Konsekvensanalyse vedrørende data-beskyttelse

Anvendelse af udvalgte applikationer og Cloudtjenester i Microsoft 365 samt supportydelser i forbindelse hermed

Dataansvarlig	Statens It
Ansvarlige for udarbejdelse af konsekvensanalysen	Statens It
Ansvarlige kontaktpersoner hos Statens It	Helle Uldbæk Sørensen
Databeskyttelsesrådgiver (DPO) - dataansvarlige	Laurits Ketscher

Indhold

1. SAMMENFATNING

Denne konsekvensanalyse er udarbejdet af Statens It i samarbejde med Økonomistyrelsen.

Formålet med analysen er at give de dataansvarlige offentlige myndigheder ("De Dataansvarlige") et grundlag for at:

- Vurdere lovligheden af behandlingen af personoplysninger
- Vurdere de risici, som behandlingen kan medføre for de registreredes rettigheder og frihedsrettigheder.

Analysen er udarbejdet i henhold til artikel 35 i databeskyttelsesforordningen, og den tager udgangspunkt i brugen af Microsoft 365 (M365) og de tilhørende supportydelser.

Det konkluderes i konsekvensanalysen, at der er en række risici, der kan mitigeres med effektive foranstaltninger, så den samlede risiko vurderes til at være lav-mellem for de registrerede, hvilket anses for tilfredsstillende.
I konsekvensanalysen konkluderes det overordnet, at De Dataansvarlige offentlige myndigheders behandling ved brug af M365 kan ske inden for rammerne af databeskyttelsesforordningens regler. Dette gælder også i forhold til behandling af personoplysninger ved eventuelle overførsler til tredjelande samt ved udleveringsanmodninger, som er vurderet i det vedlagte Bilag F - Transfer Impact Assessment (TIA).
I konsekvensanalysen er der identificeret og vurderet følgende risici for de registreredes rettigheder og frihedsrettigheder:

1. Manglende gennemsigtighed i behandling af systemgenererede personoplysninger om systembrugere og håndtering af de registreredes rettigheder.
2. Manglende iagttagelse af princippet om formålsbegrænsning.
3. Microsoft indsamler og genererer for mange personoplysninger om de registrerede i forbindelse med systemlogfiler og diagnostiske data.
4. Anonymisering af personoplysninger til forretningsaktiviteter er ikke tilstrækkelig effektiv.

Der er desuden i TIA'en identificeret og vurderet en række risici i forbindelse med opbevaring af personoplysninger i EU i forhold til udleveringsanmodninger fra tredjelande samt ved overførsler af personoplysninger til usikre tredjelande. Her konkluderes det, at den samlede risiko for de registreredes rettigheder og frihedsrettigheder efter implementering af mitigerende foranstaltninger vurderes at være lav-mellem.
På denne baggrund konkluderes det i konsekvensanalysen, at der ikke vil være pligt til at høre Datatilsynet om behandlingen af personoplysninger ved brug af M365 efter databeskyttelsesforordningens artikel 36.

Denne konsekvensanalyse opdateres løbende, når det skønnes nødvendigt. Supplerende til konsekvensanalysen vil der blive gennemført løbende audits af Microsofts processer.

Det skal bemærkes, at da der er tale om en "paraply-konsekvensanalyse", skal analysen også suppleres af De Dataansvarlige hver især i lyset af deres individuelle, varierende behandlinger af personoplysninger ved brug af M365, som beskrevet i afgrænsningerne i afsnit 2.4 og 2.5.

Staten overvejer i overvejende grad at flytte til M365, hvor der på nuværende tidspunkt anvendes en on-premise løsning. M365 kan hostes i lokale datacentre, men under visse begrænsninger, hvilket medfører, at det fulde potentiale af cloudløsningen ikke kan realiseres.

2. BAGGRUND, FORMÅL OG AFGRÆNSNING

2.1. Baggrund

M365 er en clouddrevet produktivitetsplatform, der indeholder tre typer af services: software, online tjenester og professionelle services. Staten afsøger mulighederne for, at staten i overvejende grad flytter til M365, hvor der på nuværende tidspunkt anvendes en on-premise løsning. M365 kan hostes i lokale datacentre, men under visse begrænsninger, hvilket betyder, at det fulde potentiale af cloudløsningen ikke kan realiseres. Ved at flytte til cloudløsningen kan den fulde version af M365 anvendes med undtagelse af få funktioner, jf. afsnit 2.4.

M365-licenser indkøbes igennem statens licenspartner Atea A/S, der sørger for levering af bl.a. M365-produkter til De Dataansvarlige i henhold til aftale indgået med Økonomistyrelsen. Dette er reguleret af Kontrakt Deaftale 1 og Delaftale 2 mellem Økonomistyrelsen og Atea A/S, som Økonomistyrelsen udover at være part i samtidig har indgået på vegne af De Dataansvarlige.
Da Atea A/S er licenspartner, betyder det, at fakturering sker gennem Atea A/S. Microsoft sender fakturaer til Atea A/S om statens forbrug, hvorefter Atea A/S videresender fakturaerne til staten. Atea A/S' behandling af oplysninger vedrører aggregerede data[1], som Microsoft har redegjort for, er aggregeret til et niveau, hvor oplysningerne ikke er personhenførbare (anonyme data).

I Delaftale 1, punkt 10, og Delaftale 2, punkt 9, henvises der til, at kundens brugsrettigheder til softwareprodukterne er reguleret af Microsofts standardlicensvilkår med de modifikationer, som fremgår af bl.a. Bilag 2 (Kravspecifikation) og Bilag 6 (Standardvilkår). Bilag 6 henviser til en række underbilag, herunder standardvilkår fra Microsoft Ireland, såsom Master Business Service Agreement (MBSA) og ændringer til standardvilkårene (amendments).

1 Microsoft data protection and security terms for products and services: Business operations

Disse tillæg med ændringer er indgået direkte mellem Microsoft Ireland og Økonomistyrelsen på egne vegne og på vegne af de kunder, der er omfattet af aftalen med Atea A/S.
Når De Dataansvarlige anvender M365, behandler Microsoft Ireland som databehandler personoplysninger på vegne af De Dataansvarlige. Økonomistyrelsen indgår ikke databehandleraftale med Microsoft Ireland på vegne af de dataansvarlige. Databehandleraftalen med Microsoft Ireland indgås af Statens It, mens Statens It og de dataansvarlige indgår en særskilt databehandleraftale vedrørende de Microsoft-onlinetjenester, som de dataansvarlige benytter.
Parterne vil indgå Microsoft Irelands standarddatabehandleraftale Microsoft Products and Services Data Protection Addendum, hvor den seneste version er fra den 1. september 2025 (Bilag C).
Atea A/S vil ikke indgå i denne konsekvensanalyse grundet sin rolle i aftalekonstruktionen, og da Atea A/S' behandling af oplysninger alene vedrører aggregerede data[2].
Microsoft Ireland, som har lokation i Irland, har et moderselskab, Microsoft Corporation, med lokation i USA. Staten er opmærksom på muligheden for eventuelle tredjelandsoverførsler af data, herunder personoplysninger om borgere og ansatte.

2.1.1. Statens It

Statens It tilbyder sine tilsluttede statslige ministerier, styrelser og selvejende uddannelsesinstitutioner brug af M365. Statens It leverer it-drift og services til cirka 40.000 brugere fordelt på 21 ministerområder[3].
Ansvaret for driften af statslige myndigheders basale it-systemer er ressortoverdraget fra de respektive ressortministre til finansministeren ved kongelige resolutioner[4]. Dette indebærer ligeledes en overdragelse af ansvaret for kontrakter og informationssikkerhed.
Økonomistyrelsen har ansvaret for Statens Indkøbsprogram og udbyder i den sammenhæng bl.a. en rammeaftale om standardsoftware, hvor staten kan indkøbe standardsoftware fra Microsoft, aktuelt gennem forhandleren Atea A/S.
De Dataansvarlige beslutter selv, hvilke af de tilbudte produkter og services fra M365 der ønskes anvendt. De har desuden ansvaret for behandling af personoplysninger i forbindelse med brug af M365, hvilket betyder, at De Dataansvarlige hver især er dataansvarlige efter databeskyttelsesforordningens regler.

2 Microsoft data protection and security terms for products and services: Business operations,

3 For en uddybning af hvem der specifikt er omfattet, henvises til oplistningen heraf på Statens It's hjemmeside: https://statens-it.dk/om-os/hvem-leverer-vi-til/ (senest tilgået den 20. maj 2024).

4 For et eksempel på en kongelig resolution kan der henvises til bekendtgørelse nr. 110 af 4. februar 2020

Statens It er forvalter af den fælles M365-tenant, der oprettes for samtlige kunder. Statens It opretter brugerne og sørger for, at disse får adgang til tenanten. Statens It er således databehandler for De Dataansvarlige, og der er indgået en databehandleraftale mellem Statens It og De Dataansvarlige, som enten også vil gælde eller blive opdateret i forbindelse med, at M365 tages i brug.

2.2. Pligten til at udarbejde en konsekvensanalyse vedrørende databeskyttelse

Udarbejdelse af en konsekvensanalyse vedrørende databeskyttelse er efter databeskyttelsesforordningens artikel 35, stk. 1, kun obligatorisk, hvis behandlingen sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder.
Databeskyttelsesforordningens artikel 35, stk. 3, opregner en række tilfælde, hvor det navnlig er påkrævet at udarbejde en konsekvensanalyse. Artikel 29-Gruppen (nu Det Europæiske Databeskyttelsesråd – EDPB) har i deres retningslinjer fastsat kriterier, der kan hjælpe til at identificere de behandlinger, der kræver en konsekvensanalyse.
Retningslinjerne fastslår, at en dataansvarlig i de fleste tilfælde skal overveje at udføre en konsekvensanalyse, når to af de pågældende kriterier er opfyldt, men at dette også kan være tilfældet for behandlinger, der alene opfylder ét af kriterierne.
Da behandlingen af personoplysninger ved brug af M365 vil ske som led i varetagelse af lovbestemte opgaver, herunder afgørelsesvirksomhed, faktisk forvaltningsvirksomhed og personaleadministration samt visse administrative formål (herefter samlet benævnt sagsbehandling og personaleadministration), vil behandlingen hos De Dataansvarlige være kontinuerlig og regelmæssig.

Behandlingen vil desuden:

- Vedrøre et omfattende antal registrerede.
- Omfatte en stor mængde personoplysninger, afhængigt af De Dataansvarliges specifikke behandlinger.
- Potentielt indebærer overførsel af personoplysninger til tredjelande, herunder USA, da nogle af de underdatabehandlere, som Microsoft Ireland anvender, er lokaliseret udenfor EU/EØS.
- Omfatte følsomme personoplysninger, jf. databeskyttelsesforordningens artikel 9.
- Omfatte sårbare personer.

På baggrund af ovenstående vurderes behandlingen at være omfattende i henhold til EDPB's retningslinjer for udarbejdelse af konsekvensanalyser vedrørende databeskyttelse.

Derved er mindst tre ud af ni kriterier opfyldt i henhold til EDPB's retningslinjer[5]:

- Kriterium 4: Behandling af følsomme oplysninger eller oplysninger af meget personlig karakter.
- Kriterium 5: Omfattende behandling.
- Kriterium 7: Behandling af oplysninger om sårbare registrerede.

Ifølge EDPB medfører opfyldelsen af disse kriterier, at der skal udarbejdes en konsekvensanalyse vedrørende databeskyttelse.
På den baggrund har Statens It og Økonomistyrelsen besluttet at udarbejde en konsekvensanalyse for behandlingen af personoplysninger ved brug af M365, inklusive supportydelser i forbindelse hermed.

2.3. Formålet med konsekvensanalysen

Formålet med denne konsekvensanalyse vedrørende databeskyttelse er at beskrive den behandling af personoplysninger, som De Dataansvarlige vil foretage i forbindelse med en eventuel anvendelse af M365, såfremt denne løsning tages i brug.

Konsekvensanalysen indeholder også en vurdering af behandlingens lovlighed, dvs. om behandlingen overholder reglerne i databeskyttelsesforordningen[6] og databeskyttelsesloven[7].
Formålet er endvidere at afdække risici for fysiske personers rettigheder og frihedsrettigheder, som kan opstå ved De Dataansvarliges behandling af personoplysninger i forbindelse med brug af M365, samt at bidrage til at håndtere disse risici. Dette sker ved at:

- Vurdere de identificerede risici.
- Fastlægge passende og effektive foranstaltninger til at afhjælpe risiciene.

Hvis konsekvensanalysen viser, at behandlingen af personoplysninger ved brug af M365 vil føre til en høj risiko for de registrerede, og hvis De Dataansvarlige ikke kan reducere risikoen til et acceptabelt niveau (residualrisiko), skal Datatilsynet høres om behandlingen, inden denne påbegyndes, jf. databeskyttelsesforordningens artikel 36, stk. 1.
Konsekvensanalysen er også en forudsætning for at overholde databeskyttelsesforordningens grundlæggende princip om ansvarlighed (dokumentation for overholdelse af forordningens regler), jf. artikel 5, stk. 2, og artikel 24.

5 Artikel 29-Gruppen, nu EDPB, Retningslinjer for konsekvensanalyse vedrørende databeskyttelse (DPIA) og bestemmelse af, om behandlingen "sandsynligvis indebærer en høj risiko" i henhold til forordning (EU) 2016/679, WP 248, rev. 01, revideret og senest vedtaget den 4. oktober 2017, s. 12.

6 Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse).

7 Bekendtgørelse nr. 289 af 8. marts 2024 af lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesloven).

Derudover har konsekvensanalysen en naturlig sammenhæng med reglerne om databeskyttelse gennem design og standardindstillinger. Dette kan give værdifuldt input til vurdering af løsningsdesignet, herunder:

- Opsætning og konfiguration af M365.
- Implementering af afhjælpende foranstaltninger for at minimere risici.

2.4. Afgrænsning af konsekvensanalysen

Konsekvensanalysen vedrører den behandling af personoplysninger, som De Dataansvarlige foretager ved brug af M365, som beskrevet i afsnit 2.1.
Konsekvensanalysen omfatter både De Dataansvarliges anvendelse af M365 og den databehandling, som Microsoft Ireland foretager som databehandler for De Dataansvarlige i forbindelse med levering af tjenesten. Desuden omfatter analysen de supportydelser, som leveres af Microsoft Ireland som en del af Microsoft Irelands Professional Services. Konsekvensanalysen inkluderer ved version 2.0 endvidere værktøjer omfattet af E5-licensen, hvis indhold er nærmere angivet i bilag M.

Konsulentydelser er undtaget, da de ikke vil blive anvendt af De Dataansvarlige.

Konsekvensanalysen omfatter også den databehandling, som underdatabehandlere til Microsoft Ireland foretager i forbindelse med levering af ydelserne, herunder eventuelle overførsler til tredjelande.
Endelig omfatter konsekvensanalysen en vurdering af lovligheden af eventuelle videregivelser af personoplysninger fra De Dataansvarlige til Microsoft Ireland til brug for Microsoft Irelands egne formål.

2.4.1. Anvendelse og brugere

Konsekvensanalysen omfatter udelukkende de situationer, hvor brugerne er ansatte hos De Dataansvarlige, f.eks. sagsbehandlere eller andre systembrugere.
Det omfatter behandlingen af personoplysninger i forbindelse med:

- Sagsbehandling
- Personaleadministration

Konsekvensanalysen omfatter ikke situationer, hvor andre persongrupper er brugere, f.eks. elever eller borgere, der anvender M365 som led i faktisk forvaltningsvirksomhed, f.eks. undervisning eller drift af uddannelsesinstitutioner.

2.4.2. Systemer uden for konsekvensanalysen

Den behandling, der sker i andre systemer hos De Dataansvarlige, herunder browser og ESDH-systemer, er ikke omfattet af denne konsekvensanalyse.

Dette skyldes, at anvendelsen af M365 i udgangspunktet sker gennem applikationer og services, og ikke gennem en browser.
Det er hensigten at anvende OneDrive og SharePoint sideløbende med eksisterende ESDH-systemer som F2 eller WorkZone.
Denne konsekvensanalyse omfatter kun behandlingsaktiviteter i M365, der er cloudbaserede. Behandling i ESDH-systemer er således ikke en del af denne analyse.

2.4.3. Undtagelser

Konsekvensanalysen omfatter ikke:

- AI-produkter, herunder Copilot for M365. Der er særskilt for Copilot for M365 udarbejdet en konsekvensanalyse af Økonomistyrelsen og Statens It med bistand fra Kammeradvokaten, "Konsekvensanalyse vedrørende databeskyttelse: Behandling af personoplysninger ved brug af Microsoft Copilot for Microsoft 365". Konsekvensanalysen for Copilot for M365 indgår i den samlede offentliggjorte SIA 365- materialepakke og læses i nær sammenhæng med nærværende konsekvensanalyse.
- Konsulentydelser i form af Microsoft Unified Support, da disse ikke er omfattet af statens aftale.

Hvis behandlingen senere udvides til at omfatte andre dele af M365, såsom Copilot eller Unified Support, vil konsekvensanalysen blive opdateret, så den tillige omfatter disse behandlinger.

2.4.4. Sagstyper og områder uden for konsekvensanalysen

Følgende sagstyper og områder er undtaget fra konsekvensanalysen:

- Sager omfattet af retshåndhævelsesloven[8], herunder straffesager.
- Systematisk behandling af helbredsoplysninger, genetiske data og biometriske data, f.eks. i nationale sundhedsregistre eller databaser, herunder hos Sundhedsdatastyrelsen og Nationalt Genom Center.
- Udlændingesager med høj risiko for de registrerede, f.eks. asylsager under Udlændingeministeriet.
- Sager om væsentlige sociale forhold, misbrug mv., der omfatter sårbare registrerede, f.eks. børnesager eller sager hos Ankestyrelsen.
- Særlige områder inden for Forsvaret, hvor der behandles oplysninger om sikkerhedspersonel eller rigets sikkerhed.

8 Lov nr. 410 af 27. april 2017 om retshåndhævende myndigheders behandling af personoplysninger (med senere ændringer).

Hvis M365 ønskes anvendt til de ovennævnte sagstyper eller områder, skal de pågældende myndigheder udarbejde en supplerende konsekvensanalyse, der vurderer behandlingens lovlighed samt risici forbundet hermed.

2.5. Særligt opmærksomhedspunkt i forhold til konsekvensanalysen

Konsekvensanalysen omfatter hele staten (De Dataansvarlige), som hver især har varierende lovbestemte opgaver. Der er derfor forskel på den behandling af personoplysninger, som de enkelte dataansvarlige foretager – herunder formålet med behandlingen og typen af personoplysninger, der behandles om borgere og ansatte.
Ligeledes kan der være forskelle i konfigurationen hos De Dataansvarlige, og det kan variere, hvilke funktioner der tilvælges eller fravælges. Derudover kan der være forskel på, hvilke tekniske og organisatoriske sikkerhedsforanstaltninger de enkelte dataansvarlige har fastsat.

2.5.1. Supplerende analyser hos De Dataansvarlige

Med andre ord skal konsekvensanalysen suppleres af de enkelte dataansvarlige i lyset af deres individuelle og varierende behandlinger af personoplysninger ved brug af Microsoft 365. Dette omfatter følgende forhold:

- Den nærmere og konkrete behandling af personoplysninger, herunder hvilke oplysninger der behandles af de enkelte dataansvarlige i forbindelse med deres lovbestemte opgaver. Dette inkluderer overholdelse af de grundlæggende principper i databeskyttelsesforordningens artikel 5, f.eks. fastsættelse af slettepolitikker, samt overholdelse af kravet om hjemmel til behandlingen.
- De dataansvarliges håndtering af oplysningspligten og de registreredes rettigheder.
- De dataansvarliges egen analyse af den eller de browsere, de anvender.
- Begrænsninger i konfigurationen samt interne retningslinjer for hver enkelt af de dataansvarlige, der begrænser brugen af applikationer og cloudtjenester. Dette kan eksempelvis være ved brug af Teams, herunder chatfunktion og behandling af personoplysninger under livetransmission. Det afhænger af, hvilke oplysninger der deles under mødet – eksempelvis om der nævnes følsomme personoplysninger, som kan henføres til en bestemt person. Afhængigt af interne retningslinjer hos den enkelte dataansvarlige, kan det også være begrænset, hvis det fremgår, at følsomme oplysninger ikke må deles i Teams, ligesom optagelse af møder og deling af lokationsdata kan være deaktiveret som sikkerhedsforanstaltning.
- Oplysninger om overførsler af personoplysninger til tredjelande i tilfælde, hvor De Dataansvarlige selv tilsigtet overfører oplysninger til en modtager i et tredjeland – eksempelvis ved at sende en e-mail med personoplysninger til en offentlig myndighed eller virksomhed i et tredjeland. De Dataansvarlige skal også selv beskrive eventuelle foranstaltninger, f.eks. interne retningslinjer i den forbindelse.

- Hvordan hver af de dataansvarlige har begrænset adgangen til personoplysninger, så kun relevante personer har adgang.
- Risikovurdering i henhold til databeskyttelsesforordningens artikel 32 samt implementering af passende sikkerhedsforanstaltninger i relation til behandlingen forbundet med brugen af Microsoft 365. Det gælder blandt andet sikker brug af løsningen, styring af roller og adgang samt logning – således at det kun er personer med et arbejdsbetinget behov, der har adgang til personoplysninger i løsningen. Herunder også vurdering af risici forbundet med anvendelse af browser og netværk.

2.5.2. Inddragelse af registrerede

På vegne af De Dataansvarlige vurderes det, at det ikke er relevant at indhente de registreredes eller deres repræsentanters synspunkter vedrørende behandlingen af personoplysninger i forbindelse med anvendelsen af M365, jf. databeskyttelsesforordningens artikel 35, stk. 9.
Økonomistyrelsen og Statens It har lagt vægt på følgende:

- Hovedparten af behandlingen af personoplysninger vil ske i henhold til lovgivning.
- Inddragelse af de registrerede anses som umulig eller uforholdsmæssigt vanskeligt, da de registrerede udgør en meget bred og omfattende gruppe, der inkluderer stort set alle borgere i samfundet samt ansatte hos De Dataansvarlige.

På denne baggrund vurderes det, at det ikke er nødvendigt at inddrage de registrerede i forbindelse med udarbejdelsen af denne konsekvensanalyse.

2.6. Processen for gennemførelsen af konsekvensanalysen

2.6.1. Metode

Databeskyttelsesforordningen artikel 35, stk. 7, fastsætter følgende minimumskrav til konsekvensanalysens indhold:
a) En systematisk beskrivelse af de planlagte behandlingsaktiviteter og formålene, herunder eventuelle legitime interesser, der forfølges af den dataansvarlige.
b) En vurdering af nødvendighed og proportionalitet af behandlingsaktiviteterne i forhold til formålene.
c) En vurdering af risiciene for de registreredes rettigheder og frihedsrettigheder.
d) De foranstaltninger, der påtænkes for at imødegå risici, herunder garantier, sikkerhedsforanstaltninger og mekanismer, som kan sikre beskyttelse af personoplysninger og påvise overholdelse af databeskyttelsesforordningen, under hensyntagen til de registreredes og andre berørte personers rettigheder og legitime interesser.

Der fremgår desuden en række kriterier for en acceptabel konsekvensanalyse i bilag 2 til Artikel 29-Gruppens (nu: EDPB) vejledning om konsekvensanalyser[9]. Nærværende konsekvensanalyse er udarbejdet i overensstemmelse med disse krav.

Databeskyttelsesforordningen fastsætter ikke i detaljer, hvilken procedure for udarbejdelse af konsekvensanalysen den dataansvarlige skal følge. Udarbejdelsen af nærværende konsekvensanalyse er navnlig sket under anvendelse af den metode, der fremgår af den internationale standard for udarbejdelse af konsekvensanalyser vedrørende databeskyttelse, ISO/IEC 29134:2023[10], med nødvendige tilpasninger af hensyn til sagens karakter.

Konsekvensanalysen omfatter hele staten (De Dataansvarlige), der hver især har varierende lovbestemte opgaver.
Der er derfor forskel på den behandling af personoplysninger, De Dataansvarlige hver især foretager, herunder formålet med behandlingen og typen af personoplysninger der behandles om borgerne og ansatte.
Ligeledes kan der være forskel på konfigurationen for De Dataansvarlige, og det kan være forskelligt, hvilke funktioner der tilvælges og fravælges. Desuden kan det være forskelligt, hvilke eventuelle tekniske og organisatoriske sikkerhedsforanstaltninger hver af De Dataansvarlige har fastsat.

Der er med andre ord tale om, at konsekvensanalysen skal suppleres af De Dataansvarlige hver især i lyset af deres individuelle, varierende behandlinger af personoplysninger ved brug af Microsoft 365, herunder følgende forhold:

- Den nærmere og konkrete behandling af personoplysninger, herunder hvilke personoplysninger som foretages af De Dataansvarlige hver især i forbindelse med de lovbestemte opgaver, herunder overholdelse af de grundlæggende principper i databeskyttelsesforordningens artikel 5, f.eks. fastsættelse af slettepolitikker m.v., samt overholdelse af kravet om hjemmel til behandlingen af personoplysninger.
- De Dataansvarliges varetagelse af oplysningspligten og de registreredes rettigheder.
- De Dataansvarliges egen analyse af den/de browsere, de anvender.
- Begrænsninger ved konfiguration samt interne retningslinjer, der begrænser brugen af applikationer og cloudtjenester. Det kan f.eks. være ved anvendelse af Teams, herunder chat samt personoplysninger der afgives i forbindelse med livetransmission. Afhængig af De Dataansvarliges interne retningslinjer kan dette også være begrænset, såfremt det fremgår heraf, at følsomme

9 Artikel 29-Gruppen (nu Det Europæiske Databeskyttelsesråd, herefter forkortet "EDPB"): Retningslinjer for konsekvensanalyse vedrørende databeskyttelse (DPIA) og bestemmelse af, om behandlingen "sandsynligvis indebærer en høj risiko" i henhold til forordning (EU) 2016/679, WP 248, rev. 01, revideret og endeligt vedtaget den 4. oktober 2017.

10 ISO/IEC 29134:2023 "Information technology — Security techniques — Guidelines for privacy impact assessment".

personoplysninger ikke må deles i forbindelse med anvendelsen af Teams, ligesom optagelse af transmissionen og deling af lokationsdata kan være deaktiveret som en sikkerhedsforanstaltning.

- Oplysninger om overførsler af personoplysninger til tredjelande i tilfælde, hvor De Dataansvarlige selv tilsigtet overfører personoplysninger til en modtager i et tredjeland – f.eks. ved at sende en e-mail indeholdende personoplysninger til en modtager i en myndighed eller virksomhed i et tredjeland – ligesom De Dataansvarlige selv sørger for at belyse eventuelle foranstaltninger såsom retningslinjer herfor.
- Hvordan hver af De Dataansvarlige har begrænset adgangen til personoplysninger, sådan at det kun er relevante personer, der har adgang hertil.

Risikovurdering efter databeskyttelsesforordningens artikel 32 og implementering af passende sikkerhedsforanstaltninger for den behandling, der er forbundet med brug af Microsoft 365, herunder sikker brug af løsningen, rolle- og adgangsstyring og logning, således at alene personer med et arbejdsbetinget behov for adgang til personoplysninger i løsningen, samt vurdering af risici forbundet med brug af browser og netværk.

3. BRUGERNES ANVENDELSE AF DE UDVALGTE APPLIKATIONER OG CLOUDTJENESTER I MICROSOFT 365

3.1. Generelt om Microsoft 365 og sammenhæng

M365 er en abonnementstjeneste, der tilbyder en række cloudbaserede produktivitets- og samarbejdsværktøjer. Platformen omfatter software, cloudtjenester og supporttjenester.
Værktøjerne leveres som Software-as-a-Service (SaaS), hvor Microsoft Ireland hoster og driver infrastrukturen, platformen og applikationerne, som brugerne kan tilgå via internettet.
M365 kan anvendes både som en cloudbaseret løsning og som en on-premise løsning, hvor visse funktioner hostes i kundens datacenter. Anvendelsen af cloudtjenester er dog begrænset ved on-premise løsninger, da de primært kræver Microsofts infrastruktur.

3.1.1. Desktopapplikationer vs. Cloudtjenester og Cloud Apps

Desktopapplikationer og cloudtjenester/Cloud apps adskiller sig ved, hvor behandling og lagring af data finder sted.
Valget har betydning for adgang, datakontrol og krav til sikkerhedsforanstaltninger.

- Desktopapplikationer:
- Cloudtjenester/Cloud Apps:

- Software, der kan downloades og installeres på brugerens enhed.
- Muliggør offline adgang til funktioner i M365.
- Applikationerne downloades fra M365-platformen og kan integreres med cloudtjenesterne.

- Services, der leveres over internettet.
- Brugerne kan tilgå data og applikationer via browser, desktopapplikationer eller dedikerede apps.
- Brugen af cloudtjenester kræver ofte ikke en installering af et program (mindre klienter kan have behov for en installering).
- Data opbevares og behandles på Microsoft Irelands servere.

Sondringen mellem Cloudtjenester og Cloud Apps er navnlig følgende:

- Cloudtjenester er alle typer IT-Ressourcer leveret over internettet (lagring, servere, databaser, software m.m.)
- Cloud Apps er de specifikke programmer/applikationer, som brugeren arbejder i, og som kører via cloudtjenesterne

Brug af M365-cloudtjenester via browser kan ske gennem forskellige browsere[11]. Browser-brug er ikke omfattet af konsekvensanalysen.

3.1.2. Begreber og vilkår i M365

Microsoft Ireland anvender forskellige begreber til at gruppere værktøjer med ensartede vilkår. Disse begreber omfatter:

Begreb	**Værktøj(er)**
Office 365 Services	Alle 365 Cloudtjenester omfattet af konsekvensanalysen. (Word, PowerPoint, Excel, Outlook, Office for the web, OneDrive, Exchange Online, SharePoint, Teams, Defender Suit, XDR, Purview, Sentinel, Power BI, eDiscovery)
Online Service	Alle 365 Cloudtjenester omfattet af konsekvensanalysen og Entra ID.

11 Microsofts hjemmeside: https://support.microsoft.com/da-dk/office/hvilke-browsere-fungerer-med-microsoft-365-til-internettet-og-microsoft-365-tilf%C3%B8jelsesprogrammer-ad1303e0-a318-47aa-b409-d3a5eb44e452 (senest tilgået den 27. februar 2024).

Core Online Service	Alle 365 Cloudtjenester omfattet af konsekvensanalysen og Entra ID.
EU Data Boundary Services	Alle 365 Cloudtjenester omfattet af konsekvensanalysen *undtagen* Exchange Online Protection og Entra ID.
Cloud Apps	Alle 365 Cloudtjenester omfattet af konsekvensanalysen og Entra ID.
E3 vs. E5	E3-licensen indeholder virksomhedsstandardpakken til produktivitet inklusiv baselinesikkerhed. E5-licensen indeholder samtlige værktøjer i E3 samt mulighed for mere avancerede valg med sikkerhedskomponenter samt avanceret compliance, tele-foni og analytics.

3.1.3. EU Data Boundary Services

Værktøjerne, der er omfattet af konsekvensanalysen, konfigureres i videst muligt omfang som EU Data Boundary Services.
Ældre funktioner, der ikke er aktiveret som standard, og som kan føre til dataoverførsel uden for EU

Data Boundary, vil ikke blive aktiveret i Statens tenant (en isoleret instans, hvor en organisation har sine egne brugere, data og konfigurationer)), som f.eks.:

- Research[12] i Word, Excel og PowerPoint.
- Shared Tunnel Invitations i Teams.[13]
- Azure Bot Services i Teams App.

3.1.4. Dokumentation og vilkår

Information om M365 og behandlingen af data heri fremgår primært af:

- Microsoft Irelands databehandleraftale (Bilag C).
- Microsofts Product Terms (Bilag B).
- Online dokumentation (Bilag H). 1415

12 EU Data Boundary dokumentationen ("Microsoft 365 Applications", "Research").

13 EU Data Boundary dokumentationen ("Microsoft 365 Applications", "Shared Channel Invitations").

14 EU Data Boundary dokumentationen ("Microsoft 365 Applications", "Research").

15 EU Data Boundary dokumentationen ("Microsoft 365 Applications", "Research").

3.1.5. Professional Services

Udover applikationer og cloudtjenester kan der tilvælges Professional Services, herunder konsulent- og supportydelser.
Denne konsekvensanalyse er afgrænset fra konsulentydelser, da dette ikke er en del af statens aftale med Microsoft.

3.2. Metode til konsekvensvurdering og kategorisering af aktiver i Microsoft 365

Denne DPIA omfatter flere applikationer og tjenester i Microsoft 365-miljøet. For at sikre en ensartet, proportional og dokumenterbar vurdering af risici for de registrerede anvendes en fælles metode til konsekvensvurdering, kategorisering og dokumentation af alle aktiver.

Metoden understøtter, at aktiver kan behandles samlet i en DPIA, samtidig med at vurderings- og dokumentationsdybden differentieres efter aktivets faktiske risiko og betydning. Aktiver med lavere konsekvens dokumenteres i aktivlisten (bilag til DPIA), mens aktiver med høj konsekvens dokumenteres individuelt i DPIA'en.

3.2.1. Indledende screening og konsekvensvurdering

Ved oprettelse af nye aktiver eller ved væsentlige ændringer foretager De Dataansvarlige en screening, der som minimum afdækker:

- Aktivets formål og funktion
- Datatyper (ingen, almindelige, fortrolige, følsomme, strafbare)
- Omfang (antal berørte registrerede / organisatorisk udbredelse)
- Leverancetype (Microsoft-standard, tredjepart, cloud-app)

Hvis aktivet ikke behandler personoplysninger, registreres det i aktivlisten og afsluttes, og aktivet kan anvendes og rulles ud til de brugere der ønsker det.

3.2.2. Risikovurdering (scoringmodel)

Aktiver, der behandler personoplysninger, vurderes efter fem risikofaktorer:
(1) oplysningstype, (2) antal registrerede, (3) forretningskritikalitet, (4) tekniske kompleksitet/integrationer, (5) adgang/deling. Hver faktor vurderes på en skala fra 1 (lav) til 3 (høj). Den samlede score (5-15) anvendes til at fastlægge konsekvensniveau og dokumentationskrav:

Samlet score	Samlet konsekvensniveau	Udfør

5-7	Lav	Aktiv registreres i aktivlisten (kategori C eller D afhængigt af persondata).
8-11	Middel	Aktiv registreres i aktivlisten som kategori B og indgår i den samlede risikovurdering i DPIA'en.
12-15	Høj	Aktiv eskaleres til DPO med henblik på beslutning om fuld DPIA-behandling og individuel beskrivelse (kategori A).

3.2.3. Kategorisering og dokumentation

Efter konsekvensvurderingen placeres hvert aktiv i en af følgende kategorier, som styrer dokumentationsniveauet:

Kategori	Typiske datatyper og risikoniveau	Dokumentation
D – Uden persondata	Ingen personoplysninger. Ingen konsekvens.	Aktivlisten.
C – Støtte- og tekniske aktiver (lav konsekvens)	Almindelige oplysninger (fx navn, e-mail, IP, bruger-id).	Aktivlisten + kort beskrivelse.
B – Forretningsunderstøttende aktiver (middel konsekvens)	Almindelige og fortrolige oplysninger (fx ansættelsesdata, økonomi, sagsoplysninger).	Aktivlisten + beskrivelse; indgår samlet i DPIA'en.
A – Centrale aktiver (høj konsekvens)	Følsomme oplysninger (art. 9), strafbare forhold (art. 10) eller fortrolige oplysninger i kritiske processer.	Aktivlisten + individuel DPIA-beskrivelse.

Kun aktiver i kategori A beskrives individuelt i DPIA'ens hovedtekst. Øvrige aktiver dokumenteres kun i aktivlisten der findes i DPIA'ens bilagsmateriale (bilag L). Ønskes yderligere dokumentation eller ved tvivl om datatyper eller kategorisering eskaleres der til DPO.

3.2.4. Vedligehold, ændringshåndtering og governance

Metoden understøtter løbende vedligehold af DPIA'en ved ændringer i Microsoft 365-miljøet:

- Nye aktiver: gennemgår screening og konsekvensvurdering og registreres i aktivlisten i korrekt kategori.
- Ændrede aktiver: revurderes ved væsentlige ændringer i funktionalitet, datatyper, integrationer eller deling/adgang.
- Skift af kategori: hvis revurderingen medfører ny kategori, opdateres aktivlisten og tilhørende dokumentation.
- Opgradering til kategori A: medfører opdatering af DPIA'en med fuld beskrivelse af aktivet.

Der gennemføres mindst årlig gennemgang af aktivlisten, og DPIA'en opdateres, når der identificeres væsentlige ændringer, særligt for aktiver i kategori A.

3.3. Governance og ansvarsplacering

For at sikre løbende vedligehold og rettidig opdatering, er følgende governance principper fastlagt:

Den ansvarlige for det tekniske og driftsmæssige ansvar i organisationen har ansvar for at anmelde ændringer i aktiver, herunder:

- Indførelse af nye funktioner, datatyper eller integrationer.
- Ændringer i eksisterende løsninger, der kan påvirke databehandlingen
- Oprettelse af nye aktiver i aktivlisten

Hvis der opstår tvivl om, hvorvidt aktivet behandler personoplysninger, eller hvilken kategori det tilhører, sendes sagen til den dataansvarliges DPO (Data Protection Officer), eller tilsvarende GDPR-ansvarlige for vurdering.

