Bilag C - Risici ved Digitaliseringsstyrelsens behandling af personoplysninger som databehandler

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. INDLEDNING OG SAMMENFATNING

Digitaliseringsstyrelsen har i løbet af 2. og 3. kvartal 2021 i samarbejde med Kammeradvokaten udarbejdet en Konsekvensanalyse vedrørende databeskyttelse angående behandling af personoplysninger i Næste generation Digital Post (herefter "Konsekvensanalysen"). Konsekvensanalysen vedrører alene behandling af personoplysninger, som Digitaliseringsstyrelsen foretager i sin rolle som dataansvarlig.

I forbindelse med analysen har styrelsen dog 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. Digital Post-lovens § 2 a, stk. 3 og 4. Idet Digitaliseringsstyrelsen ifølge § 10, stk. 3, i 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 ("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.

Udover de nedenfor beskrevne risici har Digitaliseringsstyrelsen som led i gennemførelse af Konsekvensanalysen identificeret en række risici, som tillige kan være relevante for de dataansvarlige, dvs. offentlige afsendere og juridiske enheder. Der er tale om følgende risici: risiko nr. 2: Tilsidesættelse af princippet om dataminimering, risiko nr. 3: Tilsidesættelse af princippet om rigtighed, risiko nr. 4: Tilsidesættelse af princippet om opbevaringsbegrænsning, risiko nr. 5: Manglende eller langvarig behandling af rettighedsanmodninger fra de registrerede, risiko nr. 9: Insiderangreb, risiko nr. 10: DDoS-angreb mod Digital Post-løsningen, risiko nr. 11: Ransomware-angreb mod Digital Post-løsningen, risiko nr. 12: Nedbrud af Digital Post-løsningen, risiko nr. 13: Leverandørsvigt (udvikling og drift), risiko nr. 16: Integrationsfejl i Digital Post-løsningens komponenter, risiko nr. 20: Utilstrækkelig kvalitet af Digital Post-løsningen, herunder integrationer samt risiko nr. 22: Andre fejl i forbindelse med betjening 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. Digital Post-lovens § 2 a, stk. 3 og 4.

Digitaliseringsstyrelsen har identificeret følgende 4 risici forbundet med denne behandling:

1. En digital postmeddelelse 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

1.1.1 Hvor høje risici behandlingen indebærer

Digitaliseringsstyrelsen vurderer, at konsekvenserne for de registrerede, hvis risiciene indtræffer uden fastlæggelse og implementering af de mitigerende foranstaltninger, fsva. risici nr. 1 og 3 er kritiske, for risiko nr. 4 betydelige og for risiko nr. 2 begrænsede. 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.

Sammenfattende er risikoen for de 4 identificerede risici nedbragt til lav eller medium. Fsva. risiko nr. 1 og 3 er det Digitaliseringsstyrelsens vurdering, at denne risiko alene kan nedsættes, såfremt hhv. afsenderne og virksomhederne følger Digitaliseringsstyrelsens anbefalinger, hvorfor restrisikoen for denne risiko er angivet som høj-medium.

2. BAGGRUND OG FAKTUELLE FORHOLD

Digitaliseringsstyrelsen gennemførte i løbet af 2017 et EU-udbud om levering af en ny Digital Post-løsning som erstatning for den daværende Digital Post-løsning, der blev driftet af e-Boks. Udbuddet blev vundet af Netcompany A/S, som Digitaliseringsstyrelsen derfor i efteråret 2019 indgik en kontrakt med om levering af den nye Digital Post.

Folketinget har i forbindelse med overgangen til den nye Digital Post-løsning vedtaget ændringer af lov om Digital Post fra offentlige afsendere[1], hvorefter Digitaliseringsstyrelsen ifølge den nyaffattede § 2, stk. 2, udpeges til at sikre udvikling, drift, vedligeholdelse og forvaltning af postløsningen. Digitaliseringsstyrelsen er dataansvarlig for Digital Post-løsningen efter § 2 a, stk. 1, jf. § 2.

