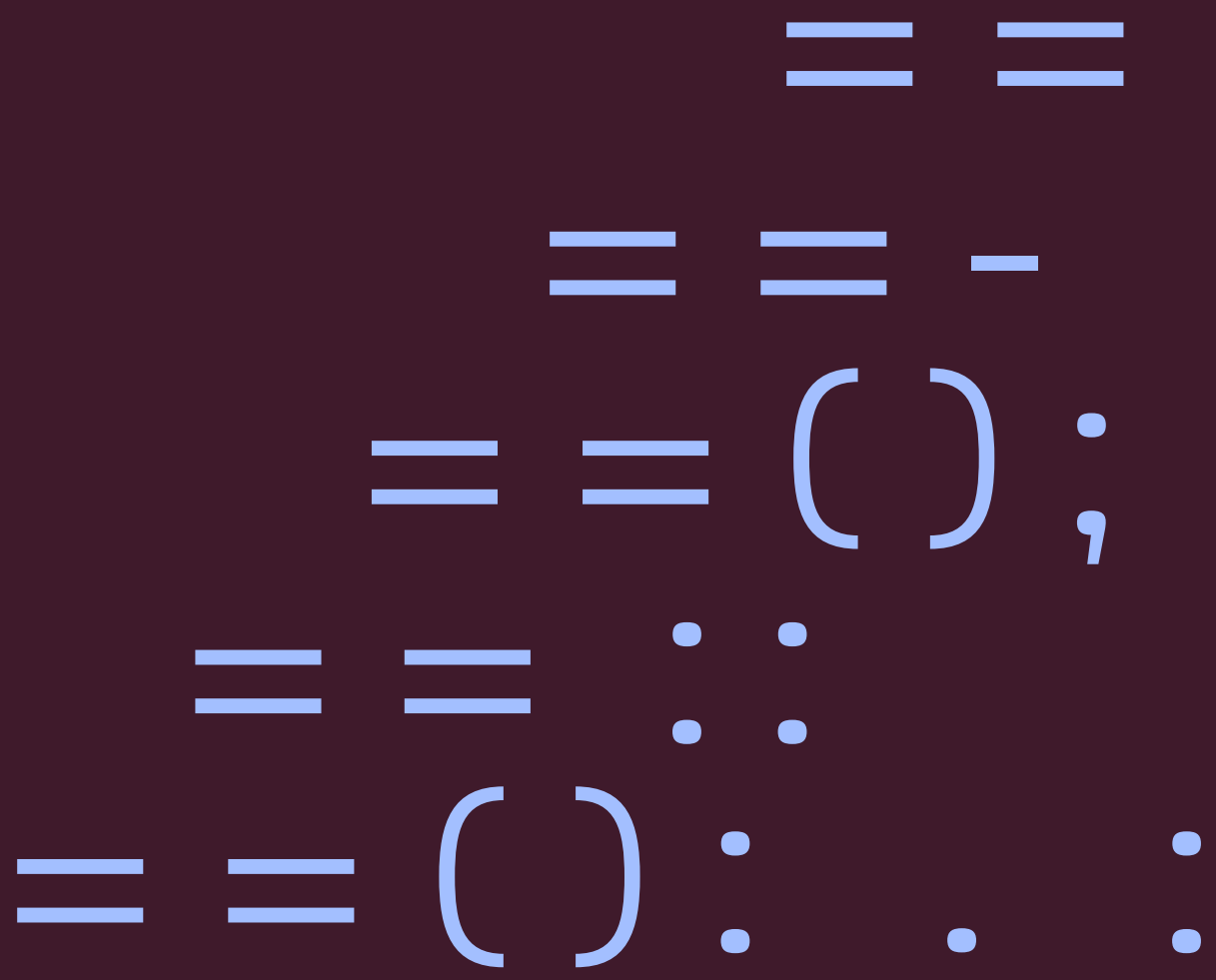
Digitaliserings-
styrelsen

Bilag C

Risici ved Digitaliseringsstyrelsens behandling af personoplysninger som databehandler



November 2024

Indhold

Versionsstyring

Version	Kommentar
1.0 af 5. januar 2023	Endelig version af bilag C med bl.a. flere af DPO's bemærkninger indarbejdet.
1.1 af 14. september 2023	Udtrykket "NgDP" er generelt ændret til "Digital Post" eller "Digital Post-løsning" samt andre småjusteringer af lignende karakter.
1.2. af 11. november 2024	Opdatering af bilag C med nye risici og efter Digitaliseringsstyrelsens bemærkninger samt generel ajourføring.

1. Indledning og sammenfatning

Digitaliseringsstyrelsen har i løbet af 2024 i samarbejde med Kammeradvokaten genvurderet konsekvensanalysen vedrørende databeskyttelse angående behandling af personoplysninger i Digital Post (herefter "Konsekvensanalysen"). Konsekvensanalysen vedrører alene behandling af personoplysninger, som Digitaliseringsstyrelsen foretager i sin rolle som dataansvarlig.

I forbindelse med analysen har styrelsen identificeret flere risici relateret til den behandling af personoplysninger i Digital Post-løsningen (eller Digital Post), som Digitaliseringsstyrelsen som databehandler foretager på vegne af andre dataansvarlige, dvs. offentlige afsendere og juridiske enheder, jf. § 2 a, stk. 3 og 4 i lov om Digital Post[1]. Idet Digitaliseringsstyrelsen ifølge § 10, stk. 3 i bekendtgørelse nr. 2019 af 29. oktober 2021 og bekendtgørelse nr. 2020 af 29. oktober 2021 om ansvar, opgaver og tilsyn i forbindelse med behandlingen af personoplysninger i forbindelse med forsendelse af digital post fra offentlige afsendere/juridiske enheder ("Digital Post-bekendtgørelsen"), skal bistå den dataansvarlige med at sikre overholdelse af den offentlige afsenders forpligtelser i medfør af databeskyttelsesforordningens artikel 32-36 og retshåndhævelseslovens §§ 25-29 under hensyntagen til behandlingens karakter og de oplysninger, der er tilgængelige for Digitaliseringsstyrelsen som databehandler, har Digitaliseringsstyrelsen udarbejdet dette bilag til Konsekvensanalysen.

Formålet med bilaget er således at identificere, beskrive og evaluere risici samt at pege på mulige mitigerende foranstaltninger, som enten de dataansvarlige eller Digitaliseringsstyrelsen som databehandler, kan eller bør implementere. Uanset at bilaget tager afsæt i Konsekvensanalysen, kan bilaget dermed samtidig anvendes som et selvstændigt dokument for både afsendere og Digitaliseringsstyrelsen i forbindelse med brugen af Digital Post-løsningen.

1.1 Sammenfatning

Fokus for dette notat er risici forbundet med behandling af personoplysninger i Digital Post-løsning, som Digitaliseringsstyrelsen foretager på vegne af de dataansvarlige, dvs. offentlige afsendere og juridiske enheder, jf. § 2 a, stk. 3 og 4 i lov om Digital Post.

Digitaliseringsstyrelsen har identificeret følgende 8 risici forbundet med denne behandling:

1. En digital meddelelse sendes til en forkert modtager
2. En masseforsendelse sendes til forkerte modtagere
3. Uvedkommendes adgang til virksomheders digitale postkasser
4. Høj organisatorisk, teknisk og juridisk kompleksitet
5. Fejl i modtagersystemet hos offentlige afsendere
6. Dataansvarskonstruktionen ved fejl i levering af meddelelser
7. Læse- og skriveadgang
8. Dataophobning for ophørte virksomheder

1.1.1 Hvor høje risici behandlingen indebærer

Digitaliseringsstyrelsen vurderer, at konsekvenserne for de registrerede, hvis risiciene indtræffer foruden fastlæggelse og implementering af de mitigerende foranstaltninger, fsva. risici nr. 1, 3 og 8 er

[1] Lovbekendtgørelse nr. 686 af 15. april 2021 om Digital Post fra offentlige afsendere

kritiske, for risiko nr. 2, 4, 5 og 6 betydelige og for risiko nr. 7 er lav. Sandsynligheden for, at disse indtræder, er i udgangspunktet **moderat**.

1.1.2 Medium eller lave risici efter mitigerende foranstaltninger

Digitaliseringsstyrelsen har genevalueret de ovennævnte risici hver især i forhold til effekten af de mitigerende foranstaltninger på de identificerede konsekvenser.

Der er identificeret 8 risici. Risikoen for 1 af de identificerede risici nedbragt til lav, og 5 risici er nedbragt til medium. Fsva. risiko nr. 2 og 3 er det Digitaliseringsstyrelsens vurdering, at denne risiko alene nedsættes, såfremt afsenderne følger Digitaliseringsstyrelsens anbefalinger, hvorfor restrisikoen for risiko 2 er angivet som lav-medium og for risiko 3 medium-høj.

2. Baggrund og faktuelle forhold

Digitaliseringsstyrelsen er i henhold til § 2, stk. 2 i lov om Digital Post udpeget til at sikre udvikling, drift, vedligeholdelse og forvaltning af Digital Post-løsningen. Digitaliseringsstyrelsen er dataansvarlig for Digital Post-løsningen, jf. § 2 a, stk. 1, jf. § 2 i lov om Digital Post.

Digital Post-løsningen består først og fremmest af borgeres og virksomheders digitale postkasser, hvor man kan logge sig ind og læse og besvare post fra offentlige myndigheder. Digital Post er derudover bygget op omkring en række centrale komponenter og en ny it-arkitektur, der er baseret på fællesoffentlige principper om at sikre sammenhæng, effektivitet og genbrug af data. Digital Post-løsningen vil dels interagere med offentlige og kommercielle visningsklienter, dels integrere med en anden fællesoffentlig digital infrastruktur, såsom MitID.

Digitaliseringsstyrelsen vil i forbindelse med driften af Digital Post som dataansvarlig behandle almindelige personoplysninger, herunder personnumre, CVR-numre, e-mail og telefonnumre o.lign. ca. 7,7 mio. fysiske personer (fysiske personer der er registreret i CPR-registreret herunder udrejste) og ca. 840.000 juridiske enheder (aktive og inaktive virksomheder). Skriftlig kommunikation mellem offentlige afsendere på den ene side og borgere eller virksomheder på den anden side vil som altovervejende hovedregel ske gennem Digital Post. Denne kommunikation – digitale meddelelser – kan indeholde alle kategorier og typer af personoplysninger, herunder følsomme personoplysninger og oplysninger om strafbare forhold, og Digitaliseringsstyrelsen vil derfor, som databehandler for de offentlige afsendere og juridiske enheder, behandle disse typer af personoplysninger i Digital Post-løsningen.

