|  |
| --- |
| Konsekvensanalyse vedrørende databeskyttelse  Anvendelse af udvalgte applikationer og cloudtjenester i Microsoft 365 samt supportydelser i forbindelse hermed |

Dataansvarlig: Økonomistyrelsen

Ansvarlige for udarbejdelse af konsekvensanalysen: Økonomistyrelsen og Statens It

Ansvarlige kontaktpersoner hos Statens It og Økonomistyrelsen: Helle Uldbæk Sørensen og Nicolaj Haahr Hartbøl

Dato: 26. september 2024

Databeskyttelsesrådgiver (DPO) hos den dataansvarlige: Maibritt Zuchske

|  |  |
| --- | --- |
| Version | Kommentar |
| 1.0 september 2024 | Første version af konsekvensanalyse |

Indhold

[1. Sammenfatning 6](#_Toc170816034)

[2. Baggrund, formål og afgrænsning 8](#_Toc170816035)

[2.1 Baggrund 8](#_Toc170816036)

[2.2 Pligten til at udarbejde en konsekvensanalyse vedrørende databeskyttelse 10](#_Toc170816037)

[2.3 Formålet med konsekvensanalysen 11](#_Toc170816038)

[2.4 Afgrænsning af konsekvensanalysen 12](#_Toc170816039)

[2.5 Særligt opmærksomhedspunkt i forhold til konsekvensanalysen 14](#_Toc170816040)

[3. Processen for gennemførelsen af konsekvensanalysen 16](#_Toc170816041)

[3.1 Metode 16](#_Toc170816042)

[3.2 Inddragelse af de registrerede 17](#_Toc170816043)

[4. Brugernes anvendelse af de udvalgte applikationer og cloudtjenester i Microsoft 365 18](#_Toc170816044)

[4.1 Generelt om Microsoft 365 og sammenhæng 18](#_Toc170816045)

[4.2 Cloudtjenester og applikationer omfattet af konsekvensanalysen 20](#_Toc170816046)

[4.2.1 Word, PowerPoint, Excel 20](#_Toc170816047)

[4.2.2 Office for the web 21](#_Toc170816048)

[4.2.3 Outlook og Exchange Online 21](#_Toc170816049)

[4.2.4 Teams 21](#_Toc170816050)

[4.2.5 Sharepoint og OneDrive for Business 22](#_Toc170816051)

[4.2.6 Entra ID 22](#_Toc170816052)

[4.3 Formålet med behandlingen 22](#_Toc170816053)

[4.4 Behandlingen af personoplysninger 24](#_Toc170816054)

[4.4.1 Behandlingens karakter og omfang 24](#_Toc170816055)

[5. Microsofts behandling af personoplysninger, databehandleraftale og vilkår 25](#_Toc170816056)

[5.1 Microsofts datakategorier 26](#_Toc170816057)

[5.2 Microsoft Irelands databehandleraftale 34](#_Toc170816058)

[5.2.1 Anvendelsesområde 34](#_Toc170816059)

[5.2.2 Generelt om Microsofts behandling af data 35](#_Toc170816060)

[5.2.3 Generelt om behandling med henblik på at levere produkter og services 35](#_Toc170816061)

[5.2.4 Generelt om behandling for at understøtte ”business operations” 40](#_Toc170816062)

[5.3 Microsofts business operations white paper 41](#_Toc170816063)

[5.3.1 Særligt om Diagnostic Data 49](#_Toc170816064)

[5.4 Audit og kontrolmuligheder 51](#_Toc170816065)

[6. roller i forbindelse med behandlingen af personoplysninger 51](#_Toc170816066)

[6.1 De Dataansvarliges rolle som selvstændigt dataansvarlige 51](#_Toc170816067)

[6.2 Statens It’s rolle som databehandler 52](#_Toc170816068)

[6.3 Microsofts databeskyttelsesretlige rolle 52](#_Toc170816069)

[6.3.1 Microsofts rolle som databehandler ved levering af produkterne og services 52](#_Toc170816070)

[6.3.2 Microsofts rolle ved behandling af anonymiserede oplysninger til forretningsaktiviteter (business operations) 58](#_Toc170816071)

[7. Microsofts placering af data og tredjelandsoverførsler 63](#_Toc170816072)

[8. Vurdering af nødvendigheden og proportionaliteten 65](#_Toc170816073)

[8.1 De grundlæggende principper 66](#_Toc170816074)

[8.1.1 Princippet om lovlighed, rimelighed og gennemsigtighed 66](#_Toc170816075)

[8.1.2 Princippet om formålsbegrænsning 69](#_Toc170816076)

[8.1.3 Princippet om dataminimering 74](#_Toc170816077)

[8.1.4 Princippet om rigtighed 78](#_Toc170816078)

[8.1.5 Princippet om opbevaringsbegrænsning 79](#_Toc170816079)

[8.1.6 Princippet om integritet og fortrolighed (behandlingssikkerhed) 81](#_Toc170816080)

[8.2 Hjemmelsgrundlag 88](#_Toc170816081)

[8.2.1 Databeskyttelseslovgivningen 88](#_Toc170816082)

[8.2.2 Vurdering af grundlaget for behandling til De Dataansvarliges formål 96](#_Toc170816083)

[8.2.3 Vurdering af grundlag for aggregering og efterfølgende behandling til Microsofts forretningsaktiviteter 98](#_Toc170816084)

[8.3 De registreredes rettigheder 100](#_Toc170816085)

[8.3.1 Oplysningspligten 100](#_Toc170816086)

[8.3.2 Øvrige rettigheder 100](#_Toc170816087)

[8.4 Overførsel af personoplysninger til modtagere i tredjelande og internationale organisationer 104](#_Toc170816088)

[8.5 Databeskyttelse gennem design og standardindstillinger 105](#_Toc170816089)

[9. Identifikation og evaluering af risici samt foranstaltninger til at håndtere risici 107](#_Toc170816090)

[9.1 Indledning 107](#_Toc170816091)

[9.2 Valg af evalueringskriterier for sandsynlighed og konsekvens 108](#_Toc170816092)

[9.3 Identificerede risici samt mitigerende foranstaltninger 110](#_Toc170816093)