Digital Post-løsningen består først og fremmest af borgere 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 som både dataansvarlig og databehandler i forbindelse med driften af Digital Post behandle almindelige personoplysninger, herunder personnumre, cvr-numre, e-mail og telefonnumre o.lign. om størstedelen af den danske befolkning, aktuelt estimeret til 5 mio. borgere og 700.000 virksomheder. Skriftlig kommunikation mellem offentlige afsendere på den ene side og borgere eller virksomheder på den anden side vil efter idriftsættelsen som altovervejende hovedregel ske gennem Digital Post. Denne kommunikation – digitale postmeddelelser – 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 efter idriftsættelsen 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 postmeddelelser, men tillige til opbevaring af indkomne postmeddelelser. Idet brugen af Digital Post-løsningen derudover er forbundet med

[1] Lov nr. 1941 af 15. december 2020 om ændring af lov om Digital Post fra offentlige afsendere.

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 Digital Post-loven

I forbindelse med overgangen til den nye Digital Post-løsning har Folketinget vedtaget ændringer af Digital Post-loven, således at den persondataretlige rollefordeling nu fremgår direkte af Digital Post-loven.

Det følger således 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.

Om rollefordelingen fremgår følgende 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. Modtageløsningen 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 opbevaringen.*
>
> *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 postmeddelelser 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]:

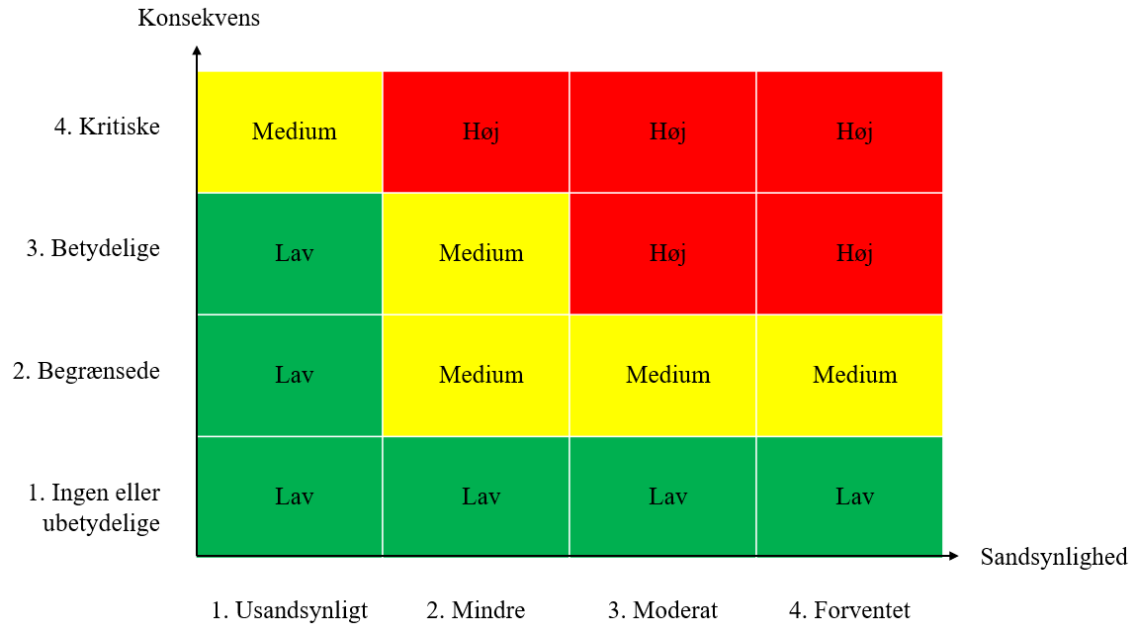
4	**Kritiske konsekvenser**: De registrerede kan opleve kritiske konsekvenser, som de ikke nødvendigvis kan overvinde, f.eks. økonomisk nød som betydelig gæld eller manglende evne til at arbejde, langsigtede psykiske eller fysiske lidelser, død m.v.
3	**Betydelige konsekvenser**: De registrerede oplever betydelige konsekvenser, som de kan overvinde, om end med alvorlige vanskeligheder, f.eks.