Karakteren af Digital Post-løsningen, herunder især det forhold at skriftlig kommunikation mellem offentlige afsendere på den ene side og borgere eller virksomheder på den anden side som altovervejende hovedregel vil ske gennem Digital Post, indebærer, at der behandles en betydelig mængde almindelige, fortrolige og følsomme personoplysninger. Dertil kommer, at Digital Post for virksomheder ikke alene kan anvendes til afsendelse og modtagelse af meddelelser, men tillige til opbevaring af indkomne meddelelser. Idet brugen af Digital Post-løsningen derudover er forbundet med retsvirkninger for de registrerede, indebærer den behandling af personoplysninger, som Digitaliseringsstyrelsen foretager på vegne af de dataansvarlige, i udgangspunktet en høj risiko for de registrerede personer.

For en mere omfattende beskrivelse af behandlingen af personoplysninger i Digital Post henvises til konsekvensanalysens afsnit 5.

3. Retsgrundlag

3.1 Databeskyttelsesforordningens regler om konsekvensanalyser

Det følger af databeskyttelsesforordningens artikel 35, stk. 1, at hvis en type behandling, navnlig ved brug af nye teknologier og i medfør af sin karakter, omfang, sammenhæng og formål, sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder, foretager den dataansvarlige forud for behandlingen en analyse af de påtænkte behandlingsaktiviteters konsekvenser for beskyttelse af personoplysninger.

Forpligtelsen til at udarbejde en konsekvensanalyse påhviler således ifølge artikel 35, stk. 1, den dataansvarlige.

Dog fremgår det tillige af databeskyttelsesforordningens artikel 28, stk. 3, litra f, at databehandleren bistår den dataansvarlige med overholdelse af forpligtelserne i databeskyttelsesforordningens artikel 32-36, dvs. bl.a. forordningens bestemmelse om konsekvensanalyser.

Det fremgår af Datatilsynets og Justitsministeriets Vejledning om Konsekvensanalyser, marts 2018, at:

> *"Du har som dataansvarlig alene pligt til at foretage en konsekvensanalyse i de tilfælde, hvor der sandsynligvis er høj risiko for fysiske personers rettigheder og frihedsrettigheder, herunder beskyttelse af personoplysninger. Har du konstateret, at der sandsynligvis er en høj risiko, er det ligeledes dig, der har ansvaret for at foretage en konsekvensanalyse. Foretages en behandling af en databehandler, skal denne hjælpe dig som dataansvarlig med at udføre konsekvensanalysen. Databehandleren skal endvidere sørge for at give dig den nødvendige information for at gennemføre analysen."*

3.2 Lov om Digital Post

Det følger af § 2 a, stk. 1, at Digitaliseringsstyrelsen er dataansvarlig for Digital Post, jf. lovens § 2.

Videre fremgår det af lovens § 2 a, stk. 3, at offentlige afsendere er dataansvarlige for indholdet af de meddelelser, de sender via Digital Post, og Digitaliseringsstyrelsen er databehandler for offentlige afsenderes forsendelse af meddelelser.

Juridiske enheder er dataansvarlige for indholdet af de meddelelser, de sender via og opbevarer i Digital Post. Digitaliseringsstyrelsen er databehandler for juridiske enheders forsendelse og opbevaring af meddelelser, jf. § 2 a, stk. 4.

Rollefordelingen fremgår af de specielle bemærkninger til § 2 a i lovforslag nr. 47 af 8. oktober 2020 om ændring af lov om Digital Post fra offentlige afsendere:

"Forslaget til bestemmelsen i stk. 3, fastlægger, at offentlige afsendere er dataansvarlige for indholdet af de meddelelser, de sender via Digital Post. Bestemmelsen fastlægger desuden, at Digitaliseringsstyrelsen er databehandler for offentlige afsenderes forsendelser i postløsningen.

[...]

Som nævnt bliver Digitaliseringsstyrelsen dataansvarlig for den kommende postløsning, idet Digitaliseringsstyrelsen bestemmer formål og afgør med hvilke hjælpemidler, der må foretages behandling af personoplysninger i postløsningen. Imidlertid bliver de offentlige afsendere dataansvarlige for indholdet af de meddelelser, de sender via postløsningen, hvilket er uændret i forhold til gældende ret. Digitaliseringsstyrelsen bliver dermed databehandler for forsendelser af meddelelser i postløsningen. Digitaliseringsstyrelsen har således hverken indflydelse på, hvornår meddelelser er afsendt eller på indholdet af meddelelserne.

I den kommende postløsning vil offentlige afsendere blive pålagt at have et modtagesystem. Modtage-løsningen indebærer, at opbevaringen af digital post hos offentlige afsendere sker, når modtageløsningen hos den pågældende offentlige afsender har modtaget posten. Digitaliseringsstyrelsen opbevarer dermed ikke posten for de offentlige afsendere, og Digitaliseringsstyrelsen bliver derfor ikke databehandler for op-bevaringen.

Forslaget til bestemmelsen i stk. 4, fastlægger, at virksomheder er dataansvarlige for indholdet af de meddelelser, de sender via og opbevarer i Digital Post. Digitaliseringsstyrelsen er databehandler for virksomheders forsendelse og opbevaring af meddelelser i postløsningen.

Opbevaringen vil ske i virksomhedens digitale postkasse, der udgør en del af den kommende Digital Post-løsning."

Omfanget af den databehandling Digitaliseringsstyrelsen foretager på vegne af virksomheder er således større end den behandling, Digitaliseringsstyrelsen foretager på vegne af offentlige afsendere, idet Digitaliseringsstyrelsen ift. sidstnævnte ikke opbevarer digitale meddelelser på vegne af offentlige afsendere.

4. Identifikation og evaluering af risici

Digitaliseringsstyrelsen har nedenfor identificeret risici for de registreredes rettigheder og frihedsrettigheder (risikoidentifikation) forbundet med Digitaliseringsstyrelsens behandling af personoplysninger i Digital Post som databehandler samt evalueret disse risici ud fra deres sandsynlighed og alvorlighed (risikoevaluering), jf. databeskyttelsesforordningens artikel 35, stk. 7, litra c. Nærmere bestemt har styrelsen foretaget en vurdering af risikoens oprindelse, karakter, særegenhed og alvorlighed, jf. databeskyttelsesforordningens præambelbetragtninger 84 og 90. Vurderingen foretages i det følgende for hver enkelt identificeret risiko set ud fra den registreredes perspektiv, men på et objektivt grundlag.

En risiko defineres som et scenarie, der beskriver en hændelse og konsekvenserne heraf, som vurderes i forhold til alvor og sandsynlighed.

Efter at have identificeret og evalueret de forskellige risici er næste skridt at identificere foranstaltninger for at kunne håndtere disse risici. Formålet er at nedbringe de identificerede risici til et acceptabelt niveau. De typiske risikostyringsstrategier vil være at enten eliminere, reducere eller acceptere den identificerede risiko. Idet Digitaliseringsstyrelsen i relation til de risici, der identificeres i regi af dette notat, alene handler som databehandler, og hverken organisatorisk eller teknisk har indflydelse på den fulde behandlingsaktivitet, vil Digitaliseringsstyrelsen – udover at pege på "egne" mitigerende foranstaltninger – i nødvendigt og relevant omfang pege på mulige mitigerende foranstaltninger, som de dataansvarlige offentlige afsendere eller private virksomheder kan eller bør implementere med henblik på at imødegå en identificeret risiko.

4.1 Valg af evalueringskriterier for sandsynlighed og konsekvens

I denne konsekvensanalyse anvendes følgende evalueringskriterier for sandsynlighed:

4	**Forventet:** Det forventes, at hændelsen vil forekomme, herunder f.eks.: - Man har gentagen erfaring med hændelsen inden for de sidste 12 måneder. - Hænder jævnligt hos andre offentlige myndigheder og private virksomheder (omtales ofte i pressen).
3	**Moderat sandsynligt**: Det er moderat sandsynligt, at hændelsen vil forekomme, herunder f.eks.: - Man har erfaring med hændelsen, men ikke inden for de sidste 12 måneder. - Kendes fra andre offentlige myndigheder og private virksomheder i Danmark (omtales årligt i pressen).
2	**Mindre sandsynligt**: Hændelsen forventes ikke at forekomme, herunder f.eks.: - Ingen eller særdeles begrænset erfaring med hændelsen. - Kendes fra få andre offentlige myndigheder og private virksomheder.

1	**Usandsynligt**: Det anses for næsten udelukket, at hændelsen nogensinde kan forekomme, herunder f.eks.: - Ingen erfaring med hændelsen. - Kendes fra få andre offentlige myndigheder og private virksomheder, men ikke i Danmark.

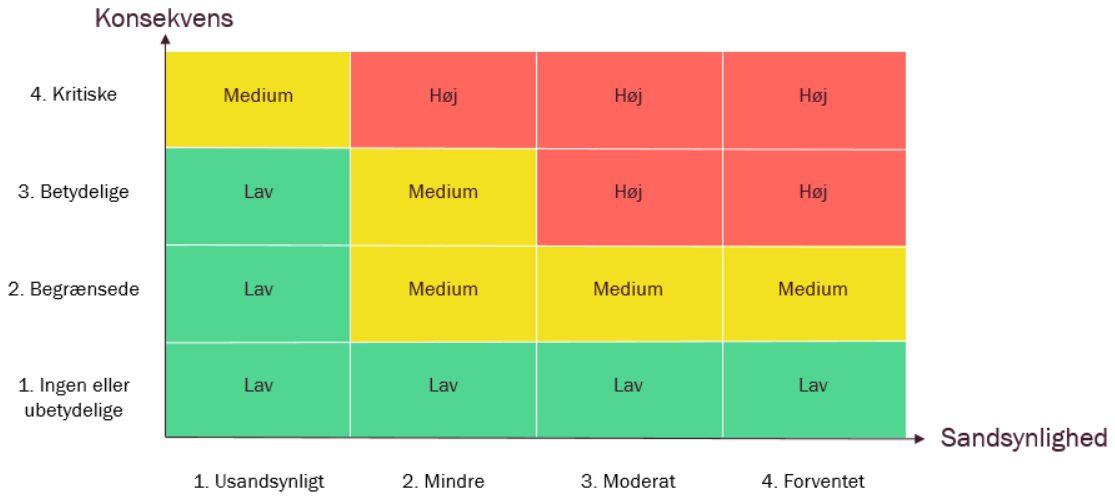
Tabel 1. Evalueringskriterier for sandsynlighed

I denne konsekvensanalyse anvendes følgende evalueringskriterier for konsekvens[2]:

4	**Kritiske konsekvenser:** De registrerede kan opleve kritiske konsekvenser, som de ikke nødvendigvis kan overvinde, f.eks. økonomisk nød som betydelig gæld eller manglende evne til at arbejde, langsigtede psykiske eller fysiske lidelser, død m.v.
3	**Betydelige konsekvenser**: De registrerede oplever betydelige konsekvenser, som de kan overvinde, om end med alvorlige vanskeligheder, f.eks. identitetstyveri eller -svig, finansielle tab, blacklisting af banker, ejendomsskade, tab af beskæftigelse, stævning, forværring af sundhedstilstanden, tab af fortrolighed af personoplysninger, der er omfattet af tavshedspligt m.v.
2	**Begrænsede konsekvenser**: De registrerede oplever begrænsede konsekvenser, som de vil være i stand til at overvinde med få vanskeligheder, f.eks. ekstra omkostninger, nægtelse af adgang til forretningstjenester, manglende forståelse, frygt, stress, mindre fysiske påvirkninger m.v.
1	**Ingen eller ubetydelige konsekvenser**: De registrerede bliver enten ikke påvirket eller udsættes alene for få generende konsekvenser, som de uden problemer kan håndtere, f.eks. tidsforbrug brugt på at genindtaste oplysninger, irritationer, dårlig brugeroplevelse m.v.