[9.3.1 Risiko nr. 1: Manglende gennemsigtighed i behandling af systemgenererede personoplysninger om systembrugere og håndtering af de registreredes rettigheder 111](#_Toc170816094)

[9.3.2 Risiko nr. 2: Manglende iagttagelse af princippet om formålsbegrænsning 113](#_Toc170816095)

[9.3.3 Risiko nr. 3: Microsoft indsamler og genererer for mange personoplysninger om de registrerede i forbindelse med Diagnostic Data og System-Generated Logs (manglende iagttagelse af dataminimeringsprincippet) 115](#_Toc170816096)

[9.3.4 Risiko nr. 4: Anonymisering af personoplysninger til forretningsaktiviteter er ikke tilstrækkelig effektiv 116](#_Toc170816097)

[9.4 Evaluering af risici 117](#_Toc170816098)

[9.4.1 Overblik over evaluering og håndtering af risici 117](#_Toc170816099)

[9.4.2 Samlet residualrisiko 119](#_Toc170816100)

[10. Eventuel høring af Datatilsynet ved høj residualrisiko 119](#_Toc170816101)

[11. Dokumentation af DPO’ens synspunkter 120](#_Toc170816102)

[12. Ledelsens godkendelse af konsekvensanalysen 120](#_Toc170816103)

[13. Vedligeholdelse og ajourføring af konsekvensanalysen 120](#_Toc170816104)

**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, January 02, 2024

Bilag D: Microsoft data protection and security terms for products and services: Business operations, March 2023

Bilag E: Microsofts documentation 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

# Sammenfatning

Denne konsekvensanalyse vedrørende databeskyttelse er udarbejdet af Statens It og Økonomistyrelsen som en konsekvensanalyse, som de dataansvarlige offentlige myndigheder (”De Dataansvarlige”) kan anvende til brug for vurderingen af lovligheden og risiciene forbundet med behandlingen af personoplysningerne efter databeskyttelsesforordningens regler ved brug af udvalgte applikationer og cloudtjenester i cloudløsningen Microsoft 365 samt supportydelser i forbindelse hermed.

Det konkluderes i konsekvensanalysen, at der er en række risici, der kan mitigeres med effektive foranstaltninger, således at 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 de omfattede produkter og services kan ske inden for rammerne af databeskyttelsesforordningens regler. Det gælder også i forhold til behandling af personoplysninger i forbindelse med eventuelle overførsler af personoplysninger til tredjelande samt ved udleveringsanmodninger, som er nærmere beskrevet og vurderet i en såkaldt Transfer Impact Assessment (TIA), som er vedlagt konsekvensanalysen.

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 Diagnostic Data og Service-Generated Logs.
4. Anonymisering af personoplysninger til forretningsaktiviteter er ikke tilstrækkelig effektiv.

Der er endvidere i TIA’en identificeret og vurderet en række risici i forbindelse med opbevaring af personoplysninger i EU i forhold til udleveringsanmodninger fra tredjelande i henhold til tredjelands ret samt i forbindelse med overførsler af personoplysninger til usikre tredjelande. Her konkluderes det, at den samlede risiko for de registreredes rettigheder og frihedsrettigheder efter 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 tjenesterne og services omfattet af konsekvensanalysen efter databeskyttelsesforordningens artikel 36.

Denne konsekvensanalyse opdateres løbende, når det skønnes nødvendigt. Supplerende til konsekvensanalysen vil der blive lavet løbende audit 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 Microsoft 365, som nærmere beskrevet i afgrænsningerne i afsnit 2.4 og 2.5.

Denne konsekvensanalyse opdateres løbende, når det skønnes nødvendigt.

Staten afsøger mulighederne for, at staten skal, i overvejende grad, flytte til cloudløsningen Microsoft 365, hvor der på nuværende tidspunkt anvendes en *on premise* løsning, hvor Microsoft 365 kan hostes i lokale datacentre, men under visse begrænsninger, der medfører, at det fulde potentiale af cloudløsningen ikke kan realiseres. Statens It overvejer at tilbydefølgende applikationer fra Microsoft 365, som er behandlet i denne konsekvensanalyse:

* Word
* Excel
* Outlook
* PowerPoint
* Teams

Herudover vil også følgende cloudtjenester blive anvendt i tilknytning til applikationerne:

* Exchange online
* OneDrive
* Sharepoint
* Teams online
* Entra ID.

# Baggrund, formål og afgrænsning

## Baggrund

Microsoft 365 er en clouddrevet produktivitetsplatform, der indeholder tre typer af services: software, online tjenester og professionelle services. Staten afsøger mulighederne for, at staten skal, i overvejende grad, flytte til cloudløsningen, hvor der på nuværende tidspunkt anvendes en *on premise* løsning, hvor Microsoft 365 kan hostes i lokale datacentre, men under visse begrænsninger, der medfører, at det fulde potentiale af cloudløsningen ikke kan realiseres. Ved at flytte til cloudløsningen kan den fulde version af Microsoft 365 anvendes med udtagelse af få applikationer, jf. afsnit 2.4.

Microsoft 365-licenser indkøbes igennem statens licenspartner Crayon A/S, der sørger for levering af bl.a. Microsoft-produkter til De Dataansvarlige i henhold til aftale indgået med Økonomistyrelsen. Det er reguleret af rammeaftale 1D1 og 1D2 mellem Økonomistyrelsen og Crayon A/S, som Økonomistyrelsen udover at være part i samtidig har indgået på vegne af De Dataansvarlige. Da Crayon A/S er licenspartner, betyder det, at fakturering sker igennem Crayon A/S, hvor Microsoft sender fakturaer til Crayon A/S om statens forbrug, hvorefter Crayon A/S videresender fakturaerne til staten. Crayon A/S’ behandling af oplysninger vedrører aggregerede data[[1]](#footnote-1), som Microsoft har redegjort for, er aggregeret til et niveau, hvor oplysningerne ikke er personhenførbare (anonyme data).