[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.

	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

4.2 Identifikation, evaluering og håndtering af risici

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

Vurdering af risikoen

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

Fremsendelse af en digital postmeddelelse til en forkert modtager kan ske på forskellige måder. Det kan således først og fremmest ske ved, at en offentlig afsender sender en postmeddelelse 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. Digital Post-lovens § 2 a, stk. 3. Tilsvarende hvis en virksomhed sender en postmeddelelse til en forkert modtager. Derudover kan en digital postmeddelelse sendes til en forkert modtager pga. systemfejl, f.eks. hvis der sker kodefejl i forbindelse med ændringer i Digital Post-løsningen.

Sandsynligheden for, at en postmeddelelse i den beskrevne situation sendes til en forkert modtager vurderes som ***moderat sandsynlig*** (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 postmeddelelse 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 postmeddelelse 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 postmeddelelse 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 postmeddelelser 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.

Digitaliseringsstyrelsen tilstræber generelt at informere de offentlige afsendere om, at de skal være opmærksomme på korrekt angivelse af, hvem der skal modtage en postmeddelelse. 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 postmeddelelsen, eksempelvis det korrekte personnummer. Digitaliseringsstyrelsen anbefaler derfor klart, 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.

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 postmeddelelser. Disse vil således i et vist omfang med relativt få vanskeligheder kunne overvindes af den registrerede.

På baggrund af de identificerede foranstaltninger, vurderes det, at sandsynligheden for, at de registrerede enten modtager en forkert digital postmeddelelse eller får at vide, at den registreredes egen digitale postmeddelelse er sendt til en forkert modtager, nedjusteres til ***usandsynligt*** (nr. 1) eller ***mindre sandsynligt*** (nr. 2), mens konsekvenserne forbliver ***kritiske*** (nr. 4). Baggrunden for denne sandsynlighedsvurdering er, at denne efter Digitaliseringsstyrelsens opfattelse alene kan nedsættes til usandsynlig, såfremt afsenderne følger Digitaliseringsstyrelsens anbefalinger. Såfremt afsenderne vælger alene implementere den ene af de beskrevne foranstaltninger, 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-høj***.

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 postmeddelelse 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 postmeddelelser 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 postmeddelelser 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 postmeddelelser 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 postmeddelelsen.

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

Foranstaltninger til at håndtere risikoen
Det bemærkes indledningsvis, at Digitaliseringsstyrelsen i forbindelse med masseforsendelser alene handler som databehandler for de offentlige afsendere eller virksomhederne.

Digitaliseringsstyrelsen informerer generelt de dataansvarlige om, at de skal være opmærksomme på korrekt angivelse af, hvem der skal modtage en postmeddelelse. 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 postmeddelelser. 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 postmeddelelser 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 postmeddelelsen via fysisk post.

Når alle kontroller er sket, vil postmeddelelsen blive sendt til modtagers digitale postkasse.

På baggrund af de beskrevne foranstaltninger vurderes det, at sandsynligheden for, at en masseforsendelse af digitale postmeddelelser 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 postmeddelelser på vegne af private juridiske enheder, jf. Digital Post-lovens § 2 a, stk. 4. 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 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 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.

Dette kan især udgøre en udfordring 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 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.