Tabel 2. Evalueringskriterier for konsekvens

Når evalueringskriterierne for sandsynlighed og konsekvens er fastlagt, kan hver enkelt identificeret risiko vurderes og kortlægges på et såkaldt risikokort. I denne konsekvensanalyse anvendes følgende risikokort:



Figur 1. Risikokort

[2] Se f.eks. punkt A.2 i Annex A til ISO/IEC 29134:2017; Datatilsynet m.fl., Vejledning om behandlingssikkerhed og databeskyttelse gennem design og standardindstillinger, juni 2018, s. 9; Digitaliseringsstyrelsen, Vejledning i vurdering af offentlige it-projekters potentielle konsekvenser for privatlivet, maj 2013, s. 12

4.2 Identifikation, evaluering og håndtering af risici

4.2.1 Risiko nr. 1: En digital meddelelse sendes til en forkert modtager

Vurdering af risikoen

Borgere og virksomheder har i den eksisterende Digital Post-løsning oplevet at modtage en digital meddelelse forkert, således at borgere/virksomhed enten har modtaget en andens meddelelse, eller at en borger/virksomhed er blevet opmærksom på, at ens egen meddelelse er sendt til en forkert modtager.

Fremsendelse af en digital meddelelse til en forkert modtager kan ske på forskellige måder. Det kan således først og fremmest ske ved, at en offentlig afsender sender en meddelelse til en forkert borger, f.eks. ved at indtaste et forkert personnummer. I denne situation vil Digitaliseringsstyrelsen være databehandler for den offentlige myndighed, som er dataansvarlig, jf. § 2 a, stk. 3 i lov om Digital Post. Tilsvarende hvis en virksomhed sender en meddelelse til en forkert modtager.

Derudover kan en digital meddelelse sendes til en forkert modtager pga. systemfejl, f.eks. hvis der sker kodefejl i forbindelse med ændringer i Digital Post-løsningen, hvormed dataansvaret er Digitaliseringsstyrelsens og ikke den offentlige afsenders, jf. § 2 a, stk. 1 i lov om Digital Post.

Sandsynligheden for, at en meddelelse i den beskrevne situation sendes til en forkert modtager vurderes som ***moderat*** s***andsynlig*** (nr. 3). Dette skyldes, at der i denne situation både kan være tale om systemfejl og menneskelige fejl, f.eks. ved at en medarbejder hos en afsender taster et forkert personnummer, idet menneskelige fejl erfaringsmæssigt kan forekomme, hvorfor denne risiko også må antages at kunne indtræde.

Det er Digitaliseringsstyrelsens vurdering, at konsekvenserne forbundet med, at en meddelelse sendes til en forkert modtager, for de registreredes rettigheder og frihedsrettigheder, kan være **kritiske** (nr. 4). Der lægges i den forbindelse vægt på, at der kan være tale om alle typer af personoplysninger, herunder følsomme personoplysninger, om enhver registreret i Digital Post, ligesom selv fremsendelse af almindelige oplysninger til en forkert modtager kan have kritiske konsekvenser, f.eks. hvis der er tale om fremsendelse af oplysninger om en registreret persons beskyttede adresse til en person, som den pågældende har et tilhold imod. Dertil kommer, at disse konsekvenser kan være vanskelige for den registrerede selv at overvinde, selv såfremt den forkerte modtager sletter den forkert sendte/modtagne digitale meddelelse eller misbruger oplysninger, som den forkerte modtager har fået adgang til i forbindelse med forsendelsen.

På baggrund af vurderingen af sandsynligheden og konsekvensen er den samlede vurdering af risikoen ***høj***.

Foranstaltninger til at håndtere risikoen

Når en meddelelse sendes forkert i Digital Post-løsningen, vil dette oftest hænge sammen med en menneskelig fejl begået af afsenderen, dvs. den dataansvarlige offentlige afsender eller juridiske enhed eller den registrerede selv. Det er således langt mindre sandsynligt, at fejlforsendelse sker pga. en systemfejl. Digital Post-løsningen (it-systemet) kan ikke i sig selv sende meddelelser til en anden modtager, end den systemet får besked på. Digitaliseringsstyrelsen vil derfor i langt de fleste tilfælde

af fremsendelse af digital post til en forkert modtager handle som databehandler og ikke som dataansvarlig, idet Digitaliseringsstyrelsen alene vil være dataansvarlig i tilfælde, hvor styrelsen selv agerer som offentlig afsender, eller hvor der er tale om en fejl i Digital Post-løsningen, som styrelsen er ansvarlig for. I den forbindelse tester og kvalitetssikrer Digitaliseringsstyrelsen løsningen med henblik på at sikre sig mod systemfejl i forbindelse med fremsendelse af meddelelser.

Digitaliseringsstyrelsen tilstræber generelt at informere de offentlige afsendere om, at de skal være opmærksomme på korrekt angivelse af, hvem der skal modtage en meddelelse. Digital Post-løsningen afleverer automatisk meddelelsen til den angivne modtager. Hvis den angivne modtager ikke er identisk med den tilsigtede modtager, påhviler dette ansvar afsenderen. Dette kan ikke løses i selve Digital Post-løsningen, men skal i stedet for håndteres i den offentlige afsenders afsendersystem, f.eks. ved at indbygge en validering af det indtastede personnummer.

Det er ikke muligt for Digitaliseringsstyrelsen i regi af Digital Post at foretage validering af, at afsenderen – hvad enten der er tale om en offentlig afsender, en borger eller en privat virksomhed – har indtastet de korrekte oplysninger om modtageren af meddelelsen, eksempelvis det korrekte personnummer. Digitaliseringsstyrelsen anbefaler derfor, at afsenderne implementerer en sådan funktionalitet i deres afsendersystemer med henblik på at nedbringe sandsynligheden for den identificerede risiko.

Digitaliseringsstyrelsen gør afsenderne bekendte med dette bilag, herunder anbefalingen om implementering af validering af de indtastede oplysninger, i forbindelse med tilslutning til Digital Post-løsningen eller – ved allerede tilsluttede afsendere – ved fremsendelse af information til de pågældende afsendere om den identificerede risiko samt mulige mitigerende foranstaltninger.

Såfremt der først er sket en fejlforsendelse, har den offentlige afsender mulighed for at tilbagekalde denne før valørdato nås. Hvis der ikke er angivet en valørdato, og meddelelsen dermed afleveres med det samme, vil afsenderen ikke kunne tilbagekalde meddelelsen. Dette med undtagelse af, at der foreligger en instruks, der på baggrund af lovgivning eller retskendelse giver hjemmel til, at meddelelsen kan trækkes tilbage. Baggrunden er, at meddelelser modtaget i Digital Post er omfattet af beskyttelsen i grundlovens § 72, hvoraf følger, at indgreb heri kun kan ske på baggrund af retskendelse eller særhjemmel.

Derudover vil den registrerede have mulighed for at kontakte Digitaliseringsstyrelsen eller styrelsens hotline om identitetstyveri med henblik på at imødegå eventuelle konsekvenser forbundet med forkert forsendelse af meddelelser. Disse vil således i et vist omfang kunne overvindes af den registrerede.

På baggrund af de identificerede foranstaltninger, vurderes det, at sandsynligheden for, at de registrerede enten modtager en forkert digital meddelelse eller får at vide, at den registreredes egen digitale meddelelser er sendt til en forkert modtager, nedjusteres til ***mindre sandsynligt*** (nr. 2), mens konsekvenserne nedjusteres til ***betydelige*** (nr. 3). Baggrunden for denne sandsynlighedsvurdering er, at denne efter Digitaliseringsstyrelsens opfattelse alene kan nedsættes til usandsynlig, såfremt afsenderne følger Digitaliseringsstyrelsens anbefalinger. Konsekvens kan reduceres, da det er muligt at få hjælp mod muligt identitetstyveri eller optagelse af lån. Såfremt afsenderne vælger alene implementere den ene af foranstaltningen, kan sandsynligheden kun nedsættes til mindre sandsynligt. Dette gælder især, hvis der ikke implementeres modtagervalidering. Samlet betyder dette, at den samlede vurdering af residualrisikoen er ***medium***.

4.2.2 Risiko nr. 2: En masseforsendelse sendes til forkerte modtagere

Vurdering af risikoen

Offentlige afsendere kan – ligesom i dag – også fremover sende en meddelelser med identisk indhold til mange borgere/virksomheder på én gang ved en såkaldt masseforsendelse. Det samme kan i princippet gøre sig gældende for juridiske enheder, f.eks. hvis disse har et kundeforhold til flere af landets kommuner.

Ligesom ved enkeltforsendelser til navngivne modtagere kan en masseforsendelse sendes til forkerte modtagere. Digital Post-løsningen (it-systemet) kan heller ikke ved masseforsendelser i sig selv sende meddelelser til andre modtagere, end dem systemet får besked på. Digitaliseringsstyrelsen vil derfor handle som databehandler i tilfælde af, at en masseforsendelse sendes til forkerte modtagere.

Sandsynligheden for, at en masseforsendelse af digitale meddelelser sendes til forkerte modtagere, vurderes som ***moderat sandsynligt*** (nr. 3). Dette skyldes, at der erfaringsmæssigt – især når der sendes mange generiske breve til en stor mængde registrerede – må forventes at ske fejlforsendelser af disse. Fremsendelse af en masseforsendelse til forkerte modtagere kan ske, hvis der dannes f.eks. flere lister over modtagere og meddelelser sendes til den forkerte liste, dvs. hvor et udtræk er specificeret forkert så forkerte modtagere indgår i en liste, der efterfølgende sendes meddelelser til.