I rammeaftale 1D1, punkt 10, og 1D2, punkt 9, henvises der til, at kundens brugsrettigheder til softwareprodukterne er reguleret af softwareproducentens standardlicensvilkår med de modifikationer, som fremgår af bl.a. bilag 6. Bilag 6 henviser til en række underbilag, herunder standardvilkår fra Microsoft Ireland, f.eks. *Master Business Service Agreement* (herefter ”MBSA”) og ændringer til standardvilkårene (*amendments*), f.eks. et ændringstillæg til MBSA’en. 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 Crayon A/S.

Når De Dataansvarlige anvender Microsoft 365, behandler Microsoft Ireland som databehandler personoplysninger på vegne af De Dataansvarlige. Økonomistyrelsen indgår ikke databehandleraftale med Microsoft Ireland på vegne af De Dataansvarlige. De Dataansvarlige indgår i stedet selv en databehandleraftale direkte med Microsoft Ireland. Parterne vil indgå Microsoft Irelands standard databehandleraftale ”*Microsoft Products and Services Data Protection Addendum”,* hvor den seneste version er fra den 2. januar 2024(herefter ”Microsoft Irelands databehandleraftale”) (Bilag C)*.*

Crayon A/S vil ikke indgå i nærværende konsekvensanalyse grundet sin rolle i aftalekonstruktionen, og da Crayon A/S’ behandling af oplysninger alene vedrører aggregerede data.[[2]](#footnote-2)

Microsoft Ireland, der selv 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, herunder pårørende og værger, (herefter benævnt samlet ”borgere”) samt nuværende ansatte, tidligere ansatte og kollegaer hos andre myndigheder (herefter samlet benævnt ”ansatte”).

**Statens It**

Statens It overvejer at tilbyde sine tilsluttede statslige ministerier, styrelser og selvejende uddannelsesinstitutioner brug af cloudløsningen Microsoft 365. Statens It leverer it-drift og services til tilsluttede statslige ministerier, styrelser og selvejende uddannelsesinstitutioner. Det omfatter i alt cirka 40.000 brugere, hvoraf størstedelen er inden for 21 ministerområder.[[3]](#footnote-3)

Ansvaret for driften af de statslige myndigheders basale it-systemer er (og bliver løbende i forbindelse med tilgang af nye kunder) ressortoverdraget fra de respektive ressortministre til finansministeren ved kongelige resolutioner.[[4]](#footnote-4) Dette indebærer ligeledes en overdragelse af ansvaret for kontrakter og informationssikkerhed. Økonomistyrelsen har ansvaret Statens Indkøbsprogram og udbyder i den sammenhæng bl.a. en rammeaftale om standardsoftware, hvor staten kan indkøbe standardsoftware fra Microsoft, aktuelt gennem forhandleren Crayon A/S. De tilsluttede institutioner (herefter ”De Dataansvarlige”) beslutter dog selv, hvilke af de tilbudte produkter og services der ønskes anvendt. De Dataansvarlige har tillige ansvaret for behandling af personoplysninger i forbindelse med brug af produkter og services, hvilket vil sige, at De Dataansvarlige hver især er dataansvarlige efter databeskyttelsesforordningens regler.

Statens It overvejer at tilbyde De Dataansvarlige brug af cloudløsningen Microsoft 365. Produkt og service tilbydes af Microsoft Ireland Operations, Ltd. (herefter ”Microsoft Ireland”) som aftalepart. Statens It overvejer at tilbyde følgende applikationer fra Microsoft 365-licensen:

* Word
* Excel
* Outlook
* PowerPoint
* Teams

Herudover vil også følgende cloudtjenester blive anvendt i tilknytning til applikationerne:

* Exchange online
* OneDrive
* Sharepoint
* Teams online
* Entra ID.

Statens It er forvalter af den fælles tenant for Microsoft 365, der oprettes for samtlige kunder. Det er Statens It, der 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 Microsoft 365 tages i brug.

## 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 med en konsekvensanalyse. Artikel 29-Gruppen (nu Det Europæiske Databeskyttelsesråd, herefter forkortet ”EDPB”) har i deres retningslinjer herom[[5]](#footnote-5) fastsat kriterier, der kan hjælpe til at identificere de behandlinger, der vil kræve en konsekvensanalyse.

Retningslinjerne fastslår, at en dataansvarlig i de fleste tilfælde skal overveje at udføre en konsekvensanalyse, hvor to af de pågældende kriterier er opfyldt, men at dette også – i nogle tilfælde – kan overvejes for behandlinger, der alene opfylder ét af kriterierne.

Da behandlingen af personoplysninger ved brug af Microsoft 365 vil ske som led i varetagelse af lovbestemte opgaver, herunder afgørelsesvirksomhed, faktisk forvaltningsvirksomhed og personaleadministration samt visse administrative formål (herefter ”sagsbehandling og personaleadministration”), vil behandlingen hos De Dataansvarlige være kontinuerlig og regelmæssig, ligesom den vil vedrøre et omfattende antal registrerede. Afhængig af De Dataansvarlige og de behandlinger, som de enkelte dataansvarlige foretager, kan det også vedrøre en stor mængde af personoplysninger. Desuden kan det ikke udelukkes, at personoplysninger vil blive overført til modtagere i tredjelande, herunder USA, da en række af de underdatabehandlere, som Microsoft Ireland anvender til levering af tjenesteydelser, er lokaliseret udenfor EU/EØS. Behandlingen vurderes derfor som omfattende i henhold til EDPB’s retningslinjer for udarbejdelse af konsekvensanalyser vedrørende databeskyttelse, jf. s. 10 ff. Behandlingen kan endvidere efter omstændighederne vedrøre følsomme personoplysninger omfattet af databeskyttelsesforordningens artikel 9, ligesom behandlingen kan vedrøre sårbare personer.

Derved er mindst tre ud af ni kriterier, herunder kriterium nr. 4 (følsomme oplysninger eller oplysninger af meget personlig karakter), kriterium nr. 5 (omfattende behandling) samt kriterium nr. 7 (oplysninger om sårbare registrerede) opfyldt i henhold til EDPB’s retningslinjer, hvilket ifølge EDPB medfører, at der skal laves en konsekvensanalyse vedrørende databeskyttelse. Statens It og Økonomistyrelsen har derfor besluttet at udarbejde en konsekvensanalyse vedrørende databeskyttelse af behandlingen af personoplysninger ved brug af de udvalgte applikationer og cloudtjenester fra Microsoft 365 samt supportydelser i forbindelse hermed.