DPO eller den ansvarlige rolle/enhed for databeskyttelse ved den dataansvarlige
Har ansvar for at vedligeholde relevante databeskyttelsesretlige forhold og ændringer i aktivlisten, koordinere reevalueringer og sikre, at ændringer håndteres i overensstemmelse med DPIA-metoden.
DPO vurderer og beslutter, hvordan ændringer påvirker DPIA'en, herunder om en ny eller opdateret konsekvensanalyse er påkrævet.

IT-koordinatorer eller tilsvarende teknisk personale
Leverer input og teknisk gennemgang ved ændringer i systemarkitektur, integrationer og konfigurationer i Microsoft 365, som kan have betydning for risikobilledet.

Enheden bistår DPO og ansvarlige rolle for det tekniske og driftsmæssige ansvar i egne services med vurdering af tekniske risici og kontrolforanstaltninger.
Der foretages årligt gennemgang af aktivlisten, og DPIA'en opdateres, når væsentlige ændringer i kategori A-aktiver identificeres.

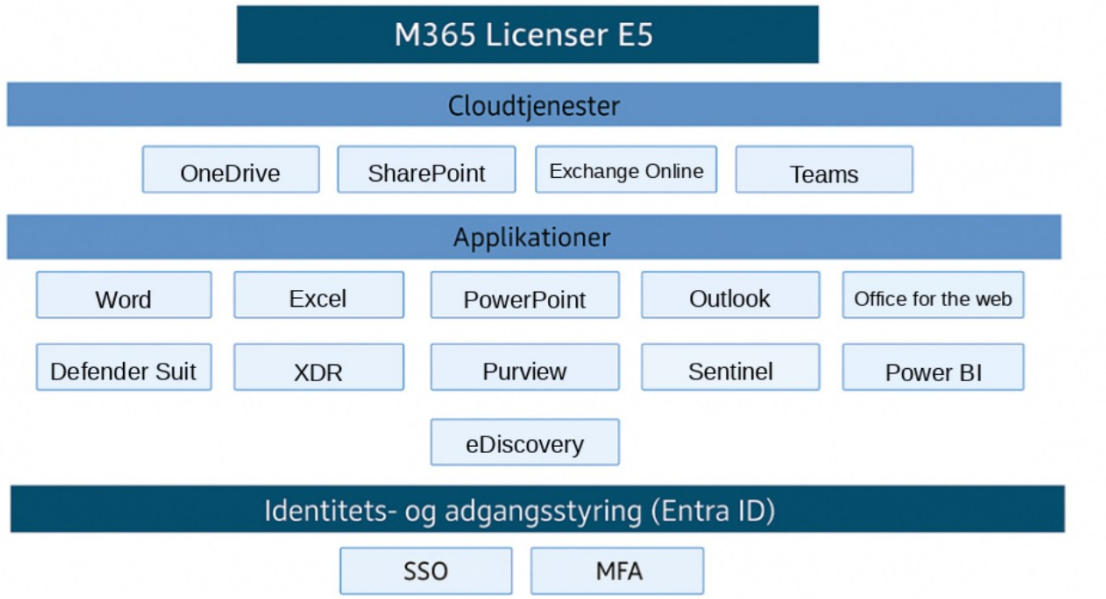
3.4. Cloudtjenester og Cloud-applikationer omfattet af konsekvensanalysen

Denne konsekvensanalyse omfatter udvalgte værktøjer i M365 licens E5, herunder:

- Word, PowerPoint, Excel og Outlook – klassiske produktivitetsapplikationer til dokumenthåndtering, præsentationer, regneark og e-mail.
- Office for the web – webbaserede versioner af Office-applikationerne, som giver online adgang til Word, Excel, PowerPoint og Outlook.
- OneDrive, Exchange Online, SharePoint og Teams – cloudtjenester til filhåndtering, kommunikation og samarbejde.
- Microsoft Defender Suite, Microsoft XDR, Microsoft Purview og Microsoft Sentinel – sikkerheds- og complianceværktøjer til trusselsbeskyttelse, hændelseshåndtering, databeskyttelse og governance.
    - Microsoft Purview – samlet compliance- og datastyringsplatform i M365, der bl.a. understøtter klassificering/mærkning, DLP, informationsbeskyttelse, datalivscyklus/records, insider risk/audit samt eDiscovery som en delkomponent.
- Power BI – analyse- og rapporteringsplatform til datamodeller, dashboards og deling/eksport.
- eDiscovery (Purview eDiscovery Standard & Premium) – søgning, bevissikring, case-styring, gennemgang og eksport på tværs af Exchange, SharePoint, OneDrive og Teams; kun autoriserede roller, fuld logning.

3.4.1. Strukturen og sammenhængen mellem de omfattede værktøjer i M365

Derudover anvendes Entra ID (tidligere Active Directory), som er Microsofts løsning til identitets- og adgangsstyring. Entra ID er en central del af Microsoft Azure Core Services og benyttes til godkendelse, brugeradministration og sikkerhedsforanstaltninger.
Nedenstående grafik illustrerer strukturen og sammenhængen mellem de omfattede værktøjer i M365:



Figur 1 M365-værktøjer

3.5. Detaljerede beskrivelser af aktiver

3.5.1. Word, Excel, PowerPoint

Word, Excel og PowerPoint udgør centrale komponenter i Microsofts produktivitetssuite og stilles til rådighed som enkeltstående applikationer eller samlet som en del af Office 365- eller Microsoft 365-licenserne. Disse applikationer er udbredt og integreret i den daglige opgaveløsning hos ansatte i de dataansvarlige, myndigheder.

Applikationerne anvendes til følgende hovedformål:

- Word: Anvendes til udarbejdelse af breve, notater, sagsfremstillinger, afgørelser og øvrige dokumenter relateret til sagsbehandling, borgerkontakt og administrativ kommunikation.
- Excel: Anvendes til databehandling, beregninger, budgetlægning, registrering og analyseformål, ofte i forbindelse med personaleadministration, økonomistyring eller ledelsesrapportering.
- PowerPoint: Anvendes til udarbejdelse af præsentationer, intern videndeling, introduktioner og undervisningsmateriale, typisk i forbindelse med møder, kurser og organisatorisk koordinering.

Brugen af disse værktøjer sker i en forvaltningsretlig kontekst, hvor der bl.a. behandles personoplysninger i forbindelse med myndighedsudøvelse. Eksempler på dette kan være:
- Udarbejdelse af dokumenter, der indeholder identificerbare oplysninger om borgere og medarbejdere
- Indtastning og beregning af data i regneark, der kan indeholde følsomme eller fortrolige oplysninger

- Udarbejdelse af præsentationer med henblik på organisatoriske beslutningsprocesser, som kan inkludere personoplysninger

Formålet med behandlingen af personoplysninger i disse applikationer omfatter:
- Overholdelse af notatpligten og den journaliseringspligt, som følger af forvaltningsretlige regler
- Understøttelse af kommunikation med borgere og ansatte, herunder som led i sagsbehandling og personaleforhold
- Sikring af dokumentation for administrative beslutninger og processer, i overensstemmelse med officialprincippet og krav om ansvarlig databehandling

Behandlingen kan omfatte både almindelige og følsomme personoplysninger, afhængigt af anvendelsesscenariet og dokumentets karakter. Dette forudsætter, at applikationerne anvendes under passende tekniske og organisatoriske sikkerhedsforanstaltninger, jf. databeskyttelsesforordningens artikel 32.

3.5.2. Outlook og Exchange Online

Outlook-klienten fungerer som primær brugerflade til Exchange Online og anvendes bredt af medarbejdere i de dataansvarlige myndigheder. Exchange Online leverer funktionalitet til e-mail, kalender og kontaktadministration, som er centrale for den daglige drift og kommunikation.

Komponenterne anvendes til følgende formål:
- Outlook: Giver brugerne adgang til e-mails, kalenderposter, kontaktoplysninger og opgavestyring via en klientbaseret grænseflade.
- Exchange Online Archiving: Muliggør langtidsarkivering af e-mails og opfylder krav til dokumentation, gennemsigtighed og eDiscovery i forbindelse med retslige og organisatoriske krav.
- Exchange Online Protection: Leverer sikkerhedslag til e-mailtrafik og beskytter mod spam, malware og andre uønskede trusler.

De oplysninger, der behandles i Outlook og Exchange Online, omfatter:
- Personoplysninger om borgere, ansatte og eksterne samarbejdspartnere
- Indhold i e-mails, mødeindkaldelser, kalenderposter og vedhæftede dokumenter

Behandlingen sker i følgende formål:
- Understøttelse af effektiv og dokumentérbar forretningskommunikation
- Muliggørelse af rettidig og korrekt oplysning af sager, herunder som led i forvaltningsretlig oplysningspligt
- Overholdelse af arkivlovgivningens krav om bevaring, journalisering og udtræk

Behandlingen af personoplysninger i disse komponenter forudsætter passende tekniske og organisatoriske sikkerhedsforanstaltninger, herunder adgangskontrol, kryptering og logning, jf. databeskyttelsesforordningens artikel 32.

3.5.3. Teams

Microsoft Teams[16] stiller funktioner til rådighed som chat, lyd- og videomøder, skærmdeling og fildeling, og kan tilgås via både desktopapplikation og webbrowser. Tjenesten er tæt integreret med SharePoint Online og OneDrive for Business for effektiv håndtering af fillagring og samarbejde.
Teams anvendes i både intern og ekstern kommunikation samt i gruppearbejde og projektstyring. Der behandles typisk kontaktoplysninger, projektdata og andre forretningsrelevante informationer. Afhængigt af indholdet i møder og chats kan der også behandles følsomme eller fortrolige personoplysninger.
Behandlingen forudsætter passende tekniske og organisatoriske foranstaltninger, herunder logning, adgangsstyring og beskyttelse af kommunikationsindhold, jf. databeskyttelsesforordningens artikel 32.

3.5.4. SharePoint Online

SharePoint Online fungerer som den centrale platform til intranet, dokumenthåndtering, versionsstyring og workflowautomatisering. Tjenesten anvendes bredt til lagring og deling af sagsdokumenter, interne politikker og administrative procedurer.
Med funktioner som metadataadministration og detaljeret rettighedsstyring understøtter SharePoint en kontrolleret og dokumentérbar behandling af oplysninger. De behandlede dokumenter kan indeholde personoplysninger og kræver derfor passende adgangs- og logningskontrol i henhold til databeskyttelsesforordningen.

3.5.5. OneDrive for Business

OneDrive[17] for Business er en personlig cloudlagringsløsning, som giver brugerne mulighed for at synkronisere dokumenter på tværs af enheder, tilgå versionshistorik og dele filer midlertidigt.

16 Microsofts hjemmeside: https://learn.microsoft.com/en-us/office365/servicedescriptions/teams-service-description (senest tilgået den 13. april 2026) (Microsoft 365 and Office 365 service descriptions side 522).

17 Microsofts hjemmeside: https://www.microsoft.com/da-dk/microsoft-365/onedrive/onedrive-for-business?rtc=1 og https://learn.microsoft.com/en-us/office365/servicedescriptions/onedrive-for-business-service-description (senest tilgået den 13. april 2026) (Microsoft 365 and Office 365 service descriptions side 463).

Brugerne anvender løsningen til opbevaring af arbejdspapirer, udkast og midlertidigt materiale, som kan indeholde personoplysninger, før disse overføres til permanente systemer såsom SharePoint Online eller ESDH-systemer. Derfor gælder samme krav til adgangskontrol, dataminimering og sikkerhed i behandlingen.

3.5.6. Entra ID

Entra ID (tidligere Azure Active Directory) håndterer identitets- og adgangsstyring på tværs af Microsoft 365-platformen. Tjenesten understøtter single sign-on (SSO), multifaktorgodkendelse (MFA) og betinget adgang baseret på faktorer som brugerroller, enhedens sikkerhedstilstand og geografisk placering.
Systemet sikrer, at kun autoriserede brugere får adgang til personoplysninger – under kontrollerede og dokumentérbare forhold. Det sker via rollebaseret adgangsstyring, livscyklushåndtering af brugere samt overvågning og logning af adgangsforsøg.
Entra ID udgør således en kritisk teknisk og organisatorisk sikkerhedsforanstaltning i overensstemmelse med databeskyttelsesforordningens artikel 32, og er central for at sikre fortrolighed, integritet og tilgængelighed i behandlingen af personoplysninger i Microsoft 365.

3.5.7. Customer Lockbox

Customer Lockbox er en avanceret sikkerhedsfunktion i Microsoft 365, som kræver eksplicit godkendelse fra den dataansvarlige, hvis Microsoft-teknikere skal tilgå kundedata i forbindelse med support eller fejlfinding.
Formålet er at sikre maksimal kontrol, dataminimering og gennemsigtighed ved ekstern adgang til personoplysninger. Løsningen reducerer risikoen for uautoriseret adgang og giver den dataansvarlige direkte kontrol over adgangstilladelser.
Customer Lockbox understøtter overholdelsen af databeskyttelsesforordningens principper om ansvarlighed og integritet, jf. artikel 5 og artikel 32.

3.5.8. Access

Microsoft Access er en desktopbaseret databaseapplikation, som muliggør oprettelse og håndtering af relationelle databaser med brugerdefinerede formularer og forespørgsler. Løsningen anvendes typisk i lokale scenarier, hvor der er behov for fleksibel dataregistrering, f.eks. til statistiske formål, opgavelister, lokal journalisering eller administrative datasæt uden systemunderstøttelse.

Access anvendes ofte til behandling af personoplysninger, f.eks.:

- Interne databaser med medarbejderdata
- Midlertidige registreringer før integration i permanente systemer
- Forespørgsler eller rapporteringer baseret på manuelle datakilder

Da Access-databaser som udgangspunkt er lagret lokalt og kan være ukrypterede, er det særligt vigtigt at sikre, at der er implementeret passende adgangskontrol og backup-rutiner. Brug af Access i GDPR-reguleret kontekst bør ske under hensyntagen til dataminimering, livscyklus for data og systemets egnethed til behandlingsformål.

3.5.9. Defender Suite inkl. Endpoint

Microsoft Defender Suite er en integreret sikkerhedsplatform, der omfatter Detektion, beskyttelse og respons på sikkerhedstrusler i realtid. Omfatter antivirus, trusselsanalyse, sandboxing og sikkerheds-rapportering på tværs af Microsoft 365 og slutpunkter.

Funktionaliteten inkluderer:

- Trusselsdetektion og -respons (EDR) på endpoints
- Realtidsovervågning af adfærd og sikkerhedshændelser
- Automatisk inddæmning og afhjælpning (auto-remediation)

Der behandles metadata og systemrelaterede oplysninger, herunder IP-adresser, brugerkonti og enhedsoplysninger. Systemet er en central del af myndighedens sikkerhedsforanstaltninger og understøtter opfyldelse af artikel 32 (integritet, fortrolighed og tilgængelighed).

3.5.10. Microsoft Purview

Microsoft Purview er en cloudbaseret platform til data governance, compliance og informationsbeskyttelse. Purview anvendes til at identificere, klassificere og beskytte følsomme oplysninger i Microsoft 365. Det bruges også til at etablere og håndhæve compliance-politikker og få indblik i databehandlingens omfang.

Typiske anvendelser inkluderer:

- Identifikation og beskyttelse af personoplysninger og følsomme data
- Konfiguration og håndhævelse af DLP-politikker og kryptering
- Audit og compliance-rapporter ift. GDPR, NIS2 og ISO 27001

Purview giver mulighed for at dokumentere databehandlingsaktiviteter, begrænse utilsigtet datalækage og fremme en kontrolleret datakultur. Løsningen er særlig relevant i miljøer med høj kompleksitet, decentral datadeling og regulatoriske krav.

3.5.11. Microsoft Sentinel

Microsoft Sentinel er en cloudbaseret SIEM- og SOAR-løsning (Security Information and Event Management / Security Orchestration, Automation and Response. Sentinel anvendes til overvågning, alarmering og analyse af sikkerhedshændelser i Microsoft 365 og tilknyttede systemer. Det giver mulighed for central logindsamling, trusselsdetektion og hændelsesrespons.

Sentinel anvendes til:

- Central logindsamling og overvågning fra Microsoft 365, endpoints, netværk og on-prem-systemer
- Automatisk trusselsidentifikation og hændelsesrespons
- Overholdelse af logningsforpligtelser og dokumentation

Sentinel behandler systemmetadata, brugeraktiviteter, adgangslogs og sikkerhedshændelser, og bør konfigureres med opmærksomhed på dataminimering, adgangsbegrænsning og formålsbegrænsning jf. databeskyttelsesretlige krav. Endvidere behandler Sentinel sikkerheds- og aktivitetslogs (metadata), som kan være knyttet til brugere (fx brugernavn, IP, enheds-id). Adgang begrænses til autoriserede roller, og relevante handlinger/logadgange dokumenteres.

3.5.12. Microsoft XDR (Defender)

Extended Detection and Response (XDR) er Microsofts samlede tilgang til trusselsdetektion på tværs af endpoints, cloud, identiteter og e-mail. XDR-løsningen sammenkobler data fra Defender-produkterne og

muliggør hurtig, kontekstbaseret respons. XDR muliggør central korrelation af trusselsdata fra enheder, mails, identiteter og applikationer – og muliggør automatisk eller semi-automatisk respons.

Funktionaliteten inkluderer:

- Tværgående detektion af trusler og kompromitteringer
- Analyse af hændelsesforløb på tværs af systemer og brugere
- Automatiserede svar baseret på risikoniveau og politik

Behandling omfatter sikkerhedsrelevante metadata og logs, som indirekte kan knyttes til brugere og følsomme ressourcer. Løsningen betragtes som en organisatorisk og teknisk foranstaltning under artikel 32.

3.5.13. eDiscovery (Purview)

eDiscovery er en cloudbaseret løsning i Microsoft Purview til søgning, bevissikring (*Legal Hold*), gennemgang og eksport af data i forbindelse med juridiske forespørgsler, klager, interne undersøgelser og sikkerhedshændelser. Tjenesten findes i to varianter, *Standard* og *Premium,* som giver mulighed for casestyring, filtrering, annotering og dokumenteret sporbarhed på tværs af Exchange, SharePoint, OneDrive og Teams.

eDiscovery anvendes til:

Søgning af indhold og metadata på tværs af Exchange, SharePoint, OneDrive og Teams
Bevissikring af oplysninger ved hjælp af *Legal Hold* for at forhindre sletning under igangværende sager
Gennemgang og filtrering af resultater i forbindelse med juridiske eller forvaltningsmæssige forespørgsler
Eksport af identificerede data til godkendte modtagere med henblik på vurdering, dokumentation eller myndighedskontrol
Logning og revision af alle handlinger for at sikre fuld sporbarhed og ansvarlighed

Behandlingen kan omfatte almindelige og særlige kategorier af personoplysninger, afhængigt af hvilke data der findes i de tilknyttede Microsoft 365-tjenester. Data forbliver inden for Microsofts EU Data Boundary, og eksporteret materiale opbevares udelukkende i godkendte og beskyttede områder, som slettes ved sagsafslutning eller udløb af opbevaringspligt.

Foranstaltningerne skal samlet opfylde kravene i databeskyttelsesforordningens artikel 32 om fortrolighed, integritet og tilgængelighed.

Adgang er kun tilladt for autoriserede roller som eDiscovery Manager eller eDiscovery Admin via Microsoft Purview, og alle handlinger bliver logget. Eksporter opbevares i godkendte og beskyttede områder og slettes, når sagen afsluttes/når opbevaringspligten udløber.

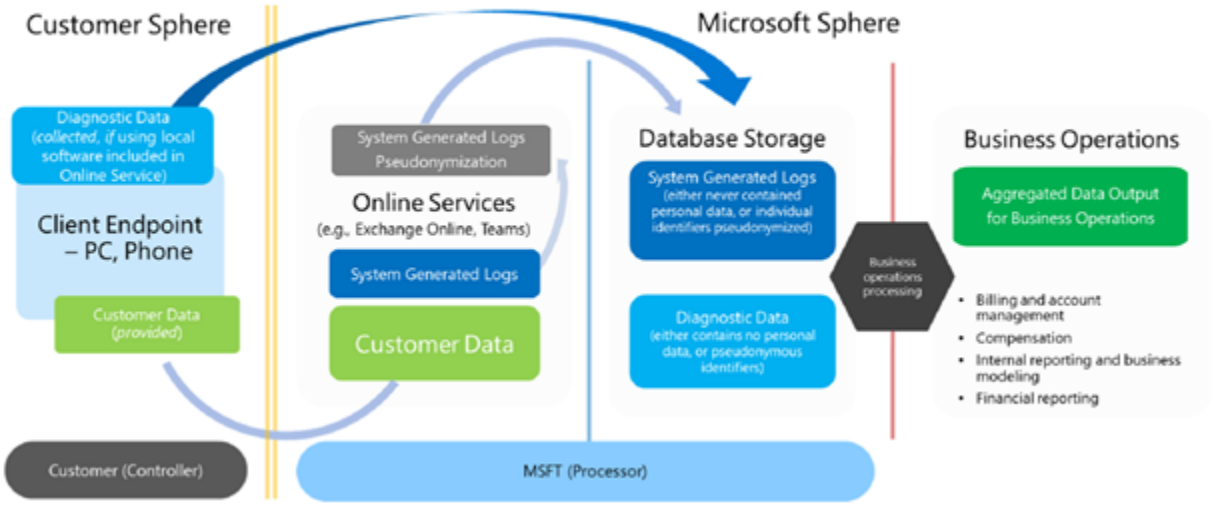
3.6. Formålet med behandlingen

De dataansvarliges formål med behandlingen af personoplysninger er at varetage lovbestemte opgaver, herunder sagsbehandling og personaleadministration. Formålet kan variere mellem de enkelte dataansvarlige, afhængigt af hvilke opgaver de er pålagt i henhold til lovgivningen. Derfor skal hver dataansvarlig supplere denne konsekvensanalyse med en konkret beskrivelse af formålet med deres specifikke behandling af personoplysninger.

Udførelsen af de dataansvarliges opgaver sker primært gennem brug af it-systemer. Behandlingen af personoplysninger omfatter, at medarbejdere hos de dataansvarlige indtaster, redigerer, indsamler, sletter og modtager personoplysninger via de udvalgte applikationer og cloudtjenester i Microsoft 365.
Formålet med anvendelsen af disse tjenester er at understøtte de lovpligtige opgaver, men omfanget og konfigurationen af de anvendte applikationer kan variere. Nogle dataansvarlige kan anvende flere eller færre applikationer, og deres konfiguration kan være forskellig.
I forbindelse med anvendelsen af applikationerne og cloudtjenesterne indsamler Microsoft Ireland forskellige typer data fra brugerne:

- Diagnostic Data: Indsamles fra applikationer og inkluderer oplysninger om brugen af tjenesterne.
- Systemgenererede logfiler: Genereres af cloudtjenesterne og kan indeholde oplysninger om brugen af tjenesterne.
- Customer Data: Oplysninger, der indtastes af brugerne selv gennem applikationerne.

Dataflowet for Microsoft Irelands behandling af data er illustreret i figuren nedenfor:



Figur 2 Illustration af dataflowet for Microsoft Irelands behandling af data

Som det fremgår af figuren, sker der følgende:

- Pseudonymisering: Diagnostic Data og Customer Data, herunder Systemgenererede logfiler, pseudonymiseres inden videre behandling.
- Aggregering: Data aggregeres, inden de anvendes til interne forretningsformål hos Microsoft Ireland.
- Formål: Behandlingen sker både til opfyldelse af de dataansvarliges formål og til Microsoft Irelands egne formål, hvilket uddybes i afsnit 5.
-

Formålet med behandlingen i de enkelte applikationer og cloudtjenester er beskrevet mere detaljeret i afsnit 4.2.

3.7. Behandlingen af personoplysninger

3.7.1. Behandlingens karakter og omfang

Behandlingen af personoplysninger udføres af de ansatte hos de dataansvarlige med henblik på at varetage lovpligtige opgaver såsom sagsbehandling og personaleadministration.

Der behandles potentielt alle typer af personoplysninger, herunder:

- Ikke-følsomme personoplysninger: F.eks. navne, adresser og kontaktoplysninger.

- Følsomme personoplysninger: F.eks. helbredsoplysninger, race eller etnisk oprindelse, fagforeningsmæssigt tilhørsforhold.
- Fortrolige oplysninger: F.eks. økonomiske oplysninger og oplysninger om ansættelsesforhold.
- Oplysninger om strafbare forhold: F.eks. straffedomme og lovovertrædelser.

Disse personoplysninger indsamles og behandles potentielt i forbindelse med anvendelsen af Microsoft 365-applikationer som f.eks. Word, Excel, Outlook, Teams, OneDrive og SharePoint.

Behandlingstyper og applikationer

1. Dokumentbehandling i Word, Excel og e-mails:
   - Personoplysninger kan forekomme i dokumenter, regneark og e-mails, herunder vedhæftninger.
   - Indholdet kan omfatte alt fra sagsnumre, navne og adresser til vurderinger, ansættelsesoplysninger, økonomiske data og helbredsoplysninger.

2. Kalenderfunktion i Outlook:
   - Kalenderaftaler kan indeholde oplysninger om deltagere, mødested og formål med møder.
   - For de fleste kalenderposter vil der typisk være tale om ikke-følsomme personoplysninger.

3. Teams (chat og livetransmission):
   - Ved brug af chatfunktioner og livetransmission kan der afgives personoplysninger, herunder også følsomme oplysninger.
   - Omfanget af følsomme personoplysninger afhænger af, hvad brugerne selv deler i chatbeskeder eller under møder.
   - Optagelse af Teams-møder samt deling af lokationsdata kan være deaktiveret som en sikkerhedsforanstaltning, afhængigt af de dataansvarliges interne retningslinjer.
   - Datatilsynets afgørelse af 17. januar 2013 vedrørende transmission af gudstjenester[18] fastslår, at livetransmission af lyd, video og skærmdeling – uanset om denne lagres eller ej – er omfattet af databeskyttelsesforordningens anvendelsesområde, jf. artikel 2, stk. 1.[19]

4. OneDrive og SharePoint:
   - Selv om ESDH-systemerne er de primære lagringssteder for dokumenter, kan OneDrive og SharePoint også anvendes til lagring og deling af personoplysninger.
   - Behandlingen i ESDH-systemerne er dog ikke omfattet af denne konsekvensanalyse.

18 Datatilsynets afgørelse 2012-218-0006 af 17. januar 2013: Transmission af gudstjenester.

19 Justitsministeriets betænkning nr. 1565, del 1, side 31.

5. Databaseopbygning og registrering i Microsoft Access
   - Microsoft Access anvendes til lokal opbygning og vedligeholdelse af mindre databaser i forbindelse med administrative og faglige opgaver.
   - Der behandles ofte personoplysninger i forbindelse med f.eks. kontaktopfølgning, tilsyn, intern registrering eller mindre sagsgange.
   - Oplysninger kan inkludere navne, kontaktoplysninger, CPR-numre og andre sagsdata afhængigt af den konkrete databaseopsætning.
   - Adgang styres via lokale netværksrettigheder, og data lagres typisk på fællesdrev uden integration til Microsoft Entra ID.

6. Formularindsamling i Microsoft Forms
   - Forms anvendes til indsamling af input fra medarbejdere og eksterne brugere via spørgeskemaer og tilmeldingsformularer.
   - Formularer kan indeholde både almindelige og følsomme personoplysninger afhængigt af opsætningen – f.eks. navne, e-mail, fritekstbesvarelser mv.
   - Svar gemmes i Microsoft 365-miljøet og kan analyseres direkte eller eksporteres til Excel.
   - Der kan benyttes anonymiseringsfunktioner og DLP-politikker til at minimere risiko.

7. Notetagning og projektarbejde i OneNote
   - OneNote anvendes til strukturering af noter, referater, mødeforberedelse og dokumentation i interne sammenhænge.
   - Noter kan indeholde personoplysninger, herunder navne, e-mails, CPR-numre og fritekstoplysninger relateret til sager.
   - Notesbøger kan deles og synkroniseres på tværs af enheder og afdelinger og anvendes ofte sammen med Outlook og Teams.
   - Dataminimering og adgangsbegrænsning er afgørende for at forebygge utilsigtet deling.

8. Opgavestyring og samarbejde i Microsoft Planner
   - Planner anvendes til fordeling og opfølgning på opgaver i arbejdsgrupper og projekter.
   - Der kan optræde personoplysninger i opgavebeskrivelser og fritekstfelter, herunder navne, bruger-id og kommentarer.
   - Deling og adgang sker via Entra ID og kan styres med rollebaseret adgang.
   - Risikoen for utilsigtet datadeling reduceres via DLP-politikker og awareness-tiltag.

9. Endpoint- og mailsikkerhed med Microsoft Defender Suite inkl. Endpoint
   - Defender Suite beskytter slutpunkter, brugere og e-mailmodtagere mod trusler, malware og angreb via realtidsovervågning og cloudbaseret analyse.

- Personoplysninger som bruger-id, e-mailmetadata og loginoplysninger behandles i forbindelse med detektion og hændelseshåndtering.
- Løsningen understøtter compliance-funktioner og er integreret i Microsofts sikkerhedsarkitektur.
- Adgang kontrolleres centralt, og risici håndteres med politikbaseret styring og isolationsfunktioner.

10. Trusselskorrelation og respons via Microsoft XDR (Defender)
    - Microsoft XDR samler data fra Defender-suiten for at identificere avancerede angrebsmønstre og koordinere respons.
    - Behandler en lang række logs, herunder sessioner, e-mails, brugermønstre og endpoint-aktiviteter.
    - Formålet er at reducere reaktionstiden og øge opdagelsesgraden af komplekse trusler.
    - Automatisk klassificering, rollebaseret adgang og integration med Sentinel understøtter databeskyttelsen.

11. Mærkning og compliance-styring med Microsoft Purview
    - Microsoft Purview benyttes til at identificere og mærke personoplysninger i M365 ved hjælp af automatiske politikker og metadata.
    - Alle relevante datatyper i Word, Outlook, SharePoint, OneDrive og Teams kan analyseres og tagges.
    - Løsningen muliggør anvendelse af DLP, retention-politikker og auditlogning.
    - Risici imødegås bl.a. gennem trinvis implementering, manuel policy-review og begrænset adgang til følsomme logs.

12. Overvågning og loganalyse via Microsoft Sentinel
    - Sentinel fungerer som central SIEM-platform og analyserer logdata fra hele Microsoft 365-miljøet og øvrige systemer.
    - Der behandles brugerrelaterede logoplysninger som IP-adresser, loginforsøg, adgangslogs og hændelser.
    - Formålet er at opdage, forebygge og dokumentere sikkerhedsbrud og efterleve krav til logning.
    - Logadgang er begrænset og understøttet af connector-validering og manuel kontrol.

Behandlingens omfang

De dataansvarlige behandler personoplysninger om en bred gruppe af registrerede, herunder:

- Borgere i forbindelse med sagsbehandling.
- Ansatte i forbindelse med personaleadministration.
- Andre myndigheder og eksterne aktører, hvis oplysninger indgår i sagsbehandlingen.

Personoplysningerne kan indsamles fra:

- Direkte kontakt med borgere.
- Offentlige registre og andre myndigheder (f.eks. Skatteforvaltningen og Rigspolitiet).
- Intern kommunikation fra andre ansatte.

Adgangskontrol og sikkerhedsforanstaltninger

Adgangen til personoplysninger er generelt begrænset til et arbejdsbetinget behov og understøttes af:

- Tekniske foranstaltninger, der begrænser adgangen til data.
- Interne retningslinjer**,** som fastlægger, hvem der må tilgå og behandle personoplysninger.

De dataansvarlige har implementeret adgangsstyring, der sikrer, at kun relevante medarbejdere har adgang til de nødvendige personoplysninger. Dette gælder også for deling af data inden for og uden for organisationen.

Databehandlingens form og karakter

Personoplysninger, som indtastes, modtages eller behandles via Microsoft 365, vil som udgangspunkt være i klar tekst, hvilket betyder, at de kan læses direkte og er personhenførbare.

- Der kan også forekomme pseudonymiserede data, f.eks. systemgenererede logs.
- Derimod vil data som udgangspunkt ikke være anonymiseret, da formålet med behandlingen kræver, at oplysningerne kan henføres til specifikke registrerede.

Microsoft Ireland fungerer som databehandler for de dataansvarlige og vil derfor behandle personoplysninger på deres vegne. Visse oplysninger kan dog også anvendes af Microsoft Ireland til egne formål, hvilket uddybes i afsnit 5.

4. MICROSOFTS BEHANDLING AF PERSONOPLYSNINGER, DATABEHANDLERAFTALE OG VILKÅR

Når brugerne indtaster personoplysninger i løsningerne eller modtager personoplysninger via disse, behandler Microsoft Ireland personoplysninger via applikationer og cloudtjenester som databehandler som led i kundernes brug af disse og levering af tjenesteydelser. Ved at konfigurere og anvende disse applikationer og cloudtjenester instrueres Microsoft Ireland samtidig af kunden i at foretage behandling af personoplysninger. Til brug for nærværende konsekvensanalyse har Microsoft Danmark således i svar af den 2. april 2024 (Bilag I) uddybet, at:

> *"the customer issues their full instructions by using and configuring the cloud services after deciding to do so based on their study of the applicable product and services terms and product documentation."*

Udover det indhold og de personoplysninger, som kunderne selv genererer ved at indtaste eller modtage personoplysninger og anvende Microsofts tjenester (Customer Data og Professional Services Data), genererer systemet (og derved Microsoft) både diagnostiske data (Diagnostic Data) og logs (Systemgenererede logfiler) om brugernes interaktion med Microsoft 365. Visse af disse personoplysninger behandles af Microsoft Ireland som databehandler for De Dataansvarlige, og visse oplysninger behandles efterfølgende også til Microsoft Irelands egne formål i anonymiseret form.

I det følgende beskrives den behandling, som Microsoft Ireland foretager som databehandler for De Dataansvarlige, herunder generering af nye data om brugerne, og som Microsoft Ireland tillige foretager til egne forretningsaktiviteter i forbindelse med og i forlængelse af brugernes anvendelse af de udvalgte applikationer og cloudtjenester i Microsoft 365 platform[20].

4.1. Microsofts datakategorier

Microsoft Corporation har generelt defineret fem datakategorier, hvortil de data, Microsoft Ireland behandler, kan henføres. Datakategorierne er kort præsenteret nedenfor og indgår i Microsofts forskellige vilkår samt Microsoft Irelands databehandleraftale. Til brug for nærværende konsekvensanalyse har Microsoft ved svar af den 2. april 2024 (Bilag I), side 2 selv beskrevet sammenhængen sådan:

> *"Microsoft describes personal data processing in online services via a Data Protection Addendum (DPA) to the Product and Services Terms for online services (PT). The DPA provides a foundation for the personal data processing instructions from the customer. To ensure the customer knows the personal data processing design of the online services the DPA describes the set of data types that may contain personal data when processing (including transfer and including by sub processors) may occur."*

Datakategori	**Beskrivelse**
Personal Data	Kategorien omfatter personoplysninger. Definitionen af Personal Data findes i Microsoft Irelands databehandleraftale og svarer til databeskyttelsesforordningens definition. Personal Data er i databehandleraftalen defineret således:

20 Se Microsofts hjemmeside: https://learn.microsoft.com/en-us/office365/servicedescriptions/office-applications-service-description/office-applications-service-description (senest tilgået den 13. april 2026) (Bilag H, side 395).

> *"means any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."*

Personal Data er nærmere beskrevet nedenfor i afsnit 4.24.2 om Microsoft Irelands databehandleraftale.

Customer Data

Kategorien omfatter kundens data i Microsoft 365-cloudtjenester (Online Services), dvs. den data, som kunden lagrer i, behandler og genererer i cloudtjenesterne. Customer Data indeholder (også) Personal Data. Definitionen findes i Microsoft Irelands databehandleraftale, hvor følgende er anført:

> *"Means all data, including all text, sound, video, or image files, and software, that are provided to Microsoft by, or on behalf of, Customer through use of the Online Service. Customer Data does not include Professional Services Data."*[21]

Customer Data er nærmere beskrevet nedenfor i afsnit 4.24.2 om Microsoft Irelands databehandleraftale.

Professional Services Data

Kategorien omfatter data, som behandles i forbindelse med Microsofts konsulent- og supportydelser. Professional Services Data indeholder (også) Personal Data. Definitionen findes i Microsoft Irelands databehandleraftale, hvor følgende er anført:

> *"Means all data, including all text, sound, video, image files or software, that are provided to Microsoft, by or on behalf of a Customer (or that Customer authorizes Microsoft to obtain from a Product) or otherwise obtained or processed by or on behalf of Microsoft through an engagement with Microsoft to obtain Professional Services."*[22]

21 Microsoft Irelands databehandleraftale, side 4," Definitions".

22 Microsoft Irelands databehandleraftale, side 4," Definitions".

	Det er kun supportydelser, der er omfattet af De Dataansvarliges brug og således denne konsekvensanalyse. Professional Services Data er nærmere beskrevet nedenfor i afsnit 4.24.2 om Microsoft Irelands databehandleraftale.
Systemgenererede logfiler	Kategorien omfatter data, som genereres om brugernes interaktion med cloudtjenesterne. Systemgenererede logfiler indeholder Personal Data. Systemgenererede logfiler pseudonymiseres og bruges til i) at levere tjenesteydelser og sørge for sikkerheden samt at disse fungerer efter hensigten og ii) "business operations". Systemgenererede logfiler er nærmere beskrevet i afsnit 4.34.3.
Diagnostic Data	Kategorien omfatter data, som indsamles fra desktop-applikationer med henblik på at sikre, at applikationerne fungerer efter hensigten. Diagnostic Data indeholder Personal Data[23]. Diagnostic Data er nærmere beskrevet i afsnit 4.3 4.3 og 4.3.14.3.1.