Det er videre Digitaliseringsstyrelsens vurdering, at konsekvenserne forbundet med, at en masseforsendelse af digitale meddelelser sendes til forkerte modtagere, for de registreredes rettigheder og frihedsrettigheder vil være ***betydelige*** (nr. 3), idet masseforsendelser som klar hovedregel ikke vil indeholde følsomme personoplysninger, men omvendt godt kan indeholde fortrolige oplysninger. Dertil kommer, at de registrerede i de fleste tilfælde som udgangspunkt vil være i stand til at overvinde denne type konsekvenser med få vanskeligheder, f.eks. ved at tage telefonisk kontakt til afsendermyndigheden, såfremt de undrer sig over meddelelsen.

På baggrund af vurderingen af sandsynligheden og konsekvensen er den samlede vurdering af risikoen ***høj***.

Foranstaltninger til at håndtere risikoen

Grundlæggende er der ikke forskel på behandlingen af enkelt- og masseforsendelser. Det bemærkes indledningsvis, at Digitaliseringsstyrelsen i forbindelse med masseforsendelser alene handler som databehandler for de offentlige afsendere eller virksomhederne. Fejl i it-systemet kan også forekomme, jf. risiko nr. 1.

Digitaliseringsstyrelsen informerer generelt de dataansvarlige om, at de skal være opmærksomme på korrekt angivelse af, hvem der skal modtage en meddelelser. Digital Post-løsningen afleverer automatisk meddelelsen til den angivne modtager. Hvis den angivne modtager ikke er identisk med den tilsigtede modtager, påhviler dette ansvar afsenderen. Dette kan ikke løses i selve Digital Post-løsningen, men skal i stedet for håndteres i afsenderens afsendersystem, f.eks. ved at indbygge en validering af de indtastede oplysninger. Digitaliseringsstyrelsen anbefaler derfor, at afsenderne implementerer en sådan funktionalitet i deres afsendersystemer med henblik på at nedbringe sandsynligheden for den identificerede risiko.

Digitaliseringsstyrelsen gør afsenderne bekendte med dette bilag, herunder anbefalingen om implementering af en validering af de indtastede oplysninger, i forbindelse med tilslutning til Digital Post-løsningen eller – ved allerede tilsluttede afsendere – ved fremsendelse af information om denne risiko og de identificerede mitigerende foranstaltninger.

Såfremt der først er sket en fejlforsendelse af en masseforsendelse, har den offentlige afsender mulighed for at tilbagekalde masseforsendelsen, før valørdato nås. Hvis der ikke er angivet en valørdato, og meddelelsen dermed afleveres med det samme, vil afsenderen ikke kunne tilbagekalde meddelelsen. Derudover vil den registrerede have mulighed for at kontakte Digitaliseringsstyrelsen eller styrelsens hotline om identitetstyveri med henblik på at imødegå eventuelle konsekvenser forbundet med forkert forsendelse af meddelelser. Disse vil således i et vist omfang med relativt få vanskeligheder kunne overvindes af den registrerede.

Digitaliseringsstyrelsen er allerede i dag bekendt med problemstillingen om, at masseforsendelser af digitale meddelelser sendes til forkerte modtagere.

Der sker i Digital Post en validering af meddelelsen med henblik på kontrol af, om de indtastede personnumre eller CVR-numre er oprettet som modtagere i Digital Post. Der tjekkes også her for fritagelsesstatus, herunder om der skal ske fremsendelse af meddelelsen via fysisk post. Når alle kontroller er sket, vil meddelelsen blive sendt til modtagers digitale postkasse.

På baggrund af de beskrevne foranstaltninger vurderes det, at sandsynligheden for, at en masseforsendelse af digitale meddelelser sendes til forkerte modtagere, nedjusteres til **usandsynligt** (nr. 1) eller ***mindre sandsynligt*** (nr. 2), mens konsekvenserne forbliver ***betydelige*** (nr. 3). Baggrunden for denne sandsynlighedsvurdering er, at denne efter Digitaliseringsstyrelsens opfattelse alene kan nedsættes til usandsynlig, såfremt afsenderne følger Digitaliseringsstyrelsens anbefaling. Den samlede vurdering af residualrisikoen er på den baggrund ***lav-medium***.

4.2.3 Risiko nr. 3: Uvedkommendes adgang til virksomheders digitale postkasser

Vurdering af risikoen

Digitaliseringsstyrelsen vil som databehandler opbevare meddelelser på vegne af private juridiske enheder, jf. § 2 a, stk. 4 i lov om Digital Post. Disse meddelelser kan eksempelvis indeholde oplysninger om medarbejdere, kunder o.lign. Disse meddelelser kan endvidere både indeholde følsomme og fortrolige personoplysninger.

Sandsynligheden for, at uvedkommende skaffer sig adgang til en virksomheds postkasse, vurderes som ***mindre sandsynligt*** (nr. 2). Dette skyldes på den ene side, at Digital Post i sin opbygning er indrettet således, at det ved "brute force" er særdeles vanskeligt uberettiget at skaffe sig adgang til hele postkasser, og på den anden side at menneskelige fejl, såsom fejl i bruger- og rettighedsstyring og vedligeholdelse af adgang og rettigheder, erfaringsmæssigt kan indebære, at uvedkommende der ikke har fået tilladelse til adgang, får adgang til digitale postkasser.

Det er videre Digitaliseringsstyrelsens vurdering, at konsekvenserne forbundet med, at uvedkommende får adgang til en virksomheds digitale postkasse, for de registreredes rettigheder og frihedsrettigheder vil være ***kritiske*** (nr. 4), idet der kan være tale om visse typer af følsomme personoplysninger, såsom helbredsoplysninger, ligesom uvedkommendes adgang til visse almindelige oplysninger

kan have betydelige konsekvenser, f.eks. hvis der er tale om en registreret persons beskyttede adresse eller telefonnummer. Dertil kommer, at disse typer af konsekvenser kan være vanskelige for den registrerede selv at overvinde, såfremt den uvedkommende misbruger oplysninger, som denne har skaffet sig adgang til.

På baggrund af vurderingen af sandsynligheden og konsekvensen er den samlede vurdering af risikoen ***høj***.

Foranstaltninger til at håndtere risikoen
Digital Post-løsningen er opbygget efter principperne om databeskyttelse gennem design og databeskyttelse gennem standardindstillinger.

Det indebærer, at der i Digital Post-løsningen er indbygget en række tekniske foranstaltninger til at imødegå udefrakommendes angreb imod Digital Post-løsningen, ligesom der er udført en penetrationstest, og efter idriftsættelse årligt udføres en penetrationstest samt foretages opfølgning på risikovurderinger og revision af databehandlere.

Samlet set har Digitaliseringsstyrelsen implementeret følgende tekniske og organisatoriske tiltag i Digital Post-løsningen til at imødegå risikoen:

- Detaljeret brugerstyring, således at der sikres least-privilege adgang
- Anvendelse af personlige brugere på alle niveauer
- Stærk kryptering omkring alle komponenter
- Løbende gennemgang af rettigheder
- Politikker for håndtering og kopiering af data i Digital Post-løsningen
- Logning af dataanvendelse med henblik på sikring af detaljeret revisionsspor til at klarlægge al anvendelse af data i Digital Post-løsningen
- Antivirus- og anti-malware på alle servere
- Anti-virus og anti-malware på computere
- Anti-phishing filtre ved modtagelse af mails samt ved håndtering af alle links i mails
- Jump-servere til at tilgå alle miljøer i Digital Post-løsningen
- Løbende gennemgang af sårbarheder af den centrale sikkerhedsansvarlige og den Digital Post-specifikke sikkerhedsansvarlige
- Løbende patching i henhold til patch management-politikken
- Baselining for sikring af komponenter
- Høj netværkssikkerhed i driftsmiljøer, hvor den samlede løsning er isoleret i eget netværk
- Adgang til API'er begrænses via API-whitelisting
- Overvågning af netværk og sikkerhedslogs
- Retningslinjer hos de dataansvarlig for tildeling og tilbagekaldelse af adgange

Derudover anbefaler Digitaliseringsstyrelsen, at de dataansvarlige virksomheder gennem interne procedurer, retningslinjer el.lign. klæder medarbejdere på til at sikre imod, at uvedkommende pga. menneskelige fejl får adgang til virksomhedernes digitale postkasser.

På baggrund af de beskrevne foranstaltninger vurderes det, at sandsynligheden for, at der vil ske et fortrolighedstab i Digital Post-løsningen, nedjusteres til ***usandsynligt*** (nr. 1), forudsat at de dataansvarlige virksomheder implementerer ovennævnte anbefaling. Såfremt anbefalingen ikke følges, kan

sandsynligheden alene nedjusteres til ***mindre sandsynligt*** (nr. 2). Konsekvenserne forbliver den samme ***kritisk*** (nr. 4). Det betyder, at den samlede vurdering af residualrisikoen er ***medium-høj***.

4.2.4 Risiko nr. 4: Høj organisatorisk, teknisk og juridisk kompleksitet

Vurdering af risikoen

Digital Post-løsningen består af et centralt it-system, som er integreret med en lang række andre private og offentlige it-systemer. Tilsvarende er organiseringen omkring Digital Post-løsningen præget af en række forskellige dataansvarlige, heriblandt Digitaliseringsstyrelsen og de offentlige afsendere, private juridiske enheder samt offentlige og kommercielle visningsklienter, herunder borger.dk, Virk, mit.dk og e-Boks, samt flere databehandlere og underdatabehandlere, f.eks. Netcompany. Der består således en betydelig kompleksitet omkring den tekniske og organisatoriske håndtering af Digital Post. Som konsekvens heraf indebærer behandlingen tillige en væsentlig juridisk kompleksitet vedrørende rollefordelingen og hver aktørs forpligtelser ift. de registrerede.

Samlet set kan den høje organisatoriske, tekniske og juridiske kompleksitet betyde, at behandlingen af personoplysninger i og omkring Digital Post-løsningen kan være vanskelig for de registrerede at få indsigt i og forholde sig til. Dette må antages især at komme til at gøre sig gældende i forholdet mellem Digitaliseringsstyrelsen, de offentlige afsendere og de private juridiske enheder samt i forholdet mellem visningsklienterne, såvel de offentlige som de kommercielle visningsklienter.

Den høje organisatoriske, tekniske og juridiske kompleksitet kan for de registrerede (og andre udefrakommende) være kompliceret at overskue og forholde sig til. Dette gælder især rollefordelingen imellem aktørerne, som f.eks. har betydning for de registrerede, når disse vil gøre brug af deres rettigheder efter databeskyttelsesforordningen. Derudover kan kompleksitetsniveauet være en udfordring i forbindelse med fastlæggelsen af, hvilke aktører der har ansvaret for f.eks. sikkerhedstiltag o.lign. i og omkring Digital Post-løsningen.