## 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 de udvalgte applikationer og cloudtjenester i Microsoft 365, såfremt denne løsning tages i brug.

Konsekvensanalysen indeholder også en vurdering af behandlingens lovlighed, dvs. om behandlingen overholder reglerne i databeskyttelsesforordningen[[6]](#footnote-6) og databeskyttelsesloven.[[7]](#footnote-7)

Konsekvensanalysen har endvidere til formål at afdække risici for fysiske personers rettigheder og frihedsrettigheder forbundet med De Dataansvarliges behandling af personoplysninger ved brug af de udvalgte applikationer og cloudtjenester i Microsoft 365 samt at bidrage til at håndtere disse risici. Det sker ved at vurdere risiciene og fastlægge solide og effektive foranstaltninger til at afhjælpe dem.

Hvis konsekvensanalysen viser, at behandlingen af personoplysninger ved brug af de udvalgte applikationer og cloudtjenester i Microsoft 365 vil føre til en høj risiko for de registrerede i mangel af foranstaltninger truffet af De Dataansvarlige for at begrænse risikoen (residualrisikoen), skal Datatilsynet høres om behandlingen, inden behandlingen foretages, jf. databeskyttelsesforordningens artikel 36, stk. 1.

Konsekvensanalysen er endelig en forudsætning for overholdelse af databeskyttelsesforordningens grundlæggende princip om ansvarlighed (dokumentation for overholdelse af forordningens regler), jf. forordningens artikel 5, stk. 2, og artikel 24. Konsekvensanalysen har herudover en naturlig sammenhæng med reglerne om databeskyttelse gennem design og gennem standardindstillinger og kan give værdifuldt input til vurdering af løsningsdesignet, herunder ved opsætning og konfiguration samt mitigerende foranstaltninger.

## Afgrænsning af konsekvensanalysen

Konsekvensanalysen vedrører den behandling af personoplysninger, som De Dataansvarlige foretager ved brug af de udvalgte applikationer og cloudtjenester i Microsoft 365, som er nævnt ovenfor i afsnit 2.1.

Konsekvensanalysen omfatter både De Dataansvarliges anvendelse af de applikationer og cloudtjenester og den databehandling, som Microsoft Ireland foretager som databehandler for De Dataansvarlige med henblik på at levere ydelsen. Desuden omfatter det supportydelser fra Microsoft Ireland til De Dataansvarlige, som er en del af Microsoft Irelands Professionel Services. Undtaget er konsulentydelser, da det ikke vil blive anvendt af De Dataansvarlige. Samtidig omfatter konsekvensanalysen den behandling, som underdatabehandlere til Microsoft Ireland foretager med henblik på at levere ydelsen, herunder overførsler til tredjelande. Endelig omfatter konsekvensanalysen en vurdering af lovligheden af eventuelle videregivelser af personoplysninger fra De Dataansvarlige til Microsoft Ireland til anvendelse til Microsoft Irelands egne formål.

Konsekvensanalysen omfatter de situationer, hvor brugerne er ansatte ved De Dataansvarlige, f.eks. sagsbehandlere eller andre systembrugere. Det vedrører den behandling, som ansatte hos De Dataansvarlige foretager i forbindelse med sagsbehandling og personaleadministration. Konsekvensanalysen omfatter således ikke situationer, hvor andre persongrupper er brugere, f.eks. elever eller i øvrigt borgeres eventuelle brug af de udvalgte applikationer og services, som De Dataansvarlige stiller til rådighed i forbindelse med faktisk forvaltningsvirksomhed som f.eks. drift af uddannelsesinstitutioner, herunder undervisning, m.v.

Den behandling, der i øvrigt sker hos De Dataansvarlige i andre systemer, herunder browser samt ESDH-system, er ikke omfattet af denne konsekvensanalyse, jf. herom også afsnit 2.5 nedenfor. Det skyldes, at anvendelsen af Microsoft 365 i udgangspunktet vil ske gennem en række applikationer (programmer) og ikke gennem en browser.

Det er hensigten at anvende Onedrive og Sharepoint sideløbende med det hidtil anvendte ESDH-system, f.eks. F2 eller WorkZone. Denne konsekvensanalyse er afgrænset til at omfatte de behandlingsaktiviteter, som udføres af De Dataansvarliges brugere i de applikationer og services, som er cloudbaserede. Den behandling, der vedrører ESDH-systemer, er derfor ikke en del af denne konsekvensanalyse.

Konsekvensanalysen omfatter ikke AI-produkter, f.eks. Copilot for Microsoft 365. Konsulentydelser i form af Microsoft Unified Support er ikke en del af konsekvensanalysen, da produktet ”Unfied Support” favner klassiske konsulentydelser, som ikke er en del af statens aftale. Hvis behandlingen senere udvides til at omfatte andre dele af Microsoft 365-licensen, f.eks. Copilot eller ”Unified Support”, vil denne konsekvensanalyse blive opdateret, så den tillige omfatter behandlingen af personoplysninger forbundet hermed.

Endelig bemærkes det, at denne konsekvensanalyse ikke omfatter behandling af personoplysninger på følgende sagstyper/-områder:

* Sager omfattet af retshåndhævelsesloven[[8]](#footnote-8), herunder straffesager.
* Systematisk behandling af helbredsoplysninger samt genetiske og biometriske data i f.eks. nationale sundhedsregistre og databaser, herunder hos Sundhedsdatastyrelsen og Nationalt Genom Center.
* Udlændingesager med oplysninger af høj konsekvens for de registrerede, hvis udenforstående får adgang til dem, herunder asylsager på Udlændingeministeriets område.
* Sager baseret på personoplysninger vedrørende væsentlige sociale forhold, misbrug m.v. om sårbare registrerede, hvilket f.eks. kan omfatte børnesager og sager hos Ankestyrelsen.
* Særlige områder inden for Forsvaret, hvor der behandles informationer om sikkerhedspersonel samt rigets sikkerhed.