Datakategorierne er nærmere beskrevet i de følgende afsnit, herunder i hvilke af Microsoft Irelands dokumenter de indgår.

Microsoft Corporation har i marts 2023 udgivet dokumentet "*Microsoft data protection and security terms for products and services: Business operations*" (herefter benævnt "Microsoft business operations white paper"), og i 2024 udgav de dokumentet *"System-generated logs in the Microsoft cloud – Purposes, types, customer access and privacy by design/default*" (herefter benævnt "Microsoft business operations white paper vol. 2") (Bilag G), som nærmere beskriver behandlingen af personoplysninger i forbindelse med business operations. Hverken Microsoft Irelands databehandleraftale eller Microsofts business operations white paper indeholder dog en udførlig beskrivelse af de konkrete oplysninger, der logges i Systemgenererede logfiler.

23 Microsoft Irelands databehandleraftale, side 4," Definitions".

Af Microsofts business operations white paper fremgår[24], at *"Microsoft designs logs to be generated and retained only as necessary to support security and efficacy of the online services. The management of access to the raw logs is governed by Microsoft, although Microsoft does make relevant logging available to the Customer's tenant administrators."*

Det fremgår ikke, hvad der skal forstås ved, at "relevant logging" gøres tilgængelig for kunden, og om der er forskel på indhold i "raw logs" og de logs, som kunden kan tilgå. I Microsofts business operations white paper vol. 2 fremgår imidlertid, at kunden kan få adgang til *"logs generated within Microsoft enterprise cloud services*". "Microsoft enterprise cloud services" er ikke defineret i white paper, men det er vores forståelse, at der er tale om det fulde datasæt i Systemgenererede logfiler, idet System-Generated data er beskrevet som "records of events that occur in Microsoft cloud services."[25]

Af Microsoft Danmarks svar af 23. april 2024 (Bilag J), fremgår således følgende svar på følgende spørgsmål:

> *"We understand that Microsoft provides the ability to give access to personal data entailed in Systemgenererede logfiler (System Generated Data) that may be necessary to complete a DSR. Does Microsoft also provide the ability to give access to personal data entailed in Diagnostic Data that may be necessary to complete a DSR?*
>
> *Yes, the tool provided by Microsoft and described at the link provided provides records from both Service Generated Data and Diagnostic Data that has been collected. For details see our answer to A.1 below. Diagnostic Data is only collected in the scenario where the customer is using on-premises Microsoft provided software products in conjunction with cloud services. Provided it is set up in advance, Customers can implement the Diagnostic Data viewer to inspect all diagnostic data that has been collected in many different Microsoft products and sent to Microsoft and confirmed by the Microsoft system as received.*
>
> *[…]*
>
> *Do the logs that Microsoft can extract/generate constitute an exhaustive extraction of the logs that are made?*
>
> *Yes, the tool will provide the records in Microsoft enterprise "system generated logs" where there is a pseudonymous token that matches the user identity the customer enters, when they*

[24] Microsofts business operations white paper, side 4, 'Overview of processing in the Microsoft cloud', 'Privacy by Design'.

[25] Microsofts business operations white paper vol. 2, side 1.

> *use the tool and that shows the logs associated with the identified user's activity in the online service, including user activity when users use on-premise software with the Online Services and Diagnostic Data is collected."*

Det kan dog være vanskeligt at forstå, hvilke personoplysninger de log-oplysninger, der hentes ud som anført ovenfor i det citerede, faktisk dækker over. Det betyder dog også, at andre på samme måde vil have svært ved at udlede nogen egentlige personoplysninger ud fra disse logs. Denne foranstaltning er af hensyn til dataminimeringsprincippet, pseudonymisering og sikkerhed, idet færre personer derved kan udlede personoplysninger heraf, og som beskrevet i Microsofts svar af 2. april 2024, side 7 (Bilag I):

> *"The practical way to assess risks associated with engineers reviewing logs remotely is to consider the nature of the logs (pseudonymized personal data only) and the factors that drive them to be i) created (user activity) and ii) to be transferred (real-time engineering operations). […] The records themselves, and especially the pseudonymous tokens representing a customer user, are useless outside of the context of an engineer familiar with Microsoft service internals who is looking at a log record in an internal Microsoft tool. In many cases, enabling logs to be interpreted in a broader context would weaken the security posture of the service."*

De Dataansvarlige har dog stadig brug for, at deres registrerede faktisk kan udøve deres rettigheder og opnå indsigt i personoplysninger, der behandles om de registrerede. Microsoft Danmark har dog samtidig ved svar af 2. april 2024 (Bilag I) oplyst at ville hjælpe med den nødvendige information og samarbejde for at besvare henvendelser fra de registrerede:

> *"Provide the data controller with the necessary information and cooperation to enable the data controller to respond to the DSRs within the prescribed time limit (usually one month, with a possibility of extension in some cases)"*

Personal Data kan være omfattet af en af datakategorierne Customer Data eller Professional Services Data, men kan også være *"data generated, derived or collected by Microsoft, including data sent to Microsoft as a result of a Customer's use of service-based capabilities or obtained by Microsoft from locally installed software*"[26]. Microsoft Irelands databehandleraftale indeholder ikke en nærmere beskrivelse af, hvornår data er genereret, afledt eller indsamlet af Microsoft Ireland.

Microsoft Danmark har desuden til brug for nærværende konsekvensanalyse ved svar af 2. april 2024 (Bilag I) side 2 ff. uddybet definition og beskrivelse af datakategorier således:

[26] Microsoft Irelands databehandleraftale, side 7, "Processing of Personal Data; GDPR".

"Microsoft describes data and activity on data or causing Microsoft's possession of data based on wording that arises, from these sources:

1) The text of the GDPR: Microsoft accepts definitions therein into the contract instruction as defined terms.
2) Where the GDPR (by design) lacks the specificity to address the scenarios that arise in Microsoft's cloud computing data categories or processing actions, or to support a commitment to customers, Microsoft defines terms in our DPA that comport to our actual handling of data within the service design and operations.

Microsoft does not define terminology in ways that redefines concepts, data types, or processing activity that the GDPR has defined.

Descriptive language arising from other sources may not align cleanly with Microsoft's taxonomy for data types and data processing arising from the GDPR. Microsoft checks for alignment of our processing activity with regulatory guidance such as may be issued from time to time by the EDPB or similar organizations.

[…]

Items in the diagram below have reference numbers applied solely for cross reference in the text of this response document. The table only addresses cloud services.

Tabel 1 Datakategorier for cloudservices (bilag I)

	Contractual Data Categories for Microsoft Cloud		
	Diagnostic Data (3)	Customer Data (1)	Service Generated Data (2)
How it comes to Microsoft possession	Microsoft software products the customer runs are instrumented to **collect** this data because the customer instructs Microsoft to keep the product secure, up to date and working as expected.	Customer **provides** this data to Microsoft for processing as per the instructions. Also, any results the cloud service computes using this provided data and returns to the customer's cloud service instance for storage and further processing is also Customer Data.	Microsoft cloud services **generate** this data in the course of their operations to provide the cloud service as instructed.
May contain GDPR personal data	**Yes**	**Yes**	**Yes**
May contain directly identifiable elements of personal information about a user	**No**	Yes, in some cloud services	**No**
May contain information the customer has provided for processing	**No.** Tokens map to customer provided user records.	Yes in 100% of cloud services	**No.** Tokens map to customer provided user records.

The data categories (1), (2) and (3) are designed to be the "entire universe" of personal data that Microsoft processes as processor to provide the cloud services to the customer.

Customer Data (1) *Any data the customer or their users provides to Microsoft during the use of the cloud services is Customer Data. This includes data entered into a cloud user experience (UX) by a user or transmitted on the customer's behalf to Microsoft by software tools or programs that the customer is running (e.g., Entra ID Connect). This category also includes any results computed from other provided data and delivered to the cloud service tenant or instance. Customer Data is the customer's Confidential Information and is subject to the strictest handling controls at Microsoft. For example, Microsoft personnel are not allowed to access this data unless necessary to provide the service as documented and contracted. Microsoft Personnel are not permitted to have standing authority to access it; any such access requires case by case authorization by Microsoft.*

Service Generated Data (2) *This data comprises records and logs generated by the cloud service. These are intentional artifacts of the cloud services' design by Microsoft. These records enable Microsoft to provide the cloud services as instructed. Our obligations include keeping the cloud service secure and auditable. To do that we need factual authoritative*

records of user actions and user triggered events in the services, all, retained for durations as required by technical necessity or applicable legal or contractual requirements.

There are no elements of provided personal information (Customer Data (1)) in this data. Since this data category is examined by engineers using tools to do their work monitoring the cloud services, then to achieve privacy by design we do not allow any personal data attributes that the customer has provided to be in records of this data type; instead, Microsoft generates pseudonymized tokens as necessary to maintain the required factual records.

***Diagnostic Data (3)** Customers can obtain software from Microsoft that works with cloud services. When they do, they instruct Microsoft to make sure when it is used it is up to date, secure, and working the way Microsoft expected. To do this Microsoft collects diagnostic data as the software works. The customer's user doesn't take any action to provide this data and this collection occurring is invisible to the user.*

Diagnostic Data only exists in a context where software is being used on premises but also cloud services (e.g., Microsoft Word opening files or saving files that are in OneDrive for Business.) Microsoft does not allow anything the customer, or their users, provides to cloud services to be in Diagnostic Data nor any of the content of the data provided to the software by the user of it (e.g., Microsoft Word document content or filename).

Customer Data (1) will contain anything a user or the customer's organization has provided to the cloud service. This includes the personal data of employees which might be uploaded to the user directory by the customer, or the personal data of other data subjects the customer's employees work with outside the organization – such as email correspondents or parties outside the organization who join a Teams call. Microsoft assumes Customer Data is personal data and leaves determining if it is or is not case by case to the customer.

Service Generated Data (2) and Diagnostic Data (3) are not permitted to hold any customer provided personal data attributes. This data is used by Microsoft engineers so it must be private by design. It only holds pointers, tokens or identifiers that reference the user associated with the activity being logged (2) or the use of the software product (3). Whenever documentation at Microsoft explains that pseudonymous personal data is being used or transferred by Microsoft, the documentation is referring to the data in these two categories.

Processing activities performed by Microsoft to provide the service to the customer do not target any specific customer. They are always performed across the body of the relevant data in the cloud services that are used by multiple customers at the same time."

Microsoft Ireland behandler også aggregerede (anonymiserede) oplysninger. Både Microsofts business operations white paper og Microsofts business operations white paper vol. 2 gælder også for den behandling, som Microsoft Ireland foretager i forbindelse med aftaleforholdet, hvor Microsoft Ireland er aftalepart. Statens It og Økonomistyrelsen kan heraf udlede, at de personoplysninger i Diagnostic Data og Systemgenererede logfiler, der anvendes til forretningsaktiviteter, er aggregerede data outputs og statistikker afhængig af det specifikke forretningsformål. Disse outputs indeholder ikke personoplysninger, heller ikke i pseudonymiseret form, og er blevet kombineret med data fra tilstrækkeligt mange dataemner, så individuelle attributter ikke længere kan henføres til en bestemt identificerbar fysisk person.[27] Oplysningerne vurderes derfor som værende anonymiseret. Til brug for nærværende konsekvensanalyse har Microsoft Danmark ligeledes ved besvarelse af den 2. april 2024 (Bilag I), side 26 til spørgsmål om, hvorvidt oplysningerne, der anvendes til forretningsformål, er anonymiseret, svaret følgende:

> *"Microsoft creates aggregated statistical, non-personal data from data containing pseudonymized identificers (such as usage logs containing unique, pseudonymized identificers) and calculates statistics related to Customer Data or Professional Services Data. All purposes for which these non-personal Business Operations data are used, are defines in the DPA [...]."*

Personoplysninger anonymiseres eller slettes som en afslutning på den databehandling, som Microsoft Ireland foretager på vegne af De Dataansvarlige i overensstemmelse med Microsoft Irelands databehandleraftale samt databeskyttelsesforordningens artikel 28, stk. 3.

4.2. Microsoft Irelands databehandleraftale

4.2.1. Anvendelsesområde

Microsoft Irelands databehandleraftale finder anvendelse ved behandling af "Customer Data", "Professional Services Data" og "Personal Data" i forbindelse med Microsoft Irelands "Products and Services" og gælder, medmindre andet specifikt er anført i relation til et specifikt "Product" eller "Service".[28]

"Product" er defineret på følgende måde i Microsoft Irelands databehandleraftale:

[27] Microsofts business operations white paper, side 11, 'Details on the data used for business operations'.

[28] Microsoft Irelands databehandleraftale, side 5, "Scope".

> *"Product" has the meaning provided in the volume license agreement. For ease of reference, "Product" includes Online Services and Software, each as defined in the volume license agreement."*

Der er ikke indgået en volume license agreement om køb af Microsoft 365-licenser forud for udarbejdelse af konsekvensanalysen, men det lægges til grund, at de i afsnit 3.43.4 omfattede cloudtjenester og applikationer – i overensstemmelse med Microsofts Product Terms i øvrigt – vil være omfattet af begreberne "Online Services" and "Software" og dermed omfattet af Microsoft Irelands databehandleraftale.

Afgrænsningen af Microsoft Irelands databehandleraftales anvendelsesområde kan illustreres på følgende måde, hvor data indeholdt i de blå bokse er defineret i databehandleraftalen, og den hvide boks vedrører Systemgenererede logfiler og Diagnostic Data, som gennemgås nedenfor i afsnit 4.34.3.

Customer Data	**Personal data**
Professional Services Data	
"Data generated, derived, or collected by Microsoft."	

4.2.2. Generelt om Microsofts behandling af data

Microsoft Irelands databehandleraftale fastlægger to hovedformål med Microsoft Irelands behandling af Customer Data, Professional Services Data og Personal Data:

> *"(a) to provide Customer the Products and Services in accordance with Customer's documented instructions and (b) for business operations incident to providing the Products and Services to Customer. […]"*

4.2.3. Generelt om behandling med henblik på at levere produkter og services

Formålet i relation til *"(a) to provide Customer the Products and Services in accordance with Customer's documented instructions"* er nærmere beskrevet i Microsoft Irelands databehandleraftale – der af Microsoft Ireland i det citerede nedenfor forkortes som "DPA" – som følger[29]:

[29] Microsoft Irelands databehandleraftale, side 6," Processing to Provide Customer the Products and Services".

"For purposes of this DPA, "to provide" a Product consists of:

- *Delivering functional capabilities as licensed, configured, and used by Customer and its users, including providing personalized user experiences;*
- *Troubleshooting (preventing, detecting, and repairing problems); and*
- *Keeping Products up to date and performant, and enhancing user productivity, reliability, efficacy, quality, and security.*

For purposes of this DPA, "to provide" Professional Services consists of:

- *Delivering the Professional Services, including providing technical support, professional planning, advice, guidance, data migration, deployment, and solution/software development services.*
- *Troubleshooting (preventing, detecting, investigating, mitigating, and repairing problems, including Security Incidents and problems identified in the Professional Services or relevant Product(s) during delivery of Professional Services); and*
- *Enhancing delivery, efficacy, quality, and security of Professional Services and the underlying Product(s) based on issues identified while providing Professional Services, including fixing software defects and otherwise keeping Products and Services up to date and performant.*

In each case, providing the Products and Services is conducted in view of security obligations under Data Protection Requirements.

When providing Products and Services, Microsoft will not use or otherwise process Customer Data, Professional Services Data, or Personal Data for: (a) user profiling, (b) advertising or similar commercial purposes, or (c) market research aimed at creating new functionalities, services, or products or any other purpose, unless such use or processing is in accordance with Customer's documented instructions."

Microsoft Danmark har ved besvarelse af den 2. april 2024 (Bilag I) side 20 suppleret denne beskrivelse med en overordnet beskrivelse af, hvilke personoplysninger om ansatte/brugere af Microsoft 365, der behandles i forbindelse med formålene, ligesom Microsoft Danmark har anført Microsoft Irelands rolle i denne sammenhæng, sådan som Microsoft opfatter det:

ID	Purpose	Is Microsoft data controller (own purposes) or data processor?	What personal data about employees
1	Delivering functional capabilities as licensed, configured, and used by Customer and its users, including providing personalized user experiences	DATA PROCESSOR	The employee personal data in the services is i) information the customer has provided to the services directory, ii) pseudonymous tokens Microsoft has recorded that index those directory entries and iii) uses of those tokens in service generated logs that log user activity or system activity related to that users actions.
2	Troubleshooting (preventing, detecting, and repairing problems)	DATA PROCESSOR	The employee personal data in the services is i) information the customer has provided to the services directory, ii) pseudonymous tokens Microsoft has recorded that index those directory entries, iii) uses of those tokens in service generated logs that log user activity or system activity related to that users actions, and iv) pseudonymous tokens in Diagnostic Data collected from on premise software that is working with the online services.
3	Keeping Products up to date and performant, and enhancing user productivity, reliability, efficacy, quality, and security	DATA PROCESSOR	The employee personal data in the services is i) information the customer has provided to the services directory, ii) pseudonymous tokens Microsoft has recorded that index those directory entries, iii) uses of those tokens in service generated logs that log user activity or system activity related to that users actions, and pseudonymous tokens in Diagnostic Data collected from on premise software that is working with the online services.

ID	Purpose	Is Microsoft data controller (own purposes) or data processor?	What personal data about employees are processed?
Appendix ID4	Delivering the Professional Services, including providing technical support, professional planning, advice, guidance, data migration, deployment, and solution/software development services	Microsoft is data processor for Professional Services Data Professional Services Data means all data, including all text, sound, video, image files, or software, that is provided to Microsoft by, or on behalf of, customers (or that customers authorize Microsoft to obtain from an Online Service) through an engagement with Microsoft to obtain Professional Services. This may include information collected over phone, chat, e-mail, or web form. It may include description of problems, files transferred to Microsoft to resolve support issues, automated troubleshooters, or by accessing customer systems remotely with customer permission.	This is determined by customer (as data controller).
Appendix ID5	Troubleshooting (preventing, detecting, investigating, mitigating, and repairing problems, including Security Incidents and problems identified in the Professional Services or relevant Product(s) during delivery of Professional Services	Same as above	Same as above
Appendix ID6	Enhancing delivery, efficacy, quality, and security of Professional Services and the underlying Product(s) based on issues identified while providing Professional Services, including fixing software defects and otherwise keeping Products and Services up to date and performant	Same as above	Same as above

Microsoft Danmark har uddybet "user activity or system activity related to that users action", herunder dataminimering og nødvendighed, ved besvarelse af 23. april 2024 (Bilag J), side 3:

"To be precise the answer is/was: "The employee personal data in the services is

1. *information the customer has provided to the services directory,*
2. *pseudonymous tokens Microsoft has recorded that index those directory entries,*
3. *uses of those tokens in service generated logs that log user activity or system activity related to that users actions, and*
4. *pseudonymous tokens in Diagnostic Data collected from on-premise software that is working with the online services."*

Therefore, as it is based on "information the customer has provided to the services directory," Microsoft cannot list the types of personal data this may include. Every customer may include different personal data in the directory. There are some attributes built into the design of online services directory that constitute the minimum set: https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/reference-connect-sync-attributes-synchronized#attributes-to-synchronize.

[…] Microsoft conducts privacy review of all new and significantly changed functionality and annually for each service regardless of changes. To that extent Microsoft "continually reviews" the personal data being processed for every relevant function whether business operation or services feature."

4.2.4. GENERELT OM BEHANDLING FOR AT UNDERSTØTTE "BUSINESS OPERATIONS"

Formålet i relation til "*(b) for business operations incident to providing the Products and Services to Customer*" er nærmere beskrevet som følger i Microsoft Irelands databehandleraftale:[30]

"For purposes of this DPA, "business operations" means the processing operations authorized by customer in this section.

Customer authorizes Microsoft:

(i.) to create aggregated statistical, non-personal data from data containing pseudonymized identifiers (such as usage logs containing unique, pseudonymized identifiers); and

(ii.) to calculate statistics related to Customer Data or Professional Services Data

[30] Microsoft Irelands databehandleraftale, side 6, "Processing for Business Operations Incident to Providing the Products and Services to Customer".

in each case without accessing or analyzing the content of Customer Data or Professional Services Data and limited to achieving the purposes below, each as incident to providing the Products and Services to Customer.

Those purposes are:

- *billing and account management;*
- *compensation such as calculating employee commissions and partner incentives;*
- *internal reporting and business modeling, such as forecasting, revenue, capacity planning, and product strategy; and*
- *financial reporting.*

When processing for these business operations, Microsoft will apply principles of data minimization and will not use or otherwise process Customer Data, Professional Services Data, or Personal Data for: (a) user profiling, (b) advertising or similar commercial purposes, or (c) any other purpose, other than for the purposes set out in this section. In addition, as with all processing under this DPA, processing for business operations remains subject to Microsoft's confidentiality obligations and commitments under Disclosure of Processed Data."

Microsoft Danmark har ved besvarelse af den 2. april 2024 (Bilag I), side 26, til spørgsmålet om, hvilke personoplysninger om ansatte/brugere der behandles, svaret "*none*" og uddybet, at Microsoft Ireland danner aggregerede statistiske ikke-personoplysninger fra "*data containing pseudonymized identifiers (such as usage logs containing unique, pseudonymized identifiers)*".

4.3. Microsofts business operations white paper

Microsoft Ireland har, som beskrevet ovenfor i afsnit 4.14.1 i Microsofts business operations white paper og Microsofts business operations white paper vol. 2, præciseret, hvilke oplysninger Microsoft Ireland bruger i forbindelse med forretningsaktiviteterne, og hvordan de behandles af Microsoft Ireland. Microsoft Ireland anmoder, indsamler eller genererer ikke data indeholdende personoplysninger udelukkende med business operations for øje[31], men aggregerer udelukkende de personoplysninger, der i forvejen er indsamlet til brug for varetagelsen af Microsoft Irelands behandling som databehandler, som nærmere beskrevet ovenfor. Der er tale om en aggregering, der indebærer anonymisering af data, jf. nærmere herom nedenfor.

[31] Microsofts business operations white paper, side 10, 'Details on the data used for business operations', 'Overview', samt side 14.

Microsoft Ireland anvender overordnet set tre typer data – herunder personoplysninger – i forbindelse med sine forretningsaktiviteter:
i) diagnostiske data (Diagnostic Data),
ii) systemgenererede logoplysninger (System-Generated Logs), samt
iii) oplysninger relateret til kundedata (Customer Data).

Der henvises i den forbindelse til Microsoft Danmarks beskrivelse af Diagnostic Data og systemgenererede logoplysninger i besvarelsen af 2. april 2024 (Bilag I), jf. også afsnit 4.1ovenfor.

Diagnostic Data er i Microsofts business operations white paper beskrevet som data, der "*may be collected from software the customer runs on premises if that software is provided as part of or in conjunction with the online service and used to obtain some or all of the online services outcomes. Diagnostic Data is collected so that Microsoft can tell the software is working as expected, up to date and operating securely*".

Systemgenererede logfiler er i Microsofts business operations white paper beskrevet som data, der "*are generated as users interact with the online services. These records, logs and data are essential to cloud operations and the services customers have instructed Microsoft to provide. They constitute a factual record of the activity of the online services on the customer's behalf and as instructed by the customer's users and administrators. Systemgenererede logfiler help Microsoft maintain quality, performance and capacity of the services*".

Diagnostic Data bliver således kun indsamlet fra desktopapplikationerne, når og hvis disse har forbindelse til en cloudtjeneste. Diagnostic Data indeholder enten ikke personoplysninger, eller også vil personoplysninger være pseudonymiseret ("pseudonymous identifiers").[32]

Microsoft Danmark har ved besvarelse af 2. april 2024 side 8 (Bilag I) uddybet dette på følgende måde:

> *"No directly identifiable info is permitted in Diagnostic Data - No email, or other human readable personal data. There are tokens/pseudonyms for the user that is logged on. Other Personal Data tokens here may include an software build or instance ID that is unique to the build, and IP addresses and other similar system information. Customer can reject optional diagnostic data systemically for all users.*
>
> *Diagnostic Data is collected from software the customer is running on their premises or run by their users. Diagnostic Data is information about the health and operating conditions of*

[32] Microsofts business operations white paper, side 9 f., 'Details on the data used for business operations'.

> *the software in question (e.g. Microsoft Word). This diagnostic data (sometimes called telemetry) is required by Microsoft policy to be de-identified with no directly identifiable information within it. The diagnostic data is collected only for the purposes of keeping the software up to date, secure and working as Microsoft expected. Some of the pseudonymous tokens may refer to items sufficiently unique as to be attributable to a specific user (e.g. MS Word installation ID) and others may clearly be pertaining to a specific user (e.g. a token that uniquely represents the authenticated user). Business operations are performed on aggregated data sets that do not contain any of these personal data tokens."*

Systemgenererede logfiler genereres derimod i forbindelse med brug af cloudtjenester og sker således inden for Microsofts sfære.

Systemgenererede logfiler indeholder en systematisk optegnelse over begivenheder/aktiviteter, der sker i cloudtjenesterne ("Microsoft cloud services"). Aktiviteterne kan genereres af mange forskellige komponenter, herunder f.eks. firewalls, styresystemer; netværksudstyr og hardware.[33]

Om formålet med at danne Systemgenererede logfiler fremgår følgende af Microsofts business operations white paper vol. 2, side 2:

> *"Logging" (the storage and processing of logs) is essential to identify, detect, respond to, and prevent operational problems, policy violations, and fraudulent activity; optimize system, network, and application performance; assist in security investigations and resilience activities; and, to comply with laws and regulations.*
>
> *Logging purposes fall into either or both of two general categories: (1) operations and system health logging – used to track events that are necessary to keep systems and services secure, performant, and up to date; and (2) audit logging – used to track significant events in the system, either for Microsoft to meet its contractual obligations to customers or as a business requirement to support customers in meeting their own independent business and regulatory requirements. The focus is on system events, not individuals.*
>
> *A given log record may be used to achieve either or both of the above purposes. Analysis and cross-reference of logs can reveal trends and patterns that may provide insights into past events (e.g., security patterns) or predictions of future events (e.g., capacity seasonality and trends)."*

[33] Microsofts business operations white paper vol. 2, side 1.

Microsoft Ireland iagttager princippet om dataminimering ved dannelse af disse logs, idet det fremgår af Microsofts business operations white paper vol. 2, at "*logs are created only when needed to achieve cloud service technical goals, such as performance, security, or audit trail outcomes.*" Systemgenererede logfiler genereres i henhold til Microsofts business operations white paper som det klare udgangspunkt i en form, hvor personoplysninger, der gør det muligt at identificere en bestemt fysisk person, erstattes med pseudonymer. Microsoft Danmark har også ved besvarelse af 2. april 2024 (Bilag I) oplyst følgende:

> *"The user personal data in the service logging maps to the record of that user that customer has put in the service.*
>
> *Engineers in Online Services have to consult system logs as part of the normal course of their duties. Because the logs need to be the factual record of user activity, the logs use a "privacy by design" approach that ensures no directly identifiable information about a user is stored in them. Engineers have no need to know this information in the normal performance of their duties. Nonetheless, the tokens substituted to reference the user activity in the log ("pseudonymization") are personal data and the remote viewing of these logs by engineers amounts to a "transfer of personal data" under the GDPR. Note that this transfer results in no permanent relocation or copy of any personal data.*
>
> *There are many services and sub-services in cloud services that together power the aggregate customer experience, and as a requirement to security all of the services create log records of activity in or by the services. Nonetheless, no personal data is permitted to be stored by Microsoft that is not necessary to the functional outcomes including effective security and audit trail of activity (ROPA, Personal Data Minimization).*
>
> *[…] inspection of the fields or record types […] requires intimate knowledge of the logging activity of each Microsoft program that records a log. The records themselves, and especially the pseudonymous tokens representing a customer user, are useless outside of the context of an engineer familiar with Microsoft service internals who is looking at a logrecord in an internal Microsoft tool. In many cases, enabling logs to be interpreted in a broader context would weaken the security posture of the service. For the European Union Data Boundary commitment, Microsoft implemented a new internal log storage solution that stores Microsoft logs at rest only within the countries of the EU and EFTA."*

Systemgenererede logfiler gennemgår dog også en efterfølgende automatiseret pseudonymiseringsproces, hvor personoplysninger, der af den ene eller anden grund ikke skulle være blevet pseudonymiseret i første

omgang, pseudonymiseres.[34] Det gælder også tilfælde, hvor en bruger ved en fejl skulle have inkluderet personoplysninger i f.eks. navn på dokumenter o.l. Dette er ligeledes uddybet af Microsoft Danmark i svar af den 2. april 2024 (Bilag I), side 9:

> *"User entered data is not permitted to be included in Diagnostic Data.*
>
> *If an end user (customer's authorized user, whether employee, contractor or other collaborator registered by the customer in the service directory) introduces personal data about a citizen into service object names (e.g., SharePoint Online list names), the names can potentially be included in Service Generated Data even when the Service Generated Data records may not contain any token that maps to the user themselves. Microsoft works continually to eliminate the use of clear text object names in service generated data and to prefer system object tokens, but technical considerations make complete avoidance impossible.*
>
> *In such scenarios, the nature of the data would not be searchable/identifiable or linked to any citizen identifier."*

Systemgenererede logfiler, der indeholder ikke-pseudonymiserede personoplysninger, behandles i henhold til Microsofts business operations white paper som Customer Data.[35]

Pseudonymiserede Systemgenererede logfiler og Diagnostic Data, der skal anvendes til forretningsaktiviteter (business operations), flyttes til Microsoft Irelands "Database Storage", som nu befinder sig inden for EU/EØS for tilfælde omfattet af EU Data Boundary.[36] Flytningen sker som oplyst på møde med Microsoft Danmark inden for Microsoft Irelands sfære og således ikke til Microsoft Corporations sfære. Det samme gør data *om* Customer Data.

Data *om* Customer Data genereres uden at tilgå eller analysere dataindholdet, men omfatter f.eks. oplysninger om mængden (datavolumen) af Customer Data.[37]

Microsoft Danmark har til brug for nærværende konsekvensanalyse desuden mundtligt uddybet, at der f.eks. genereres logs i forbindelse med, at der sendes en e-mail, logges ind m.v., og at nogle af disse logs efter den pågældende handling ikke længere er relevante og således er slettet inden for en time.

[34] Microsofts business operations white paper, side 6, 'Overview of processing in the Microsoft cloud'.

[35] Microsofts business operations white paper, side 5, 'Overview of processing in the Microsoft cloud' og Microsofts business operations white paper vol. 2, side 5.

[36] Vol. 2, side 6.

[37] Microsofts business operations white paper, side 10, 'Details on the data used for business operations'.

Efter flytningen af de relevante Diagnostiske Data og pseudonymiserede Systemgenererede logfiler til Microsofts "Database Storage", danner Microsoft Ireland aggregerede data outputs og statistikker afhængig af det specifikke forretningsformål. Disse outputs indeholder ikke personoplysninger, heller ikke i pseudonymiseret form, og er blevet kombineret med data fra tilstrækkeligt mange dataemner, så individuelle attributter ikke længere kan henføres til en bestemt identificerbar fysisk person.[38] Det medfører også, at selvom de pseudonymiserede personoplysninger, der aggregeres, ikke alle slettes efterfølgende, såfremt de stadig er relevante for De Dataansvarlige, så er de aggregerede data kombineret på en måde, der vurderes at gøre det umuligt at finde tilbage til det individ, som de i forvejen pseudonymiserede personoplysninger kommer fra (anonyme data).

Hvilket niveau, data aggregeres på, afhænger som nævnt ovenfor af formålet med behandlingen, dvs. den konkrete forretningsaktivitet (fakturering, herunder licenspartner, vurdering af brugers anvendelse af funktioner, regnskabsaflæggelse m.v. som uddybet netop nedenfor), og af den kunde, som behandlingen angår.[39]

Microsoft har til brug for udarbejdelsen af denne konsekvensanalyse henvist til en revisionserklæring af den 13. marts 2024, som revisionsvirksomheden Ernst & Young har udarbejdet til brug for det hollandske justits- og sikkerhedsministerium vedrørende brug af Teams, og hvor det er kontrolleret, at der sker en effektiv aggregering, hvorefter der er tale om anonyme data.[40] Microsoft har anført følgende herom:

> *"The Dutch Ministry of Justice and Security - Assurance report related to personal data protection as part of Legitimate Business Operations issued by Ernst & Young holds the following controls.*
>
> *CO-BO-2.1: Controls must provide reasonable assurance that essential mechanisms for the appropriate pseudonymization of personal data are defined and observed within Microsoft.*
>
> *CO-BO-3.1: Controls must provide reasonable assurance that essential mechanisms for appropriate aggregation and pseudonymization of personal data are defined and observed within Microsoft.*

[38] Microsofts business operations white paper, side 11, 'Details on the data used for business operations'.

[39] Se f.eks. Microsofts business operations white paper, side 13, 'Details on each of the four business operations'.

[40] Den fulde revisionserklæring kan findes på det hollandske justits- og sikkerhedsministeriums hjemmeside her: https://slmmicrosoftrijk.nl/wp-content/uploads/2024/04/REQ6840983-Ministry-of-Justice-and-Security-Assurance-report-LBO-13-march-2024.pdf (senest tilgået den 19. juni 2024).

Regarding aggregation and its effectiveness in discarding user level personal information as examined by EY see CO-BO-3.1

CO-BO-3.1
Controls must provide reasonable assurance that essential mechanisms for appropriate aggregation and pseudonymization of personal data are defined and observed within Microsoft.

CBO3.1

Control description

Processing operations on Customer Data and Personal data for Online Services are documented in DPIAs to enable and demonstrate Microsoft's accountability to contractual commitments in the DPA.

Test procedures

Inquired Senior Product Manager and Program Manager GRC Global to understand the process of documenting information on data processing in a DPIA and the DPIA update process.

Observed, obtained and inspected relevant parts of the DPIA for (LBO) processing to determine that processing operations are documented in the DPIA, as well as (amongst others) measures contributing to the rights of data subjects and other privacy considerations.

Observations

No exceptions noted.

CBO3.2
Control description

Microsoft performs aggregation on pseudonymized data to discard user level personal information.

Test procedures

Inquired IDEAs Senior Product Manager and IDEAs Principal Program Manager to understand the process of aggregation on pseudonymized data to discard user level personal information.

Observed, obtained and inspected the code for report building to determine pseudonymized data is aggregated into counts.

Reperformed the control to determine that the resulting report does not show pseudonymized data, only aggregated data.

Observations

No exceptions noted.

Also see CO-BO-2.1 with the control objective:

Controls must provide reasonable assurance that essential mechanisms for the appropriate pseudonymization of personal data are defined and observed within Microsoft.

For all controls CBO2.1 and CBO2.3-CBO2.6

No exceptions noted

For CBO2.2
1 exception noted - due to human error, which was however addressed."

Først efter anonymiseringen overføres de nu anonymiserede data til USA med henblik på Microsoft Irelands forretningsaktiviteter. 3.6

De fire formål til forretningsaktiviteter (business operations), der er fastlagt i Microsoft Irelands databehandleraftale, og som er gengivet ovenfor i afsnit 4.2.44.2.4 er også nærmere beskrevet i Microsofts business operations white paper:

1. I relation til "Customer Billing and Account Management"[41] behandles de aggregerede data outputs dels til at fakturere services, der forbrugsafregnes, og dels til at få et overblik over de enkelte

[41] Microsofts business operations white paper, side 13, 'Customer Billing and Account Management'.

kunders forbrug for at kunne understøtte oplyst rådgivning om forbrugsmønstre, effektiv administration af omkostninger og fremtidig omkostningsoptimering. I det omfang en kunde betaler for Microsofts services gennem en "Microsoft partner", kan Microsoft dele relevante aggregerede oplysninger med sådanne partnere med henblik på customer billing and account management. For så vidt angår De Dataansvarlige, er denne partner Crayon A/S.

2. Behandlingsaktiviteten "Compensation"[42] har til formål at beregne godtgørelse/betaling til Microsoft Irelands ansatte og partnere baseret på "usage-based metrics", der er designet til at måle, om kunderne bruger og får værdi fra købte Microsoft-produkter og -services. Microsoft Irelands business operations white paper indeholder eksempler på usage-based compensation, som f.eks. kan opgøres efter antallet af brugere, der har sendt mindst én e-mail i en given måned, eller den gennemsnitlige størrelse på en e-mail indbakke.

3. Behandling med henblik på "Microsoft Internal Reporting and Business Modelling"[43] indebærer, at Microsoft Ireland behandler og anvender aggregerede data til intern rapportering og forretningsplanlægning. Det kan f.eks. ske med henblik på at udarbejde prognoser, kapacitetsplanlægning og produktstrategi.

4. Det sidste formål med behandlingen, "Financial reporting", sker med henblik på at opfylde forpligtelser i henhold til lov (primært fra USA), f.eks. om rapportering *"to ensure the transparency and efficient functioning of markets*".