Sandsynligheden for det høje kompleksitetsniveau fører til, at de registrerede ikke kan overskue behandlingen af deres personoplysninger, eller at de involverede aktører grundet misforståelser om rolle- og opgavefordeling ikke får iværksat nødvendige databeskyttelsesretlige tiltag, vurderes til at være ***moderat sandsynligt*** (nr. 3). Dette skyldes dels, at det tekniske og organisatoriske setup omkring Digital Post-løsningen er særdeles kompliceret, dels at der er tale om et kompliceret juridisk, herunder databeskyttelsesretligt, setup, som er vanskeligt at formidle og forklare på en letforståelig måde.

Det er Digitaliseringsstyrelsens vurdering, at konsekvenserne forbundet med det høje kompleksitetsniveau vil være ***betydelige*** (nr. 3). I det omfang det høje kompleksitetsniveau har konsekvenser for de registrerede, vil disse kunne overvindes med en vis indsats fra de registrerede, enten ved at kontakte Digitaliseringsstyrelsen, den offentlige afsender eller en af visningsklientudbyderne, f.eks. borger.dk. Tilsvarende vil være tilfældet internt i forholdet mellem aktørerne.

På baggrund af vurderingen af sandsynligheden og konsekvenserne er den samlede vurdering af risikoen derfor ***høj***.

Foranstaltninger til at håndtere risikoen

Digitaliseringsstyrelsen har for at imødegå den høje organisatoriske, tekniske og juridiske kompleksitet omkring Digital Post-løsningen iværksat kommunikation rettet mod de registrerede, således at disse i videst muligt omfang klædes på til at bruge den nye Digital Post-løsning samt får mest mulig

indsigt i de forskellige myndigheders og virksomheders roller ved brug af Digital Post-løsningen. Disse informationer vedrører især selve Digital Post-løsningen og Digitaliseringsstyrelsens rolle heri.

Derudover kan de registrerede finde den relevante information på Digitaliseringsstyrelsens hjemmeside, på borger.dk, på Virk og hos Det Samlede Supporttilbud, hvis de registrerede personer oplever problemer ved brug af Digital Post-løsningen. I forbindelse med introduktion af nye funktionaliteter i Digital Post-løsningen, vil Digitaliseringsstyrelsen altid sikre at beskrive behandlingen herunder dataansvarskonstruktionen for at sikre, at brugerne har indsigt i konstruktionen.

Digitaliseringsstyrelsen anbefaler i forlængelse heraf, at de dataansvarlige i hvert fald i det omfang disse foretager behandling af personoplysninger i Digital Post, som væsentligt adskiller sig fra almindelig fremsendelse af "dagligdags post", tillige iværksætter tiltag til i fornødent omfang at informere de registrerede herom, f.eks. hvis meddelelser opbevares i Digital Post eller i forbindelse med domstolenes forkyndelser. Der kan eksempelvis være tale om, at de dataansvarlige på egen hånd informerer de registrerede om behandlingen af personoplysninger i Digital Post, herunder om både den dataansvarliges og andre aktørers rolle i den forbindelse. Dette kan eventuelt indarbejdes i de dataansvarliges almindelige underretninger til de registrerede efter databeskyttelsesforordningens artikel 13 og 14.

På baggrund af de beskrevne foranstaltninger er det Digitaliseringsstyrelsens vurdering, at sandsynligheden for, at de registrerede ikke vil kunne overskue kompleksiteten omkring Digital Post-løsningen, kan nedjusteres til ***mindre sandsynligt*** (nr. 2), mens konsekvenserne kan nedjusteres til ***begrænsede*** (nr. 2), idet eventuelle udfordringer kan løses ved kontakt til Det Samlede Supporttilbud eller Digitaliseringsstyrelsen. Dette indebærer sammenfattende, at den samlede vurdering af residualrisikoen er ***medium***.

4.2.5 Risiko nr. 5: Fejl i modtagersystemet hos offentlige afsendere

Vurdering af risikoen

Når en borger, myndighed eller virksomhed sender en meddelelse via Digital Post-løsningen, kan der opstå en situation, hvor myndigheden, der skal modtage meddelelsen, har et modtagesystem, der fejler. Digital Post-løsningen vil flere gange forsøge at genfremsende meddelelsen. Såfremt myndighedens system fortsat fejler, vil meddelelsen efter 7 dage blive gjort tilgængelig på virk.dk, hvor den offentlige afsender kan læse den pågældende meddelelse. Dette gøres for at sikre, at meddelelsen kan tilgås af myndigheden, selv hvis myndighedens system er fejlbehæftet efter længere tid.

Sandsynligheden for ovenstående risiko, og at meddelelsen dermed ikke leveres (rettidigt), vurderes at være ***forventet*** (nr. 4). Dette er baseret på, at det er konstateret, at hændelsen forekommer og er forekommet.

Det vurderes, at konsekvenserne forbundet med fejl i modtagesystemet hos den offentlige afsender, vurderes at være ***betydelige*** (nr. 3). Som en konsekvens heraf kan den offentlige modtager overse meddelelser fra den registrerende, hvilket kan indebære en risiko for et (rets)tab hos den registrerede, f.eks. som følge af at en frist overskrides.

På baggrund af vurderingen af sandsynligheden og konsekvensen er den samlede vurdering af risikoen ***høj***.

Foranstaltninger til at håndtere risikoen

Det primære formål med Digital Post-løsningen er at sikre, at posten sikkert bliver leveret til rette modtager. For at imødegå risiko for fejl i modtagesystemerne hos de offentlige afsendere, vil meddelelserne blive sendt til den såkaldte Virk-postkasse i Digital Post-løsningen.

For at sikre at meddelelserne bliver leveret og dermed imødegå den beskrevne risiko, er der udviklet et såkaldt gensendelsesflow, der skal sikre, at modtagere med modtagesystemer får deres meddelelser.

Gensendelsesflowet består i, at et modtagesystem vil blive deaktiveret, hvis der i en periode på 7 dage ikke modtages en positiv forretningskvittering fra modtagesystemet efter gensendelsesforsøg, der foretages fra Digital Post-løsningen til modtagesystemet. På dag 7 vil en meddelelse blive fremsendt til primærmodtagesystemet, hvis en meddelelse fortsat ikke kan gensendes til modtagesystemet. Såfremt primærmodtagesystemet også fejler, vil de berørte meddelelser blive sendt til Virk-postkassen. Hvis en meddelelse fejler, vil kontaktpersonen for det fejlet modtagesystem blive kontaktet, inden meddelelsen bliver fremsendt til primærmodtagesystemet eller til Virk-postkassen. Modtagesystemet vil først blive deaktiveret, når alle forsøg på fremsendelse fejler.

Returnerer modtagesystemet en negativ forretningskvittering, der angiver, at meddelelsen indeholder virus, deaktiveres modtagesystemet ikke, men Digital Post-løsningen stopper gensendelsesflowet. Fejl i modtagesystemet vil altid afhjælpes af gensendelsesflowet, da meddelelserne ikke låses i systemerne, men de bliver gjort tilgængelige i Virk-postkassen. Der er derfor implementeret effektive foranstaltninger med henblik på at imødegå fejl i modtagesystemerne.

En meddelelse anses for at være kommet frem, når denne er tilgængelig for adressaten i Digital Post-løsningen, samt være afsendt af den afgivne afsender, jf. § 10 i lov om Digital Post. Borgeren er ikke ansvarlig for eventuelle tekniske eller praktiske problemer el.lign. hos den offentlige afsender.

På baggrund af de beskrevne foranstaltninger er det Digitaliseringsstyrelsens vurdering, at sandsynligheden kan nedjusteres til ***mindre sandsynligt*** (nr. 2), mens konsekvenserne kan nedjusteret til ***begrænsede konsekvenser*** (nr. 2). Det skyldes at man i hændelsesloggen altid vil kunne spore, hvornår en meddelelse er blevet sendt. Det vil sige at selvom en offentlig myndighed har overset en meddelelse, fordi den pga. en fejl kun ligger på virk.dk, vil borgeren eller virksomheden, som har afsendt meddelelsen altid kunne påvise, at meddelelsen er sendt herunder hvornår den er afsendt. Når en borger har trykket send på en meddelelse, vil meddelelsen være modtaget i myndighedens system uanset hvor den ligger. Fejl i modtagesystemet vil derfor ikke have nogen konsekvens for den borger, der f.eks. forsøger at overholde en frist i en sag. Dette indebærer sammenfattende, at den samlede vurdering af residualrisikoen er ***medium***.

4.2.6 Risiko nr. 6: Dataansvarskonstruktionen ved fejl i levering af meddelelser

Vurdering af risikoen

Det følger af § 2 a i lov om Digital Post fra offentlige afsendere, at offentlige afsendere er dataansvarlige for indholdet af de meddelelser, som de sender via Digital Post, mens Digitaliseringsstyrelsen er databehandler for offentlige afsenderes *forsendelse* af meddelelser. I forhold til de juridiske enheder vil Digitaliseringsstyrelsen være databehandler for virksomheders *forsendelse og opbevaring* af meddelelser i postløsningen. Dette er afspejlet i § 2 a, stk. 4 i lov om Digital Post.

Offentlige afsendere er pålagt et modtagesystem, hvilket indebærer, at *opbevaringen* af meddelelser sker hos de offentlige afsendere eller modtagere af digital post og ikke i selve Digital Post-løsningen[3]. Digitaliseringsstyrelsen er derfor ikke databehandler for opbevaringen. Digitaliseringsstyrelsen kan ikke inden for rammerne af lov om Digital Post opbevare posten for de offentlige afsendere.

Når der sker fejl i modtagesystemer hos offentlige afsendere, således at meddelelser ikke kan leveres, vil meddelelsen blive liggende i selve Digital Post-løsningen, som Digitaliseringsstyrelsen er dataansvarlig for. I denne situation kan der således opstå tvivl om de offentlige afsenderes/modtageres dataansvar og dermed Digitaliseringsstyrelsens databeskyttelsesretlige rolle og dermed, hvem der varetager forpligtelserne efter databeskyttelsesforordningen og databeskyttelsesloven.

Sandsynligheden for, at der sker fejl i modtagesystemer, og at dette fører til, at involverede aktører grundet misforståelse om rolle- og opgavefordeling ikke får iværksat nødvendige databeskyttelsesretlige tiltag, vurderes til at være ***forventet*** (nr. 4). Dette er baseret på, at Digitaliseringsstyrelsen, i lov og bekendtgørelserne om Digital Post, ikke er angivet som databehandler for opbevaringen af offentlige myndigheders meddelelser, når der sker fejl i modtagesystemer. Der har erfaringsmæssigt tidligere været fejl i modtagesystemer, hvorfor denne manglende præcisering i reglerne vil resultere i misforståelser om rolle- og opgavefordelingen.