Hvis Microsoft 365 ønskes anvendt på de ovenfor nævnte sagstyper/-områder, skal de pågældende myndigheder derfor supplere denne konsekvensanalyse med en vurdering af behandlingens lovlighed samt analyse af risiciene forbundet hermed.

## Særligt opmærksomhedspunkt i forhold til konsekvensanalysen

Denne konsekvensanalyse vedrørende databeskyttelse dækker behandling af personoplysninger ved brug af de udvalgte applikationer og cloudtjenester og vil beskrive de forhold, herunder behandling, lovlighed, nødvendighed og risici, der er generel og fælles for De Dataansvarlige. Det er i konsekvensanalysen lagt til grund, at der af De Dataansvarlige foretages en fuld anvendelse af de udvalgte applikationer og cloudtjenester i Microsoft 365. Konsekvensanalysen forholder sig til væsentlige og centrale spørgsmål og risici ved anvendelsen af Microsoft 365, herunder overførsler af personoplysninger til tredjelande og Microsoft Irelands eventuelle brug af personoplysninger til egne formål.

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 for hver enkelt af De Dataansvarlige, 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. Det afhænger her af, hvilke personoplysninger der afgives i forbindelse med mødet, herunder om der f.eks. nævnes følsomme personoplysninger, som kan henføres til en person. Afhængig af De Dataansvarliges interne retningslinjer kan dette også være begrænset, såfremt det fremgår heraf, at følsomme 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.

# Processen for gennemførelsen af konsekvensanalysen

## Metode

Databeskyttelsesforordningen fastsætter følgende minimumskrav til konsekvensanalysens indhold, jf. forordningens artikel 35, stk. 7:

1. En systematisk beskrivelse af de planlagte behandlingsaktiviteter og formålene med behandlingen, herunder i givet fald de legitime interesser der forfølges af den dataansvarlige.
2. En vurdering af, om behandlingsaktiviteterne er nødvendige og står i rimeligt forhold til formålene.
3. En vurdering af risiciene for de registreredes rettigheder og frihedsrettigheder.
4. De foranstaltninger, der påtænkes for at imødegå disse 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 endvidere en række kriterier for en acceptabel konsekvensanalyse i bilag 2 til Artikel 29-Gruppens (nu: EDPB) vejledning om konsekvensanalyser.[[9]](#footnote-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]](#footnote-10), med nødvendige tilpasninger af hensyn til sagens karakter.

Konsekvensanalysen er opbygget således, at den først indeholder en beskrivelse af databehandlingens formål, karakter, sammenhæng og omfang (databeskyttelsesforordningens artikel 35, stk. 7, litra a), samt en vurdering af nødvendigheden og proportionaliteten (databeskyttelsesforordningens artikel 35, stk. 7, litra b). Herefter indeholder den en identifikation og evaluering af risici samt foranstaltninger til håndtering af disse risici (databeskyttelsesforordningens artikel 35, stk. 7, litra c og d). Videre indeholder denne konsekvensanalyse en vurdering af, hvorvidt Datatilsynet skal høres, dokumentation for databeskyttelsesrådgiverens synspunkter og ledelsens stillingtagen til, om konsekvensanalysen kan godkendes. Endelig er der fastlagt en implementeringsplan.

Udarbejdelsen af denne konsekvensanalyse er sket med deltagelse af repræsentanter fra Statens It og Økonomistyrelsen, som har bidraget til at sikre den nødvendige beskrivelse af behandlingen samt identificere og håndtere risici. Derudover har databeskyttelsesrådgiveren fra Statens It været inddraget i processen og har også gennemgået konsekvensanalysen og givet sine bemærkninger hertil. Der har endvidere været afholdt en række møder med Microsoft Danmark ApS (herefter ”Microsoft Danmark”) på vegne af Microsoft Ireland, hvor behandlingen ligeledes er blevet gennemgået, drøftet og uddybet, ligesom Microsoft Danmark har afgivet skriftlige svar på en række spørgsmål vedrørende Microsofts behandling af personoplysninger i Microsoft 365. Konsekvensanalysen er udarbejdet med bistand fra Kammeradvokaten.

## Inddragelse af de 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 de udvalgte applikationer og cloudtjenester fra Microsoft 365, jf. databeskyttelsesforordningens artikel 35, stk. 9.

Økonomistyrelsen og Statens It har lagt vægt på, at hovedparten af behandlingen af personoplysninger vil ske i henhold til lov. Samtidig er det vurderet, at en inddragelse af de registrerede er umulig eller uforholdsmæssigt vanskelige henset til, at de registrerede stort set er alle borgere i samfundet eller ansatte ved De Dataansvarlige.

# Brugernes anvendelse af de udvalgte applikationer og cloudtjenester i Microsoft 365

## Generelt om Microsoft 365 og sammenhæng

Microsoft 365 er en abonnementstjeneste fra Microsoft, der tilbyder en lang række cloudbaserede produktivitets- og samarbejdsværktøjer, som f.eks. Word (tekstbehandling), Excel (regneark), PowerPoint (præsentation), Teams (kommunikation), OneDrive (cloud-lagring), SharePoint (samarbejde og dokumenthåndtering) og Outlook (mail og kalender). Microsofts portefølje er bygget op efter software (applikation), online services (cloudtjenester) og professional services (support).

Værktøjerne tilbydes som ”Software-as-a-Service”, hvor Microsoft Ireland hoster værktøjerne, som kunderne kan tilgå og anvende via internettet gennem en browser eller en dedikeret applikation. Hele teknologistakken, det vil sige infrastruktur, platform og applikationer, er altså placeret hos, drives, vedligeholdes og videreudvikles af Microsoft. Microsoft tilbyder forskellige licenssuiter, der henvender sig til forskellige behov, som kunden måtte have. Microsoft tilbyder endvidere, at Microsoft kan anvendes som en ”Software-as-a-Service”-løsning, men også som *on premise*-løsning, hvor applikationer hostes i kundens datacenter. Dette begrænser dog anvendelsesmulighederne af Microsoft 365, da cloudtjenester kun kan anvendes i Microsofts infrastruktur.

