarbeid med andre kommuner (gjerne i regi av KS) for å følge opp mistanker om enkeltfeil, vil øke sjansen for at lignende feil med fellesløsninger, som potensielt gjelder flere, oppdages og utbedres.