Det er Digitaliseringsstyrelsens vurdering, at konsekvenserne forbundet med fejl i modtagesystemer vil være ***betydelige*** (nr. 3). Risikoen er ikke inddraget i vurderingen af dataansvarskonstruktionen i Digital Post, hvorfor dette kan resultere i konsekvenser for de registrerede ved udøvelse af deres rettigheder, håndtering af sikkerhedsbrud mv., da de involverede aktører grundet misforståelse om dataansvarskonstruktionen ikke får iværksat nødvendige databeskyttelsesretlige tiltag.

På baggrund af vurderingen af sandsynligheden og konsekvenserne er den samlede vurdering af risikoen derfor ***høj***.

Foranstaltninger til at håndtere risikoen
Det vurderes, at Digitaliseringsstyrelsen i situationer, hvor der sker fejl i modtagesystemer, vil være databehandler for opbevaring offentlige afsenderes post, da posten bliver opbevaret i løsningen, indtil der sker fremsendelse til modtagesystemet eller Virk-postkassen.

Digitaliseringsstyrelsen er ved at kontakte offentlige afsendere, som ikke har etableret indført et modtagesystem. De pågældende myndigheder vil få mulighed for at etablere et modtagesystem inde for nærmere angiven frist. Ønsker en eller flere af de pågældende myndigheder ikke at indføre et modtagesystem, vil de pågældende blive ændret til at være juridisk enhed og dermed udelukket fra et være offentlig afsender.

Dette er ikke taget i betragtning i lov om Digital Post eller Digital Post-bekendtgørelsen[4], og der foreligger derfor ikke en fyldestgørende beskrivelse af dataansvarskonstruktionen. Forholdet bør beskrives i regelsættet, således at Digitaliseringsstyrelsen i tilfælde, hvor der sker fejl i modtagesystemet,

[3] Lovforslag som fremsat nr. 47 den 8. oktober 2020 om ændring af lov om Digital Post fra offentlige afsendere, afsnit 3.1
[4] Bekendtgørelse nr. 2019 af 29. oktober 2021 om ansvar, opgaver og tilsyn i forbindelse med behandlingen af personoplysninger i forbindelse med forsendelse af digital post fra offentlige afsendere

fungerer som databehandler i forhold til opbevaringen af posten. Præciseringen af rolle- og ansvarsfordelingen i loven og bekendtgørelsen vil forhindre risiko for misforståelse mellem de forskellige aktører.

På baggrund af de beskrevne foranstaltninger er det Digitaliseringsstyrelsens vurdering, at sandsynligheden kan nedjusteres til ***mindre sandsynligt*** (nr. 2). Digitaliseringsstyrelsen er i forvejen databehandler for juridiske enheder for så vidt angår opbevaring af meddelelser, jf. § 2 a, stk. 4 i lov om Digital Post. Digitaliseringsstyrelsen er derfor vant til håndteringen af meddelelser som databehandler. Indtil problematikken er løst og samtlige offentlige myndigheder enten har indført et modtagesystem eller er ophørt med at være offentlig afsender, vil Digitaliseringsstyrelsen manuelt håndtere alle henvendelser fra registrerede og/eller i samarbejde med den pågældende myndighed med henblik på at sikre, at den registrerede i overgangsperioden også er sikret under databeskyttelsesretsreglerne i overgangsperioden. Konsekvenserne kan derfor nedjusteres til ***begrænsede*** (nr. 2), idet eventuelle udfordringer, der alligevel kan opstå for den registrerede, kan løses ved kontakt til Det Samlede Supporttilbud eller Digitaliseringsstyrelsen. Dette indebærer sammenfattende, at den samlede vurdering af residualrisikoen er ***medium***.

4.2.7 Risiko nr. 7: Læse- og skriveadgang

Vurdering af risiko

Digital Post-løsningen indeholder en funktionalitet kaldet "læse- og skriveadgang". Læse- og skriveadgangen indebærer, at en borger (postkasseejeren) kan tildele en anden fysisk eller juridisk person adgang (adgangshaver) til bl.a. at læse, skrive, besvare og videresende post til offentlige myndigheder på vegne af postkasseejeren. Funktionaliteten kan ses som en udvidelse af læseadgang, der bl.a. gør det muligt skrive på vegne af postkasseejer. Når en adgangshaver anvender læse- og skriveadgang til f.eks. at sende en besked til en myndighed på vegne af en borger, vil postkasseejeren stå som afsender af beskeden, men det vil fremgå af beskeden, at beskeden er skrevet af en adgangshaver og ikke borgeren selv.

Til disse meddelelser, der er skrevet på vegne af borgeren, er der tilknyttet oplysninger om adgangshaver, således at den offentlige myndighed som modtager kan se, at meddelelsen er sendt af en anden end postkasseejeren. Når adgangshaver er en fysisk person, vil den offentlige afsender kunne tilgå navn og personnummer på ejeren af postkassen såvel som adgangshaveren af metadata. Navn og de første seks cifre i adgangshaverens personnummer (fødselsdato) vil fremgå af de tilknyttede oplysninger til meddelelsen (MeMo metadata), som adgangshaver teknisk kan fremsøge, hvorimod der i selve meddelelsen udelukkende fremgår navn på adgangshaver. Når adgangshaveren er en juridisk person, vil navnet på virksomheden og CVR-nummer fremgå. De offentlige myndigheders systemer er dermed i stand til at identificere adgangshaver.

Løsningen indebærer, at meddelelser sendt af adgangshaver gemmes i borgerens "Sendt post"-mappe og vil indeholde navn på adgangshaver, der har sendt meddelelserne. Hvis der er flere adgangshavere tilknyttet en borgers postkasse, er der derfor en risiko for, at andre end postkasseejeren og adgangshaveren selv, altså andre adgangshavere, får adgang til adgangshaveres oplysninger. Der kan kun opnås adgang til en adgangshavers navn såfremt adgangshaveren har fremsendt en meddelelse på vegne af postkasseejeren.

Sandsynligheden for, at andre adgangshavere, får adgang til en adgangshavers navn og fødselsdato, vurderes som ***moderat sandsynligt*** (nr. 3).

Det er Digitaliseringsstyrelsens vurdering, at konsekvenserne forbundet med, at andre adgangshavere får adgang til adgangshaveres navn og fødselsdato, vil være ***ubetydelige konsekvenser*** (nr. 1), da der er tale om personer, der har en relation eller på anden måde har en funktion som en betroet rolle til postkasseejeren. Der lægges i den forbindelse vægt på, at der vil være tale om tab af fortrolighed på en begrænset mængde almindelige, ikke-følsomme personoplysninger i form af navn. Fødselsdato kan endvidere alene teknisk fremsøges. Dertil kommer, at det er afgrænset, hvilke personer der kan få adgang (kun nye adgangshavere til postkassen).

På baggrund af vurderingen af sandsynligheden og konsekvensen er den samlede vurdering af risikoen ***lav***.

Foranstaltninger til håndtering af risiko
Alle handlinger der foretages i en postkasse, registreres i en log. I loggen er det muligt at se, hvem der har foretaget handlinger på vegne af en postkasseejer. Dette sikrer en gennemsigtighed i de handlinger, som en adgangshaver foretager i postkassen, i forhold til andre mulige adgangshavere.

Det vil være muligt for de adgangshavere, der har adgang til samme postkasse, at se andre adgangshaveres navn i "Sendt-post"-mappe, hvilket begrænser eksponeringen til få parter. Offentlige afsendere vil kunne se det fulde personnummer og navn på adgangshaveren.

Det er således alene offentlige myndigheder, der vil få adgang til adgangshaverens fulde personnummer. Offentlige myndigheder har hjemmel til at behandle oplysninger om personnummer med henblik på entydig identifikation efter databeskyttelseslovens § 11, stk. 2, hvilket er nødvendigt for at kunne regulere funktionaliteten, læse- og skriveadgang.
Digitaliseringsstyrelsen oplyser adgangshaveren ved oprettelsen af læse- og skriveadgangen, at det er muligt at tilgå navn på de andre adgangshavere, hvis der er flere adgangshavere tilknyttet en postkasse.

På baggrund af de beskrevne foranstaltninger er det Digitaliseringsstyrelsens vurdering, at sandsynligheden kan nedjusteres til ***usandsynligt*** (nr. 1), mens konsekvenserne også kan bevares til det ***ubetydelige*** (nr. 1), da der ikke gives adgang til oplysninger om det fulde personnummer til andre end offentlige modtagere af meddelelser. Dette indebærer sammenfattende, at den samlede vurdering af residualrisikoen er ***lav***.

4.2.8 Risiko nr. 8: Dataophobning for ophørte virksomheder

Vurdering af risikoen
For så vidt angår virksomheder fremgår det af § 12, stk. 2 i ansvarsbekendtgørelsen vedrørende juridiske enheder[5], at virksomhederne har råde- og ejendomsret over modtagne digitale meddelelser, hvilket medfører at Digitaliseringsstyrelsen ikke har mulighed for eller kompetence til at slette meddelelserne. Personoplysningerne der indgår i selve meddelelserne opbevares i kontaktregistret og opbevaringskomponenten i en periode på 10 år efter ophør af virksomhed.

[5] Bekendtgørelse nr. 2020 af 29. oktober 2021 om ansvar, opgaver og tilsyn i forbindelse med behandlingen af personoplysninger indeholdt i meddelelser og opbevaring heraf i juridiske enheders digitale postkasse

Når den dataansvarlige virksomhed ophører, vil den ophørte virksomhed som udgangspunkt ikke kunne varetage de registreredes rettigheder. Der vil potentielt ske dataophobning af personoplysninger i Digital Post-løsningen, hvor alle kategorier af personoplysninger kan indgå. Dernæst opstår en risiko i forhold til råde- og ejendomsretten over modtagne digitale meddelelser, da den dataansvarliges rolles kan fremstå uklar.

Ophør af virksomheder vil grundlæggende enten ske ved konkurs/tvangsauktion, salg eller lukning. Ved afsigelse af konkursdekretet, indtræder kurator i skyldnerens (hidtidige ledelses) sted. Kurator skal ved udførelsen af sit hverv bl.a. varetage boets interesser, herunder sikre boets aktiver og foretage de fornødne skridt til værn mod uberettigede dispositioner over aktiverne samt repræsentere boet i enhver henseende, jf. § 110, stk. 1 i konkurslovens. Ved sikring af boets aktiver forstås både fysiske og digitale aktiver, som kan indeholde data, herunder personoplysninger, af relevans for konkursboet. Kurator bliver ved overtagelse af konkursboet dataansvarlig, jf. artikel 4, nr. 7 i databeskyttelsesforordningen, for behandling af personoplysninger i konkursboet, idet kurator bestemmer formål og afgør med hvilke hjælpemidler, der må foretages behandling af personoplysninger i forbindelse med bobehandlingen. Ved virksomhedens ophør som følge af konkurs vil rådigheds- og ejendomsretten over de modtagne digitale meddelelser overgå til kurator.