Ved desktopapplikationer forstås software, der kan downloades og installeres på en brugers computer, hvorefter brugeren har adgang til og kan anvende softwaren offline. Applikationerne downloades fra Microsoft 365-platform.[[11]](#footnote-11) Applikationerne kan ofte anvendes i sammenhæng med cloudtjenesterne.

Ved cloudtjenester forstås services, der leveres over internettet, og som giver brugerne mulighed for at lagre, tilgå og arbejde med data og applikationer på Microsoft Irelands servere, i stedet for at have data og applikationer gemt lokalt på brugerens enhed. Cloudtjenesterne kan tilgås af brugerne gennem webbrowsere, desktopapplikationer eller (andre) dedikerede applikationer, f.eks. til mobile enheder, forudsat at brugerens PC/mobile enhed har adgang til internettet.

Brug af Microsoft 365-cloudtjenester via browser kan ske gennem mange forskellige browsere.[[12]](#footnote-12) Brug af webbrowsere er ikke omfattet af konsekvensanalysen.

Der gælder forskellige vilkår for forskellige værktøjer i Microsoft 365, og Microsoft Corporation anvender forskellige begreber til at ”pulje” værktøjer med samme vilkår. Ved gennemgang af Microsoft Irelands databehandleraftale, Product Terms og online dokumentation i øvrigt omfatter nedenstående begreber de anførte værktøjer:

|  |  |
| --- | --- |
| **Begreb** | **Værktøj(er)** |
| Office 365 Services | Alle 365 Cloudtjenester omfattet af konsekvensanalysen.  (Customer Lockbox, Exchange Online Archiving, Exchange Online Protection, Exchange Online, Microsoft Teams, Office for the web, OneDrive for Business, SharePoint) |
| Online Service | Alle 365 Cloudtjenester omfattet af konsekvensanalysen og Entra ID. |
| 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. |

Værktøjerne omfattet af konsekvensanalysen konfigureres i videst muligt omfang som EU Data Boundary Services. Der henvises i denne sammenhæng til afsnit 7. Ældre funktioner, der ikke er aktiveret som default features i værktøjerne, og som medfører, at der behandles data uden for EU Data Boundary i videre omfang, end det fremgår af Transfer Impact Assessment (herefter ”TIA”) (bilag F), vil ikke blive aktiveret på Statens tenants, f.eks. featuren ”Research”[[13]](#footnote-13) i Word, Excel, og PowerPoint. Det samme gælder for funktionen ”Shared Tunnel Invitations”[[14]](#footnote-14) i Teams som følge af konfiguration af et ”cross-tenant relationship”, Azure Bot Services i Teams App.

Information om Microsoft 365 og behandlingen af data heri findes i det væsentligste i Microsoft Irelands databehandleraftale (Bilag C), Microsofts Product Terms (Bilag B) og online dokumentation (Bilag H).

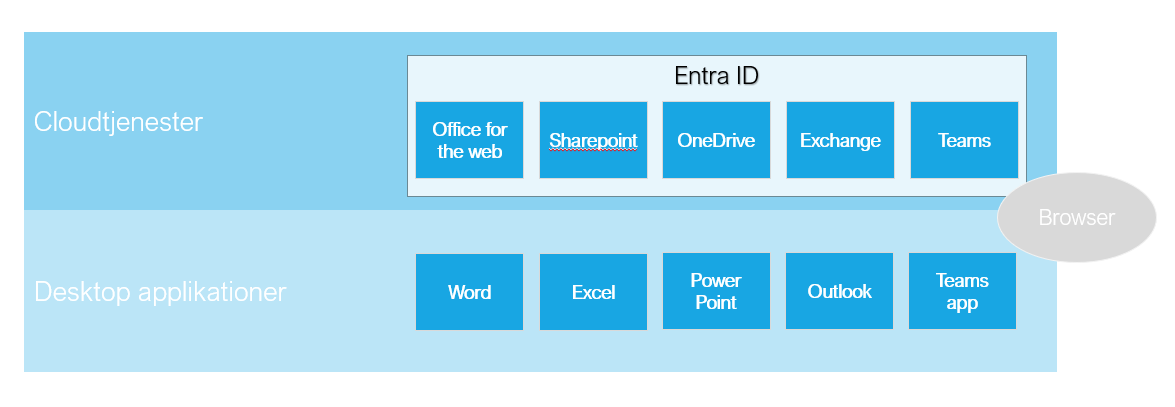
Udover applikationer og cloudtjenester kan der desuden tilvælges Professional Services i form af konsulent- og supportydelser, hvor i nærværende konsekvensanalyse er afgrænset fra konsulentydelser, da dette ikke er en ydelse på statens aftale med Microsoft.

## Cloudtjenester og applikationer omfattet af konsekvensanalysen

Denne konsekvensanalyse omfatter udvalgte værktøjer i Microsoft 365 licens E5, nemlig Word, PowerPoint, Excel og Outlook samt Office for the web, Onedrive, Exchange Online, Sharepoint og Teams.

Herudover anvendes tjenesten Entra ID (tidligere Active Directory), som er Microsofts løsning til identitets- og adgangsstyring, der er en del af Microsoft Azure Core Services.

De pågældende værktøjer er nærmere beskrevet nedenfor og kan i forhold til Microsoft 365 illustreres på følgende måde:



### Word, PowerPoint, Excel

Word, PowerPoint og Excel er en del af en ”suite” af Microsoft-applikationer, der kan aftages som enkelte produkter gennem Office 365-licensen eller Microsoft 365-licensen.

Brugerne, der er ansatte hos De Dataansvarlige, vil anvende Word, PowerPoint og Excel i forbindelse med sagsbehandling og personaleadministration, hvor der f.eks. udarbejdes breve, regneark, notater, noter, slideshows, referater o.l. med henblik på kommunikation med borgere og ansatte, samt overholdelse af officialprincippet vedrørende en forsvarlig oplysning af sagerne. På samme måde sker det med henblik på dokumentation og opfyldelse af notatpligten og i forlængelse heraf journaliseringspligten. I den forbindelse vil der blive skrevet og redigeret tekst og regneark, som indeholder personoplysninger om de registrerede.