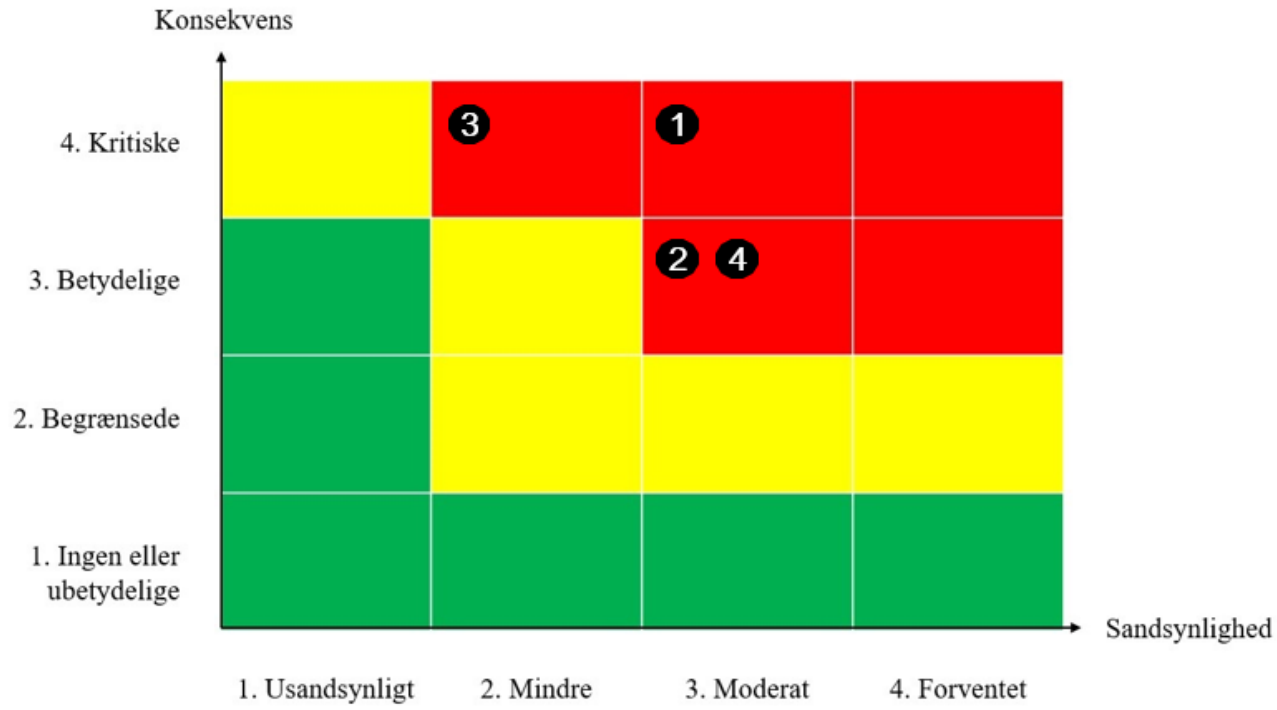
Digitaliseringsstyrelsen vil derudover sørge for, at de registrerede kan finde den relevante information på Digitaliseringsstyrelsens hjemmeside, på borger.dk, på Virk og hos Det Samlede Supporttilbud, hvis de registrerede personer oplever problemer ved brug af Digital Post-løsningen. Derudover vil Digitaliseringsstyrelsen i fornødent omfang vejlede visningsklienterne med henblik på at sikre, at visningsklienterne er eller bliver i stand til at vejlede de registrerede om behandlingen af personoplysninger i Digital Post-løsningen. Digitaliseringsstyrelsen har derudover sendt et velkomstbrev i forbindelse med idriftsættelsen af den nye Digital Post.

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 postmeddelelser 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***.

4.3 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 og 3 ovenfor. Resultatet af denne vurdering fremgår af risikokortet i figur 2 straks 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	Restrisiko	Implementeringsstatus for Digitaliseringsstyrelsen
Nr. 1: En digital postmeddelelse sendes til en	Sandsynlighed: Moderat	- Digital Post-løsningen er netop opbygget med henblik på at sikre, at postmeddelelser sendes til den korrekte modtager. Komponenterne i løsningen er derfor de-	Digitaliseringsstyrelsen anbefaler, at afsenderne implementerer funktionalitet til validering af indtastede modta-	Sandsynlighed: Usandsynligt eller mindre sandsynligt Konsekvens: Kritisk	Implementeret