4.3.1. Særligt om Diagnostic Data

Data indsamlet fra lokalt installerede desktop-applikationer hedder i Microsofts univers "Diagnostic Data". Diagnostic Data er ikke en selvstændig kategori i Microsoft Irelands databehandleraftale, men er kendt fra Microsofts business operations white paper, som beskrevet ovenfor i afsnit 4.34.3 Diagnostic Data kan[44] indeholde Personal Data, som skal behandles i overensstemmelse med Microsoft Irelands databehandleraftale. Der findes både valgfrie og obligatoriske Diagnostic Data.

[42] Microsofts business operations white paper, side 14, ' Compensation'.

[43] Microsofts business operations white paper, side 14, 'Microsoft Internal Reporting and Business Modelling'.

[44] Microsofts hjemmeside: https://support.microsoft.com/en-gb/office/diagnostic-data-in-microsoft-365-f409137d-15d3-4803-a8ae-d26fcbfc91dd, under "note" (senest tilgået den 13. april 2026).

Om de obligatoriske skriver Microsoft Corporation følgende på sin hjemmeside[45], der ligeledes er gældende for Microsoft Ireland:

> *"Required diagnostic data is the minimum amount of data that we need to collect in order to keep the product secure, up to date, and performing as expected. For example, if a Microsoft 365 application crashes, certain details about the crash, that help us to diagnose and fix the problem, are collected."*

I den detaljerede information "*Required diagnostic data for Office*" [46] (herefter "Diagnostic Data dokumentation") uddybes denne valgmulighed. Microsoft Corporation anfører således følgende:

> *"Diagnostic data is used to keep Office secure and up-to-date, detect, diagnose and fix problems, and also make product improvements. This data doesn't include a user's name or email address, the content of the user's files, or information about apps unrelated to Office.*
>
> *This diagnostic data is collected and sent to Microsoft about Office client software running on the user's device. Some diagnostic data is required, while some diagnostic data is optional. We give you the ability to choose whether to send us required or optional diagnostic data through the use of privacy controls, such as policy settings for organizations. You can see the diagnostic data being sent to us by using the Diagnostic Data Viewer.*
>
> ***Required diagnostic data** is the minimum data necessary to help keep Office secure, up-to-date, and performing as expected on the device it's installed on.*
>
> *Required diagnostic data helps to identify problems with Office that may be related to a device or software configuration. For example, it can help determine if an Office feature crashes more frequently on a particular operating system version, with newly introduced features, or when certain Office features are disabled. Required diagnostic data helps us detect, diagnose, and fix these problems more quickly so the impact to users or organizations is reduced."*

[45] Microsofts hjemmeside: https://support.microsoft.com/en-gb/office/diagnostic-data-in-microsoft-365-f409137d-15d3-4803-a8ae-d26fcbfc91dd (senest tilgået den 13. april 2026).

[46] Microsofts hjemmeside: https://learn.microsoft.com/en-us/deployoffice/privacy/required-diagnostic-data (senest tilgået den 13. april 2026).

Listen af data, der indsamles om desktopapplikationerne og brugen heraf er lang[47] og afhænger af de konkrete applikationer, der anvendes.

Diagnostic Data omfatter f.eks. følgende:

- Information om opsætningen: Information om installerede applikationer, versioner, tilladelser og installationsstatus.
- Bruger: repræsenteret ved "pseudonymous identifier" og tenant ID
- Client/device
- Brug: Visse informationer om anvendelsen af funktionalitet i applikationerne
- Events: Visse hændelser og aktiviteter, der registreres i applikationen
- Enhedsforbindelse og konfiguration: Netværksforbindelsestilstand og enhedsindstillinger såsom hukommelse.

4.4. Audit og kontrolmuligheder

Microsoft Ireland har i Attachment 1 til Microsoft Irelands databehandleraftale fastlagt supplerende vilkår, som gælder, når Microsoft Ireland behandler Personal Data som databehandler.

Attachment 1 til Microsoft Irelands databehandleraftale fastlægger grundlæggende set, at Microsoft Ireland vil overholde de i databeskyttelsesforordningen indeholdte forpligtelser som databehandler. Som led heri fastlægger vilkårene, at Microsoft Ireland vil "*make available to Customer all information necessary to demonstrate compliance with the obligations laid down in Article 28 of the GDPR and allow for and contribute to audits, including inspections, conducted by Customer or another auditor mandated by Customer.*"

Microsoft Danmark har til brug for konsekvensanalysen oplyst, at bl.a. Microsoft Ireland anvender audit- og kontrolstandarderne SOC 1 og SOC 2 til brug for rapportering. SOC, der er en forkortelse for System and Organization Controls, er oprettet af American Institute of Certified Public Accountants (AICPA). SOC 1 vedrører finansiel rapportering, og SOC 2 vedrører cybersikkerhed og indebærer en detaljeret kontrol af sikkerhed, tilgængelighed, integritet, fortrolighed og privatliv.

[47] Se "Diagnostic Data dokumentationen" på Microsofts hjemmeside: https://learn.microsoft.com/en-us/deployoffice/privacy/required-diagnostic-data fra 6. marts 2024 (senest tilgået den 13. april 2026).

5. ROLLER I FORBINDELSE MED BEHANDLINGEN AF PERSONOPLYSNINGER

5.1. De Dataansvarliges rolle som selvstændigt dataansvarlige

I henhold til databeskyttelsesforordningens artikel 4, nr. 7, defineres den dataansvarlige som en fysisk eller juridisk person, en offentlig myndighed, en institution eller et andet organ, der alene eller sammen med andre afgør, til hvilke formål og med hvilke hjælpemidler der må foretages behandling af personoplysninger.

Den dataansvarlige har som udgangspunkt ansvaret for, at behandlingen af personoplysninger sker i overensstemmelse med reglerne i databeskyttelsesforordningen.

Der er flere aktører involveret i den behandling af personoplysninger, der finder sted ved brug af de udvalgte cloudtjenester og digitale værktøjer. Det er derfor centralt at klarlægge, hvilke parter der er ansvarlige for de forskellige dele af behandlingen.

De Dataansvarlige er hver især selvstændigt dataansvarlige for deres respektive behandling af personoplysninger ved brug af disse løsninger. Dette gælder for behandlinger, der udføres af medarbejdere under De Dataansvarliges kontrol, eksempelvis når personoplysninger modtages fra borgere eller ansatte via en digital løsning, eller når tidligere indsamlede oplysninger indtastes i systemet.

Det gælder ligeledes, når leverandøren, i dette tilfælde Microsoft Ireland – optræder som databehandler og behandler personoplysninger på vegne af den enkelte dataansvarlige.

Der foreligger ikke et fælles dataansvar mellem De Dataansvarlige. Når personoplysninger udveksles mellem medarbejdere i forskellige myndigheder via platformens funktioner, behandles oplysningerne af hver myndighed som selvstændig dataansvarlig. I sådanne tilfælde er der tale om videregivelse af oplysninger mellem separate dataansvarlige enheder.

5.2. Statens rolle som databehandler

I forbindelse med varetagelsen af adgangsstyring behandler Statens-It personoplysninger som databehandler på vegne af hver enkelt dataansvarlig. Der er indgået separate databehandleraftaler mellem Statens It og hver af de dataansvarlige myndigheder vedrørende denne behandling. Statens It varetager den tekniske drift som databehandler. De enkelte myndigheder er dataansvarlige og har ansvar for lokal forankring. Den koncernfælles DPO har rådgivet om struktur, risikokriterier og konsekvensvurdering.

5.3. Microsofts databeskyttelsesretlige rolle

Som nærmere beskrevet nedenfor er det vurderingen, at Microsoft Ireland agerer som databehandler for hver af De Dataansvarlige i det omfang, personoplysninger behandles med henblik på levering af produkter og tjenester til De Dataansvarlige.

Det er desuden vurderet, at Microsoft Ireland alene er dataansvarlig for den anonymisering af pseudonyme personoplysninger, som Microsoft selv har indsamlet eller genereret i rollen som databehandler. Microsoft betragtes derimod hverken som databehandler eller dataansvarlig efter databeskyttelsesfor-

ordningen i forhold til den efterfølgende brug af de anonymiserede oplysninger til egne forretningsaktiviteter (business operations), idet databeskyttelsesforordningens regler ikke finder anvendelse på denne brug.

5.3.1. Microsofts rolle som databehandler ved levering af produkterne og services

Det fremgår af databeskyttelsesforordningens artikel 4, nr. 8, at en databehandler, er en fysisk eller juridisk person, en offentlig myndighed, en institution eller et andet organ, der behandler personoplysninger på den dataansvarliges vegne.

Det følger af databeskyttelsesforordningens artikel 28, stk. 1, at hvis en behandling skal foretages på vegne af en dataansvarlig, benytter den dataansvarlige udelukkende databehandler, der kan stille de fornødne garantier for, at de vil gennemføre de passende tekniske og organisatoriske foranstaltninger på en sådan måde, at behandling opfylder kravene i denne forordning og sikrer beskyttelse af den registreredes rettigheder.

Det fremgår uddybende af præambelbetragtning 81 bl.a., at med henblik på at sikre overholdelse af kravene i databeskyttelsesforordningen i forbindelse med behandling, der foretages af en databehandler på vegne af den dataansvarlige, når databehandleren overdrages behandlingsaktiviteter, bør den dataansvarlige udelukkende benytte sig af databehandlere, der giver tilstrækkelige garantier, navnlig i form af ekspertise, pålidelighed og ressourcer, for implementering af tekniske og organisatoriske foranstaltninger, der opfylder kravene i denne forordning, herunder med hensyn til behandlingssikkerhed.

Det følger endvidere af databeskyttelsesforordningens artikel 28, stk. 3, 1. pkt., at en databehandlers behandling skal være reguleret af en kontrakt eller et andet retligt dokument i henhold til EU-retten eller medlemsstaternes nationale ret, der er bindende for databehandleren med hensyn til den dataansvarlige, og der fastsætter genstanden for og varigheden af behandlingen, behandlingens karakter og formål, typen af personoplysninger og kategorierne af registrerede samt den dataansvarliges forpligtelser og rettigheder.

Det følger endvidere af bestemmelsen i artikel 28, stk. 3, litra a, at kontrakten skal fastsætte navnlig, at databehandleren kun må behandle personoplysninger efter dokumenteret instruks fra den dataansvarlige, herunder for så vidt angår overførsel af personoplysninger til et tredjeland eller en international organisation, medmindre det kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som databehandleren er underlagt; i så fald underretter databehandleren den dataansvarlige om dette retlige krav inden behandling, medmindre den pågældende ret forbyder en sådan underretning af hensyn til vigtige samfundsmæssige interesser.

Videre følger det af databeskyttelsesforordningens artikel 29, at databehandleren og enhver, der udfører arbejde for den dataansvarlige eller databehandleren, og som har adgang til personoplysninger, behandler kun disse oplysninger efter instruks fra den dataansvarlige, medmindre det kræves i henhold til EU-retten eller medlemsstaternes nationale ret.

EDPB har i 2021 vedtaget retningslinjer for begreberne dataansvarlig og databehandler i databeskyttelsesforordningen.[48] Det fremgår heraf, at begreberne *dataansvarlig* og *databehandler* er funktionelle begreber, der har til formål at fordele ansvaret efter de enkelte parters faktiske roller. Dette betyder, at en parts juridiske status som enten dataansvarlig eller databehandler som udgangspunkt skal fastlægges efter partens faktiske aktiviteter i en bestemt situation i stedet for den formelle udpegelse af en aktørs rolle i f.eks. en kontrakt eller lov. Tildelingen af rollerne skal således ske på grundlag af en faktuel analyse af konstruktionen.[49] Kvalifikationen som dataansvarlig eller databehandler skal vurderes med hensyn til hver specifik databehandlingsaktivitet.[50]

Det kan af ovenstående definition af en dataansvarlig udledes, at en dataansvarlig er et organ, der udøver afgørende indflydelse med hensyn til behandlingen af de pågældende personoplysninger, herunder tager beslutning om formål (”hvorfor”) og hjælpemidler (”hvordan”).

Det fremgår af EDPB's ovennævnte retningslinjer, at det alene er den dataansvarlige, der kan træffe beslutning om formålet med behandlingen og som udgangspunkt også om *væsentlige hjælpemidler*. Dette betyder også, at en part kan kvalificeres som dataansvarlig, selvom denne ikke nødvendigvis fastlægger *ikkevæsentlige hjælpemidler*.[51]

Ved væsentlige hjælpemidler forstås hjælpemidler, der er tæt forbundet med formålet og omfanget af behandlingen samt med spørgsmålet om, hvorvidt behandlingen er lovlig, nødvendig og forholdsmæssig. Modsat vedrører ikke-væsentlige hjælpemidler mere praktiske aspekter af gennemførelsen, f.eks. valget af en bestemt type udstyr eller software eller de nærmere sikkerhedsforanstaltninger.[52] På linje hermed anføres det i den daværende Artikel 29-Gruppes udtalelse 05/2012 vedrørende cloud computing, afsnit

[48] EDPB, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 2.1, Adopted on 07 July 2021.

[49] EDPB, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 2.1, Adopted on 07 July 2021, pkt. 12.

[50] EDPB, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 2.1, Adopted on 07 July 2021, pkt. 26.

[51] EDPB, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 2.1, Adopted on 07 July 2021, pkt. 39 og 40.

[52] EDPB, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 2.1, Adopted on 07 July 2021, pkt. 40.

3.3.1, at cloud-kunden kan pålægge cloud-udbyderen opgaven med at finde metoderne og de tekniske eller organisatoriske foranstaltninger, der skal anvendes for at nå den dataansvarliges mål.[53]

Det kan af ovenstående definition af en databehandler udledes, at en databehandler er en separat enhed (set i forhold til den dataansvarlige), der behandler personoplysninger efter instruks fra den dataansvarlige og herved tjener den dataansvarliges interesser. En databehandler må ikke behandle oplysningerne på anden måde end i henhold til den dataansvarliges instruks og må ikke udføre behandling til egne formål. Den dataansvarlige kan som beskrevet dog efterlade en vis skønsmargin med hensyn til, hvordan den dataansvarliges interesser bedst kan tilgodeses, så databehandleren kan vælge de mest velegnede tekniske og organisatoriske hjælpemidler.

I almindelighed vil cloududbydere blive betragtet som databehandlere, medmindre de behandler personoplysninger til egne formål, hvormed de i så fald bliver selvstændigt dataansvarlige for denne del af behandlingen til egne formål, jf. EDPB, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 2.1, Adopted on 07 July 2021, pkt. 30 og 84, EDPB's rapport "2022 Coordinated Enforcement Action – Use of cloud-based services by the public sector", vedtaget den 17. januar 2023, s. 12 f og 19 f, samt Artikel 29-Gruppens "Opinion 05/2012 on Cloud Computing", WP 196, vedtaget den 1. juli 2012, s. 7 f.

Det fremgår derudover af databeskyttelsesforordningens artikel 28, stk. 10, at hvis en databehandler overtræder forordningen ved at fastlægge formålene med og hjælpemidlerne til behandling, anses databehandleren for at være en dataansvarlig, for så vidt angår den pågældende behandling, uden at dette berører artikel 82, 83 og 84.

I Datatilsynets afgørelse af 18. august 2022[54] i Chromebook-sagen vedrørende Helsingør Kommunes – og senere også yderligere 52 kommuners – brug af Google Chromebook i folkeskolen, vurderede Datatilsynet bl.a., at Google på flere områder agerer som selvstændig dataansvarlig. Google Chromebook-sagen omfatter Datatilsynets afgørelser af 10. september 2021, 14. juli 2022, 18. august 2022, 8. september 2022 og 30. januar 2024 vedrørende kommunernes brug af Google Chromebook og Google Workspace som led i undervisning af elever i kommunens folkeskoler.

Datatilsynet udtalte i den forbindelse følgende:

> *"Helsingør Kommune har vurderet, at Google alene optræder som databehandler, men efter Datatilsynets opfattelse agerer Google på flere områder som selvstændig dataansvarlig, der*

[53] Artikel 29-Gruppen, udtalelse 05/2012 om cloud computing, WP 196, vedtaget den 1. juli 2012.

[54] Journalnummer 2020-431-0061.

behandler personoplysninger til egne formål. Dette bygger blandt andet på, at Google ifølge kommunens materiale selv opfatter sig som dataansvarlig på en række områder.

[…]

Med andre ord genereres og indsamles der således – efter Datatilsynets opfattelse – ved elevernes og lærernes brug af Google Chromebooks og Workspace en række yderligere oplysninger, som videregives til Google med henblik på, at Google behandler disse personoplysninger til egne formål, jf. ovenfor.

[…]

Datatilsynet har herved navnlig lagt vægt på, at Helsingør Kommunes instruks til Google om alene at behandle "Customer Personal Data" til kommunens formål ikke omfatter alle de personoplysninger, der behandles ved kommunens elevers brug af Google Chromebooks og Workspace, og at der er en række personoplysninger i form af "Service Data", der indsamles og videregives til Google til brug for Googles egne formål."

Datatilsynet har ikke udtalt sig konkret om Microsofts rolle ved leveringen af Microsoft 365, men angiver i udtalelse til Region Syddanmark af 15. februar 2024, journalnummer 2023-431-0012, at det i den sammenhæng er:

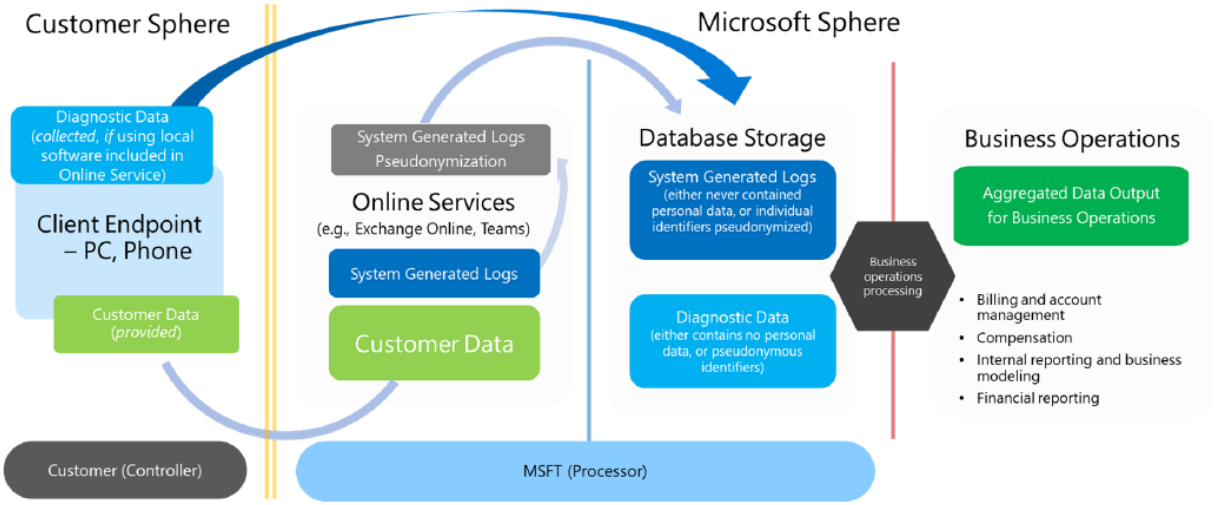
"en grundlæggende forudsætning for lovlig behandling af personoplysninger, at den dataansvarlige – i dette tilfælde Region Syddanmark – har kendskab til og har kortlagt, hvilke personoplysninger der behandles og til hvilke(t) formål.

Det omfatter bl.a. en afdækning af, om cloudserviceleverandøren – i dette tilfælde Microsoft – behandler de personoplysninger, som leverandøren får overladt, til egne formål. I bekræftende fald skal regionen vurdere, om oplysningerne kan videregives til leverandøren, og i så fald med hvilken hjemmel."

Videre fremgår følgende af samme udtalelse:

"Grundlæggende er det Datatilsynets opfattelse, at offentlige myndigheder har en vis adgang til at videregive personoplysninger til it-leverandører til brug for leverandørens egne formål. Det kan bl.a. ske med henblik på levering af tjenesten, forbedring af sikkerheden og pålideligheden af tjenesten, overholdelse af retlige forpligtelser mv."

For så vidt angår Microsoft Irelands behandling af personoplysninger som databehandler kan der indledningsvist henvises til figur 1, hvor dataflowet for behandlingen fremgår, herunder hvilke overordnede typer af personoplysninger der behandles. Figuren er gengivet igen nedenfor. Der indsamles, registreres/modtages og genereres således personoplysninger af Microsoft Ireland som databehandler, hvoraf aggregerede data senere anvendes til Microsoft Irelands forretningsformål.



Figur 2 Illustration af dataflowet for Microsoft Irelands behandling af data

Om Microsoft Irelands rolle i forbindelse med levering af produkter og services, som er beskrevet ovenfor i afsnit4.2.3 4.2.3 fremgår følgende af Microsoft Irelands databehandleraftale (Bilag C), side 7:

> *"Customer and Microsoft agree that Customer is the controller of Personal Data and Microsoft is the processor of such data, except (a) when Customer acts as a processor of Personal Data, in which case Microsoft is a subprocessor; or (b) as stated otherwise in the Product-specific terms or this DPA."*

Ved besvarelser af 2. april 2024 (Bilag I) og 6. maj 2024 (Bilag K) har Microsoft Danmark bekræftet, at Microsoft Danmark også selv anser sig for at være databehandler i forbindelse med levering af produkter og services.

Datatilsynet har ved udtalelse af 15. februar 2024 til Region Syddanmark vedrørende brug af Microsoft 365 udtalt, at regionen bl.a. skal kortlægge, afklare og vurdere følgende:

> *"Hvilke specifikke formål vil Microsoft konkret behandle oplysninger til som led i at holde "produkter opdateret og ydende samt forbedre brugernes produktivitet, pålidelighed, effektivitet, kvalitet og sikkerhed", og i hvilken rolle?"* (Vores understregning).

Det citerede formål er, som beskrevet ovenfor i afsnit 4.2.34.2.3 et af de formål, hvortil Microsoft behandler personoplysninger i forbindelse med levering af produkter, og i Microsoft Irelands databehandleraftale er Microsoft Ireland angivet som databehandler herfor.

På baggrund af Datatilsynets ovennævnte udtalelse til Region Syddanmark har Statens It og Økonomistyrelsen vurderet Microsoft Irelands databeskyttelsesretlige rolle for så vidt angår behandling af personoplysninger til dette formål om at holde produkter opdateret og ydende samt forbedre brugernes produktivitet, pålidelighed, effektivitet, kvalitet og sikkerhed, ligesom Microsoft Danmark er blevet adspurgt herom. Det samme gør sig gældende for så vidt angår formål 3 om levering af Professional Services, der rummer nogle af de samme formål (*Enhancing delivery, efficacy, quality, and security of Professional Services and the underlying Product(s) based on issues identified while providing Professional Services, including fixing software defects and otherwise keeping Products and Services up to date and performant).*

Som ovenfor nævnt er det Microsoft Danmarks opfattelse, at Microsoft Ireland er databehandler. I overensstemmelse hermed er det fortsat Statens It's og Økonomistyrelsens opfattelse, at Microsoft varetager disse formål på De Dataansvarliges vegne og efter instruks fra De Dataansvarlige, og at Microsoft Ireland således retteligt behandler personoplysninger til dette formål som databehandler for De Dataansvarlige, da det er i De Dataansvarliges interesse. Det bemærkes i den sammenhæng, at Microsoft Ireland netop ikke – som også bemærket af Datatilsynet i udtalelsen – vil

> *"bruge eller på anden vis behandle Kundedata, Data fra Professionelle ydelser eller Personoplysninger ved levering af Produkter og Tjenester i forbindelse med: (a) brugerprofilering, (b) annoncering eller lignende kommercielle eller (c) markedsundersøgelser, der har til formål at oprette nye funktioner, tjenester eller produkter eller noget andet formål, medmindre en sådan brug eller behandling er i overensstemmelse med Kundens dokumenterede instruks."*

Det bemærkes, at Datatilsynet d. 29. januar 2026 har truffet en nyere afgørelse i den såkaldte Chromebook-sag55. Afgørelsen giver anledning til skærpet opmærksomhed på navnlig krav til dokumentation af behandlingernes lovlighed, behandlingskonstruktioner og tredjelandsoverførsler. Det vurderes imidlertid, at afgørelsen ikke i sig selv ændrer det overordnede risikobillede i nærværende konsekvensanalyse.

55 Journalnummer: 2025-431-0053

Der henvises i den forbindelse til den gennemførte Transfer Impact Assessment (TIA) (bilag F) samt øvrige relevante afsnit i denne DPIA, hvor disse forhold er behandlet.

5.3.2. Microsofts rolle ved behandling af anonymiserede oplysninger til forretningsaktiviteter (business operations)

Ved behandling af Personal Data med henblik på at understøtte de forretningsmæssige formål ("*business operations incidents*"), som er beskrevet ovenfor i afsnit 4.2.45.3.2, har Microsoft Ireland i databehandleraftalen tilføjet, at Microsoft anerkender, at disse formål kan blive anset for at være til Microsoft Irelands egne formål, og Microsoft Ireland angiver derfor at ville agere som selvstændig dataansvarlig i denne sammenhæng og overholde de forpligtelser efter databeskyttelsesforordningen, der påhviler en dataansvarlig. Af Microsoft Irelands databehandleraftale (Bilag C), side 7, fremgår således følgende:

> *"To the extent Microsoft uses or otherwise processes Personal Data subject to the GDPR for business operations incident to providing the Products and Services to Customer, Microsoft will comply with the obligations of an independent data controller under GDPR for such use."*

Microsoft Ireland fastslår dermed ikke, om Microsoft Ireland er databehandler eller dataansvarlig i forbindelse med de forretningsmæssige formål, men angiver at ville overholde relevante forpligtelser som dataansvarlig. Dette skal ses i forlængelse af Microsoft Irelands tilkendegivelser i Microsoft data protection and security terms for products and services: Business operations (Bilag D), side 7, hvoraf det kan udledes, at Microsoft Ireland (og formentlig Microsoft Corporation) tidligere selv har opfattet forretningsaktiviteterne (business operations), som forenelige med det at levere tjenesten, hvilket kan indikere, at de i disse situationer betragtede (og måske stadig betragter) sig selv som databehandler, når behandlingen sker til disse formål:

> *"Microsoft previously included business operations processing in the DPA as part of Microsoft's processing data for "purposes compatible with providing" the Online Services. In response to input from customers and regulators, Microsoft replaced the "compatible purposes" with more specific information in the DPA about Microsoft's "business operations"."*

Efterfølgende angiver Microsoft Ireland at have erkendt, at andre anser Microsoft Irelands rolle i forbindelse med behandlingen til business operations som dataansvarlig, og synes således at lade det være åbent, hvordan dette ønskes tolket, men angiver samtidig på side 16, at Microsoft uanset opfattelsen heraf vil overholde de forpligtelser, der påhviler den dataansvarlige i forbindelse med behandling til forretningsmæssige formål:

> *"However, due to customer and regulatory input, we recognize some would construe this processing as operating as a controller. Thus, as applicable based on regulatory interpretation in a given jurisdiction, the processing would consist either of*
>
> *(i) Microsoft taking on controller responsibilities related to generating statistics or aggregated data from pseudonymized personal data that had previously been generated or collected to provide the service and Microsoft using that aggregated data for business operations purposes, subject to Microsoft being contractually limited to aggregating the pseudonymized personal data for the four business operations, or*
>
> *(ii) Microsoft performing the processing operation of generating statistics or aggregating the pseudonymized personal data as a processor on behalf of the customer and pursuant to the customer's instructions to generate statistics or aggregate data from pseudonymized personal data that had previously been generated or collected to provide the service for the four business operations."*

Ved vurderingen af Microsofts databeskyttelsesretlige rolle ved brug af oplysninger til forretningsaktiviteter (business operations) må der lægges vægt på, at de pseudonymiserede personoplysninger, som Microsoft har indsamlet/genereret i rollen som databehandler for De Dataansvarlige til levering af tjenesterne og services, aggregeres af Microsoft til et niveau, hvor de udgør anonyme, ikke-personhenførbare oplysninger, jf. nærmere herom afsnit 4.14.1 og 4.3 4.3 Der er med andre ord tale om, at Microsoft således ikke indsamler eller genererer pseudonyme personoplysninger *udelukkende* til varetagelse af Microsofts egne forretningsmæssige formål.

Det er omdiskuteret, hvorvidt anonymisering udgør en behandling i sig selv, som der skal være hjemmel til at foretage. Ved "behandling" forstås efter artikel 4, nr. 2, enhver aktivitet eller række af aktiviteter – med eller uden brug af automatisk behandling – som personoplysninger eller en samling af personoplysninger gøres til genstand for, f.eks. indsamling, registrering, organisering, systematisering, opbevaring, tilpasning eller ændring, genfinding, søgning, brug, videregivelse ved transmission, formidling eller enhver anden form for overladelse, sammenstilling eller samkøring, begrænsning, sletning eller tilintetgørelse.

Det anføres i Kristian Korfits Nielsen og Anders Lotterup, Databeskyttelsesforordningen og databeskyttelsesloven med kommentarer, 1. udg., DJØF Forlag, 2020, s. 253, at behandlingsbegrebet i nogle situationer bør fortolkes og anvendes med nogen smidighed for, at forordningen i praksis kan blive velfungerende. Der henvises til Peter Blume, Personoplysningsloven, 1. udg., Greens§Jura, Akademisk Forlag A/S, 2020, s. 44, hvor der argumenteres for, at den tilsvarende definition af behandlingsbegrebet i den tidligere persondatalov ikke burde omfatte det forhold, at der sker anonymisering, idet anonymisering

netop sker med det formål for øje, at der ikke længere skal være tale om en behandling af personoplysninger, som er omfattet af forordningens anvendelsesområde, jf. artikel 2, stk. 1, sammenholdt med artikel 4, nr. 1 og betragtning 26.

Heroverfor anføres det i Artikel 29-Gruppens (nu EDPB) "Opinion 05/2014 on Anonymisation Techniques", WP216, vedtaget den 10. april 2014, s. 7, at anonymisering skal anses for at udgøre en (videre)behandling af personoplysninger omfattet af det dagældende databeskyttelsesdirektiv. Smh. Christopher Kuner m.fl. (red.), The EU General Data Protection Regulation (GDPR) – A Commentary, 1. udg., Oxford University Press, 2020, s. 121.

Datatilsynet har i en sag om Region Syddanmarks påtænkte brug af Microsoft 365 udtalt følgende om spørgsmålet vedrørende anonymisering af personoplysninger ved brug af cloudtjenester[56]:

> *"Grundlæggende er det Datatilsynets opfattelse, at offentlige myndigheder har en vis adgang til at videregive personoplysninger til it-leverandører til brug for leverandørens egne formål. Det kan bl.a. ske med henblik på levering af tjenesten, forbedring af sikkerheden og pålideligheden af tjenesten, overholdelse af retlige forpligtelser mv.*
>
> *Det beror imidlertid på en vurdering af det retsgrundlag, som berettiger eller forpligter myndigheden til at udføre sine opgaver, præcist i hvilket omfang, myndigheden kan videregive personoplysninger til leverandøren. I vurderingen indgår også, hvilke oplysninger der vil blive videregivet.*
>
> *Endvidere er databeskyttelsesreglerne ikke til hinder for at videregive anonymiserede oplysninger. Det skyldes, at anonymiserede oplysninger ikke er omfattet af databeskyttelsesreglerne. Tilsvarende vil personoplysninger altid lovligt kunne anonymiseres med henblik på, at de anonymiserede oplysninger kan videreanvendes.*
>
> *I konteksten af levering af cloudservices er det afgørende, hvornår personoplysningerne anonymiseres. Der vil ikke være tale om videregivelse af personoplysninger, hvis oplysningerne anonymiseres lokalt, hvorefter det alene er de anonymiserede oplysninger, der videregives til leverandøren. Anderledes forholder det sig, hvis personoplysninger indsamles og videregives til leverandøren, hvorefter leverandøren som selvstændigt dataansvarlig vælger at anonymisere oplysningerne. I sidstnævnte tilfælde er der tale om videregivelse af personoplysninger."* (Vores understregninger.)

[56] Datatilsynets udtalelse af 15. februar 2024 vedrørende Region Syddanmarks påtænkte brug af Microsoft 365, tilsynets j.nr. 2023-431-0012.

Hvis anonymiseringen ikke anses for at være en behandling, der kræver selvstændig hjemmel, taler dette for, at den aggregering, som Microsoft Ireland foretager med henblik på at behandle de anonyme oplysninger til brug for deres egne forretningsaktiviteter, ligeledes ikke udgør en behandling, der kræver hjemmel. I så fald vil hverken Microsoft Irelands aggregering af de pseudonymiserede personoplysninger til Microsoft Irelands egne forretningsmæssige formål eller den efterfølgende behandling af de nu anonymiserede data kræve selvstændig hjemmel. Tilsvarende vil overførslen af personoplysningerne fra De Dataansvarlige til Microsoft med henblik på denne aggregering ikke indebære en videregivelse af personoplysninger, der kræver selvstændig hjemmel, idet Microsoft netop ikke har indsamlet/genereret pseudonyme personoplysninger udelukkende med det formål at varetage sine egne forretningsmæssige formål.

Hvis den aggregering af de pseudonyme personoplysninger, som Microsoft Ireland foretager, i stedet skal anses for at være en behandling af personoplysninger, der kræver selvstændig hjemmel, sker denne behandling til Microsoft Irelands formål ud fra midler fastsat af Microsoft Ireland. I så fald vil Microsoft Ireland være selvstændigt dataansvarlig for den behandling, der sker i forbindelse med aggregeringen af personoplysninger til et niveau, hvor de efterfølgende kan siges at være anonymiseret. Det vurderes i så fald, at De Dataansvarlige vil have hjemmel til at videregive personoplysningerne til Microsoft Ireland med henblik på at foretage denne anonymisering, jf. databeskyttelsesforordningens artikel 6, stk. 1, litra e, ligesom behandlingen, med det formål at anonymisere personoplysningerne, ikke er uforenelig med de oprindelige formål, som oplysningerne blev indsamlet til, jf. databeskyttelsesforordningens artikel 5, stk. 1, litra b, smh. artikel 6, stk. 4. Det vurderes endvidere, at Microsoft Ireland vil have hjemmel til at foretage aggregeringen med hjemmel i databeskyttelsesforordningens artikel 6, stk. 1, litra f. Microsofts efterfølgende behandling af de nu anonymiserede oplysninger til forretningsaktiviteter vil dog ikke medføre en rolle som dataansvarlig for Microsoft Ireland, idet der ikke (længere) er tale om personoplysninger.

Efter Økonomistyrelsens og Statens It's opfattelse er det mest rigtigt at anskue forholdet således, at selve Microsofts anonymisering af de pseudonymiserede personoplysninger udgør en elektronisk behandling af personoplysninger omfattet af databeskyttelsesforordningen. Selvom anonymiseringen fremgår af instruksen fra De Dataansvarlige til Microsoft, er der tale om en behandling, som Microsoft er dataansvarlig for, da anonymiseringen har til formål at skabe anonyme data udelukkende til brug for Microsofts egne forretningsmæssige formål. Der er dog ikke tale om en videregivelse af personoplysninger fra De Dataansvarlige til Microsoft af de pseudonymiserede personoplysninger, der kræver selvstændig hjemmel, idet Microsoft alene aggregerer pseudonymiserede personoplysninger, som Microsoft har behandlet som databehandler, således at der ikke er tale om, at Microsoft udelukkende har indsamlet de pseudonymiserede personoplysninger til egne forretningsmæssige formål. Endvidere er der ikke tale om, at Micro-

soft er dataansvarlig for den efterfølgende brug af de nu anonyme oplysninger til Microsofts forretningsmæssige formål, da der ikke er tale om personoplysninger, hvorfor databeskyttelsesforordningens regler ikke finder anvendelse for så vidt angår den efterfølgende brug af disse anonyme oplysninger.

Inddelingen i databeskyttelsesretlige roller ser herefter således ud:

Tabel II Microsofts behandling af personoplysninger til De Dataansvarliges formål ved levering af produkter og services

Microsofts behandling af personoplysninger til De Dataansvarliges formål, hvor De Dataansvarlige er dataansvarlig og Microsoft Ireland er databehandler.	
Overordnet formål	Specifikt formål
Levering af Tjeneste – produkt	1. Levering af funktionsmuligheder som licenseret, konfigureret og anvendt af Kunden og dennes brugere, herunder levering af tilpassede brugeroplevelser.
	2. Fejlfinding (forhindre, konstatere og afhjælpe problemer).
	3. Holde produkter opdateret og ydende samt forbedre brugernes produktivitet, pålidelighed, effektivitet, kvalitet og sikkerhed.
Levering af Tjeneste – service	4. Levering af de Professionelle ydelser, herunder levering af teknisk support, professionel planlægning, rådgivning, vejledning, datamigrering, udrulning og tjenester til løsnings-/softwareimplementering.
	5. Fejlfinding (forhindre, registrere, undersøge, afhjælpe og udbedre problemer), herunder Sikkerhedshændelser, og problemer der identificeres i de Professionelle ydelser eller det eller de relevante Produkter under leveringen af Professionelle ydelser.
	6. Forbedring af levering, effektivitet, kvalitet og sikkerhed af Professionelle ydelser og det eller de underliggende Produkter baseret på problemer, der er identificeret under levering af Professionelle ydelser, herunder rettelse af softwarefejl og på anden vis holde Produkter og Tjenester opdateret og ydende.