### Office for the web

Office for the web er en cloudbaseret tjeneste, hvorigennem (dele af) funktionaliteten i Word, PowerPoint og Excel tilgås via en webbrowser. Brug af Office for the web kræver altså ikke installation af en applikation. Tjenesten understøtter fildeling mellem brugere af tjenesten.[[15]](#footnote-15)

### Outlook og Exchange Online

Outlook er en desktop-applikation, der installeres og kører lokalt på brugerens computer. For at kunne sende og modtage e-mails, synkronisere kalendere m.m. skal Outlook anvendes sammen med en cloudtjeneste eller mailserver, f.eks. Microsoft 365-tjenesten, ”Exchange online”.

Exchange Online er en cloudbaseret e-mail, kalender og kontaktstyringstjeneste. Exchange Online tilgås over internettet og fungerer sammen med en lang række Microsoft 365-applikationer, herunder Outlook og Teams, samt med mobile enheder.

Tilsammen understøtter Microsoft Outlook og Exchange Online således udveksling og organisering af e-mails, oprettelse og organisering af kontaktpersoner, og kalenderstyring hvor det er muligt at oprette beskeder/opgaver, egne aftaler samt at indkalde andre til møder, herunder via Teams, med angivelse af tid, lokation, emne, deltagere og evt. uddybende tekstbesked.

Tjenesterne Exchange Online Archiving (datalagring) og Exchange Online Protection (e-mail sikkerhedstjeneste) anvendes sammen med Exchange Online.

### Teams

Teams er en cloudbaseret kommunikations- og samarbejdsapplikation, der kan benyttes til bl.a. onlinemøder, chat, fillagring og -deling samt til integration med andre applikationer. Den understøtter således lyd- og videokald, online møder, udveksling af beskeder og dokumenter mm. Teams kan integreres med en lang række øvrige Microsoft 365-tjenester og applikationer.[[16]](#footnote-16) Teams kan anvendes gennem en understøttet internetbrowser eller en desktop-applikation.

### Sharepoint og OneDrive for Business

SharePoint er en cloudbaseret tjeneste, der fungerer som et centralt sted for lagring, adgang og samarbejde på filer og understøtter både intranet- og internetwebsteder. SharePoint tilbyder forskellige funktioner såsom dokumenthåndtering, projektstyring, automatisering af arbejdsprocesser og integration med andre Microsoft 365-værktøjer.

OneDrive er en cloudbaseret lagrings- og fildelingstjeneste, der giver brugerne mulighed for at gemme filer og data online og få adgang til dem fra enhver enhed via en internetbrowser eller en desktop-applikation.[[17]](#footnote-17) OneDrive er integreret med andre Microsoft 365-værktøjer. OneDrive tilbyder funktioner såsom automatisk filsynkronisering, som sikrer, at den seneste version af en fil er tilgængelig på alle enheder, filversionering, som tillader brugere at gendanne tidligere versioner af filer, og muligheden for at dele filer og mapper med specifikke personer eller offentligt.

Formålene med De Dataansvarliges brug af Sharepoint og OneDrive, herunder hvilke personoplysninger der deles i de to tjenester, afdækkes af De Dataansvarlige selv.

### Entra ID

Microsoft Entra ID er Microsofts løsning til identitets- og adgangsstyring og bruges sammen med Microsoft 365 til at administrere adgangen til cloudtjenester og applikationer. Entra ID indeholder funktioner som single sign on, multifaktorgodkendelse, godkendelse uden adgangskode og betinget adgang.

## Formålet med behandlingen

De Dataansvarliges formål med behandlingen af personoplysninger er varetagelse af de lovbestemte opgaver, herunder sagsbehandling og personaleadministration. Det er dog forskelligt for hver af De Dataansvarlige, hvilke opgaver disse i henhold til lovgivningen er blevet pålagt. De Dataansvarlige skal hver især supplere nærværende konsekvensanalyse med formålet med deres behandling af personoplysninger.

Udførelsen af De Dataansvarliges opgaver sker i almindelighed ved brug af it. Der sker en elektronisk behandling af personoplysninger, når brugerne, dvs. de ansatte hos De Dataansvarlige, indtaster, redigerer, indsamler, sletter og modtager m.v. personoplysninger i og via de udvalgte applikationer og cloudtjenester i Microsoft 365. Formålet med anvendelsen af disse er således at udføre de lovbestemte opgaver og dermed fælles for De Dataansvarlige, om end nogle af De Dataansvarlige måske bruger flere eller færre af de udvalgte applikationer og cloudtjenester end andre, ligesom konfigurationen kan være forskellig.

I forbindelse med at De Dataansvarliges medarbejdere anvender applikationerne og cloudtjenesterne, vil Microsoft Ireland indsamle Diagnostic Data fra applikationer, danne System-Generated Logs fra cloudtjenester og modtage Customer Data, som genereres eller indtastes af brugerne i applikationer og cloudtjenester. Dataflowet ved Microsoft Irelands behandling er illustreret ved følgende figur:

Et billede, der indeholder tekst, skærmbillede, Font/skrifttype, Brand

Automatisk genereret beskrivelse

Som det fremgår af figuren ovenfor, pseudonymiseres Diagnostic Data og Customer Data, herunder System-Generated Logs inden brug. Videre sker der en aggregering heraf, inden data anvendes til Microsoft Irelands egne formål. Den behandling, som Microsoft Ireland udfører i forbindelse med levering af tjenesten og Microsoft Irelands forretningsaktiviteter, herunder både til De Dataansvarliges formål og til Microsoft Irelands egne formål, er nærmere beskrevet nedenfor i afsnit 5.

Formålet med den behandling der sker i de respektive applikationer og cloudtjenester er beskrevet ovenfor i afsnit 4.2.

## Behandlingen af personoplysninger

### Behandlingens karakter og omfang

Behandlingen af personoplysninger foretages af de ansatte hos De Dataansvarlige med henblik på sagsbehandling og personaleadministration.