Ved salg af en virksomhed antages det, at råde- og ejendomsret over modtagne digitale meddelelser vil overgå til køber af virksomheden. Som udgangspunkt vil køber træde i sælgers sted, hvorfor køberen ved overtagelse af virksomheden bliver dataansvarlig, jf. artikel 4, nr. 7 i databeskyttelsesforordningen, for behandling af personoplysninger i virksomheden.

Ved lukning af en virksomhed skal den senest fungerende ledelse sikre, at regnskabsmateriale fortsat opbevares i overensstemmelse med bogføringslovens regler, jf. § 14 i bogføringsloven. Virksomheden skal i forbindelse med lukningen også fortsat overholde databeskyttelsesreglerne, herunder tage stilling til princippet om opbevaringsbegrænsning i henhold til § 5, stk. 1, litra e i databeskyttelsesforordningen, for at vurdere, om der stadig er et sagligt formål med opbevaring af oplysninger efter virksomhedens ophør. Det er endvidere præciseret i artikel 28, stk. 3, litra g i databeskyttelsesforordningen, at databehandleren enten skal slette eller alternativt tilbagelevere alle personoplysninger til den dataansvarlige, efter at behandlingen er ophørt. Endvidere skal der foreligge en instruks til at slette eksisterende kopier, medmindre EU-retten eller medlemsstaternes nationale ret foreskriver opbevaring af personoplysninger. Af denne grund er det ligeledes af væsentlig betydning at præcisere instruksen for sletning i regelsættet, herunder i relation til virksomheders ophør og den deraf følgende ophør af behandlingsaktiviteter. Som beskrevet ovenfor kan der være flere lovgivningsmæssige forpligtelser, som virksomheden skal overholde i forbindelse med lukningen. Virksomhedens ophør vil som udgangspunkt kræve en underretning af de registrerede (f.eks. eventuelle kunder og samarbejdspartnere), hvorefter de registrerede får mulighed for at varetage deres interesser.

Der foreligger en risiko for, at virksomhederne i forbindelse med ophør, ikke henter deres post ned og foretager sletning i postkasserne. Det bemærkes i forlængelse heraf, at virksomheder i forbindelse med ophør vil blive gjort opmærksomme på, at de forud for ophøret af virksomheden bør slette eller hente post i deres digitale postkasser. Digitaliseringsstyrelsen må kun slette, såfremt der foreligger en instruks fra de dataansvarlige virksomheder, da Digitaliseringsstyrelsen som databehandler alene må handle efter dokumenteret instruks fra den dataansvarlige, jf. artikel 28, stk. 3, litra a i databeskyttelsesforordningen. Instruksen til sletning er ikke indskrevet i bekendtgørelsen. Digitaliseringsstyrelsens manglende hjemmel til at slette meddelelserne i inaktive virksomheders postkasser udgør derfor en risiko for de registrerede i form af dataophobning som beskrevet ovenfor. Formålet med Digital Post er overordnet at stille en digital postkasse til rådighed, hvor bl.a. virksomheder kan opbevare meddelelser, som er modtaget fra eller sendt til offentlige myndigheder. Virksomhedernes forpligtelser til at opbevare selskabsdokumenter, der vedrører selskabet ender ikke i forbindelse med, at

en virksomhed lukker. I henhold til § 17 i selskabsloven[6] og § 15 c i erhvervsvirksomhedslovens[7] er virksomhedens ledelse forpligtet til at opbevare selskabsdokumenter på betryggende vis i 5 år. Herudover fremgår det af § 34 a, stk. 4 i skatteforvaltningsloven[8] at skattekrav (herunder dækningsafgift) under visse omstændigheder først forældes efter 10 år. Virksomhederne kan derfor lide et potentielt økonomisk eller retligt tab, hvis Digitaliseringsstyrelsen sletter dokumenter i Digital Post, som virksomheden ellers havde forventet at kunne finde i den digitale postkasse og derfor ikke har opbevaret andre steder. Når en virksomhed lukker, vil ejerne af virksomheden kunne få adgang til virksomhedens postkasse ved at fremlægge en attest fra SKAT (*et ophørsbevis*), som dokumenterer ejerforholdet til virksomheden.

Sandsynligheden for, at der vil ske dataophobning af personoplysninger grundet uklarhed om dataansvarskonstruktionen mellem Digitaliseringsstyrelsen og virksomheder og den manglende instruks til Digitaliseringsstyrelse omkring sletning, er vurderet til ***forventet*** (nr. 4). Baggrunden for vurderingen skyldes, at virksomheden ikke er opmærksomme på, at de er dataansvarlige og Digitaliseringsstyrelsen alene er databehandler efter virksomheden er lukket.

Konsekvenserne forbundet med dataophobning er for de registreredes rettigheder og frihedsrettigheder vurderet til at være ***kritiske*** (nr. 4). Vurderingen er begrundet i, at de registrerede vil blive påvirket af, at der behandles personoplysninger om dem i længere tid end nødvendigt af hensyn til formålet med behandlingen af personoplysningerne. Det er i den forbindelse væsentligt, at Digitaliseringsstyrelsen ikke er dataansvarlig for personoplysninger indeholdt i meddelelserne, hverken under forsendelse eller efter disse er kommet frem. Der er endvidere lagt vægt på, at de konsekvenser, som de registrerede kan opleve, vil være særdeles vanskelige for de registrerede at overskue.
På baggrund af vurderingen af sandsynligheden og konsekvensen er den samlede vurdering af risikoen ***høj***.

Foranstaltninger til at håndtere risikoen
Digitaliseringsstyrelsen har igangsat et projekt for at få indskrevet sletning ind i regelsættet i 2025, således at der foreligger en instruks til at slette i overensstemmelse med databeskyttelsesforordningens artikel 28, stk. 3.

Det er vurderingen, at lukkede virksomheder har et behov for at have adgang til selskabsdokumenter i den digitale postkasse i op til 10 år efter virksomheden er lukket ned. I henhold til artikel 4, nr. 7 i databeskyttelsesforordningen medfører det, at den tidligere ledelse bliver dataansvarlig for den selskabsdokumentation til brug for dette formål. Det er også alene den tidligere ledelse, der kan få udstedt en ophørsattest, som giver den pågældende ret til adgang til den digitale postkasse. Såfremt en lukket virksomhed ikke ønsker, at opbevaringen skal ske i Digital Post, skal den pågældende virksomhed instruere Digitaliseringsstyrelsen i at slette oplysningerne, jf. artikel 28, stk. 3 i databeskyttelsesforordning. Den digitale postkasse vil dog blive slettet 10 år efter virksomheden er lukket, da forældelsesfristen på de krav, som lukkede virksomheder kan blive mødt med, ikke længere eksisterer. Det er fastlagt i lovgivningen, at virksomhederne har rådigheds- og ejendomsret over modtagne digitale meddelelser, hvorfor Digitaliseringsstyrelsen ikke kan tillægges et afledt ansvar i tilfælde af virksomhedens ophør. De inaktive virksomheder, herunder eventuel kurator, vil være forpligtet til at iagttage de registreredes rettigheder i forbindelse med virksomhedens ophør.

[6] Lovbekendtgørelse nr. 1168 af 9. januar 2023 om aktie- og anpartsselskaber (herefter selskabsloven)
[7] Lovbekendtgørelse nr. 249 af 2. januar 2021 om visse erhvervsdrivende virksomheder (herefter erhvervsvirksomhedsloven)
[8] Lovbekendtgørelse nr. 1053 af 20. september 2024 Skatteforvaltningsloven

På baggrund af de beskrevne foranstaltninger vurderes det, at sandsynligheden for dataophobning af personoplysninger grundet uklarhed om dataansvarskonstruktionen mellem virksomheden og Digitaliseringsstyrelsen, og den manglende instruks om sletning til Digitaliseringsstyrelsen, ikke kan nedjusteres, og derfor fortsat er ***forventet*** (nr. 4). Det må dog forventes, at såfremt en registreret ønsker at gøre brug af sine rettigheder, vil vedkommende henvende sig til virksomheden og ikke Digitaliseringsstyrelsen. Skulle Digitaliseringsstyrelsen modtage en henvendelse fra den registrerede, vil Digitaliseringsstyrelsen henvise til den tidligere virksomhed, som i kraft af råde- og ejendomsretten, som de eneste vil have mulighed for at varetage de registreredes rettigheder. Behandlingen af de pågældende oplysninger er i øvrigt begrænset til opbevaring, som sker i en meget sikker løsning, hvortil uvedkommende ikke har adgang. Konsekvensen kan derfor nedjusteres til ***begrænsede*** (nr. 2), hvilket betyder, at den samlede vurdering af residualrisikoen er ***medium.***

4.3 Evaluering af risikoscoring

Digitaliseringsstyrelsen har herefter evalueret de ovennævnte risici hver især i forhold til deres konsekvenser for de registrerede og sandsynligheden for, at følgerne af risiciene indtræffer. Dette er sket ved brug af evalueringskriterierne nævnt i tabel 2 ovenfor. Resultatet af denne vurdering fremgår af risikokortet i figur 2 nedenfor:

Figur 2. Risikokort over risici før mitigerende foranstaltninger

4.3.1 Overblik over evaluering og håndtering af risici

De ovennævnte risici i risikokortet kan evalueres og håndteres som følger:

Risikoen	Samlet risikovurdering	Digitaliseringsstyrelsens foranstaltninger til håndtering af risiko	Forslag til evt. yderligere foranstaltninger hos de dataansvarlige	Effekt på risiko	Restrisiko	Implementeringsstatus for Digitaliseringsstyrelsen
Nr. 1: **En digital meddelelse sendes til en forkert modtager**	**Sandsynlighed:** Moderat **Konsekvens:** Kritisk **Risiko:** Høj	- Digital Post-løsningen er netop opbygget med henblik på at sikre, at meddelelser sendes til den korrekte modtager. Komponenterne i løsningen er derfor designet til at understøtte dette. - Bistand fra Digitaliseringsstyrelsen til registrerede med at overvinde konsekvenser. - Information til offentlige afsendere om, at de skal være opmærksomme på korrekt angivelse af, hvem der skal modtage en meddelelse.	Digitaliseringsstyrelsen anbefaler, at afsenderne implementerer funktionalitet til validering af indtastede modtagere i afsendersystemer samt angivelse af valørdato med henblik på at nedbringe sandsynligheden for den identificerede risiko.	Reduceret	**Sandsynlighed:** Mindre **Konsekvens:** Betydelig **Risiko:** Medium	Implementeret