Tabel III Microsofts behandling af anonymiserede oplysninger til Microsoft Irelands egne formål

Microsoft Ireland er alene dataansvarlig for selve anonymiseringen af de pseudonyme personoplysninger, men hverken databehandler eller dataansvarlig efter databeskyttelsesforordningen for så vidt angår den efterfølgende brug af de anonymiserede oplysninger.	
Overordnet formål	Specifikt formål
Forretningsaktiviteter	7. Fakturerings- og kontoradministration.
	8. Aflønning (f.eks. beregning af medarbejderprovision og partnerincitamenter).
	9. Intern rapportering og forretningsmodellering (f.eks. udarbejdelse af prognoser, omsætning, kapacitetsplanlægning og produktstrategi).
	10. Økonomisk rapportering.

6. MICROSOFTS PLACERING AF DATA OG TREDJELANDSOVERFØRSLER

Det følger af Microsoft Irelands databehandleraftale[57], at Microsoft Ireland overfører

> "*Customer Data, Professional Services Data, and Personal Data to the United States or any other country in which Microsoft or its Subprocessors operate and to store and process Customer Data, and Personal Data to provide the Products, except as described elsewhere in the DPA Terms".*

Microsoft Irelands databehandleraftale indeholder herefter følgende undtagelser, der gælder i relation til "Core Online Services" og "EU Data Boundary Online Services":

> *"For the Core Online Services, Microsoft will store Customer Data at rest within certain major geographic areas (each, a Geo) as set forth in the Product Terms.*
>
> *For EU Data Boundary Online Services, Microsoft will store and process Customer Data and Personal Data within the European Union as set forth in the Product Terms."*

Alle cloudtjenester omfattet af konsekvensanalysen er "Core Online Services".[58]

[57] Microsoft Irelands databehandleraftale, side 9 (Bilag C), "Data Transfers and Location".

[58] Bilag B, side 20.

Alle cloudtjenester omfattet af konsekvensanalysen undtagen Exchange Online Protection er "EU Data Boundary Online Services".[59]

De installerbare skrivebordsprogrammer, der udgør en del af Microsoft 365-platformen, er ikke omfattet af begreberne "Core Online Services" eller "EU Data Boundary Online Services" og kan derfor ikke placeres inden for EU Data Boundary.
Som beskrevet i afsnit 4.3 er det dog oplyst af Microsoft Danmark, at den databaseopbevaring (Database Storage), hvortil diagnostiske data og pseudonymiserede systemgenererede logoplysninger overføres efter indsamling og generering, er placeret inden for EU/EØS – ligesom kundens Microsoft 365-tenant.

Om EU Data Boundary Services fremgår følgende af Microsoft Product Terms[60]:

> ***"Location of Customer Data for EU Data Boundary Services***
> *For EU Data Boundary Services, Microsoft will store and process Customer Data and Personal Data within the EU Data Boundary as detailed below.*
>
> *Customer must configure EU Data Boundary Services as follows:*
>
> *[…]*
>
> *For Microsoft 365, if Customer provisions a tenant in the EU or EFTA, that tenant will be in-scope for the EU Data Boundary, except for those tenants where Customer has also purchased the Microsoft 365 Multi-Geo Capabilities add-on that enables customers to expand Microsoft 365 tenant presence to multiple geographic regions or countries (*https://learn.microsoft.com/microsoft-365/enterprise/microsoft-365-multi-geo?view=o365-worldwide).
>
> *Use of EU Data Boundary Services may result in limited transfers of Customer Data or Personal Data outside the EU Data Boundary, as set forth below and further detailed in transparency documentation for the EU Data Boundary located at https://learn.microsoft.com/en-us/privacy/eudb/eu-data-boundary-learn or successor location. Any such transfers will be conducted in accordance with the Data Protection Addendum and the Product Terms."*

[59] Bilag B, side 23.

[60] Side 23 f.

Det er Statens It, der er ansvarlig for den fælles tenant for alle Statens It's kunder (De Dataansvarlige), og da placeringen heraf er inden for EU, er behandlingen ligeledes omfattet af EU Data Boundary Services. Den i Product Terms nævnte "*transparency documentation for the EU Data Boundary*" (herefter "EU Data Boundary dokumentationen"), indeholder en beskrivelse af de enkelte situationer, hvor data behandles uden for EU Data Boundary.

De overførsler af personoplysninger til tredjelande, der potentielt kan ske, beskrives og vurderes samlet i en transfer impact assessment ("TIA") for disse overførsler, der er vedlagt som Bilag F til denne konsekvensanalyse. Der henvises således hertil.

7. VURDERING AF NØDVENDIGHEDEN OG PROPORTIONALITETEN

I henhold til databeskyttelsesforordningens artikel 35, stk. 7, er det et krav, at De Dataansvarlige foretager en vurdering af lovligheden og nødvendigheden af de behandlingsaktiviteter, der udføres i de udvalgte applikationer og cloudtjenester i Microsoft 365. Dette omfatter også en vurdering af eventuelle videregivelser af personoplysninger til Microsofts egne formål.
Det skal desuden vurderes, om behandlingen står i rimeligt forhold til formålet. Formålet med vurderingen er bl.a. at sikre, at der kun behandles personoplysninger, som er nødvendige, og som er relevante i forhold til det formål, De Dataansvarlige lovligt forfølger. Behandlingen må ikke gå videre end det, der er nødvendigt for at opfylde disse formål.

7.1. De grundlæggende principper

7.1.1. Princippet om lovlighed, rimelighed og gennemsigtighed

Det fremgår af databeskyttelsesforordningens artikel 5, stk. 1, litra a, at personoplysninger skal behandles lovligt, rimeligt og på en gennemsigtig måde i forhold til den registrerede.

Princippet om lovlighed har en nær sammenhæng med kravet om behandlingshjemmel i databeskyttelsesforordningen. Det følger således heraf, at De Dataansvarlige kan indsamle og behandle personoplysninger om de registrerede, hvis de har hjemmel til det. Der skal være hjemmel til behandling til alle de formål, som De Dataansvarlige behandler personoplysninger til. Det samme gælder den behandling, databehandleren foretager på vegne af De Dataansvarlige ved levering af tjenesterne og services i Microsoft 365. Eventuelle videregivelser af personoplysninger til Microsofts egne formål kræver endvidere hjemmel.

I forhold til særligt offentlige myndigheder uddybes dette af Datatilsynet i afgørelse af 30. januar 2024, hvor tilsynet gav påbud i den såkaldte Google Chromebook-sag[61]:

> *"Princippet om lovlighed i forvaltningen (legalitetsprincippet) indebærer, at en offentlig myndigheds afgørelser og forvaltning i øvrigt skal have støtte i lov eller andet retsgrundlag.*
>
> *Når det gælder databeskyttelsesreglerne, indebærer dette princip, at offentlige myndigheder – foruden at sikre, at myndighedernes egen opgaveløsning sker i overensstemmelse med databeskyttelsesreglerne – også skal sikre, at de it-løsninger, som myndighederne beslutter at bruge til at understøtte myndighedernes opgaveløsning, ligger inden for rammerne af de databeskyttelsesretlige regler.*
>
> *Offentlige myndigheder skal derfor sikre sig og træffe foranstaltninger med henblik på, at myndighederne ikke designer, udvikler eller anskaffer og tager løsninger i brug, som ikke overholder databeskyttelsesreglerne. Det kan bl.a. ske ved, at myndigheder i deres anskaffelsesprocedurer og projektmodeller fastsætter relevante krav, der sikrer anskaffelse eller udvikling af løsninger i overensstemmelse med databeskyttelsesreglerne. Omfanget af disse krav kan efter Datatilsynets opfattelse variere under hensyntagen til karakteren, omfanget og formålet med den behandlingsaktivitet, som løsningen skal understøtte, samt de risici for borgerne, der kan være forbundet med brug af løsningen. Under alle omstændigheder skal disse krav bestå af mere end blot et enkelt krav til leverandøren om, at løsningen skal overholde databeskyttelsesreglerne. Kravene kan f.eks. afspejle de foranstaltninger, som myndigheden har vurderet, at det er nødvendigt at træffe på baggrund af sin risikovurdering eller konsekvensanalyse for at sikre løsningens lovlighed.*
>
> *Endelig bemærker Datatilsynet, at funktionaliteten af de løsninger, der ønskes anvendt, eller markedspositionen af den leverandør, der ønskes valgt, ikke kan begrunde en manglende overholdelse af databeskyttelsesreglerne. En standardiseret opbygning af løsningerne eller den blotte anvendelse af et standardprodukt kan ligeledes ikke begrunde en manglende overholdelse af databeskyttelsesreglerne."*

Nedenfor i afsnit 7.2.27.2 vil hjemmelsgrundlag for De Dataansvarliges behandling af personoplysninger ved brug af Microsoft 365 blive vurderet. Ligeledes vurderes hjemmelsgrundlag for en eventuel videregivelse af personoplysninger til Microsoft som selvstændig dataansvarlig til Microsofts egne formål i afsnit 7.2.37.2.2.

[61] Journalnummer 2023-431-0001.

I kravet om rimelighed ligger navnlig, at det skal sikres, at der ikke sker forskelsbehandling, at behandlingen er proportional, at behandlingen er forventelig for den registrerede, at den registreredes interesser i, at dennes personoplysninger ikke behandles, ikke overstiger behandlingens formål m.v.

De Dataansvarlige behandler hovedsageligt personoplysninger om ansatte i forbindelse med personaleadministration og om borgere samt brugere af systemerne (ansatte) som led i de lovbestemte opgaver, som de varetager, og i den sammenhæng også om pårørende, værger, konsulenter samt kollegaer indenfor og udenfor samme organisation.

De Dataansvarlige skal selv supplere nærværende konsekvensanalyse med en vurdering af, om der sker en lovlig, rimelig og gennemsigtig behandling af ansatte og borgeres personoplysninger, når De Dataansvarlige behandler personoplysninger til varetagelse af deres respektive sagsbehandling og personaleadministration. Til brug for denne paraply-konsekvensanalyse lægges det således til grund, at De Dataansvarliges behandling af personoplysninger er lovlig, rimelig og gennemsigtig.

Microsoft Irelands behandling af personoplysninger – herunder Diagnostic Data, systemgenererede logfiler og personoplysninger, som enten indtastes af brugerne eller genereres under brug – foretages primært automatisk i systemet og er ensartet for alle registrerede.
Ifølge Microsoft Danmarks svar af 2. april 2024 (Bilag I, side 4), sker denne behandling på tværs af kunder og er derfor typisk ikke knyttet til en enkelt kunde, men gennemføres ens for flere kunder.
:

> *"Processing activities performed by Microsoft to provide the service to the customer do not target any specific customer. They are always performed across the body of the relevant data in the cloud services that are used by multiple customers at the same time."*

Dette gælder også i forbindelse med sikkerhed, hvor behandlinger indledningsvist sker automatisk. Der fremgår således følgende af EU Data Boundary dokumentationen:

> *"We design our services and processes to maximize the ability of DevOps personnel to operate the services without requiring access to Customer Data, employing automated tooling to identify and repair issues. In rare cases when a service is down or in need of a repair that can't be effectuated with automated tooling, authorized Microsoft personnel may require remote access to data stored within the EU Data Boundary, including Customer Data."*

Når der er behov for, at en ingeniør ser nærmere på en sikkerhedshændelse, tilgår ingeniørerne dette på samme måde for alle kunder afhængig af problemet i overensstemmelse med deres arbejdsopgaver, sådan som det også fremgår af Microsoft Danmarks svar af 2. april 2024 (Bilag I), side 7:

> *"Engineers in Online Services have to consult system logs as part of the normal course of their duties."*

Endelig instrueres supportere også i at behandle personoplysninger i overensstemmelse med en brugers anmodning om support, og også dette sker således ens for alle registrerede, idet behandlingen sker ud fra brugerens anmodning.

Der er desuden en rimelighed i omfanget af behandling, idet Microsoft Danmark den 2. april 2024 (Bilag I), s. 12 har svaret:

> *"Frequency of transfers of pseudonymized "system-generated logs" and "Diagnostic Data" is proportional to the customer's extent and frequency of use of the Microsoft 365 Online Services and cannot be quantified in the manner requested. The EU Data Boundary documentation provides guidance on the circumstances that can trigger a transfer to occur."*

På denne baggrund vurderes De Dataansvarliges behandling af personoplysninger i forbindelse med anvendelsen af de udvalgte applikationer og cloudtjenester i Microsoft 365 for at være rimelig, jf. databeskyttelsesforordningens artikel 5, stk. 1, litra a.

I kravet om gennemsigtighed ligger ifølge databeskyttelsesforordningens præambelbetragtning 39 bl.a., at "*det bør være gennemsigtigt for de pågældende fysiske personer, at personoplysninger, der vedrører dem, indsamles, anvendes, tilgås eller på anden vis behandles, og i hvilket omfang personoplysningerne behandles eller vil blive behandlet*". Princippet handler især om, at den dataansvarlige skal informere den registrerede om, hvordan deres personoplysninger behandles. Det sker gennem opfyldelse af oplysningspligten i artikel 13 og 14 og ved at give den registrerede adgang til sine oplysninger, som beskrevet i artikel 15 om indsigt.

Det må i dag anses for almindeligt og forventeligt for både borgere og ansatte i Danmark, at deres personoplysninger behandles digitalt i forbindelse med offentlige myndigheders lovbestemte opgaver, herunder sagsbehandling og personaleadministration. Denne behandling foregår typisk ved brug af værktøjer og cloudtjenester inden for Microsoft 365-platformen.
Tilsvarende er det forventeligt for systembrugere, at der i forbindelse med brugen af Microsoft 365 indsamles systemgenererede personoplysninger, såsom diagnostiske data og logoplysninger, der dokumenterer, hvordan brugeren interagerer med systemet. I et vist omfang anvender brugerne selv disse oplysninger som en del af deres arbejde – eksempelvis for at få indsigt i dokumentaktivitet, herunder hvem der sidst har redigeret et dokument, og hvornår.

Det anses også for almindelig viden, at et vist indblik i systemanvendelsen er nødvendigt for at kunne yde brugersupport, foretage fejlsøgning og håndtere sikkerhedshændelser. Tekniske foranstaltninger som logning og overvågning anses i dag som væsentlige elementer i beskyttelsen af personoplysninger og som en integreret del af informationssikkerheden i løsninger som Microsoft 365.
De Dataansvarlige har desuden interne retningslinjer og procedurer for håndtering af oplysningspligten og anmodninger om indsigt fra registrerede, hvilket De Dataansvarlige selv supplerer nærværende konsekvensanalyse med oplysninger om. Se endvidere om varetagelsen af de registreredes rettigheder og oplysningspligten nedenfor.

Det vurderes på baggrund af ovenstående samt nedenstående gennemgang af hjemmelsgrundlag, at De Dataansvarlige lever op til kravet om lovlighed, rimelighed og gennemsigtighed ved behandlingen af personoplysninger i forbindelse med de udvalgte applikationer og cloudtjenester i Microsoft 365.

7.1.2. Princippet om formålsbegrænsning

Personoplysninger skal efter databeskyttelsesforordningens artikel 5, stk. 1, litra b, indsamles til udtrykkeligt angivne og legitime formål og må ikke viderebehandles på en måde, der er uforenelig med disse formål; viderebehandling til arkivformål i samfundets interesse, til videnskabelige eller historiske forskningsformål eller til statistiske formål i overensstemmelse med artikel 89, stk. 1, skal ikke anses for at være uforenelige med de oprindelige formål ("formålsbegrænsning").

Som nærmere beskrevet i afsnit 3.67.3.2 er formålet med De Dataansvarliges behandling af personoplysninger omfattet af denne konsekvensanalyse at efterleve de lovbestemte opgaver, som hver af De Dataansvarlige har, herunder sagsbehandling og personaleadministration. Det er antaget, at De Dataansvarlige kun indsamler, behandler og opbevarer de personoplysninger, der er nødvendige for varetagelsen af de pålagte opgaver, der er fastsat for hver af De Dataansvarlige, og i overensstemmelse med de forvaltningsretlige principper der gælder for offentlige myndigheder, herunder journaliserings- og notatpligten samt officialprincippet. De Dataansvarlige supplerer selv nærværende konsekvensanalyse med en vurdering heraf, herunder til hvilke konkrete formål, der kan behandles personoplysninger efter de lovbestemte opgaver, samt en vurdering af at der ikke foretages en behandling af personoplysninger til formål, der er uforenelige med de oprindelige formål i form af de lovbestemte opgaver.

De lovbestemte opgaver udføres i almindelighed i dag af alle De Dataansvarlige ved brug af it, hvilket også er den strategi, der bl.a. er lagt i forbindelse med den fællesoffentlige digitaliseringsstrategi. Til varetagelse af De Dataansvarliges formål til sagsbehandling og personaleadministration foretager cloudleverandøren, Microsoft, levering af tjenesteydelser og services. De Dataansvarlige behandler derfor også personoplysninger, som brugerne indtaster og som genereres af Microsoft ved brugernes interaktion,

samt til håndtering af sikkerhedshændelser, sikre en høj sikkerhed, yde support samt sikre at applikationer og cloudtjenester fungerer i overensstemmelse med den ønskede konfiguration samt uden fejl. Disse formål har en sådan tilknytning til kerneformålet – opfyldelse af en myndighedsopgave – at de må anses for at være nødvendige til opfyldelse heraf, uagtet at visse aktiviteter kan betragtes som værende assessoriske, f.eks. håndtering af sikkerhedshændelse eller support. Det er således vurderingen, at behandlingen er en del af De Dataansvarliges oprindelige formål og tæt knyttet hertil.

Det er i Microsoft Irelands databehandleraftale, side 6, konkret fastsat, til hvilke formål Microsoft Ireland som databehandler for De Dataansvarlige må behandle personoplysninger:

> *"For purposes of this DPA, "to provide" a Product consists of:*
> - *Delivering functional capabilities as licensed, configured, and used by Customer and its users, including providing personalized user experiences;*
> - *Troubleshooting (preventing, detecting, and repairing problems); and*
> - *Keeping Products up to date and performant, and enhancing user productivity, reliability, efficacy, quality, and security.*
>
> *For purposes of this DPA, "to provide" Professional Services consists of:*
> - *Delivering the Professional Services, including providing technical support, professional planning, advice, guidance, data migration, deployment, and solution/software development services.*
> - *Troubleshooting (preventing, detecting, investigating, mitigating, and repairing problems, including Security Incidents and problems identified in the Professional Services or relevant Product(s) during delivery of Professional Services); and*
> - *Enhancing delivery, efficacy, quality, and security of Professional Services and the underlying Product(s) based on issues identified while providing Professional Services, including fixing software defects and otherwise keeping Products and Services up to date and performant."*

I forlængelse heraf er det desuden fastsat, til hvilke formål Microsoft ikke må behandle personoplysninger:

> *"When providing Products and Services, Microsoft will not use or otherwise process Customer Data, Professional Services Data, or Personal Data for: (a) user profiling, (b) advertising or similar commercial purposes, or (c) market research aimed at creating new functionalities, services, or products or any other purpose, unless such use or processing is in accordance with Customer's documented instructions."*

Microsoft Danmark har på et møde, som blev afholdt i tilknytning til udarbejdelse af nærværende konsekvensanalyse, oplyst, at Microsoft ved opbygningen af deres services har vurderet, hvilke behandlinger

der er relevante at foretage for at kunne levere deres ydelser, herunder applikationer og cloudtjenester i Microsoft 365, som databehandler. I svar af 6. maj 2024 (Bilag K), side 3, har Microsoft uddybet følgende:

> *"Microsoft conducts privacy review of all new and significantly changed functionality and annually for each service regardless of changes. To that extent Microsoft "continually reviews" the personal data being processed for every relevant function whether business operation or services feature."*

Ud fra en vurdering af de behandlinger af personoplysninger – dvs. undtaget er behandling af oplysninger der ikke er personoplysninger – som Microsoft Corporation har vurderet nødvendige i relation til deres forpligtelser som databehandler og levering af de aftalte ydelser, er behandlingerne blevet grupperet til varetagelse af ovenstående formål. Herved sikres det, at de behandlinger, der vedrører personoplysninger, udelukkende sker til disse formål, sådan at der ikke sker en behandling til øvrige formål. Microsoft har herefter vurderet, hvilke data, herunder personoplysninger, der til brug herfor vil være relevante at indsamle for at kunne varetage disse formål som databehandler. Hvilke behandlinger, der foretages i forbindelse med den enkelte bruger og registreret, og hvilke personoplysninger der i den forbindelse indsamles, registreres og genereres, afhænger af den interaktion der sker, og de handlinger en bruger foretager ved anvendelse af applikationer og cloudtjenester.

EDPS har i afgørelse af den 8. marts 2024 udtalt, at når det ikke er muligt at foretage en udtømmende datamapning af foretagne logs, vil det heller ikke være muligt at fastsætte, præcist hvilke formål disse personoplysninger behandles til og i den forbindelse vurdere, om princippet om formålsbegrænsning er opfyldt.

Microsoft Danmark har i forlængelse heraf oplyst, at systemerne, og de behandlinger der udføres heri eller i tilknytning hertil, løbende ændrer sig. Det betyder ifølge Microsoft Danmark, at de konkrete behandlinger og relevante datapunkter løbende ændrer sig, og at det således vil være en umulig eller uforholdsmæssig opgave at fastsætte præcis hvilke data, herunder personoplysninger, der indsamles, da en sådan liste hurtigt bliver forældet. Samtidig må der henses til, at en sådan datamapning heller ikke er i de registreredes interesse, så længe de registrerede orienteres om, at alle deres handlinger foretaget i systemerne logges, og de foretagne logs regelmæssigt gennemgås. Dette skyldes, at oplysninger om, hvilke logs der foretages, herunder hvilke logs der undlades, vurderes at skabe en sårbarhed, som ellers ikke vil være til stede. Dette er ikke i de registreredes interesse. Hvis angribere ved præcis, hvilke aktiviteter der logges, og hvilke der ikke logges, kan de tilpasse deres angrebsmetoder til at undgå at blive opdaget. For eksempel kan de undgå bestemte handlinger eller bruge teknikker, der ikke genererer logposter. Angribere kan udnytte kendte logningshuller eller svagheder i logningens dækning. Hvis de ved, at bestemte typer af aktiviteter ikke logges, kan de målrette deres angreb mod disse områder. Hvis det

bliver kendt, at logning kun sker på bestemte tidspunkter eller intervaller, kan angribere forsøge at udføre deres aktiviteter uden for disse tidsvinduer. Med viden om logningsmetoderne kan angribere forsøge at manipulere eller slette logdata for at dække deres spor. De kan også prøve at indsætte falske logposter for at skabe forvirring eller skjule deres aktiviteter.

Det vurderes derfor både at være i de registreredes og De Dataansvarliges interesse – og i overensstemmelse med pligten til at fastsætte passende sikkerhedsforanstaltninger efter databeskyttelsesforordningens artikel 32 – at der ikke søges eller offentliggøres detaljer om Microsofts logningsstrategier og -kapaciteter. Kun de medarbejdere hos Microsoft, der har et behov for at kende disse oplysninger (f.eks. sikkerhedsteams), bør have adgang til dem. Det vurderes derfor, at detaljer om den præcise logning, der foretages, vil udgøre en sikkerhedsrisiko ved at give angribere værdifuld information til at omgå sikkerhedsforanstaltninger.

Behandlinger af personoplysninger vil dog altid ske til de formål, der er aftalt med De Dataansvarlige og fremgår af Microsoft Irelands databehandleraftale, som vurderes at være de overordnede formål, der er nødvendige til levering af ydelserne. Som nævnt i det citerede netop ovenfor evaluerer Microsoft løbende herpå.

Som beskrevet ovenfor i afsnit 4.14.34.1, 4.3 og 5.3.25.3.2 vurderes det, at der heller ikke sker en videregivelse af personoplysninger, som Microsoft behandler til brug for levering af ydelserne, til Microsoft med henblik på en behandling heraf til Microsofts egne forretningsmæssige formål (business operations). Som det er udførligt gennemgået i afsnit 5.3.25.3.2 vurderes det, at selve Microsofts anonymisering af de pseudonymiserede personoplysninger, som Microsoft har indsamlet/genereret som databehandler, udgør en elektronisk behandling af personoplysninger omfattet af databeskyttelsesforordningen. Selvom anonymiseringen fremgår af instruksen fra De Dataansvarlige til Microsoft, er der tale om en behandling, som Microsoft er dataansvarlig for, da anonymiseringen har til formål at skabe anonyme data udelukkende til brug for Microsofts egne forretningsmæssige formål. Der er dog ikke tale om en videregivelse af personoplysninger fra De Dataansvarlige til Microsoft af de pseudonymiserede personoplysninger, der kræver selvstændig hjemmel, idet Microsoft alene aggregerer pseudonymiserede personoplysninger, som Microsoft har behandlet som databehandler, således at der ikke er tale om, at Microsoft udelukkende har indsamlet de pseudonymiserede personoplysninger til egne forretningsmæssige formål. Endvidere er der ikke tale om, at Microsoft er dataansvarlig for den efterfølgende brug af de nu anonyme oplysninger til Microsofts forretningsmæssige formål, da der ikke er tale om personoplysninger, hvorfor databeskyttelsesforordningens regler ikke finder anvendelse for så vidt angår den efterfølgende brug af disse anonyme oplysninger.

Hvis det måtte lægges til grund, at der er tale om behandling af personoplysninger til Microsofts forretningsaktiviteter – og hvis det måtte lægges til grund, at oplysningerne anvendt til Microsofts egne forretningsmæssige formål ikke er tilstrækkeligt anonymiseret og dermed udgør personoplysninger – vurderes det, at også disse forretningsmæssige formål er tilstrækkeligt konkret angivet, og at der således ikke behandles personoplysninger til yderligere formål end følgende:

- *billing and account management;*
- *compensation such as calculating employee commissions and partner incentives;*
- *internal reporting and business modeling, such as forecasting, revenue, capacity planning, and product strategy; and*
- *financial reporting.*

For at kunne levere det af Microsoft Ireland bestilte, anvendes oplysningerne således også til, at Microsoft kan fakturere for ydelserne og holde regnskab, herunder af lovgivningsmæssige grunde. Desuden anvendes oplysningerne til at beregne den korrekte lønning af Microsoft Irelands egne medarbejdere på baggrund af de solgte ydelser og anvendelsen heraf. Behandlingen hos Microsoft Ireland sker efter det af Microsoft Danmark oplyste ved, at Microsoft Ireland på baggrund af pseudonymiserede personoplysninger, f.eks. brugerlogs med unikke pseudonymiserede identifikationsnumre, skaber aggregerede, statistiske datasæt med henblik på varetagelse af de beskrevne formål. Denne behandling har nær forbindelse til De Dataansvarliges formål med behandling af personoplysninger i de udvalgte applikationer og clouddtjenester i Microsoft 365, idet det uden denne behandling hverken er muligt for De Dataansvarlige at købe de nødvendige produkter og services hos Microsoft eller muligt for Microsoft at levere disse produkter og services uden at kunne behandle udvalgte oplysninger til fakturering, beregning af medarbejderkommission, intern afrapportering og planlægning, herunder kapacitetsplanlægning, og finansiel afrapportering. Tilsvarende gælder de data, som Microsoft anvender til at forbedre produkterne for kunderne. Microsoft har endvidere i Microsoft Irelands databehandleraftale anført følgende:

> *"When processing for these business operations, Microsoft will apply principles of data minimization and will not use or otherwise process Customer Data, Professional Services Data, or Personal Data for: (a) user profiling, (b) advertising or similar commercial purposes, or (c) any other purpose, other than for the purposes set out in this section. In addition, as with all processing under this DPA, processing for business operations remains subject to Microsoft's confidentiality obligations and commitments under Disclosure of Processed Data."*

Det vurderes således endvidere, at Microsofts behandling af personoplysninger i så fald ville være forenelige med de oprindelige formål, som oplysningerne er indsamlet til, jf. databeskyttelsesforordningens artikel 6, stk. 4, jf. artikel 5, stk. 1, litra b.

7.1.3. Princippet om dataminimering

Personoplysninger skal være tilstrækkelige, relevante og begrænsede til, hvad der er nødvendigt i forhold til de formål, hvortil de behandles (dataminimering), jf. databeskyttelsesforordningens artikel 5, stk. 1, litra c.

De dataansvarlige supplerer denne paraply-konsekvensanalyse med en konkret vurdering af dataminimeringsprincippet. Det indebærer, at der alene må indsamles, behandles og opbevares personoplysninger, som er nødvendige og relevante i forhold til det formål, de er indsamlet til, herunder også med henblik på at overholde forvaltningsretlige principper.

Som led i denne vurdering kan De Dataansvarlige også fastsætte interne foranstaltninger, f.eks. retningslinjer for, hvilke typer personoplysninger der må indsamles, registreres, beriges og opbevares i forbindelse med sagsbehandling og personaleadministration. Det kan herunder også være relevant at afgrænse, hvilke oplysninger der ikke må anvendes i løsninger som Teams og Outlook.
I relation til den behandling af personoplysninger, som Microsoft Ireland foretager som databehandler på vegne af De Dataansvarlige, sikres overholdelse af dataminimeringsprincippet bl.a. ved dannelse af f systemgenererede logoplysninger, da det fremgår af Microsofts business operations white paper vol. 2, at

> "*logs are created only when needed to achieve cloud service technical goals, such as performance, security, or audit trail outcomes."*

Som beskrevet ovenfor i afsnit 7.1.27.1.2 gennemgår Microsoft Ireland også løbende relevansen af de behandlinger, der udføres, og data der indsamles, ligesom

> *"Microsoft conducts privacy review of all new and significantly changed functionality and annually for each service regardless of changes. To that extent Microsoft "continually reviews" the personal data being processed for every relevant function whether business operation or services feature."*

Der henvises i øvrigt til beskrivelsen ovenfor i afsnit 7.1.27.1.2, for så vidt angår indblik i de personoplysninger der behandles og begrænsningen heraf til relevante formål og behandlinger.

Det fremgår af EDPS' afgørelse af den 8. marts 2024 vedrørende EU-Kommissionens brug af Microsoft 365, at "*it is not necessary to specify individual datasets, but rather the types of personal data processed*", jf. afgørelsens punkt 48. Det er dog af Microsoft Ireland oplyst, at det ikke er muligt at angive præcist de mange typer af personoplysninger, der indgår i systemgenererede logoplysninger , da det netop vedrører

mange personoplysninger, som også er under konstant udvikling og ændring alt efter behovet og formålet med behandlingen. Når det således vurderes, at en oplysning ikke længere er relevant i henhold til de formål, hvortil den behandles, så indsamles denne personoplysning ikke længere, hvorefter listen over de personoplysninger, der konkret indsamles, ligeledes skal ændres. Det kan sammenlignes med videoovervågning, hvor man også søger at optage alt, der sker inden for vinklen, for senere at kunne bruge dette fuldt ud i en evt. efterfølgende vurdering. Der optages således også oplysninger, der i nogle sammenhænge ender med ikke at være relevante og i andre kan være altafgørende. Det er således ikke på forhånd muligt at vide, hvad der vil blive optaget og fremgå af videoovervågning, da det afhænger af det, der sker. Det samme gør sig gældende for så vidt angår de systemgenererede logs og diagnostiske data, både for så vidt angår hvilke logs og data der indsamles og genereres, hvilket afhænger af de individuelle brugeres handlinger og brug af systemet, ligesom det ikke på forhånd er til at vide, hvilke oplysninger der senere vil være relevante i forbindelse med f.eks. en sikkerhedshændelse. Det er ligeledes oplyst af Microsoft i forbindelse med konsekvensanalysen, at *"This data is only generated in proportion to the activity of users in the cloud service."* Indsamler man færre oplysninger, risikerer man at gå på kompromis med sikkerheden, da det kan være, at en afgørende oplysning så ikke er tilgængelig.

Det er i den sammenhæng Statens It's og Økonomistyrelsens opfattelse, at der kan trækkes en parallel til EDPB's retningslinjer for så vidt angår videoovervågning[62]. I anbefalingerne fremhæves det for så vidt angår personoplysninger, at der bør ske en dataminimering i form af overvejelse af, hvor lang tid det er nødvendigt at opbevare optagelserne. Herudover er det særligt relevant at fastsætte formålet med overvågningen og se på den sammenhæng, som videoovervågningen foretages i, herunder om de registrerede må forvente overvågning (f.eks. ikke på toiletter) samt omfanget heraf, og hvilke typer af personoplysninger der forventes at indgå i videoovervågningen (f.eks. oplysninger om strafbare forhold eller følsomme personoplysninger). Der er ingen anbefaling til at oplyse alle de typer af personoplysninger, der forventes at kunne blive fanget af videoovervågningen.

Selvom der ved brug af Microsoft 365 foretages en betydelig logning, hvor brugernes handlinger i alt væsentligt registreres og gemmes, vurderes det i de registreredes interesse, at denne logning foretages, da logningen bl.a. er begrundet i systemernes sikkerhed, jf. herved også pligten til at fastsætte fornødne tekniske sikkerhedsforanstaltninger efter databeskyttelsesforordningens artikel 32. Som offentlige myndigheder vil der forventeligt være betydelige trusler rettet mod de systemer, som myndighederne anvender til deres sagsbehandling, jf. Center for Cyber-sikkerheds trusselsvurdering af cyber-truslen mod Danmark af 8. maj 2023.[63] Én af de væsentligste foranstaltninger til at forøge sikkerheden for de registrerede er logning af samtlige handlinger i de systemer, som anvendes (Detect, Prevent, Response).

[62] EDPB: Guidelines 3/2019 on processing of personal data through video devices, version 2.0, vedtaget den 29. januar 2020.

[63] Fra CFCS' hjemmeside her: https://www.cfcs.dk/da/cybertruslen/trusselsvurderinger/cybertruslen-mod-danmark/ (senest tilgået den 23. maj 2024).

Detaljeret logning muliggør overvågning af alle aktiviteter i systemet, hvilket giver Microsoft Irelands sikkerhedsteams mulighed for at identificere anomalier og mistænkelige mønstre tidligt. Dette er essentielt for at opdage potentielle sikkerhedstrusler, før de eskalerer til alvorlige hændelser. Med flere data kan sikkerhedsteams opdage subtile angrebsmønstre og anomalier, der ellers kunne være gået ubemærket hen.

Når en sikkerhedshændelse opstår, giver dybdegående logdata Microsoft Irelands sikkerhedsteams de nødvendige informationer til hurtigt at forstå og reagere på truslen. Med detaljerede logs kan man hurtigt spore hændelsens kilde, vurdere omfanget af kompromitteringen, og implementere afbødende foranstaltninger for at forhindre yderligere skader.

I tilfælde af en sikkerhedshændelse, der fører til databrud, kan detaljerede logs tjene som afgørende bevismateriale for de dataansvarlige. De giver et nøjagtigt og uforanderligt spor af hændelser, som kan bruges til at underbygge hændelsesforløbet.

Ønsket om detaljeret logning er understøttet af gængse internationale standarder på området, herunder NIST CSF, sektion "DE.AE-3: Event Data are Collected", ISO 27001 Annex A.12.4 (Logging and monitoring) og CIS Control 6 (Maintenance, Monitoring, and Analysis of Audit Logs).

Samlet vurderes det derfor, at risikoen for de registrerede mindskes, når alle handlinger i de anvendte systemer logges.

Microsoft Danmark har tillige i svar af 2. april 2024 (Bilag I), side 4, oplyst, at:

> *"[…] customers can realize the attributes applicable to this data [(Diagnostic Data and Systemgenererede logfiler)]:*
>
> > *A) It is generated and used only to provide outcomes Microsoft is instructed to provide."*

Microsoft Danmark har desuden oplyst i svar af den 2. april 2024 (Bilag I), side 7, at indsamling, generering og anvendelse af personoplysninger sker i overensstemmelse med dataminimeringsprincippet:

> *"Engineers in Online Services have to consult system logs as part of the normal course of their duties. Because the logs need to be the factual record of user activity, the logs use a "privacy by design" approach that ensures no directly identifiable information about a user*

> *is stored in them. Engineers have no need to know this information in the normal performance of their duties. Nonetheless, the tokens substituted to reference the user activity in the log ("pseudonymization") are personal data and the remote viewing of these logs by engineers amounts to a "transfer of personal data" under the GDPR. Note that this transfer results in no permanent relocation or copy of any personal data. There are many services and sub-services in cloud services that together power the aggregate customer experience, and as a requirement to security all of the services create log records of activity in or by the services. Nonetheless, no personal data is permitted to be stored by Microsoft that is not necessary to the functional outcomes including effective security and audit trail of activity (ROPA, Personal Data Minimization)."*

Det vurderes på denne baggrund, at den behandling Microsoft Ireland foretager på vegne af De Dataansvarlige i forbindelse med disses brug af de udvalgte applikationer og cloudtjenester i Microsoft 365 er inden for rammerne af dataminimeringsprincippet i databeskyttelsesforordningens artikel 5, stk. 1, litra c.