forkert modtager	Konsekvens: Kritisk Risiko: Høj	signet 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 postmeddelelse.	gere i afsendersystemer samt angivelse af valørdato med henblik på at nedbringe sandsynligheden for den identificerede risiko.	Risiko: Medium-høj	
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 postmeddelelse, 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	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.	Sandsynlighed: Usandsynligt eller mindre sandsynligt Konsekvens: Betydelige Risiko: Lav-medium	Implementeret

		om der skal ske fremsendelse af postmeddelelsen via fysisk post.			
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 - Jump-servere til at tilgå alle miljøer i Digital Post-løsningen	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.	Sandsynlighed: Usandsynligt eller mindre sandsynligt Konsekvens: Kritisk Risiko: Medium-høj	Implementeret

		- 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			
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 til-	Sandsynlighed: Mindre Konsekvens: Begrænsede Risiko: Medium	I gang.

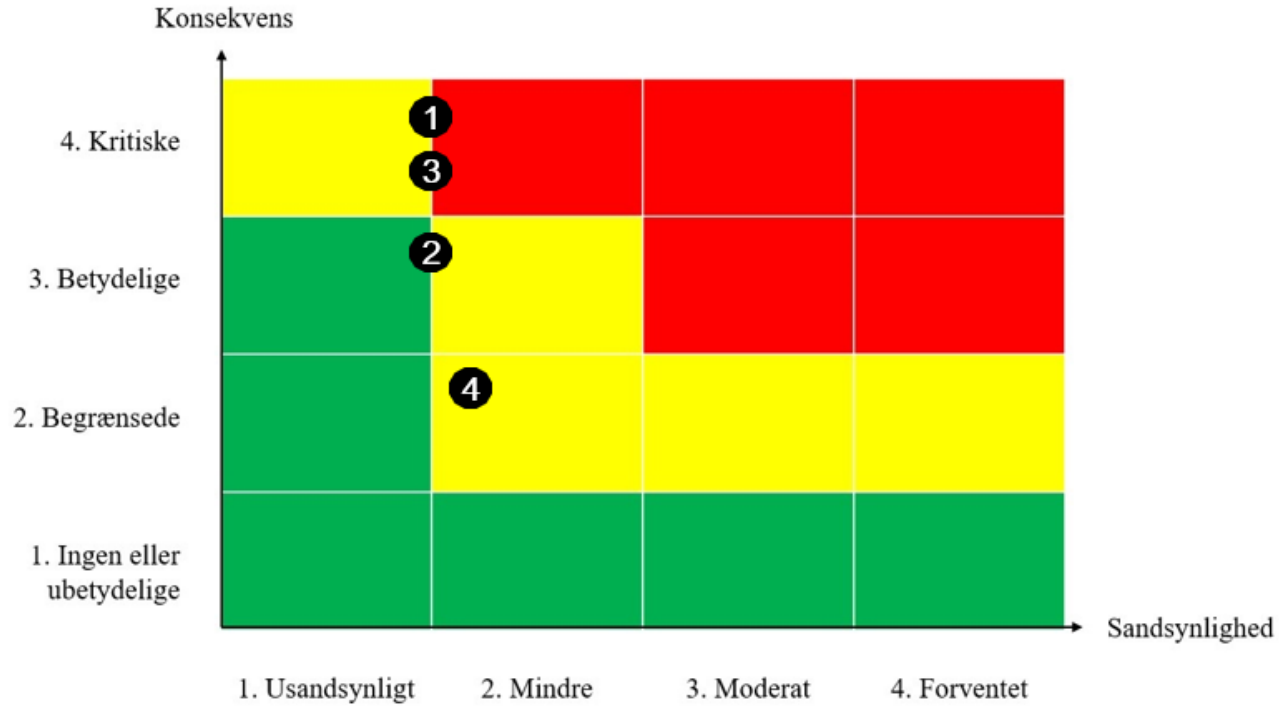
			tag til at informere de registrerede herom.		

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

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



Figur 3. Risikokort med overblik over risici efter implementering af mitigerende foranstaltninger pr. den 28. november 2022