Risikoen	Samlet risikovurdering	Digitaliseringsstyrelsens foranstaltninger til håndtering af risiko	Forslag til evt. yderligere foranstaltninger hos de dataansvarlige	Effekt på risiko	Restrisiko	Implementeringsstatus for Digitaliseringsstyrelsen
Nr. 2: **En masseforsendelse sendes til forkerte modtagere**	**Sandsynlighed**: Moderat **Konsekvens**: Betydelige **Risiko**: Høj	- Digitaliseringsstyrelsen informerer generelt de dataansvarlige om, at de skal være opmærksomme på korrekt angivelse af, hvem der skal modtage en meddelelse, idet Digital Post-løsningen automatisk afleverer meddelelsen til den angivne modtager. - Der sker i Digital Post-løsningen en validering af meddelelsen med henblik på kontrol af, om disse stemmer overens med de indtastede personnumre eller CVR-numre er oprettet som modtagere i Digital Post. Der tjekkes også her for fritagelsesstatus, herunder om der skal ske fremsendelse af meddelelsen via fysisk post.	Digitaliseringsstyrelsen anbefaler, at afsenderne implementerer funktionalitet til validering af indtastede modtagere i afsendersystemer samt gør angivelse af valørdato med henblik på at nedbringe sandsynligheden for den identificerede risiko.	Reduceret	**Sandsynlighed:** Usandsynligt eller mindre **Konsekvens:** Betydelige **Risiko**: Lav-medium	Implementeret

Nr. 3: Uvedkommendes adgang til virksomheders digitale postkasser	**Sandsynlighed**: Mindre **Konsekvens**: Kritisk **Risiko**: Høj	- Detaljeret brugerstyring, således at der sikres least-privilege adgang - Løbende gennemgang af rettigheder - Politikker for håndtering og kopiering af data i Digital Post-løsningen - Anvendelse af personlige brugere på alle niveauer - Logning af dataanvendelse med henblik på sikring af detaljeret revisionsspor til at klarlægge al anvendelse af data i løsningen - Anti-virus- og anti-malware på alle servere - Anti-virus og anti-malware på computere - Anti-phishing filtre ved modtagelse af mails samt ved håndtering af alle links i mails	Digitaliseringsstyrelsen anbefaler, at de dataansvarlige virksomheder gennem interne procedurer, retningslinjer el.lign. klæder medarbejdere på til at sikre imod, at uvedkommende pga. menneskelige fejl får adgang til virksomhedernes digitale postkasser.	Bevares/reduceret	**Sandsynlighed**: Usandsynligt eller minde **Konsekvens**: Kritisk **Risiko**: Medium-høj	Implementeret

Risikoen	Samlet risikovurdering	Digitaliseringsstyrelsens foranstaltninger til håndtering af risiko	Forslag til evt. yderligere foranstaltninger hos de dataansvarlige	Effekt på risiko	Restrisiko	Implementeringsstatus for Digitaliseringsstyrelsen
		- Jump-servere til at tilgå alle miljøer i Digital Post-løsningen - Løbende gennemgang af sårbarheder af den centrale sikkerhedsansvarlige og den Digital Post-specifikke sikkerhedsansvarlige - Løbende patching i henhold til patch management-politikken - Baselining for sikring af komponenter - Høj netværkssikkerhed i driftsmiljøer, hvor den samlede løsning er isoleret i eget netværk - Adgang til API'er begrænses via API-whitelisting - Overvågning af netværk og sikkerhedslogs				

Risikoen	Samlet risikovurdering	Digitaliseringsstyrelsens foranstaltninger til håndtering af risiko	Forslag til evt. yderligere foranstaltninger hos de dataansvarlige	Effekt på risiko	Restrisiko	Implementeringsstatus for Digitaliseringsstyrelsen
Nr. 4: **Høj organisatorisk, teknisk og juridisk kompleksitet**	**Sandsynlighed**: Moderat **Konsekvens**: Betydelige **Risiko**: Høj	- Information rettet mod registrerede, - Information i orienteringsskrivelser fra dataansvarlige - Support hos Det Samlede Supporttilbud	Digitaliseringsstyrelsen anbefaler, at de dataansvarlige i det omfang disse foretager behandling af personoplysninger i Digital Post, som væsentligt adskiller sig fra almindelig fremsendelse af "dagligdags post", tillige iværksætter tiltag til at informere de registrerede herom.	Reduceret	**Sandsynlighed**: Mindre **Konsekvens**: Begrænsede **Risiko**: Medium	Implementeret.
Nr. 5: **Fejl i modtagersystemet hos offentlige afsendere**	**Sandsynlighed**: Forventet **Konsekvens**: Betydelige **Risiko**: Høj	- Gensendelsesflow, der skal sikre, at modtagere med modtagersystemer får deres post.		Reduceret	**Sandsynlighed**: Mindre **Konsekvens**: Begrænsede **Risiko**: Medium	Implementeret.

Nr. 6: Dataansvarskonstruktionen ved fejl i levering af meddelelser	**Sandsynlighed**: Forventet **Konsekvens**: Betydelige **Risiko**: Høj	- Digitaliseringsstyrelsen er databehandler for opbevaringen i Digital Post-løsningen, når der sker fejl i modtagesystemer. - Dataansvarskonstruktionen beskrives i lovgivningen. - Digitaliseringsstyrelsen er ved at kontakte offentlige afsendere, som ikke har indført et modtagesystem. De pågældende offentlige myndigheder vil få mulighed for at indføre et modtagesystem inden for nærmere angiven frist. Ønsker en eller flere af de pågældende offentlige afsendere ikke at indføre et modtagesystem, vil de pågældende umiddelbart blive udelukket for at kunne anvende Digital Post, medmindre der kan findes en anden løsning.		Reduceret	**Sandsynlighed**: Mindre **Konsekvens**: Begrænsede **Risiko**: Medium	Delvis implementeres.

Risikoen	Samlet risikovurdering	Digitaliseringsstyrelsens foranstaltninger til håndtering af risiko	Forslag til evt. yderligere foranstaltninger hos de dataansvarlige	Effekt på risiko	Restrisiko	Implementeringsstatus for Digitaliseringsstyrelsen
Nr. 7: Læse- og skriveadgang	**Sandsynlighed**: Moderat **Konsekvens**: Ubetydelige **Risiko**: Lav	- Alene offentlige afsendere har adgang til en adgangshavers fulde CPR-nummer. - Tredjeparter med adgang til postkasse, kan alene få adgang til fulde navn og fødselsdato på adgangshaver. - Alle handlinger, der foretages af en tredjepart i en postkasse, registreres i en log for at sikre gennemsigtighed, samt i forbindelse med oprettelse af læse- og skriveadgangen.		Bevares	**Sandsynlighed**: Usandsynligt **Konsekvens**: Ubetydelige **Risiko**: Lav	Implementeret.

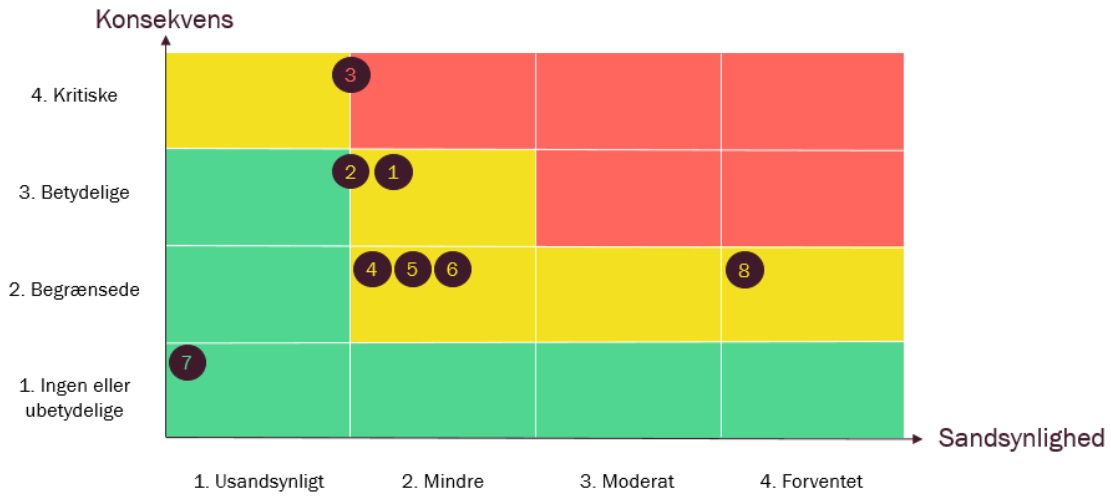
Risiko 8: Dataophobning for ophørte virksomheder	**Sandsynlighed:** Forventet **Konsekvens:** Kritiske **Risiko:** Høj	- Digitaliseringsstyrelsen har igangsat et projekt for at få indskrevet sletning ind i regelsættet i 2025, således at der foreligger en instruks til at slette i overensstemmelse med databeskyttelsesretlige regler.	Såfremt en lukket virksomhed ikke ønsker, at opbevaringen skal ske i Digital Post, skal den pågældende virksomhed instruere Digitaliseringsstyrelsen i at slette oplysningerne, jf. artikel 28, stk. 3 i databeskyttelsesforordning. Den digitale postkasse vil dog blive slettet 10 år efter virksomheden er lukket, da forældelsesfristen på de krav, som lukkede virksomheder kan blive mødt med, ikke længere eksisterer. Det er fastlagt i lovgivningen, at virksomhederne har rådigheds- og ejendomsret over modtagne digitale meddelelser, hvorfor Digitaliseringsstyrelsen ikke kan tillægges et afledt ansvar i tilfælde af virksomhedens ophør. De inaktive virksomheder, herunder eventuel kurator, vil være forpligtet til at iagttage de registreredes rettigheder i forbindelse med virksomhedens ophør.	Reduceret	**Sandsynlighed:** Forventet **Konsekvens:** Begrænsede **Risiko:** Medium	Igangsat

Tabel 3. Overblik over evaluering af risici samt residualrisiko efter implementering af mitigerende foranstaltninger

4.3.2 Samlet residualrisiko

Digitaliseringsstyrelsen har herefter genevalueret de ovennævnte risici hver især i forhold til effekten af de mitigerende foranstaltninger på de identificerede konsekvenser. Sammenfattende er risikoen for 1 af de identificerede risici nedbragt til lav, og 5 risici er nedbragt til medium. Fsva. risiko nr. 2 og 3 er det Digitaliseringsstyrelsens vurdering, at denne risiko alene nedsættes, såfremt afsenderne følger Digitaliseringsstyrelsens anbefalinger, hvorfor restrisikoen for risiko 2 er angivet som lav-medium og for risiko 3 medium-høj.

Resultatet af denne vurdering fremgår af risikokortet i figur 3 nedenfor:



Figur 3. Risikokort med overblik over risici efter implementering af mitigerende foranstaltninger pr. den 21. november 2024

Digitaliserings-
styrelsen