For det tilfælde at Microsoft Irelands behandling af oplysninger til forretningsaktiviteter måtte anses for en behandling af personoplysninger – idet anonymiseringen måtte anses for utilstrækkelig – bemærkes, at Microsoft Ireland også i denne henseende har angivet at ville overholde dataminimeringsprincippet. Det fremgår således af Microsoft Irelands databehandleraftale side 6, at

> *"When processing for these business operations, Microsoft will apply principles of data minimization and will not use or otherwise process Customer Data, Professional Services Data, or Personal Data […]"*

Ligeledes anføres der følgende i Microsoft Irelands "Business operations white paper" (Bilag D):

> "*The limited data used for business operations processing are objectively necessary to achieve the described legitimate interest. There is no milder means. While the aggregated data is non-personal and does not permit singling out individuals, it would not, for example, be possible to use anonymous data to develop the aggregations since this would not allow reaching the business operations purposes.*"

og

> "*[…] (b) deploys additional safeguards effectively blocking a reversal of such measures in business operations processing, in order til avoid prejudice to data subjects' interests and to ensure the proportionality of the data processing.*"

Som beskrevet ovenfor i dette afsnit og afsnit 7.1.27.1.4 har Microsoft Danmark blandt andet oplyst, at der jævnligt tjekkes for, om de oplysninger, der anvendes til levering af tjenesteydelse og produkt samt Microsoft Irelands egne formål er begrænset til de rigtige, sådan at det f.eks. er de korrekte og absolut nødvendige datapunkter, der indhentes til brug herfor.

En eventuel videregivelse af personoplysninger til Microsoft Ireland med henblik på deres varetagelse af forretningsmæssige formål anses på den baggrund sammenholdt med afsnit 7.1.27.1.4 for at være inden for rammerne af databeskyttelsesforordningens artikel 5, stk. 1, litra c.

7.1.4. Princippet om rigtighed

Det følger af databeskyttelsesforordningens artikel 5, stk. 1, litra d, at personoplysninger skal være korrekte og om nødvendigt ajourførte; der skal tages ethvert rimeligt skridt for at sikre, at personoplysninger, der er urigtige i forhold til de formål, hvortil de behandles, straks slettes eller berigtiges (»rigtighed«).

De Dataansvarlige supplerer selv nærværende konsekvensanalyse med oplysninger om, hvorvidt de personoplysninger, der indtastes, behandles og opbevares i de udvalgte applikationer og cloudtjenester i Microsoft 365, er rigtige. De Dataansvarlige supplerer således også selv med eventuelle foranstaltninger såsom interne retningslinjer, som skal sikre princippet om rigtighed.

Rigtigheden af de (person)oplysninger, som Microsoft Ireland i øvrigt behandler som databehandler, beror på de personoplysninger, som De Dataansvarlige har overladt til Microsoft. Microsoft Danmark har i øvrigt oplyst, at der jævnligt tjekkes for, om de oplysninger, der anvendes til levering af tjenesteydelse og produkt samt Microsoft Irelands egne formål, er det rigtige, sådan at det f.eks. er de korrekte datapunkter, der indhentes til brug herfor.

Microsoft Ireland har endvidere implementeret adækvate foranstaltninger med henblik på at sikre personoplysningers oprindelige og fortsatte kvalitet og korrekthed, herunder i forhold til de personoplysninger, som genereres i Microsofts infrastruktur ved brugernes interaktion med tjenester og services.

7.1.5. Princippet om opbevaringsbegrænsning

Det følger af princippet om opbevaringsbegrænsning i databeskyttelsesforordningens artikel 5, stk. 1, litra e, 1. led, at personoplysninger skal opbevares på en sådan måde, at det ikke er muligt at identificere de registrerede i et længere tidsrum end det, der er nødvendigt til de formål, hvortil de pågældende personoplysninger behandles.

De Dataansvarlige supplerer selv nærværende konsekvensanalyse med oplysninger om, hvorvidt de personoplysninger, De Dataansvarlige behandler ved brug af de udvalgte applikationer og cloudtjenester i Microsoft 365, kun opbevares i det omfang, det er nødvendigt af hensyn til det formål, hvortil de indsamles. De Dataansvarlige supplerer således også selv med eventuelle foranstaltninger såsom interne retningslinjer, slettepolitik, konfiguration, m.v., som skal sikre princippet om opbevaringsbegrænsning.

For så vidt angår brugernes mulighed for at slette oplysninger i systemet følger det af Microsoft Irelands databehandleraftale, side 10, at det er muligt at slette de personoplysninger, som brugerne har indtastet i systemet, ligesom det er anført, at øvrige personoplysninger slettes, når formålet med behandlingen er opfyldt:

> *"At all times during the term of Customer's subscription or the applicable Professional Services engagement, Customer will have the ability to access, extract and delete Customer Data stored in each Online Service and Professional Services Data.*
>
> *Except for free trials and LinkedIn services, Microsoft will retain Customer Data that remains stored in Online Services in a limited function account for 90 days after expiration or termination of Customer's subscription so that Customer may extract the data. After the 90-day retention period ends, Microsoft will disable Customer's account and delete the Customer Data and Personal Data stored in Online Services within an additional 90 days, unless authorized under this DPA to retain such data.*
>
> *For Personal Data in connection with the Software and for Professional Services Data, Microsoft will delete all copies after the business purposes for which the data was collected or transferred have been fulfilled or earlier upon Customer's request, unless authorized under this DPA to retain such data.*
>
> *The Online Service may not support retention or extraction of software provided by Customer. Microsoft has no liability for the deletion of Customer Data, Professional Services Data, or Personal Data as described in this section."*

I Attachment 1 til Microsoft Irelands databehandleraftale følger i overensstemmelse med databeskyttelsesforordningens artikel 28, stk. 3, at

> *"[Microsoft shall] at the choice of Customer, delete or return all the Personal Data to Customer after the end of the provision of services relating to processing, and delete existing copies unless Union or Member State law requires storage of the Personal Data"*

Desuden følger det af Appendix A, at

> *"Microsoft uses industry standard processes to delete Customer Data and Professional Services Data when it is no longer needed."*

Det lægges på baggrund heraf til grund, at personoplysninger lagres og slettes forsvarligt.

Endvidere er det af Microsoft Danmark i svar af den 2. april 2024 (Bilag I) side 4, oplyst, at

> *"[…] customers can realize the attributes applicable to this data [(Diagnostic Data and Systemgenererede logfiler)]:*
>
> > *[…]*
> > *B) It is deleted on instruction of the customer org. If the user is removed from the service, Microsoft deletes this data within 30 days of that changed processing instruction. It is also deleted if the customer leaves the service entirely."*

Om opbevaring af Systemgenererede logfiler fremgår bl.a. af Microsofts business operations white paper vol. 2, side 6:

> *"Retention periods for logs vary and are specific to service operations needs. Microsoft practices data minimization such that logs are retained only as long as required to achieve each service operations purpose, but personal data is retained no longer than 180 days after a paid subscription ends. Limited exceptions to retention periods may apply as necessary for purposes related to security, fraud prevention, billing, and to comply with legal obligations."*

Microsoft har supplerende oplyst som led i udarbejdelsen af denne konsekvensanalyse, at nogle logs opbevares i 1 time, hvorimod andre opbevares betydeligt længere afhængig af formålet med logningen.

Det er på baggrund af ovenstående vurderingen, at De Dataansvarlige lever op til princippet om opbevaringsbegrænsning i databeskyttelsesforordningens artikel 5, stk. 1 litra e.

7.1.6. Princippet om integritet og fortrolighed (behandlingssikkerhed)

Personoplysninger skal behandles på en måde, der sikrer tilstrækkelig sikkerhed for de pågældende personoplysninger, herunder beskyttelse mod uautoriseret eller ulovlig behandling og mod hændeligt tab,

tilintetgørelse eller beskadigelse, under anvendelse af passende tekniske eller organisatoriske foranstaltninger ("integritet og fortrolighed"), jf. databeskyttelsesforordningens artikel 5, stk. 1, litra f.

Dette princip suppleres af databeskyttelsesforordningens artikel 32, stk. 1, hvorefter den dataansvarlige er forpligtet til at foretage en risikovurdering og gennem passende tekniske og organisatoriske foranstaltninger opretholde et behandlingssikkerhedsniveau, der er passende ift. de identificerede risici, navnlig under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder. Ved vurderingen af hvilket sikkerhedsniveau der er passende, tages der navnlig hensyn til de risici, som behandling udgør, navnlig ved hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet, jf. databeskyttelsesforordningens artikel 32, stk. 2.

De Dataansvarliges artikel 32-risikovurdering for den behandling, deres ansatte som brugere foretager i forbindelse med brug af de udvalgte applikationer og cloudtjenester i Microsoft 365, varierer fra myndighed til myndighed, idet behandlingen og konfigurationen, samt de risici denne giver anledning, til varierer. Det er således ikke muligt at udarbejde én databeskyttelsesretlig risikovurdering for samtlige af De Dataansvarliges behandling af personoplysninger ved brug af Microsoft 365 til sagsbehandling og personaleadministration.

I stedet henvises hver enkelt af De Dataansvarlige til selv at udarbejde en risikovurdering af den behandling, de hver især foretager i forbindelse med brug af værktøjerne, som supplement til nærværende generelle konsekvensanalyse, herunder evaluere eventuelle yderligere risici udover de, der allerede er identificeret nedenfor i afsnit 8.38.3, såvel som de mitigerende foranstaltninger, De Dataansvarlige har og vil implementere.

De Dataansvarliges risikovurdering og de identificerede mitigerende foranstaltninger suppleres og understøttes af Microsofts sikkerhedsforanstaltninger, som særligt for Microsoft 365 fremgår af "Basic Security Set Up for Microsoft 365[64], ligesom der også i Microsoft Irelands databehandleraftale er beskrevet de konkrete sikkerhedsforanstaltninger, som Microsoft har fastsat. Dette beskrives overordnet i det følgende, ligesom der henvises til afsnit □7.300nedenfor, med en beskrivelse af de væsentligste tekniske, organisatoriske og kontraktuelle foranstaltninger, som gælder generelt for De Dataansvarlige, herunder sikkerhedsforanstaltninger implementeret af Microsoft.

[64] Microsofts hjemmeside: https://learn.microsoft.com/en-us/microsoft-365/community/basic-security-set-up-for-microsoft-365 (tilgået 14. marts 2024).

Således er det ifølge artikel 32 *både* den dataansvarlige *og* databehandleren, der skal foretage en risikovurdering, ligesom databehandlere efter databeskyttelsesforordningens artikel 33, stk. 2, uden unødig forsinkelse efter at være blevet opmærksom på, at der er sket et brud på persondatasikkerheden, skal underrette den dataansvarlige.

Microsoft har ifølge Appendix A til Microsoft Irelands databehandleraftale gennemført en risikovurdering før påbegyndelse af behandlingen af De Dataansvarliges oplysninger. Videre følger det af Microsoft Irelands databehandleraftale[65], at:

> "*Microsoft will implement and maintain appropriate technical and organizational measures to protect Customer Data, Professional Services Data, and Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed. Those measures shall be set forth in a Microsoft Security Policy. Microsoft will make that policy available to Customer, along with other information reasonably requested by Customer regarding Microsoft security practices and policies.*"

De konkrete sikkerhedsforanstaltninger truffet af Microsoft er beskrevet i Microsoft Irelands databehandleraftale samt i Appendix A[66] til Microsoft Irelands databehandleraftale. Foranstaltningerne knytter sig til Microsofts organisering af informationssikkerhed, styring af aktiver, personalesikkerhed, fysisk og miljømæssig sikkerhed, styring af kommunikation og drift, adgangskontrol, styring af informationssikkerhedshændelser og styring af virksomhedskontinuitet.

Microsoft er i kraft af Microsoft Irelands databehandleraftale eksempelvis forpligtet til fastlægge, implementere og løbende sikre overvågning af sikkerhedsregler og -procedurer, foretage klassificering af data og udarbejde risikovurdering inden behandling påbegyndes, sikre fysisk og teknisk sikkerhed og adgangskontrol samt føre hændelseslogs i forbindelse med adgang til og behandling af Customer Data. Microsofts adgangskontrol sikrer, at Microsofts personale ikke har "pr. default adgang" til Customer Data, men tildeles kun adgang til nødvendige data i det nødvendige tidsrum[67]. Adgang til Customer Data sker fra "sikre arbejdsstationer" (SAW's) med begrænsede funktioner, der reducerer risici for malware, phishingangreb m.m., og hvor dataekstraktion er vanskeliggjort.[68] Microsoft sikrer herudover, at Customer Data, som er i færd med at blive overført via offentlige netværk mellem kunden og Microsoft, eller mellem Microsofts datacentre, er krypterede.

[65] Bilag C, side 8.

[66] Bilag C, side 8-9 samt side 13-15.

[67] Bilag C, appendix A, og bilag E, side 6.

[68] Bilag E, side 6.

Microsoft har desuden i Attachment 1 til Microsoft Irelands databehandleraftale (bilag C) fastlagt supplerende vilkår, som vedrører Microsofts forpligtelser som databehandler for De Dataansvarlige i forbindelse med særligt databeskyttelsesforordningens artikel 5, stk. 2, artikel 28, stk. 2, artikel 28, stk. 3 og 4, artikel 31, stk. 1, 2 og 4 samt artikel 33, stk. 2 og 3.

I relation til håndtering af brud på persondatasikkerheden fremgår følgende af Microsoft Irelands databehandleraftale[69]:

> *"If Microsoft becomes aware of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data, Professional Services Data, or Personal Data while processed by Microsoft (each a "Security Incident"), Microsoft will promptly and without undue delay (1) notify Customer of the Security Incident; (2) investigate the Security Incident and provide Customer with detailed information about the Security Incident; (3) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Incident."*

Derudover forpligter Microsoft sig i Microsoft Irelands databehandleraftale til at bistå den dataansvarlige ved brud på persondatasikkerheden i overensstemmelse med artikel 33.

Tekniske foranstaltninger

FASTSAT AF STATEN

Statslige myndigheder har siden primo 2016 været forpligtet til at leve op til informationssikkerhedsstandarden ISO 27001, jf. National strategi for cyber- og informationssikkerhed 2015-2016. Denne forpligtelse gælder fortsat.

I forlængelse heraf skal de statslige myndigheder ligeledes sikre overholdelse af minimumskrav til deres it-sikkerhed. Minimumskravene blev første gang lanceret i 2020 og er efterfølgende løbende blevet justeret[70].

FASTSAT AF MICROSOFT

Kryptering

Microsoft angiver følgende i Microsoft Irelands databehandleraftales afsnit "*Data Encryption*":

[69] Bilag C, side 9.

[70] https://sikkerdigital.dk/myndighed/tekniske-tiltag/tekniske-minimumskrav/tekniske-minimumskrav-2024 (tilgået 31. marts 2026).

> *"Customer Data and Professional Services Data (each including any Personal Data therein) in transit over public networks between Customer and Microsoft, or between Microsoft data centers, is encrypted by default.*
>
> *Microsoft also encrypts Customer Data stored at rest in Online Services and Professional Services Data stored at rest. In the case of Online Services on which Customer or a third-party acting on Customer's behalf may build applications (e.g., certain Azure Services), encryption of data stored in such applications may be employed at the discretion of Customer, using either capabilities provided by Microsoft or obtained by Customer from third parties."*

Microsoft forpligter sig herved til at anvende kryptering, når der sker transmittering af Customer Data over åbne netværk samt til at kryptere Customer Data "stored at rest" i Teams. De Dataansvarlige kan i den forbindelse konstatere, at der benyttes TLS1,2 kryptering eller stærkere kryptering.

Det er De Dataansvarliges vurdering, at omend disse krypteringsforanstaltninger er med til at højne sikkerheden for behandlingen, så udgør de ikke i sig selv en effektiv krypteringsforanstaltning, der udelukker adgang til oplysninger i klar tekst i relation til den overførsel, der potentielt kan ske til tredjelande, der ikke sikrer en tilstrækkelig beskyttelse af de registreredes rettigheder og frihedsrettigheder, idet oplysninger dekrypteres, når de modtages hos Microsoft, ligesom Microsoft til enhver tid kan dekryptere oplysninger i hvile. Microsoft og dennes underdatabehandlere vil på trods af de ovenfor beskrevne krypteringsforanstaltninger således fortsat kunne behandle de overførte personoplysninger dekrypteret. De Dataansvarlige vurderer dog, at det ikke er muligt at gennemføre anden kryptering end den netop beskrevne i relation til behandlingen. For så vidt angår krypteringens betydning ved overførsler til tredjelande henvises til den til konsekvensanalysen vedlagte TIA.

Pseudonymisering

Microsoft angiver i sin transparency documentation vedrørende EU Data Boundary, at personoplysninger i Systemgenererede logfiler (brugsoplysninger, herunder aktivitetslogs) pseudonymiseres. Dette er endvidere kontrolleret af revisionsfirmaet Ernst & Young, idet der henvises herom til revisionserklæringen omtalt i afsnit 4.3. .

Logning

Det fremgår af afsnittet "*Security Practices and Policies*" i Microsoft Irelands databehandleraftale, at Microsoft har etableret procedurer for hændelseslogning. Microsoft logger, eller giver kunden mulighed for at logge, adgang til og brug af systemer med Customer Data via registrering af adgangs-id, tidspunkt, tildelt eller afvist godkendelse og relevant aktivitet. Microsoft logger også forsøg på gendannelse af slettede data.

Det fremgår videre af Microsofts transparency documentation vedrørende EU Data Boundary, at adgang til Customer Data i forbindelse med Microsoft og Microsofts underdatabehandlere logges og monitorers af Microsoft.

Tokens
I relation til Customer Data bemærkes det, at De Dataansvarlige har muligheden for at styre, hvilke persondata der danner grundlag for de *tokens* ("personal identifiers"), som logges af Microsoft.

Specifikt vil dette for medarbejdere hos De Dataansvarlige relateres til allerede pseudonymiserede oplysninger, f.eks. B-numre eller e-mailadresser. Tokens genereres på baggrund af de stamdata, som De Dataansvarlige har registreret hos Microsoft.

Microsoft forudsætter dog, at stamdata, der er registreret i *service directory* kan valideres, således at Microsoft kan være forsikret om, at det er rigtige personer, der fremgår af deres register.

Adgangsstyring
Det fremgår af afsnittet "*Data Access*" og "*Appendix A – Security Measures*" i Microsofts databehandleraftale, at adgang til data vil blive tildelt efter princippet om "least privilege".

Det fremgår videre af Microsofts transparency documentation vedrørende EU Data Boundary, at Microsoft begrænser adgangen til Customer Data til de personer, hvor brugen af adgangen indgår i jobfunktionen. Microsoft giver alene en just-in-time (JIT) access "*which are granted only for as long as is necessary to achieve that purpose*". Microsofts medarbejdere har således ikke "pr. default-adgang" til Customer Data, og adgang tildeles kun i det nødvendige tidsrum. Adgang til Customer Data sker under tilsyn fra en eller flere ledere. Microsoft har desuden procedurer, som sikrer, at adgangen til Customer Data sker uden lagring af data hos den, der tilgår Customer Data.

Anvendelse af anerkendte standarder
Det fremgår af afsnittet "*Security Practices and Policies*" i Microsoft Irelands databehandleraftale, at Microsoft vil sikre, at tekniske og organisatoriske sikkerhedsforanstaltninger fastlægges i overensstemmelse med ISO 27001, ISO 27002 og ISO 27018.

Ophør af behandling
Det fremgår af afsnittet "*Data Retention and Deletion*" i Microsoft Irelands databehandleraftale, at Microsoft har etableret processer, der muliggør, at De Dataansvarlige kan foretage udtræk og sletning af

Customer Data og dermed muliggøre flytning af løsningen. Desuden er det til brug for denne konsekvensanalyse oplyst af Microsoft, at de desuden anvender standarden ISO 27701 vedrørende privatlivsbeskyttelse.

Customer Lockbox

Foruden de sikkerhedsforanstaltninger, der er fastlagt i Microsoft Irelands databehandleraftale, tilbyder Microsoft en "Customer Lockbox service" for en række Microsoft 365-cloudtjenester. Customer Lockbox kan anvendes sammen med alle cloudtjenester omfattet af denne konsekvensanalyse (Exchange Online, SharePoint, OneDrive for Business og Teams)[71]. Customer Lockbox er en sikkerhedsfunktion, der giver kunderne kontrol over adgangen til kundens data i de tjenester, den er aktiveret for. For en detaljeret beskrivelse af Customer Lockbox henvises til TIA'en, som er vedlagt denne konsekvensanalyse.

Organisatoriske foranstaltninger

FASTSAT AF STATEN

De Dataansvarlige supplerer selv nærværende konsekvensanalyse med de interne retningslinjer, de allerede har, samt de retningslinjer de eventuelt på baggrund af risikovurderingen vil implementere.

FASTSAT AF MICROSOFT

Anvendelse af anerkendte standarder

Det fremgår af afsnittet "*Security Practices and Policies*" i Microsoft Irelands databehandleraftale, at Microsoft vil sikre, at tekniske og organisatoriske sikkerhedsforanstaltninger fastlægges i overensstemmelse med ISO 27001, ISO 27002 og ISO 27018. Microsoft har desuden selv oplyst til Statens It og Økonomistyrelsen, at ISO 27701 vedrørende privatlivsbeskyttelse tillige anvendes.

Adgangsbegrænsning

Adgang til data er tildelt efter princippet om "least privilege" (adgangsbegrænsning).

Tilsyn og audits

Det fremgår af afsnittet "*Auditing Compliance*" og "*European Union General Data Protection Regulation Terms*" i Microsoft Irelands databehandleraftale, at Statens It har mulighed for at føre kontrol med Microsofts overholdelse af forpligtelserne i databeskyttelsesforordningens artikel 28. Det indebærer også, at Statens It på vegne af De Dataansvarlige kan føre kontrol med, at Microsoft behandler personoplysningerne i overensstemmelse med instruksen, herunder i relation til de i trin 1 beskrevne overførsler.

[71] Microsofts hjemmeside: https://learn.microsoft.com/en-us/purview/customer-lockbox-requests (senest tilgået den 13. april 2026).

Det fremgår desuden af "*Appendix A – Security Measures*" i Microsoft Irelands databehandleraftale, at Microsoft desuden har udpeget en eller flere "*security officers*", som er ansvarlige for koordinering og overvågning af sikkerhedsregler og -procedurer.

Det fremgår videre af Microsoft transparency documentation, at Microsoft løbende gennemfører audits "*to review and confirm that access management measures are working in accordance with policy requirements, including Microsoft's contractual commitments*".

Gennemsigtighed vedrørende udleveringsanmodninger
Microsoft har offentliggjort forskellige rapporter og udtalelser vedrørende antallet af udleveringsanmodninger fra tredjelandes myndigheder, herunder hvor mange de har efterkommet. Der henvises herom til TIA'en, som er vedlagt denne konsekvensanalyse.

Kontraktuelle foranstaltninger

Microsoft har en række kontraktuelle foranstaltninger, som angår spørgsmålet om, hvorvidt Microsoft overfører personoplysninger til tredjelande og udleverer personoplysninger til tredjelandes myndigheder i henhold til tredjelands ret, samt vedrørende pligt til at underrette De Dataansvarlige i sådanne tilfælde. Der henvises herom til TIA'en, som er vedlagt denne konsekvensanalyse.

7.2. Hjemmelsgrundlag

7.2.1. Databeskyttelseslovgivningen

Databeskyttelsesforordningen

Databeskyttelsesforordningen finder anvendelse på behandling af personoplysninger, der helt eller delvist foretages ved hjælp af automatisk databehandling, og på anden ikkeautomatisk behandling af personoplysninger, der er eller vil blive indeholdt i et register, jf. forordningens artikel 2, stk. 1.

Som personoplysninger anses efter artikel 4, nr. 1, enhver form for information om en identificeret eller identificerbar fysisk person (»den registrerede«); ved identificerbar fysisk person forstås en fysisk person, der direkte eller indirekte kan identificeres, navnlig ved en identifikator som f.eks. et navn, et identifikationsnummer, lokaliseringsdata, en onlineidentifikator eller et eller flere elementer, der er særlige for denne fysiske persons fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sociale identitet.

Det følger af databeskyttelsesforordningens artikel 6, at behandling af ikke-følsomme personoplysninger er lovlig, hvis mindst ét af forholdene angivet i databeskyttelsesforordningens artikel 6, stk. 1, litra a-f, er opfyldt.

Databeskyttelsesforordningens artikel 6, stk. 1, litra e, fastlægger, at behandlingen er lovlig, hvis behandlingen er nødvendig af hensyn til udførelse af en opgave i samfundets interesse eller som henhører under offentlig myndighedsudøvelse, som den dataansvarlige har fået pålagt.

Ved vurdering af lovligheden af De Dataansvarliges behandling af ikke-følsomme personoplysninger i Microsoft 365 skal vurderingen foretages med udgangspunkt i artikel 6, stk. 1, litra e, idet behandlingen sker som led i de opgaver, som De Dataansvarlige er blevet pålagt som myndighed.

I forlængelse af artikel 6, stk. 1, litra e, fremgår følgende af artikel 6, stk. 3:

> *"Grundlaget for behandling i henhold til stk. 1, litra c) og e), skal fremgå af:*
>
> *1. EU-retten, eller*
>
> *2. medlemsstaternes nationale ret, som den dataansvarlige er underlagt.*
>
> *Formålet med behandlingen skal være fastlagt i dette retsgrundlag eller for så vidt angår den behandling, der er omhandlet i stk. 1, litra e), være nødvendig for udførelsen af en opgave i samfundets interesse eller som henhører under offentlig myndighedsudøvelse, som den dataansvarlige har fået pålagt. Dette retsgrundlag kan indeholde specifikke bestemmelser med henblik på at tilpasse anvendelsen af bestemmelserne i denne forordning, bl.a. de generelle betingelser for lovlighed af den dataansvarliges behandling, hvilke typer oplysninger der skal behandles, berørte registrerede, hvilke enheder personoplysninger må videregives til, og formålet hermed, formålsbegrænsninger, opbevaringsperioder og behandlingsaktiviteter samt behandlingsprocedurer, herunder foranstaltninger til sikring af lovlig og rimelig behandling såsom i andre specifikke databehandlingssituationer som omhandlet i kapitel IX. EU-retten eller medlemsstaternes nationale ret skal opfylde et formål i samfundets interesse og stå i rimeligt forhold til det legitime mål, der forfølges."*

Om bestemmelsen fremgår af databeskyttelsesforordningens præambelbetragtning nr. 45:

> *"Hvis behandling foretages i overensstemmelse med en retlig forpligtelse, som påhviler den dataansvarlige, eller hvis behandling er nødvendig for at udføre en opgave i samfundets interesse, eller som henhører under offentlig myndighedsudøvelse, bør behandlingen have*

retsgrundlag i EU-retten eller medlemsstaternes nationale ret. Denne forordning indebærer ikke, at der kræves en specifik lov til hver enkelt behandling. Det kan være tilstrækkeligt med en lov som grundlag for adskillige databehandlingsaktiviteter, som baseres på en retlig forpligtelse, som påhviler den dataansvarlige, eller hvis behandling er nødvendig for at udføre en opgave i samfundets interesse, eller som henhører under offentlig myndighedsudøvelse. (…)"

Videre fremgår om bestemmelsen i Justitsministeriets betænkning 1565/2017, side 130-131:

"Det må i den forbindelse antages, at artikel 6, stk. 1, litra e, er direkte anvendelig som behandlingsgrundlag, så længe den dataansvarlige udfører en opgave i samfundets interesse eller som henhører under offentlig myndighedsudøvelse, som den dataansvarlige har fået pålagt. Brugen af artikel 6, stk. 1, litra e, som behandlingsgrundlag forudsætter således ikke en national, implementerende hjemmelslovgivning om selve behandlingen af personoplysninger i forbindelse med udførelse af opgaver i samfundets interesse eller som led i offentlig myndighedsudøvelse.

Brugen af artikel 6, stk. 1, litra e, kræver heller ikke nødvendigvis, at opgaven, som kræver behandling af personoplysninger, udtrykkeligt i lovgivningen er pålagt myndigheden. […]

Videregivelse til tredjemand, som har fået pålagt myndighedsudøvelse
Det følger af databeskyttelsesdirektivets artikel 7, litra e, samt af persondatalovens § 6, stk. 1, nr. 6, at behandlingen må finde sted, hvis den er nødvendig af hensyn til udførelsen af en opgave, der henhører under offentlig myndighedsudøvelse, som den dataansvarlige eller en tredjemand, til hvem oplysningerne videregives, har fået pålagt.

Databeskyttelsesforordningens artikel 6, stk. 1, litra e, har ikke en tilsvarende ordlyd vedrørende den myndighedsudøvelse, som tredjemand har fået pålagt. […]

Forordningen indeholder således ikke en sådan videregivelseshjemmel. Dette ses dog reelt ikke at få nogen indholdsmæssig betydning for behandlingsreglerne.

Det må således antages, at artikel 6, stk. 1, litra e, fortsat kan bruges som hjemmelsgrundlag af en (privat) tredjemand - der har fået ansvar for offentlig myndighedsudøvelse, og til hvem oplysninger om den registrerede er videregivet - til den for myndighedsudøvelsen nødvendige behandling (indsamling mv.) af personoplysninger, da behandlingen netop henhører under "offentlig myndighedsudøvelse", jf. artikel 6, stk. 1, litra e."

Der er altså ikke krav om udtrykkelig lovhjemmel til selve behandlingen af personoplysninger i forbindelse med udførelse af opgaver i samfundets interesse eller som led i offentlig myndighedsudøvelse, men derimod krav om at behandlingen sker med henblik på at udføre en lovhjemlet opgave i samfundets interesse eller offentlig myndighedsudøvelse.

Hjemmelsgrundlaget i artikel 6, stk. 1, litra e, indeholder ifølge bestemmelsens ordlyd krav om, at behandlingen skal være »nødvendig« henset til de legitimerede formål, som bestemmelsen rummer.

Det betyder også, at personoplysninger ikke må behandles til andre formål, end det de relevante lovgrundlag foreskriver eller nødvendiggør.

Datatilsynet har bl.a. som led i den såkaldte "Google Chromebook-sag" (Datatilsynets j.nr. 2020-431-0061) udtalt sig om, hvornår behandlingen af personoplysninger, herunder ved videregivelse, kan rummes inden for databeskyttelsesforordningens artikel 6, stk. 1, litra e.

I afgørelsen af 14. juli 2022 fastslår Datatilsynet i relation til behandlingsgrundlaget:

> *"Det følger af folkeskolelovens § 2, stk. 1, at kommunalbestyrelsen har ansvaret for folkeskolen.*
>
> *[…]*
>
> *Det er Datatilsynets opfattelse, at såvel valg om brug af it i undervisningen, herunder hvilket fabrikat og software, der skal benyttes, falder inden for dette råderum.*
>
> *Datatilsynet bemærker herunder, at databeskyttelsesreglerne er teknologineutrale, og tilsynet kan alene vurdere de forhold, hvor der sker behandling af personoplysninger, jf. databeskyttelsesforordningens artikel 2, stk. 1.*
>
> *Mens folkeskoleloven – efter Datatilsynets opfattelse – tillægger kommunalbestyrelsen kompetence til at beslutte om – og i givet fald – hvilket it-udstyr, der skal benyttes i undervisningen, skal denne brug fortsat ske inden for rammerne af databeskyttelsesforordningen og databeskyttelsesloven.*
>
> *Børn og unges rettigheder nyder en særlig beskyttelse i databeskyttelsesreglerne. Det er Datatilsynets opfattelse, at dette hensyn indgår i vurderingen af hvilke behandlinger, der kan udføres på baggrund af den hjemmel, folkeskoleloven giver den enkelte kommune.*

Som det også fremgår af Datatilsynets afgørelse af 10. september 2021, er det tilsynets opfattelse, at Helsingør Kommune kan bestemme hvilke redskaber, der benyttes i kommunens folkeskoler, jf. databeskyttelsesforordningens artikel 6, stk. 1, litra e. Dette gælder også oprettelse af den enkelte elev som bruger af et sådant system.

Det er dog fortsat en væsentlig forudsætning, at databeskyttelsesforordningen og databeskyttelsesloven i øvrigt overholdes ved den behandling af personoplysninger, der finder sted."
(Vores understregninger.)

For så vidt angår vurderingen af, om databeskyttelsesforordningen i øvrigt overholdes ved kommunens brug af Google Chromebook og Google Workspace, fastlægger Datatilsynet i samme afgørelse, under overskriften "4.3. Brug af oplysninger til andre formål":

"Det er Datatilsynets opfattelse, at Helsingør Kommunes behandling af personoplysninger efter folkeskoleloven, jf. forordningens artikel 6, stk. 1, litra e, ikke omfatter situationer, hvor personoplysninger behandles til andre formål end de, der er forudsat i folkeskoleloven. Oplysningerne kan dermed heller ikke lovligt videregives til andre dataansvarlige til brug for disses formål, når der er tale om formål, som ikke er forudsat i folkeskoleloven. Dette omfatter også den behandling af personoplysninger, der kan ske ved elevernes brug af udstyret og softwaren, herunder metadataoplysninger, der benyttes til markedsføring og profilering, uanset om oplysningerne anvendes til direkte markedsføring mod den enkelte elev eller indirekte som en del af en gruppe (klasse, årgang, skole osv.)."

I afgørelse af 18. august 2022 i samme sag udtalte Datatilsynet supplerende herom:

"Det fremgår også af afgørelsen [fra 14. juli 2022, red.], at Helsingør Kommune – som den dataansvarlige – ikke kan behandle personoplysninger til andre formål, end de, der er forudsat i folkeskoleloven.

Oplysningerne kan dermed heller ikke lovligt videregives til andre dataansvarlige til brug for disses formål, når der er tale om formål, som ikke er forudsat i folkeskoleloven. Dette omfatter også den behandling af personoplysninger, der kan ske ved elevernes brug af udstyret og softwaren.

Det er Datatilsynets opfattelse, at den behandling af personoplysninger, som er forudsat i folkeskolelovens regler om undervisningspligt, og dermed kan ske efter databeskyttelsesforordningens artikel 6, stk. 1, litra e, ikke omfatter, at oplysningerne kan videregivelse til andre selvstændige dataansvarlige, herunder til brug for formål så som videreudvikling af

teknologileverandørers applikationer mv. Det er Datatilsynets opfattelse, at offentlige myndigheders videregivelse af personoplysninger til private dataansvarlige generelt kræver særskilt hjemmel, når der er tale om formål, som ligger uden for de myndighedsopgaver, som den offentlige myndighed er pålagt at varetage.

I dette tilfælde er der tale om, at Helsingør Kommune – som den dataansvarlige som følge af sin beslutning om, at kommunens folkeskoleelever skal benytte det pågældende udstyr – videregiver personoplysninger til Google til brug for Googles egne formål, der nærmere fremgår af Googles privatlivspolitik.

Det er således Datatilsynets vurdering, at de kontraktuelle foranstaltninger og udtalelser fra Google, som Helsingør Kommune har dokumenteret, er uden betydning for de forhold, der er beskrevet i Datatilsynets afgørelse af 14. juli 2022.

Datatilsynet har herved navnlig lagt vægt på, at Helsingør Kommunes instruks til Google om alene at behandle "Customer Personal Data" til kommunens formål ikke omfatter alle de personoplysninger, der behandles ved kommunens elevers brug af Google Chromebooks og Workspace, og at der er en række personoplysninger i form af "Service Data", der indsamles og videregives til Google til brug for Googles egne formål." (Vores understregning.)

I afgørelse af 30. januar 2024 i samme sag supplerede Datatilsynet ovenstående udtalelse yderligere med følgende:

"Efter Datatilsynets opfattelse har offentlige myndigheder, som det er forudsat i databeskyttelsesforordningen, præambelbetragtningerne hertil, samt Justitsministeriets betænkning nr. 1565/2017, en vid adgang til at behandle personoplysninger, når det er nødvendigt af hensyn til udførelse af deres myndighedsopgaver.

Datatilsynet anerkender, at det ovennævnte "nødvendighedskrav" er fleksibelt og giver offentlige myndigheder en bred margin for at vurdere, hvad der i det enkelte tilfælde er relevant og sagligt, dvs. nødvendigt, for at myndigheden kan varetage sine opgaver på den måde, som er tiltænkt med lovgivningen.

Spørgsmålet er herefter, i hvilket omfang kommunerne kan udstrække denne fleksibilitet til at omfatte brug af undervisnings- og læringsmidler, som gennem deres opbygning og leverancemodel indebærer, at kommunerne videregiver personoplysninger til en anden selvstændig dataansvarlig, leverandøren af læringsmidlerne – her Google – til brug for (i) levering og (ii) forbedring af læringsmidlerne samt (iii) udvikling af nye funktioner og tjenester.

Indledningsvis bemærker Datatilsynet, at KL har anført, at vurderingen af, om kommunerne har hjemmel til at videregive personoplysninger til Google skal foretages i to tempi. For det første vurderes det, om kommunerne har hjemmel til at videregive personoplysninger til Google til brug for levering af tjenesten. Dernæst vurderes det, om kommunerne har påset, om Google lovligt kan modtage og behandle personoplysningerne til andre formål, herunder udvikling af nye funktioner og tjenester, efter databeskyttelsesforordningens artikel 5, stk. 1, litra a.

Det er Datatilsynets opfattelse, at vurderingen af, om kommunerne har hjemmel til at videregive personoplysninger til Google skal foretages i lyset af alle de formål, som oplysningerne skal behandles til. Kommunerne skal derfor vurdere, om der er hjemmel til videregivelse af personoplysninger til brug for levering af tjenesten og til andre formål, herunder udvikling af nye funktioner og tjenester. Det omfatter alle de formål, som kommunerne på videregivelsestidspunktet er bekendt med, at oplysningerne vil blive behandlet til.

Datatilsynet henviser navnlig til tilsynets afgørelse over for Helsingør kommune af 18. august 2022. Heraf fremgår bl.a. følgende:

> *"Oplysningerne kan dermed heller ikke lovligt videregives til andre dataansvarlige til brug for disses formål, når der er tale om formål, som ikke er forudsat i folkeskoleloven. Dette omfatter også den behandling af personoplysninger, der kan ske ved elevernes brug af udstyret og softwaren.*
>
> *Det er Datatilsynets opfattelse, at den behandling af personoplysninger, som er forudsat i folkeskolelovens regler om undervisningspligt, og dermed kan ske efter databeskyttelsesforordningens artikel 6, stk. 1, litra e, ikke omfatter, at oplysningerne kan videregivelse til andre selvstændige dataansvarlige, herunder til brug for formål så som videreudvikling af teknologileverandørers applikationer mv. Det er Datatilsynets opfattelse, at offentlige myndigheders videregivelse af personoplysninger til private dataansvarlige generelt kræver særskilt hjemmel, når der er tale om formål, som ligger uden for de myndighedsopgaver, som den offentlige myndighed er pålagt at varetage."*

Kommunerne kan således ikke først vurdere, om der er hjemmel til videregivelse af personoplysninger til visse formål (levering af tjenesten) og herefter lægge til grund, at de øvrige formål (udvikling af nye produkter mv.), hvortil personoplysningerne også behandles, skal

vurderes som Googles egen viderebehandling af personoplysningerne til andre formål efter databeskyttelsesforordningens artikel 6, stk. 4, og stk. 1.

Datatilsynet lægger i den forbindelse særligt vægt på, at der er tale om behandlinger, der er bestemt i aftalegrundlaget og forudsat for behandlingernes udførelse, og situationen kan derfor ikke sidestilles med forholdet hvor en 3. mand efter en videregivelse, som selvstændigt dataansvarlig efterfølgende vælger at benytte persondata til nye egne formål."

I samme afgørelse udtalte Datatilsynet, at følgende formål indenfor folkeskoleloven kan anses for at være et "oprindeligt formål" til hvilke, personoplysninger kan behandles og videregives:

"(i) levering af og (ii) forbedring af sikkerheden og pålideligheden af de omhandlede tjenester mv"

Samtidig vurderede Datatilsynet, at følgende formål var "afledte formål", som ikke indenfor rammerne af folkeskoleloven kunne behandles og videregives:

"(i) vedligeholdelse og forbedring af Google Workspace for Education-tjenesten, Chrome OS samt Chrome-browseren, (ii) måling af ydeevnen af Chrome OS og Chrome-browseren, samt (iii) udvikling af nye funktioner og tjenester i Chrome OS og Chrome-browseren"

I afgørelserne fremhæves samtidig, at børn og unges rettigheder nyder en særlig beskyttelse i databeskyttelsesreglerne, og at dette hensyn indgår i vurderingen af, hvilke behandlinger der kan udføres på baggrund af det hjemmelsgrundlag, som danner grundlag for behandlingen af de pågældende personoplysninger.

Datatilsynets udtalelse må mest nærliggende betragtes som en tilkendegivelse af, at vurderingen af »nødvendigheden« af behandlingen i henhold til artikel 6, stk. 1, litra e, ikke er statisk, men at de konkrete forhold i relation til behandlingen kan have betydning for vurderingen. Når der f.eks. er tale om sårbare personoplysninger, kan det således medføre, at der skal et mere klart behandlingsgrundlag til.

At der ved nødvendighedsvurderingen skal tages hensyn til de konkrete omstændigheder, er også antaget i litteraturen. Eksempelvis fremgår af Motzfeldt, Hanne Marie, Grundlæggende databeskyttelsesret (1. udg.), 2022, Djøf Forlag, side 136:

"Ved vurderingen af, om en behandling er nødvendig for at realisere de legitimerende formål i artikel 6, stk. 1, er en række momenter relevante at inddrage. Behandlingsformen spiller

en betydelig rolle. Offentliggørelse er f.eks. klart mere indgribende end opbevaring. Oplysningstypen er også et centralt moment, idet der ikke kun kan skelnes mellem følsomme oplysninger og almindelige oplysninger. Også inden for artikel 6 er der betydelig forskel på oplysningstyperne, og nødvendighedskravet vil skærpes, jo mere privat en karakter, oplysningerne har. Kravene til nødvendighed vil således normalt være skærpede f.eks. for oplysninger om alvorlige sociale vanskeligheder i forhold til oplysninger om en registrets bopælskommune".

Det vil imidlertid ikke kun være ikke-følsomme personoplysninger, der behandles af De Dataansvarlige med henblik på at udføre de lovbestemte opgaver. Der vil således også som led heri blive indsamlet, registreret og i øvrigt behandlet følsomme personoplysninger, oplysninger om strafbare forhold samt fortrolige oplysninger, herunder cpr-nummer.

Da nærværende konsekvensanalyse er en paraply-konsekvensanalyse for alle De Dataansvarlige, vil hvert enkelt formål og dermed rette behandlingshjemmel efter databeskyttelsesforordningen og databeskyttelsesloven til behandling af følsomme personoplysninger således ikke blive gennemgået. Tilsvarende gælder i forhold til behandlinger af oplysninger om strafbare forhold og CPR-nummer.

I stedet supplerer De Dataansvarlige selv nærværende konsekvensanalyse med det rette behandlingsgrundlag for den behandling af personoplysninger, De Dataansvarlige foretager, som f.eks. kan angives i Bilag A.

Ved vurdering af lovligheden af den behandling af personoplysninger, der påtænkes i Microsoft 365, sondres i afsnit 7.2.27.2.2 mellem den behandling, der vil blive foretaget af De Dataansvarlige til varetagelse af disses lovbestemte opgaver med Microsoft som databehandler ved levering af ydelserne i Microsoft 365 og den behandling i form af anonymisering af personoplysninger, som Microsoft foretager som selvstændig dataansvarlig, idet oplysningerne skal anvendes af Microsoft til egne forretningsmæssige formål. I den sammenhæng vil der ligeledes blive sondret mellem behandling til oprindelige formål og behandling til afledte formål for hver af disse.

7.2.2. Vurdering af grundlaget for behandling til De Dataansvarliges formål

Som beskrevet ovenfor i afsnit 07.2.1 kræves der hjemmel til offentlige myndigheders behandling af personoplysninger til varetagelse af deres lovbestemte opgaver. De Dataansvarliges opgaver er fastsat i lovgivningen. Hvilket retsgrundlag, der finder anvendelse, afhænger af, hvilken myndighed det vedrører. De lovbestemte opgaver varierer, og omfanget af hvor langt myndighedens mulighed for at behandle personoplysninger, herunder eventuelt videregivelse heraf, er således meget forskelligt. De Dataansvarlige

henvises således selv til at supplere denne konsekvensanalyse med en vurdering af hjemmelsgrundlaget i den lovgivning, hvori myndighedens opgaver er fastsat.

Det er utvivlsomt, at De Dataansvarlige har klar hjemmel til efter eget skøn at beslutte valg af digitale kontorværktøjer indenfor de administrative rammer for De Dataansvarliges virke, herunder valg af leverandørfabrikat og software.

Som redegjort for ovenfor i afsnit 4.2.35.3.1 og afsnit 7.1.2 behandler Microsoft personoplysninger som databehandler i henhold til databehandleraftalen til følgende formål i forbindelse med levering af produkter:

- *Delivering functional capabilities as licensed, configured, and used by Customer and its users, including providing personalized user experiences;*
- *Troubleshooting (preventing, detecting, and repairing problems); and*
- *Keeping Products up to date and performant, and enhancing user productivity, reliability, efficacy, quality, and security.*

Videre behandler Microsoft også personoplysninger i forbindelse med levering af services til følgende formål:

- *Delivering the Professional Services, including providing technical support, professional planning, advice, guidance, data migration, deployment, and solution/software development services.*
- *Troubleshooting (preventing, detecting, investigating, mitigating, and repairing problems, including Security Incidents and problems identified in the Professional Services or relevant Product(s) during delivery of Professional Services); and*
- *Enhancing delivery, efficacy, quality, and security of Professional Services and the underlying Product(s) based on issues identified while providing Professional Services, including fixing software defects and otherwise keeping Products and Services up to date and performant.*

Ved Microsoft Irelands behandling til de ovennævnte formål som databehandler anvendes der pseudonymiserede personoplysninger i Diagnostic Data og Systemgenererede logfiler. Der behandles også ikke-pseudonymiserede personoplysninger, fortrolige oplysninger, følsomme personoplysninger samt oplysninger om strafbare forhold i Customer Data ved levering af produkterne og services. De anførte behandlingsformål vurderes at være en nødvendig forudsætning for at kunne levere de udvalgte applikationer og cloudtjenester i Microsoft 365, som De Dataansvarliges sagsbehandling samt personaleadministration skal foretages i, herunder for at sikre at de pågældende applikationer og cloudtjenester fungerer fejlfrit og sikkert.

Det vurderes derfor også, at Microsofts behandlinger som databehandler for De Dataansvarlige vil kunne rummes indenfor den samme hjemmel, som De Dataansvarlige i øvrigt behandler personoplysninger i henhold til, når De Dataansvarlige udfører de lovbestemte opgaver samt de opgaver, den pågældende myndighed qua sit virke er sat til at udføre. Som beskrevet ovenfor i relation til dataminimeringsprincippet i afsnit 7.1.37.1.3 er Microsoft Irelands behandling netop begrænset til kun at vedrøre den behandling, der er nødvendig for, at De Dataansvarlige kan løfte sine opgaver, herunder ved anvendelsen af værktøjer til brug for sagsbehandlingen og personaleadministration.

Det vurderes derfor også, at der ikke er tale om videregivelser af personoplysninger til Microsofts varetagelse af disse formål til levering af produkterne og services.

Som anført ovenfor i afsnit 4.2.35.3.1 fremgår det af Microsoft Irelands databehandleraftale, at Microsoft ikke vil bruge eller behandle Customer Data, Professional Services Data og Personal Data til brugerprofilering, reklame eller tilsvarende kommercielle formål eller markedsundersøgelser rettet mod at skabe nye funktioner, tjenester eller produkter eller ethvert andet formål, medmindre sådan brug eller behandling er i overensstemmelse med kundens dokumenterede instruktioner. Der sker således ikke en videregivelse til Microsoft af personoplysninger til sådanne formål.

7.2.3. Vurdering af grundlag for aggregering og efterfølgende behandling til Microsofts forretningsaktiviteter

Som beskrevet ovenfor i afsnit 4.2.44.3 behandler Microsoft oplysninger med henblik på følgende forretningsaktiviteter (business operations):

- *Billing and account management;*
- *Compensation such as calculating employee commissions and partner incentives;*
- *Internal reporting and business modeling, such as forecasting, revenue, capacity planning, and product strategy; and*
- *Financial reporting.*

Microsoft aggregerer de pseudonyme personoplysninger om brugernes interaktion med og brug af løsningerne (service generated logs og diagnostic data) til et anonymt niveau, dvs. hvor der ikke længere er tale om personoplysninger. Som nærmere beskrevet og vurderet ovenfor i afsnit 5.3.25.3.2 må det lægges til grund, at selve Microsofts anonymisering af de pseudonymiserede personoplysninger til brug for Microsofts egne ovennævnte forretningsaktiviteter udgør en elektronisk behandling af personoplysninger omfattet af databeskyttelsesforordningen. Selvom anonymiseringen fremgår af instruksen fra De Dataansvarlige til Microsoft, er der tale om en behandling, som Microsoft er dataansvarlig for, da anonymiseringen har til formål at skabe anonyme data udelukkende til brug for Microsofts egne forretningsmæssige

formål. Der er dog ikke tale om en videregivelse af personoplysninger fra De Dataansvarlige til Microsoft af de pseudonymiserede personoplysninger, der kræver selvstændig hjemmel, idet Microsoft alene aggregerer pseudonymiserede personoplysninger, som Microsoft har behandlet som databehandler, således at der ikke er tale om, at Microsoft udelukkende har indsamlet de pseudonymiserede personoplysninger til egne forretningsmæssige formål.

Samtidig anføres det ovenfor nævnte sted, at hvis den aggregering af de pseudonyme personoplysninger, som Microsoft Ireland foretager, i stedet skal anses for at indebære en videregivelse af personoplysninger fra De Dataansvarlige til Microsoft af de pseudonymiserede personoplysninger, der kræver selvstændig hjemmel, vurderes det i så fald, at De Dataansvarlige vil have hjemmel til at videregive personoplysningerne til Microsoft Ireland med henblik på at foretage denne anonymisering, jf. databeskyttelsesforordningens artikel 6, stk. 1, litra e. Det vurderes endvidere, at videregivelsen og behandlingen med det formål at anonymisere personoplysningerne, ikke er uforenelig med de oprindelige formål, som oplysningerne blev indsamlet til, jf. databeskyttelsesforordningens artikel 5, stk. 1, litra b, smh. artikel 6, stk. 4. Det vurderes endvidere, at Microsoft Ireland vil have hjemmel til at foretage aggregeringen med hjemmel i databeskyttelsesforordningens artikel 6, stk. 1, litra f. Microsofts efterfølgende behandling af de nu anonymiserede oplysninger til forretningsaktiviteter vil dog ikke medføre en rolle som dataansvarlig for Microsoft Ireland, idet der ikke (længere) er tale om personoplysninger.

Hvis det – mod Microsofts, Økonomistyrelsens og Statens It's opfattelse – måtte lægges til grund, at Microsoft ikke foretager en aggregering af de pseudonymiserede personoplysninger til et niveau, der udgør anonyme data, vil der derimod være tale om en videregivelse af personoplysninger omfattet af databeskyttelsesforordningens artikel 6 fra De Dataansvarlige til Microsoft, da personoplysningerne skal anvendes til Microsofts egne forretningsformål (business operations). I så fald er det Økonomistyrelsens og Statens It's opfattelse, at der vil være hjemmel til en sådan videregivelse af pseudonyme, ikke-følsomme personoplysninger i databeskyttelsesforordningens artikel 6, stk. 1, litra e. Der må ved denne vurdering lægges vægt på, at Microsoft Irelands forretningsaktiviteter har en nær forbindelse til de lovbestemte opgaver, fordi det formentlig uden denne behandling hverken er muligt for De Dataansvarlige at købe og betale for de nødvendige produkter og services hos Microsoft eller muligt for Microsoft at levere disse produkter og services uden at kunne behandle udvalgte oplysninger til fakturering, beregning af medarbejderkommission, intern afrapportering, herunder kapacitetsplanlægning, og finansiel afrapportering. Dertil kommer, at behandlingen er begrænset til, at Microsoft efter det oplyste på baggrund af pseudonymiserede personoplysninger, f.eks. brugerlogs med unikke pseudonymiserede identifikationsnumre, skaber aggregerede, statistiske datasæt med henblik på varetagelse af de beskrevne formål, således at oplysningernes karakter ikke er sensitive eller indgribende. Der er således ikke tale om viderebehandling af Customer Data, men alene ikke-følsomme personoplysninger indeholdt i / genereret i Diagnostic Data og Service-Generated Logs. Behandlingen vurderes derfor at være proportional og ikke uforenelig med de

oprindelige behandlingsformål hos De Dataansvarlige. Det må endvidere tages i betragtning, at de registrerede udgøres af brugerne – og ikke borgere – som er ansatte hos De Dataansvarlige, og hvor indsamlingen af oplysningerne angår deres brug af løsningerne som led i deres ansættelsesforhold og ikke angår deres private forhold; der er således ikke – i modsætning til Google Chromebook-sagen – tale om behandling af oplysninger om sårbare registrerede i form af borgere (børn). Endvidere vurderes det, at Microsoft – hvis der ville være tale om behandling af personhenførbare oplysninger til Microsofts egne forretningsformål – ville have hjemmel til denne behandling efter databeskyttelsesforordningens artikel 6, stk. 1, litra f.

7.3. De registreredes rettigheder

7.3.1. Oplysningspligten

Det følger af reglerne om oplysningspligt i databeskyttelsesforordningens artikel 13 og 14, at de registrerede som udgangspunkt skal underrettes om den dataansvarliges behandling af personoplysninger.

De Dataansvarlige behandler både personoplysninger, der er indsamlet fra de registrerede selv, og personoplysninger, der er indsamlet fra andre end de registrerede, herunder andre myndigheder såsom Skatteforvaltningen og offentlige kilderegistre m.v. De Dataansvarlige er derfor både omfattet af forordningens artikel 13 og 14.

De Dataansvarlige supplerer selv nærværende konsekvensanalyse med oplysninger om varetagelse af oplysningspligten, herunder en vurdering af hvorvidt der kan gøres undtagelser fra oplysningspligten.

7.3.2. Øvrige rettigheder

De Dataansvarlige supplerer selv nærværende paraply-konsekvensanalyse med, hvordan de håndterer løbende rettighedsanmodninger fra de registrerede og sikrer, at databeskyttelsesforordningens krav til håndtering af rettighedsanmodninger efterleves, herunder hvilke interne retningslinjer og procedurer for håndtering af rettighedsanmodninger der eventuelt er udarbejdet, og hvordan de er implementeret hos myndigheden.

Microsoft Ireland har som databehandler efter databeskyttelsesforordningens artikel 28, stk. 3, litra e, pligt til under hensyntagen til behandlingens karakter, så vidt muligt at bistå De Dataansvarlige ved hjælp af passende tekniske og organisatoriske foranstaltninger, med opfyldelse af De Dataansvarliges forpligtelse til at besvare anmodninger om udøvelse af de registreredes rettigheder som fastlagt i kapitel III.

I overensstemmelse hermed fremgår følgende af Microsoft Irelands databehandleraftale, side 8:

> *"Microsoft will make available to Customer, in a manner consistent with the functionality of the Products and Services and Microsoft's role as a processor of Personal Data of data subjects, the ability to fulfill data subject requests to exercise their rights under the GDPR. If Microsoft receives a request from Customer's data subject to exercise one or more of its rights under the GDPR in connection with the Products and Services for which Microsoft is a data processor or subprocessor, Microsoft will redirect the data subject to make its request directly to Customer. Customer will be responsible for responding to any such request including, where necessary, by using the functionality of the Products and Services. Microsoft shall comply with reasonable requests by Customer to assist with Customer's response to such a data subject."*

Og attachment 1:

> *"taking into account the nature of the processing, assist Customer by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Customer's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III of the GDPR."*

Desuden har Microsoft Ireland oplyst følgende ved svar af 2. april 2024 (Bilag I), side 17:

> *"As a data processor, Microsoft*
> *[...]*
> *And 'Facilitate the data controller's compliance with the data subject's rights, such as by providing the data controller with the tools or mechanisms to access, rectify, erase, restrict, or transfer the personal data, or to object to the processing, as applicable.'"*

Retten til indsigt

Det fremgår af databeskyttelsesforordningens artikel 15, stk. 1, at den registrerede har ret til at få den dataansvarliges bekræftelse på, om personoplysninger vedrørende den pågældende behandles, og i givet fald adgang til personoplysningerne og information som beskrevet i bestemmelsens litra a-h.

Udover Microsoft Irelands ovenstående tilkendegivelse i Microsoft Irelands databehandleraftale har Microsoft Danmark ved besvarelse af 2. april 2024 (Bilag I), side 17, oplyst følgende:

"Microsoft provides the ability to access Systemgenererede logfiler that may be necessary to complete a DSR. Examples of such data may include:

Product and service usage data such as user activity logs User search requests and query data Data generated by product and services resulting from system functionality and interaction by users or other systems.

Microsoft provides DSR tools to assist the customer (aka Data controller) in responding to a DSR: https://learn.microsoft.com/enus/compliance/regulatory/gdpr-dsr-office36"

[…]

As a data processor, Microsoft 'Provide the data controller with the necessary information and cooperation to enable the data controller to respond to the DSRs within the prescribed time limit (usually one month, with a possibility of extension in some cases)."

Der vil blive foretaget årlige stikprøvekontroller af logs.

Retten til berigtigelse

Det fremgår af databeskyttelsesforordningens artikel 16, at den registrerede har ret til at få urigtige personoplysninger om sig selv berigtiget af den dataansvarlige uden unødig forsinkelse. Den registrerede har under hensyntagen til formålene med behandlingen ret til få fuldstændiggjort ufuldstændige personoplysninger, bl.a. ved at fremlægge en supplerende erklæring.

For så vidt angår berigtigelse fremgår følgende af Microsoft Danmarks svar af 2. april 2024 (Bilag I), side 4:

"[…] customers can realize the attributes applicable to this data [(Diagnostic Data and Systemgenererede logfiler)]:

[…]
D) This data cannot be rectified as the only personal data are substitutions (tokens, identifiers) that point to the user who performed the logged activity or used the instrumented software. Rectification of provided personal data (aka Customer Data (1)) can be done by the customer."

Dette er uddybet i Microsoft Danmarks svar af 23. april 2024 (Bilag J), side 6:

> *"In the event Microsoft becomes aware of a rectification requirement uniquely focused on the system generated logs (e.g., the recording of the wrong user referencing pseudonymous token in a record), Microsoft will promptly rectify the system generated log and resolve the root causes of the logging errors. To rectify logs Microsoft may, in their sole discretion, elect to delete them.*
>
> *Microsoft wishes to emphasize that data in system generated logs constitutes records of factual actions. Modifications to such data would compromise the historical record of actions and could introduce risk of increased fraud and security issues."*

Retten til sletning

Af databeskyttelsesforordningens artikel 17, stk. 1, fremgår, at den registrerede har ret til at få personoplysninger om sig selv slettet af den dataansvarlige uden unødig forsinkelse, og den dataansvarlige har pligt til at slette personoplysninger uden unødig forsinkelse, hvis et af de i bestemmelsens litra a-f nævnte forhold gør sig gældende.

Videre følger det af artikel 17, stk. 3, litra b, at bestemmelsen i stk. 1 ikke finder anvendelse, hvis behandlingen er nødvendig for at udføre en opgave i samfundets interesse, eller som henhører under offentlig myndighedsudøvelse, som den dataansvarlige har fået pålagt.

Det er på den baggrund vurderingen, at personoplysninger som De Dataansvarlige og Microsoft Ireland på vegne af De Dataansvarlige behandler i Microsoft 365, som overvejende udgangspunkt vil være omfattet af undtagelsesbestemmelsen i databeskyttelsesforordningens artikel 17, stk. 3, litra b.

Det vil dog, som beskrevet ovenfor i afsnit 7.1.57.1.5 være muligt for De Dataansvarlige at slette personoplysninger, hvor det er relevant og i overensstemmelse med databeskyttelsesforordningens artikel 17.

Øvrige rettigheder

Det vurderes endvidere, at retten til begrænsning af behandling (artikel 18), underretningspligten i forbindelse med berigtigelse eller sletning af personoplysninger eller begrænsning af behandling (artikel

19), artikel 21 om retten til indsigelse samt artikel 22's rettigheder ved brug af automatiske individuelle afgørelser, herunder profilering, vil kunne varetages af De Dataansvarlige ved brug af Microsoft 365.

Forordningens artikel 20 (ret til dataportabilitet) finder ikke anvendelse, da bestemmelsen ikke finder anvendelse på behandling, der er nødvendig for udførelse af en opgave i samfundets interesse eller som henhører under offentlig myndighedsudøvelse, som den dataansvarlige har fået pålagt, jf. bestemmelsens stk. 3.

7.4. Overførsel af personoplysninger til modtagere i tredjelande og internationale organisationer

Det følger af reglerne i databeskyttelsesforordningens kapitel V, at personoplysninger alene må overføres til tredjelande eller internationale organisationer, hvis en række betingelser – ud over de krav, der i øvrigt følger af forordningen – opfyldes af den dataansvarlige og af databehandleren. Reglerne skal sikre, at det høje beskyttelsesniveau, som findes i EU/EØS, ikke undermineres ved, at personoplysningerne overføres til et tredjeland eller en international organisation, hvor databeskyttelsesforordningen ikke finder anvendelse.

Der skelnes imellem sikre og usikre tredjelande. Sikre tredjelande er lande, hvor EU-Kommissionen har foretaget en såkaldt tilstrækkelighedsvurdering i henhold til databeskyttelsesforordningens artikel 45, og har afgjort, at beskyttelsesniveauet i det pågældende land i det væsentligste svarer til beskyttelsesniveauet i EU/EØS-området. Usikre tredjelande er alle tredjelande, hvor der ikke foreligger en tilstrækkelighedsafgørelse. Virkningen af en tilstrækkelighedsafgørelse er derfor, at personoplysninger frit kan overføres fra EU til et tredjeland uden yderligere hindringer.

For så vidt angår overførsler til usikre tredjelande, skal overførselsgrundlaget som udgangspunkt findes i databeskyttelsesforordningens artikel 46. Det følger af artikel 46, stk. 2, litra c, at overførselsgrundlaget f.eks. kan etableres – uden Datatilsynets godkendelse – gennem EU-Kommissionens standardkontraktbestemmelser for overførsel af personoplysninger.

EU-Kommissionen har den 4. juni 2021 vedtaget standardkontraktbestemmelser, der erstatter de tidligere standardkontraktbestemmelser, som nu er ophævet. De nye standardkontraktbestemmelser består af fire moduler:

- Overførsler mellem dataansvarlig og dataansvarlig (Modul 1)
- Overførsler mellem dataansvarlig og databehandler (Modul 2)
- Overførsler mellem databehandler og databehandler (Modul 3)
- Overførsler mellem databehandler og dataansvarlig (Modul 4)

Opbygningen er sådan, at der gælder en række bestemmelser i standardkontraktbestemmelserne, der er fælles for alle fire ovennævnte situationer, hvorefter man vælger det specifikke modul af bestemmelser, der er relevant for den pågældende overførsel. Dataansvarlige og databehandlere kan således anvende det modul, som svarer lige præcis til deres rolle(r) og ansvar.

I forbindelse med at der skal etableres et overførselsgrundlag efter artikel 46, skal den dataansvarlige foretage en Transfer Impact Assessment (TIA), der har til formål at sikre og dokumentere, at det valgte overførselsgrundlag, sammenholdt med eventuelle supplerende foranstaltninger, giver de registrerede et beskyttelsesniveau, der i det væsentligste svarer til beskyttelsesniveauet efter reglerne i databeskyttelsesforordningen læst i lyset af EU-chartret, jf. herved EU-Domstolens dom af 16. juli 2021 i sag C-311/18, Schrems II (Schrems II-dommen).

Det Europæiske Databeskyttelsesråd (herefter "EDPB") har i rådets retningslinjer nr. 01/2020 om foranstaltninger, der supplerer overførselsværktøjer for at sikre overholdelse af EU-niveauet for beskyttelse af personoplysninger, givet retningslinjer for, hvordan dataeksportører skal forholde sig til tredjelandsoverførsler, herunder hvordan overførslernes lovlighed kan dokumenteres i en TIA.

I forbindelse med De Dataansvarliges brug af Microsoft 365 og de overførsler af personoplysninger til tredjelande, der sker i denne sammenhæng, har Statens It og Økonomistyrelsen på vegne af De Dataansvarlige foretaget en TIA, som er vedlagt denne konsekvensanalyse som Bilag F, hvortil der i øvrigt henvises for en beskrivelse af overførselsgrundlag og udleveringsanmodninger.

7.5. Databeskyttelse gennem design og standardindstillinger

Det følger af databeskyttelsesforordningens artikel 25, stk. 1, at den dataansvarlige under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder, som behandlingen indebærer, både på tidspunktet for fastlæggelse af midlerne til behandling og på tidspunktet for selve behandlingen gennemfører passende tekniske og organisatoriske foranstaltninger, såsom pseudonymisering, som er designet med henblik på effektiv implementering af databeskyttelsesprincipper, såsom dataminimering, og med henblik på integrering af de fornødne garantier i behandlingen for at opfylde kravene i denne forordning og beskytte de registreredes rettigheder.

Videre følger det af forordningens artikel 25, stk. 2, at den dataansvarlige skal gennemføre passende tekniske og organisatoriske foranstaltninger med henblik på gennem standardindstillinger at sikre, at kun personoplysninger, der er nødvendige til hvert specifikt formål med behandlingen, behandles.

Microsoft Corporation har ved udviklingen af applikationer og cloudtjenester i Microsoft 365 indtænkt databeskyttelse gennem design og standardindstillinger i vidt omfang, herunder ved implementering af organisatoriske og tekniske foranstaltninger med henblik på at sikre behandlingssikkerhed, de grundlæggende principper samt evnen til at kunne varetage de registreredes rettigheder, som nærmere gennemgået ovenfor.

Derudover kan der henvises til den til konsekvensanalysen vedlagte TIA, der indeholder detaljerede beskrivelser af de organisatoriske og tekniske privatlivsfremmende teknologier og strategier, der anvendes for at minimere overførsler til tredjelande og sikre disse overførsler bedst muligt, herunder ved anvendelse af Customer Lockbox, adgangsbegrænsninger, Just-in-time access m.v.

Særligt for så vidt angår Systemgenererede logfiler kan der henvises til "Systemgenererede logfiler in the Microsoft cloud – Purposes, types, customer access and privacy by design/default (from January 2024)" (Bilag G). Desuden har Microsoft Danmark specifikt for så vidt angår Systemgenererede logfiler i svar af 2. april 2024 (Bilag I), side 3, anført, at:

> *"There are no elements of provided personal information (Customer Data (1)) in this data. Since this data category is examined by engineers using tools to do their work monitoring the cloud services, then to achieve privacy by design we do not allow any personal data attributes that the customer has provided to be in records of this data type; instead, Microsoft generates pseudonymized tokens as necessary to maintain the required factual records.*
>
> […]
>
> *Service Generated Data (2) and Diagnostic Data (3) are not permitted to hold any customer provided personal data attributes. This data is used by Microsoft engineers so it must be private by design. It only holds pointers, tokens or identifiers that reference the user associated with the activity being logged (2) or the use of the software product (3)."*

Af side 7 i samme svar fremgår følgende:

> *"Engineers in Online Services have to consult system logs as part of the normal course of their duties. Because the logs need to be the factual record of user activity, the logs use a "privacy by design" approach that ensures no directly identifiable information about a user is stored in them. Engineers have no need to know this information in the normal performance of their duties."*

Microsoft angiver også i Microsofts EU Data Boundary dokumentation, at:

> *"Microsoft requires all personal data in Systemgenererede logfiler to be pseudonymized.*
>
> *…*
>
> *[…] we rely on technology that ensures this type of transfer is secure, with controlled access and no persistent storage at the remote access point. When such a data transfer is required, Microsoft uses state-of-the-art encryption […]."*

Der er desuden i Microsoft Irelands databehandleraftale angivet sikkerhedsforanstaltninger, som er indbygget i designet af produkterne, herunder *"Authentication"* og *"Network Design (Microsoft has controls to avoid individuals assuming access rights they have not been assigned to gain access to Customer Data or Professional Services Data they are not authorized to access)."*

Hertil kommer, at de handlinger, som en bruger foretager i forbindelse med behandlingen, logges.

Herudover krypterer Microsoft personoplysninger, og det er således uddybet i svar af 23. april 2024 (Bilag J) side 4,

> *"No Customer Data is ever transmitted in 'clear text' by Microsoft. Transmissions of Customer Data (including the Personal Data therein) over Microsoft internal or public networks are always subject to encryption. Two distinct compounded encryption modes are in simultaneous use – TLS and MACSec (IEEE 802.1AE)."*

Endvidere aggregeres og anonymiseres personoplysninger også, som nærmere beskrevet ovenfor i afsnit 4.14.1og 4.34.3.

Endelig bemærkes det, at De Dataansvarlige vil udarbejde en exitstrategi med henblik på at kunne migrere ud af Microsoft 365 på en hensigtsmæssig måde.

På denne baggrund vurderes det, at De Dataansvarliges brug af Microsoft 365 lever op til kravet i artikel 25 om databeskyttelse gennem design og gennem standardindstillinger.

8. IDENTIFIKATION OG EVALUERING AF RISICI SAMT FORANSTALTNINGER TIL AT HÅNDTERE RISICI

8.1. Indledning

Næste skridt er at identificere risici for de registreredes rettigheder og frihedsrettigheder (risikoidentifikation) samt at evaluere disse risici ud fra deres sandsynlighed og alvor (risikoevaluering), jf. databeskyttelsesforordningens artikel 35, stk. 7, litra c. Nærmere bestemt skal der navnlig foretages en vurdering af risikoens oprindelse, karakter, særegenhed og alvorlighedsgrad, jf. databeskyttelsesforordningens præambelbetragtninger 84 og 90. Vurderingen skal foretages for hver enkelt identificeret risiko set ud fra den registreredes perspektiv, men på et objektivt grundlag.

En risiko kan defineres som et scenarie, der beskriver en hændelse og konsekvenserne heraf, som vurderes i forhold til alvor og sandsynlighed.[72]

Eksempler på konsekvenser for den registrerede kan f.eks. være fysisk, materiel eller immateriel skade, forskelsbehandling, identitetstyveri eller -svig, finansielle tab, skade på omdømme, tab af fortrolighed for personoplysninger, der er omfattet af tavshedspligt, uautoriseret ophævelse af pseudonymisering eller andre betydelige økonomiske eller sociale konsekvenser, samt hvis de registrerede kan blive berøvet deres rettigheder og frihedsrettigheder eller forhindret i at udøve kontrol med deres personoplysninger, jf. præambelbetragtning 75.

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 (lav/mellem restrisiko). De typiske risikostyringsstrategier vil være enten at eliminere eller reducere den identificerede risiko. Det skal for hver enkelt identificeret risiko – der er vurderet som høj eller medium – fremgå af konsekvensanalysen, hvorvidt risikoen er elimineret, reduceret eller accepteret. Det skal også konkluderes, om den samlede restrisiko fortsat vil være høj, såfremt de påtænkte foranstaltninger implementeres, da Datatilsynet i så fald skal høres, jf. databeskyttelsesforordningens artikel 36.

8.2. Valg af evalueringskriterier for sandsynlighed og konsekvens

I denne konsekvensanalyse anvendes følgende evalueringskriterier for sandsynlighed:

Tabel IV Evalueringskriterier for sandsynlighed

4	**Forventet**: Det forventes, at hændelsen vil forekomme; f.eks. (i) Man har erfaring med hændelsen inden for de sidste 12 måneder; eller (ii) Hænder jævnligt i andre offentlige og private organisationer (omtales ofte i pressen).

[72] EDPB, WP 248, rev. 01, s. 7.

3	**Sandsynligt**: Det er sandsynligt, at hændelsen vil forekomme; f.eks. (i) Man har erfaring med hændelsen, men ikke inden for de seneste 12 måneder; eller (ii) Kendes fra offentlige og private virksomheder (omtales årligt i pressen).
2	**Mindre sandsynligt**: Hændelsen forventes ikke at forekomme; f.eks. (i) Mindre erfaring med hændelsen; eller (ii) Kendes fra offentlige og private virksomheder.
1	**Usandsynligt**: Det kan anses for næsten udelukket, at hændelsen nogensinde kan forekomme; f.eks. (i) Ingen erfaring med hændelsen; eller (ii) Kendes kun fra få og af hinanden uafhængige hændelser i offentlige og private virksomheder.

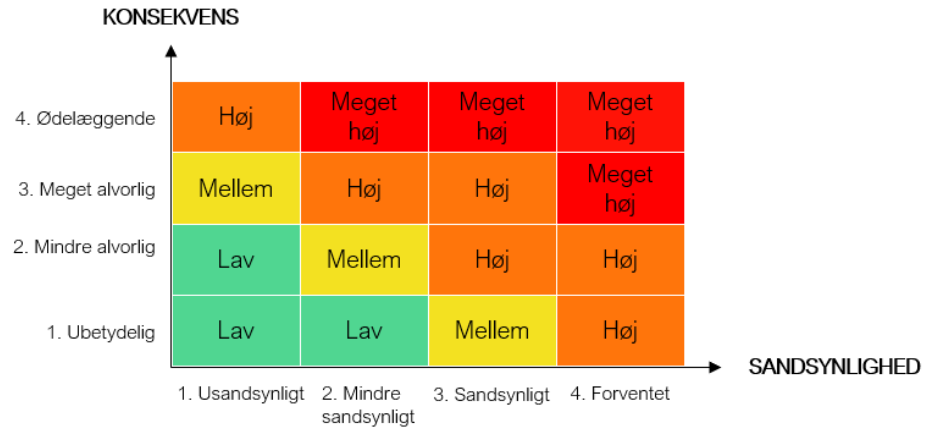
I denne konsekvensanalyse anvendes følgende evalueringskriterier for konsekvens[73]:

Tabel V Evalueringskriterier for konsekvens

4	**Ødelæggende**: Registrerede kan opleve betydelige og indgribende konsekvenser, som det ikke er muligt eller kun vanskeligt muligt at overkomme (mistet erhvervsevne, langvarige fysiske og psykiske påvirkninger, død og lignende).
3	**Meget alvorlig:** Registrerede kan opleve betydelige konsekvenser, som kun kan overkommes med betydelig indsats og konsekvenser for den enkelte (økonomiske konsekvenser, fejlkontering af midler, sortlistning eller nedgradering i kreditmuligheder, fysisk skade på aktiver, påvirkning af arbejdssituation, stævning, dårligere helbred og lignende).
2	**Mindre alvorlig**: Registrerede kan opleve betydelige uhensigtsmæssigheder, som de kan overkomme med en indsats og overvindelse af nogle få besværligheder (ekstra omkostninger, manglende adgang til forretningsservices, frygt, mangel på forståelse, stress og mindre påvirkning af fysisk karakter og lignende).
1	**Ubetydelig**: Registrerede kan opleve få uhensigtsmæssigheder, der kan overkommes og imødegås uden større indsats (tid brugt på at genindtaste oplysninger, dårlig brugeroplevelse, irritation og lignende).

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:

[73] Se f.eks. punkt A.2 i Annex A til ISO/IEC 29134:2023; Datatilsynet m.fl., Vejledning om behandlingssikkerhed og databeskyttelse gennem design og standardindstillinger, juni 2018, s. 9; Datatilsynet, skabelon til konsekvensanalyse, 22. maj 2024, tilgængelig på tilsynets hjemmeside her: https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2024/maj/nye-skabeloner-til-gennemfoerelse-af-konsekvensanalyser (senest tilgået 13. april 2026).



Figur 2 Risikokort

8.3. Identificerede risici samt mitigerende foranstaltninger

De Dataansvarlige behandler personoplysninger i forbindelse med anvendelse af de udvalgte applikationer og cloudtjenester i Microsoft 365 samt supportydelser i forbindelse hermed, ligesom Microsoft Ireland behandler disse personoplysninger som databehandler for De Dataansvarlige. Risikovurderingen er baseret på det generelle princip, at vurderinger skal baseres på objektiv information, hvormed menes de specifikke og konkrete omstændigheder, som kan udledes af den påtænkte brug. Scenarier, som hypotetisk kan udledes ved abstrakte betragtninger, er følgelig ikke identificeret. Identifikation af risici for de registreredes rettigheder og frihedsrettigheder i forbindelse med denne behandling tager sit udgangspunkt i det forhold, at behandlingen vedrører mange registrerede, herunder også potentielt børn og sårbare, og behandling af personoplysninger i stort omfang af borgere i Danmark, og at behandlingen kan omfatte både ikke-følsomme, følsomme og fortrolige personoplysninger samt oplysninger om strafbare forhold om disse. Der er endvidere henset til det forhold, at behandlingen – som nærmere beskrevet i afgrænsningen i afsnit 2.4 – ikke omfatter de nævnte fortrolige og følsomme personoplysninger i form af bl.a. genetiske data, biometriske data, straffesager, asylsager m.v.

Behandlingen foretages endvidere som led i De Dataansvarliges lovbestemte opgaver og foretages for og af en offentlig myndighed og vil derfor i de fleste tilfælde ikke være valgfrit for de registrerede. De lovbestemte opgaver vil være forskellige for hver af De Dataansvarlige, men de risici, der er i forbindelse med De Dataansvarliges brug af de udvalgte applikationer og cloudtjenester samt supportydelser, vil overordnet være de samme for alle De Dataansvarlige med undtagelse af tilfælde, hvor konkret konfigurationer valgt af den enkelte dataansvarlige medfører flere eller færre risici. I det følgende er således beskrevet de generelle risici, som det er opfattelsen vil være gældende ved brug af de udvalgte applikationer og cloudtjenester samt supportydelser.

Det er dog De Dataansvarlige hver især, der har ansvaret for at supplere risikobilledet – herunder med identifikation og evaluering af eventuelle yderligere risici – i forbindelse med De Dataansvarliges eventuelle konfigurationer og specielle brug af Microsoft 365. Det betyder, at der kan være både flere og færre risici samt mitigerende foranstaltninger end de, der er beskrevet nedenfor. Se hertil også afsnit 2.4 om afgrænsning af konsekvensanalysen, hvor det f.eks. anføres, at brug af browser og den medfølgende behandling af personoplysninger ikke er medtaget i denne konsekvensanalyse, således at De Dataansvarlige skal supplere denne konsekvensanalyse med en vurdering af denne databehandling, herunder i forhold til identifikation og evaluering af risici forbundet hermed.

Ved identificeringen og evalueringen af risici i det følgende er der taget hensyn til og inddraget forskellige relevante kilder, herunder konsekvensanalyse af 16. februar 2022 vedrørende databeskyttelse om Microsoft Teams, OneDrive, Sharepoint og Azure AD udarbejdet af bl.a. det hollandske justits- og sikkerhedsministerium, samt EDPS' afgørelse af 8. marts 2024 vedrørende EU-Kommissionens brug af Microsoft 365.

Endelig skal det bemærkes, at samtlige risici for de registrerede vedrørende overførsler af personoplysninger til tredjelande, herunder udleveringsanmodninger fra tredjelandes myndigheder i henhold til tredjelands ret, er særskilt behandlet og vurderet i TIA'en, som er vedlagt denne konsekvensanalyse, hvortil der henvises.

8.3.1. Risiko nr. 1: Manglende gennemsigtighed i behandling af systemgenererede personoplysninger om systembrugere og håndtering af de registreredes rettigheder

De registrerede er i databeskyttelsesforordningens kapitel III tillagt en række rettigheder. Dette gælder, uanset om de registrerede er de borgere, hvis personoplysninger bliver behandlet af eller på vegne af De Dataansvarlige, eller de ansatte systembrugere, hvis personoplysninger enten behandles af eller på vegne af De Dataansvarlige. I begge tilfælde med Microsoft Ireland som databehandler.

Borgere og ansatte kan gøre brug af deres rettigheder ved at rette henvendelse til De Dataansvarlige, hvorefter den pågældende myndighed vil træffe de nødvendige foranstaltninger til besvarelse af rettighedsanmodningen, herunder ved udtræk af logs fra systemet og bistand fra Microsoft Ireland. Tilsvarende vil gøre sig gældende for De Dataansvarliges behandling af personoplysninger om systembrugere. Det gælder således både den behandling, som De Dataansvarlige selv foretager ved brug af applikationer og cloudtjenester som hjælpemiddel, men det vedrører også den behandling, som Microsoft Ireland udfører som databehandler for De Dataansvarlige.

Microsoft Ireland har således også som beskrevet ovenfor i afsnit 7.3.27.3.2 forpligtet sig til at bistå De Dataansvarlige med at besvare rettighedsanmodninger.

Behandlingen af systemgenererede personoplysninger om systembrugere, der indsamles fra applikationer (Diagnostic Data) ved disses interaktion med cloudtjenester, og som der genereres af Microsoft Ireland i cloudtjenesterne (Systemgenererede logfiler), er dog relativ kompleks.

Som beskrevet ovenfor i afsnit 7.1.17.1.3 og 7.1.27.1.4 kan det være svært at gennemskue den behandling, som Microsoft Ireland foretager på vegne af De Dataansvarlige ved generering af Systemgenererede logfiler og indsamlet Diagnostic Data. Selvom De Dataansvarlige således kan lave et udtræk af logs for at give brugere indsigt, kan det være svært at se, hvilke personoplysninger der behandles om en bruger til hvilket formål. Der er således en risiko for, at de registreredes rettigheder ikke vil blive håndteret i overensstemmelse med reglerne i databeskyttelsesforordningens kapitel III, herunder kravet om at anmodninger besvares inden for tidsfristen i artikel 12, stk. 3, og på den måde lever op til kravet om, at besvarelsen skal ske i "*en kortfattet, gennemsigtig, letforståelig og lettilgængelig form og i et klart og enkelt sprog*", jf. artikel 12, stk. 1. Microsoft vil dog som også anført ovenfor i afsnit 4.14.1 "*[p]rovide the data controller with the necessary information and cooperation to enable the data controller to respond to the DSRs within the prescribed time limit (usually one month, with a possibility of extension in some cases).*"

Dertil kommer dog, at Statens It og Økonomistyrelsen tidligere har erfaret, at det selv ved eventuel bistand fra Microsoft Ireland er særdeles vanskeligt at få oplyst, hvilke personoplysninger udtræk af logs er udtryk for, og hvordan oplysningerne anvendes.

Det er på den baggrund De Dataansvarliges vurdering, at sandsynligheden for, at risikoen indtræder, er ***forventet***.

Det er dog opfattelsen, at en sådan datamapning ikke er i de registreredes interesse, så længe de registrerede orienteres om, at alle de handlinger, de foretager i systemerne, logges, og at de foretagne logs regelmæssigt gennemgås. Dette skyldes, at oplysninger om, hvilke log der foretages, herunder hvilke logs der undlades, vurderes at skabe en sårbarhed, som ellers ikke vil være til stede. Dette er ikke i de registreredes interesse, ligesom der efter omstændighederne vil kunne gives afslag på indsigt i disse oplysninger, jf. databeskyttelseslovens § 22, stk. 1-2. Der henvises i øvrigt til beskrivelsen heraf i afsnit 7.1.27.1.4.

Henset til ovenstående sikkerhedsbetragtninger samt karakteren og mængden af personoplysninger, herunder at der hovedsageligt er tale om pseudonymiserede ikke-følsomme personoplysninger i form af logs, som vedrører ansatte systembrugere og deres handlinger i Microsoft 365-applikationer og cloudtjenester, sammenholdt med at brugerne oplyses om formålene med behandlingen og den umiddelbart minimale

betydning, det vurderes at have for brugerne, at de eventuelt ikke bliver oplyst om, hvilke konkrete personoplysninger en log dækker over, vurderes konsekvenserne ved den manglende gennemsigtighed og indsigt at være ***mindre alvorlig***, herunder irritation.

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

Foranstaltning nr. 1: De Dataansvarlige støtter systembrugere, som ønsker indsigt

De Dataansvarlige sikrer, at systembrugerne modtager information via en oplysningstekst om behandlingen af personoplysninger om dem i forbindelse med deres brug af de udvalgte applikationer og cloudtjenester i Microsoft 365, herunder ved ændring i formål.

Desuden vil De Dataansvarlige støtte systembrugere og hjælpe med processen, hvis systembrugerne ønsker at gøre brug af deres ret til indsigt i relation til brug af de udvalgte applikationer og cloudtjenester i Microsoft 365. Dette gøres ved, at De Dataansvarlige sikrer, at Microsoft Ireland hjælper med at gøre logs forståelige i det omfang, det er muligt og sikkerhedsmæssigt forsvarligt.

På baggrund af de beskrevne foranstaltninger er det vurderingen, at sandsynligheden for, at den beskrevne risiko indtræder, kan nedjusteres til ***mindre sandsynligt***, mens konsekvenserne forbliver de samme.

Den samlede vurdering af residualrisikoen er ***medium***.

8.3.2. Risiko nr. 2: Manglende iagttagelse af princippet om formålsbegrænsning

Der er i Microsoft Irelands databehandleraftale beskrevet seks formål, hvortil Microsoft Ireland behandler personoplysninger på vegne af De Dataansvarlige ved levering af tjenester og services. Desuden er der yderligere fire formål, hvortil Microsoft Ireland behandler oplysninger til Microsoft Irelands egne forretningsaktiviteter (business operations). Efter EDPS' afgørelse har det imidlertid været diskuteret, hvorvidt princippet om formålsbegrænsning er iagttaget tilstrækkeligt af dataansvarlige, der anvender Microsoft som databehandler ved f.eks. at anvende Microsoft 365, ligesom Chromebook-sagen har givet anledning til at vurdere risikoen for, at der bliver viderebehandlet personoplysninger af databehandleren til andre formål.

For at være sikre på, at de anførte formål ikke indeholder andet eller mere end beskrevet, har Statens It og Økonomistyrelsen til brug for nærværende konsekvensanalyse bedt Microsoft om en konkretisering af de i Microsoft Irelands databehandleraftale oplyste formål samt hvilke personoplysninger, der behandles til hvert af disse formål. Som beskrevet ovenfor i afsnit 7.1.27.1.4 foretages der ikke behandlinger udenfor de pågældende formål, ligesom der ved ændring i disse behandlinger er fokus på de overordnede formål.

Da behandlinger imidlertid som anført løbende kan ændre sig i forbindelse med en vurdering af, hvad der er nødvendigt for at levere Microsofts produkter og services, kan det ikke udelukkes, at der fremadrettet vil ske behandling til andre formål end de oplyste.

Henset til karakteren og mængden af personoplysninger, herunder at der hovedsageligt er tale om pseudonymiserede ikke-følsomme personoplysninger, som vedrører ansatte systembrugere, men at der samtidig kan være tale om personoplysninger, herunder følsomme, om borgere sammenholdt med at det i så fald vil være Microsoft Ireland, der i givet fald foretager en behandling til et uoplyst formål til enten De Dataansvarlige eller Microsofts egne formål, vurderes risikoen at være forbundet med ***mindre alvorlige*** konsekvenser for de registrerede, herunder manglende forståelse, frygt, stress, mindre fysiske gener m.v.

Det vurderes at være ***usandsynligt***, at oplysninger om de registrerede vil blive behandlet til andre formål end de i Microsoft Irelands databehandleraftale oplyste.

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

Det vurderes ikke muligt at mitigere risikoen yderligere, idet De Dataansvarlige dog løbende vil vurdere og afdække, til hvilke formål der behandles personoplysninger, herunder om det fortsat er klart beskrevet og forståeligt, samt hvorvidt der behandles til yderligere formål end forudsat, herunder hvad de enkelte formål dækker over.

Risikoen for eventuel udlevering af personoplysninger til myndigheder i tredjelande er behandlet i TIA'en.

Risikoen for en viderebehandling af personoplysninger til Microsofts egne formål grundet en ikke tilstrækkeligt effektiv anonymisering behandles nedenfor i risiko nr. 4.

8.3.3. Risiko nr. 3: Microsoft indsamler og genererer for mange personoplysninger om de registrerede i forbindelse med Diagnostic Data og Systemgenererede logfiler (manglende iagttagelse af dataminimeringsprincippet)

Microsoft indsamler mange datapunkter, hvoraf flere udgør pseudonymiserede personoplysninger, når Microsoft indsamler Diagnostic Data og Systemgenererede logfiler om brugerne (de ansatte), som nærmere beskrevet ovenfor i afsnit 4.3.

Microsoft oplyser, at alle handlinger, foretaget af en bruger, logges. Som beskrevet ovenfor i afsnit 7.1.37.1.3 om dataminimering sker dette af sikkerhedsmæssige hensyn, jf. databeskyttelsesforordningens artikel 32, da det ikke på forhånd er muligt at vide, hvilke af de indsamlede og genererede logs, der er behov for.

Det vurderes således i de registreredes interesse, at der foretages en omfattende logning, hvor brugernes handlinger i alt væsentligt registreres og gemmes, da logningen bl.a. er begrundet i systemernes sikkerhed. Risikoen ved, at der logges mange personoplysninger, er dog allerede søgt mitigeret ved at pseudonymisere alle Diagnostic Data og Systemgenererede logfiler. Derudover foretages der også en efterfølgende automatiseret pseudonymiseringsproces, hvor personoplysninger, der af den ene eller anden grund ikke skulle være blevet pseudonymiseret i første omgang, pseudonymiseres.[74] Det gælder også tilfælde, hvor en bruger ved en fejl skulle have inkluderet personoplysninger i f.eks. navn på dokumenter o.l.

Desuden aggregeres personoplysninger til et niveau, hvor de er anonymiseret, sådan at Microsoft udelukkende anvender anonymiserede oplysninger til egne formål i form af forretningsaktiviteter (business operations) og herved ikke behandler unødvendige personoplysninger, jf. om anonymisering nærmere nedenfor behandlingen af risiko nr. 4.

Henset til karakteren og mængden af personoplysninger, herunder at der er tale om pseudonymiserede ikke-følsomme personoplysninger, som vedrører ansatte systembrugere, sammenholdt med at indsamlingen vedrører de handlinger, en bruger har foretaget, vurderes risikoen at være forbundet med ***mindre alvorlige*** konsekvenser for de registrerede, herunder manglende forståelse og frygt relateret til tvivl om, hvad oplysningerne kan anvendes til.

Det vurderes at være ***usandsynligt***, at der indsamles og genereres for mange personoplysninger om de registrerede ved Diagnostic Data og Systemgenererede logfiler, særligt også henset til det formål hvortil de behandles.

[74] Microsofts business operations white paper, side 6, 'Overview of processing in the Microsoft cloud'.

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

Det vurderes ikke muligt at mitigere risikoen yderligere med andre foranstaltninger end de, der allerede er blevet foretaget. De Dataansvarlige vurderer og afdækker dog løbende, hvilke personoplysninger der indsamles via Diagnostic Data og Systemgenererede logfiler samt til hvilke konkrete formål, ved selv at trække en oversigt over disse for tenanten og spørge Microsoft ind til dette ved audits.

8.3.4. Risiko nr. 4: Anonymisering af personoplysninger til forretningsaktiviteter er ikke tilstrækkelig effektiv

Som beskrevet nærmere i afsnit 4.1 og 4.3, omdanner Microsoft Ireland pseudonyme personoplysninger – herunder diagnostiske data og systemgenererede logoplysninger – til aggregerede, statistiske oplysninger, som ikke kan henføres til enkeltpersoner (anonyme data). Denne praksis er blevet bekræftet gennem en revisorerklæring udarbejdet af revisionsfirmaet Ernst & Young.
Derudover vil Statens It løbende gennemføre audits for at kontrollere, om anonymiseringen reelt er effektivt gennemført.

Risikoen består i, at anonymiseringen ikke er tilstrækkeligt effektiv, hvis Microsoft måtte have mulighed for at rekonstruere personoplysningerne og dermed bryde anonymiseringen.

Hvis oplysningerne viser sig ikke at være helt eller delvist anonymiserede, kan konsekvensen for de registrerede være, at Microsoft foretager yderligere behandling af de pseudonymiserede personoplysninger som led i virksomhedens egne forretningsmæssige aktiviteter (business operations).
Som beskrevet i afsnit 7.2.3 vurderes det dog, at selv hvis man – imod opfattelsen hos Microsoft, Statens It og Økonomistyrelsen – lægger til grund, at Microsoft ikke har aggregeret de pseudonymiserede data til et niveau, der udgør anonyme oplysninger, så vil en sådan behandling stadig have hjemmel. Der henvises i den forbindelse til databeskyttelsesforordningens artikel 6, stk. 1, litra e, som grundlag for videregivelse af pseudonyme, ikke-følsomme personoplysninger til disse formål.

Henset til disse forhold vurderes risikoen for de registrerede at være forbundet med ingen eller ubetydelige konsekvenser for de registrerede.

Det vurderes at være ***usandsynligt***, at de pseudonymiserede personoplysninger ikke aggregeres til et niveau svarende til en egentlig anonymisering.

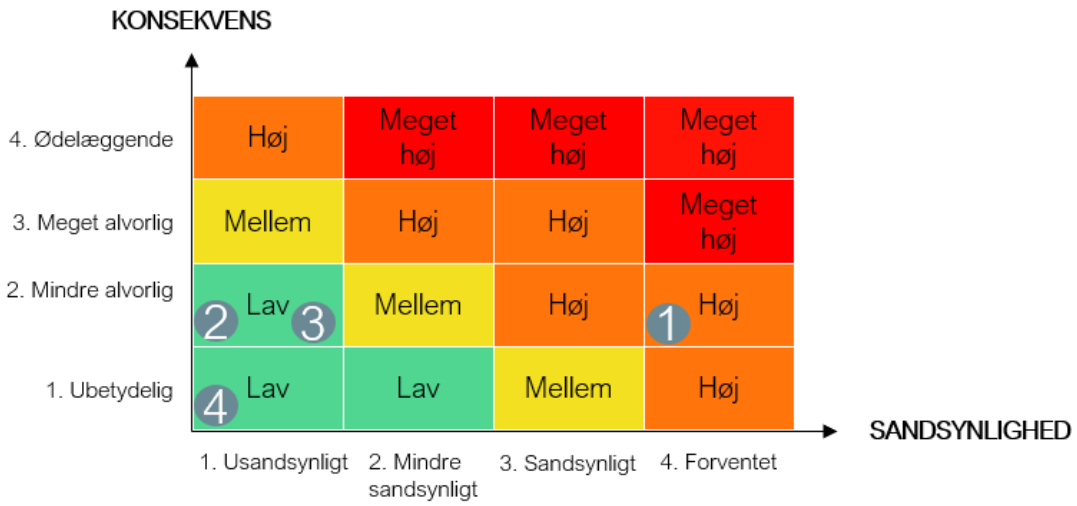
På baggrund af vurderingen af sandsynligheden og konsekvensen er den samlede vurdering af ***risikoen lav***.

Det vurderes ikke muligt at mitigere risikoen yderligere med andre foranstaltninger end de, der allerede er blevet foretaget, og som er beskrevet ovenfor under afsnit 4.1.

8.4. Evaluering af risici

Statens It og Økonomistyrelsen har evalueret de identificerede 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 IV og V i afsnit 8.28.2 ovenfor. De identificerede risici er uddybende beskrevet og evalueret ovenfor i afsnit 8.38.3. Resultatet af denne vurdering fremgår af risikokortet i figur 3 straks nedenfor.

Figur 3: Risikokort med overblik over evaluering af risici før implementering af mitigerende foranstaltninger



8.4.1. Overblik over evaluering og håndtering af risici

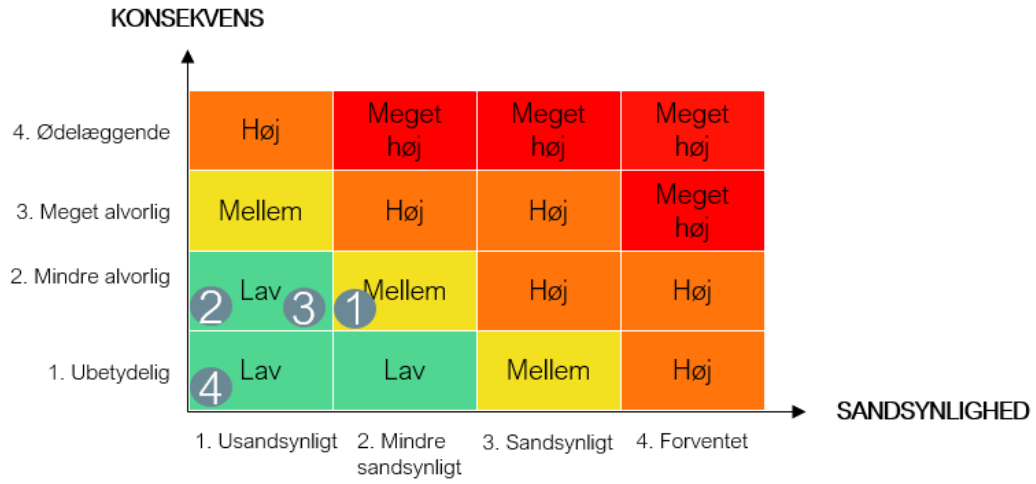
De ovenfor angivne risici i risikokortet kan evalueres og håndteres som følger:

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

Nr.	Risiko	Valg af foranstaltning for at håndtere risiko	Effekt på risiko	Restrisiko
1	Manglende gennemsigtighed i behandling af systemgenererede personoplysninger om systembrugere og håndtering af de registreredes rettigheder.	De Dataansvarlige støtter systembrugere, som ønsker indsigt, jf. afsnit 08.3.1	Reduceret	Medium
2	Manglende iagttagelse af princippet om formålsbegrænsning.	N/A	Accepteret	Lav
3	Microsoft indsamler og genererer for mange personoplysninger om de registrerede i forbindelse med Diagnostic Data og Systemgenererede logfiler (manglende iagttagelse af dataminimeringsprincippet).	N/A	Accepteret	Lav
4	Anonymisering af personoplysninger til forretningsaktiviteter er ikke tilstrækkelig effektiv.	N/A	Accepteret	Lav

Risikokortet for de ovennævnte risici *efter* implementering af mitigerende foranstaltninger vil herefter se ud som følger:

Figur 4 Risikokort med overblik over evaluering af risici efter implementering af mitigerende foranstaltninger



8.4.2. Samlet residualrisiko

Som det fremgår af figur 4 i punkt 8.4.18.4.1 ovenfor, er risiciene mitigeret til **lav-mellem** risiko. Samtidig er der i TIA'en identificeret en række risici forbundet med overførsler til tredjelande og udleveringsanmodninger til tredjelandes myndigheder i henhold til tredjelands ret, hvor det ligeledes konkluderes, at den samlede risiko for de registreredes rettigheder og frihedsrettigheder i forbindelse med overførslerne efter mitigerende foranstaltninger vurderes at være **lav-mellem**.

Den samlede residualrisiko forbundet med behandlingen af personoplysningerne i forbindelse med anvendelse af applikationer og cloudtjenester i Microsoft 365 samt supportydelser i forbindelse hermed er dermed **lav-mellem** risiko.

9. EVENTUEL HØRING AF DATATILSYNET VED HØJ RESIDUALRISIKO

Den dataansvarlige har pligt til at foretage en forudgående høring af Datatilsynet inden påbegyndelsen af en påtænkt behandling af personoplysninger, hvis konsekvensanalysen viser, at behandlingen vil føre til en høj risiko, og den dataansvarlige ikke kan begrænse denne høje risiko ved indførelse af passende foranstaltninger, jf. databeskyttelsesforordningens artikel 36.

Som det fremgår ovenfor i afsnit 8.4.28.4.2, er det vurderingen, at den samlede residualrisiko – dvs. risikobilledet *efter* indførelse af foranstaltninger til at imødegå de identificerede risici – er **lav-mellem** risiko. På denne baggrund har De Dataansvarlige ikke hørt Datatilsynet efter databeskyttelsesforordningens artikel 36.

10. DOKUMENTATION AF DPO'ENS SYNSPUNKTER

10.1. DPO'ens bemærkninger til konsekvensanalyse (DPIA) af Microsoft 365

De Dataansvarlige foranlediger hver især, at deres respektive databeskyttelsesrådgiver (DPO) får lejlighed til at gennemgå nærværende paraply-konsekvensanalyse i sammenhæng med de oplysninger og vurderinger, som De Dataansvarlige hver især er henvist til at supplere denne konsekvensanalyse med, jf. afsnit 2.5.1. De Dataansvarlige sørger herefter selv for at forholde sig til og dokumentere eventuelle kommentarer, som deres respektive databeskyttelsesrådgiver måtte komme med og inddrage disse kommentarer i den endelige vurdering.

10.2. Indledning og DPO'ens rolle

Databeskyttelsesrådgiveren (DPO'en) har i overensstemmelse med artikel 35, stk. 2, i databeskyttelsesforordningen deltaget rådgivende i udarbejdelsen af denne DPIA for Microsoft 365.
Det er blandt andet DPO'ens rolle at rådgive den dataansvarlige om databeskyttelsesmæssige risici, herunder vurdere om de identificerede risici for de registreredes rettigheder er tilstrækkeligt belyst, samt vurdere om de foreslåede foranstaltninger er egnede til at reducere risiciene til et acceptabelt niveau.
Det er ikke DPO'ens rolle at godkende behandlingen, men udelukkende at afgive faglige bemærkninger.

10.3. Overordnet vurdering af DPIA'en

Det er DPO'ens vurdering, at konsekvensanalysen strukturelt lever op til databeskyttelsesforordningens krav. Analysen indeholder en systematisk beskrivelse af behandlingsaktiviteterne, deres formål og sammenhæng, samt en selvstændig vurdering af nødvendighed og proportionalitet. Derudover er der foretaget en identifikation og evaluering af konkrete risici, og der er beskrevet afhjælpende tekniske og organisatoriske foranstaltninger.
Metodisk fremstår analysen gennemarbejdet og i overensstemmelse med gældende retningslinjer for udarbejdelse af konsekvensanalyser. Den valgte struktur understøtter ansvarlighedsprincippet, da de vurderinger og forudsætninger, der ligger til grund for konsekvensanalysen, er eksplicit dokumenteret.

10.4. Bemærkninger om DPIA'ens karakter og anvendelse

DPO'en bemærker at denne DPIA har karakter af en generel/paraply konsekvensanalyse, der er blevet udarbejdet med henblik på anvendelse af flere myndigheder. Dette er forventeligt, når der er tale om ensrettede eller sammenlignelige behandlingsaktiviteter. Dette indebærer dog, at den enkelte dataansvarlige er forpligtet til at foretage en konkret vurdering af egne behandlingsformål, datatyper, konfigurationer, slettepolitikker, aktivliste og adgangsstyring. Herunder aktive beslutninger om hvilke organisatoriske og tekniske foranstaltninger der faktisk skal implementeres, samt individuelle risici specifikke for deres organisation.

DPO'en anbefaler derfor, at de dataansvarlige der ønsker at anvende indeværende DPIA, udarbejder et lokalt tillæg eller supplerende DPIA som dokumenterer denne stillingtagen.

10.5. Vurdering af risici og residualrisiko

Analysen identificerer relevante risici for gennemsigtighed, formålsbegrænsning, dataminimering og effektiv anonymisering. DPO'en finder, at disse risici er velbegrundede og af passende prioritet.
Den samlede residualrisiko vurderes i analysen at være lav til mellem. DPO'en tiltræder denne vurdering under forudsætning af, at de beskrevne tekniske og organisatoriske foranstaltninger implementeres fuldt ud, og at der etableres løbende kontrol og opfølgning. Vurderingen bør betragtes som betinget af korrekt konfiguration og effektiv adgangsstyring.

10. 6. Microsofts behandling af data til egne formål

Konsekvensanalysen indeholder en udførlig gennemgang af Microsofts datakategorier og behandlingsaktiviteter, herunder Diagnostic Data og System-Generated Logs. Det er positivt, at der er indhentet uddybende redegørelser fra Microsoft, og at behandlingen er analyseret i forhold til både leveringen af tjenesten og eventuelle forretningsaktiviteter.
DPO'en bemærker dog, at vurderingen hviler på Microsofts egne beskrivelser og forpligtelser. Disse beskrivelser er af overordnet karakter, og det anbefales derfor, at der igangsættes løbende kontrol og audit af de faktiske behandlingsaktiviteter. Dette gælder særligt i relation til håndtering af de registreredes rettigheder, og dokumentation af anonymisering ved anvendelse til Microsofts egne formål.

10.7. Vurdering af internationale overførsler

DPO'en bemærker, at der siden udarbejdelsen af den foreliggende Transfer Impact Assessment (TIA) er sket visse udviklinger i Microsofts tekniske og kontraktuelle rammer for databehandling, herunder initiativer med henblik på øget datalokalisering i EU som implementeringen af EU Data Boundary. Disse udviklinger kan efter omstændighederne have betydning for vurderingen af risikoen for internationale overførsler og adgangen til personoplysninger fra tredjelande.

DPO'en konstaterer imidlertid, at disse forhold ikke ændrer den overordnede vurdering i den foreliggende konsekvensanalyse af Microsoft 365 egnethed, idet DPIA'en fortsat hviler på en samlet vurdering af gældende retstilstand, kendt praksis og de identificerede risici. DPO'en bemærker dog, at den vedlagte TIA bør opdateres løbende i lyset af retlige og faktiske udviklinger, herunder færdigimplementeringen af EU Data Boundary samt øvrige relevante ændringer i behandlingsopsætningen eller retspraksis.

10.8. Chromebook-sagen

DPO'en bemærker, at der siden udarbejdelsen af denne DPIA er kommet en ny afgørelse i den såkaldte Chromebook- sag (Journalnummer: 2025-431-0053). Datatilsynet har i den forbindelse udtalt sig vedrørende brugen af underdatabehandlere. DPO'en finder dog, at denne afgørelse ikke i mærkbar grad ændrer på vurderingerne i denne DPIA.

10.9. Konklusion

DPO'en konkluderer under disse forudsætninger, at der ikke foreligger en høj residualrisiko, som ville nødvendiggøre forudgående høring hos Datatilsynet efter databeskyttelsesforordningen art. 36. Denne vurdering forudsætter, at behandlingen gennemføres i overensstemmelse med de beskrevne foranstaltninger, og at væsentlige ændringer i behandlingen fører til en fornyet vurdering.
DPO'en anbefaler, at indeværende- og lokalt udarbejdede konsekvensanalyser undergives regelmæssig revision (ved væsentlige ændringer i systemanvendelsen, behandlingsaktiviteter eller risikobilledet), og at de dataansvarlige etablerer procedurer for opfølgning på de identificerede risici, herunder i forhold til Microsofts behandling til egne formål, og håndtering af de registreredes rettigheder.

11. LEDELSENS GODKENDELSE AF KONSEKVENSANALYSEN

Konsekvensanalysen har været forelagt ledelsen hos Økonomistyrelsen.

Ledelsen har besluttet følgende vedrørende konsekvensanalysen:

Tabel VII Ledelsens godkendelsesskema

Beslutning	Beskrivelse
Godkendt	Behandlingen kan herefter påbegyndes, såfremt de i konsekvensanalysen mitigerende foranstaltninger bliver implementeret.
Betinget godkendt	Behandlingen kan alene påbegyndes, hvis nærmere beskrevne ændringer foretages. Der skal derfor fremlægges en revideret konsekvensanalyse for ledelsen med henblik på endelig godkendelse.
Ikke godkendt	Behandlingen gennemføres ikke.

Direktionen i Økonomistyrelsen har **godkendt** konsekvensanalysen og har forholdt sig til de forhold, den skal suppleres med, jf. afsnit 2.5. Konsekvensanalysen vil endvidere blive ajourført løbende, og Økonomistyrelsen vil holde sig opdateret på retstilstanden, jf. DPO'ens bemærkninger og nedenstående.

12. VEDLIGEHOLDELSE OG AJOURFØRING AF KONSEKVENSANALYSEN

Statens It og Økonomistyrelsen er ansvarlige for vedligeholdelse og ajourføring af nærværende konsekvensanalyse.
Konsekvensanalysen vedrørende anvendelsen af Microsoft 365 – herunder tilknyttede applikationer, cloudtjenester og supportydelser, vil blive opdateret ved væsentlige ændringer i systemanvendelsen, behandlingsaktiviteter eller risikobilledet.

De dataansvarlige skal regelmæssigt gennemgå og opdatere konsekvensanalysen i overensstemmelse med databeskyttelsesforordningens artikel 35, stk. 11. Dette omfatter både en generel gennemgang af de databeskyttelsesretlige forhold samt vurdering af de behandlingsaktiviteter, som analysen omfatter. Der henvises til navnlig afsnit 2.2. og 2.5.1. for en nærmere gennemgang af de dataansvarliges selvstændige ansvar og forpligtelser.

12.1. Tilføjelse af nye applikationer og services

Ved tilføjelse af nye applikationer til Microsoft 365-løsningen skal der foretages en særskilt vurdering af den pågældende applikation, herunder formål, datatyper, adgangsforhold og eventuelle nye risici. Resultatet heraf indarbejdes som en del af den samlede konsekvensanalyse.

13. BILAG

Bilag A	Oversigt over behandlingsaktiviteter, som udfyldes af De Dataansvarlige
Bilag B	Microsoft Product Terms, February 02, 2024, Program: EA/EAS/SCE
Bilag C	Microsoft Products and Services Data Protection Addendum, September 01, 2025
Bilag D	Microsoft data protection and security terms for products and services: Business operations, March 2023
Bilag E	Dokumentation vedrørende EU Data Boundary ”What is the EU Data Boundary”, 01/02/2024
Bilag F	Transfer Impact Assessment (TIA) til vurdering af internationale overførsler af person-data ved brug af de udvalgte applikationer og cloudtjenester i Microsoft 365
Bilag G	Microsoft business operations white paper vol. 2
Bilag H	Microsoft 365 and Office 365 service descriptions”, fra Microsofts hjemmeside den 27. februar 2024
Bilag I	Microsofts svar af 2. april 2024
Bilag J	Microsofts svar af 23. april 2024
Bilag K	Microsofts svar af 6. maj 2024
Bilag L	Skabelon til aktivoversigt for M365-aktiver
Bilag M	Beskrivelse og oversigt over E3- og E5-licenserne

14. ÆNDRINGSLOG

Denne indholdsmæssige ændringslog supplerer den overordnede versionshistorik øverst i dokumentet. Loggen dokumenterer væsentlige og mindre ændringer i DPIA'ens indhold, herunder ændringer med betydning for risikovurderingen, i overensstemmelse med GDPR-forordningens artikel 35.

Version	Ændringstype	Indholdsmæssig ændring	Konsekvens for risikoniveau
1.0 af 26. September 2024	Første version af konsekvensanalysen.	_____	_____
1.1. af 16. juni 2025	Tilføjelse af nye aktiver til DPIA	_____	_____
2.0 af 15. April 2025	Anden version af konsekvensanalysen.	a. Opdateret bilag C b. Tilføjet bilag L og M c. Opdateret og uddybet afsnit 10 "Dokumentation af DPO'ens synspunkter" d. Opdateret afsnit 3.1.2, "Begreber og vilkår i M365", for begrebet Office 365 Services og tilføjelserne Cloud Apps samt sondring mellem E3-og E5-licensen. e. Tilføjelse af nyt afsnit 3.2. "Metode til konsekvensvurdering og kategorisering af aktiver i Microsoft 365" og afsnit 3.3. "Governance og ansvarsplacering" f. Opdateret afsnit 3.4. "Cloudtjenester og cloud-applikationer omfattet af konsekvensanalysen" g. Udgået tidligere afsnit 1.11. "Aktiver, cloudtjenester og applikationer	Ingen ændring af samlet risikoniveau.

		omfattet af DPIA" og inkorporeret i afsnit 3.2.3. og 3.5. h. Opdateret afsnit 3.5. "Aktiver, cloudtjenester og applikationer omfattet af DPIA" i. Opdateret afsnit 3.6. "Detaljerede beskrivelser af aktiver" j. Rettelse af ukorrekt datoangivelse for v. 1.0. i ændringslog for v. 1.1. af den 16. juni 2025.	