Der kan potentielt blive behandlet alle typer af personoplysninger, herunder følsomme personoplysninger, fortrolige oplysninger og oplysninger om strafbare forhold samt ikke-følsomme personoplysninger. Det vedrører de personoplysninger, som brugerne selv indtaster og genererer ved at anvende applikationerne og cloudtjenesterne. Word-dokumenter, Excel-ark og e-mails, herunder vedhæftninger, kan indeholde personoplysninger om alt fra sagsnummer, navne, (hemmelige) adresser, vurderinger og synspunkter til personoplysninger om ansættelsesforhold, økonomiske forhold, straffeforhold, helbredsoplysninger, race eller etnisk oprindelse og fagforeningsmæssigt tilhørsforhold m.v. Tilsvarende kan kalenderen i Outlook og PowerPoint-præsentationer indeholde personoplysninger, der for så vidt angår hovedparten formentlig vil vedrøre ikke-følsomme personoplysninger.

Endelig vil der blive behandlet personoplysninger ved anvendelse af Teams, herunder chat samt personoplysninger der afgives i forbindelse med livetransmission. Det afhænger her af, hvilke personoplysninger der afgives i forbindelse med mødet, herunder om der f.eks. nævnes følsomme personoplysninger, som kan henføres til en person. Afhængig af De Dataansvarliges interne retningslinjer kan dette også være begrænset, såfremt det fremgår heraf, at følsomme personoplysninger ikke må deles i forbindelse med anvendelsen af Teams, ligesom optagelse af transmissionen og deling af lokationsdata kan være deaktiveret som en sikkerhedsforanstaltning. Dette er dog noget, De Dataansvarlige hver for sig supplerer nærværende paraply-konsekvensanalyse med. Det vurderes, at livetransmission af lyd, video og skærmdeling – uanset om denne lagres eller ej – udgør en automatisk behandling af personoplysninger omfattet af databeskyttelsesforordningen, jf. dennes artikel 2, stk. 1. Se hertil bl.a. Datatilsynets afgørelse af 17. januar 2013 vedr. transmission af gudstjenester[[18]](#footnote-18), hvor Datatilsynet fandt, at en sådan transmission var omfattet af den dagældende persondatalov, hvis materielle anvendelsesområde svarer til databeskyttelsesforordningens artikel 2, stk. 1.[[19]](#footnote-19)

Som en del af anvendelsen af Microsofts produkter vil personoplysninger om brugerne blive behandlet af Microsoft Ireland som databehandler for De Dataansvarlige, ligesom visse oplysninger også vil blive anvendt af Microsoft Ireland til Microsofts egne formål. Microsoft Irelands behandling gennemgås nedenfor i afsnit 5.

Systembrugerne, der er ansatte hos De Dataansvarlige, vil behandle personoplysninger om borgere og andre ansatte. De Dataansvarlige vil i almindelighed som en del af deres lovbestemte opgaver behandle personoplysninger om alle borgere i landet og alle ansatte hos de pågældende dataansvarlige. Der behandles således personoplysninger om registrerede i stort omfang.

Personoplysninger indsamles i forbindelse med kontakt med borgere, fra andre myndigheder eller offentlige registre i forbindelse med håndtering af en borgers sag eller anden sagsbehandling, ligesom personoplysninger i forbindelse med personaleadministration hovedsageligt indsamles fra de ansatte selv, men også kan komme fra andre ansatte eller andre myndigheder, f.eks. Skatteforvaltningen og i Rigspolitiet.

De brugergenererede personoplysninger opbevares og journaliseres primært i ESDH-systemerne. Det kan dog ikke udelukkes, at OneDrive og Sharepoint vil blive anvendt sideløbende hermed. Behandlingen i ESDH-systemerne er ikke omfattet af denne konsekvensanalyse.

Adgangen til personoplysninger vil sædvanligvis være afgrænset til et arbejdsbetinget behov, som begrænses yderligere gennem tekniske foranstaltninger, ligesom der i almindelighed vil være interne retningslinjer herfor. Hver af De Dataansvarlige har begrænset adgangen til personoplysninger, sådan at det kun er relevante personer, der har nødvendig adgang hertil ud fra et arbejdsbetinget behov. Til brug for nærværende konsekvensanalyse lægges det således til grund, at dette er håndteret af De Dataansvarlige i overensstemmelse med databeskyttelsesreglerne. Det samme gør sig gældende for så vidt angår brugernes egen deling inden for og uden for organisationen af personoplysninger i forbindelse med brug af de udvalgte applikationer og cloudtjenester.

De personoplysninger, som brugerne indtaster, modtager og generelt behandler i forbindelse med anvendelsen af Microsoft 365, vil hovedsageligt være i klar tekst – dvs. i umiddelbar personhenførbar form – men kan også være pseudonymiseret. Personoplysningerne vil dog som regel ikke være anonymiseret.

# 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 (System-Generated Logs) 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.

## 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 subprocessors) 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:  *“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.”*[[20]](#footnote-20)  Personal Data er nærmere beskrevet nedenfor i afsnit 5.2om 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]](#footnote-21)  Customer Data er nærmere beskrevet nedenfor i afsnit 5.2 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]](#footnote-22)  Det er kun supportydelser, der er omfattet af De Dataansvarliges brug og således denne konsekvensanalyse.  Professional Services Data er nærmere beskrevet nedenfor i afsnit 5.2 om Microsoft Irelands databehandleraftale. |
| System-Generated Logs | Kategorien omfatter data, som genereres om brugernes interaktion med cloudtjenesterne. System-Generated Logs indeholder Personal Data.  System-Generated Logs pseudonymiseres og bruges til i) at levere tjenesteydelser og sørge for sikkerheden samt at disse fungerer efter hensigten og ii) ”business operations”.  System-Generated Logs er nærmere beskrevet i afsnit 5.3 |
| 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.  Diagnostic Data er nærmere beskrevet i afsnit 5.3 og 5.3.1. |

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 System-Generated Logs.

Af Microsofts business operations white paper fremgår[[23]](#footnote-23), 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 System-Generated Logs, idet System-Generated data er beskrevet som ”records of events that occur in Microsoft cloud services.”[[24]](#footnote-24)

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 system-generated logs (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 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*”[[25]](#footnote-25). 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:

*“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.*

Et billede, der indeholder tekst, skærmbillede, Font/skrifttype, nummer/tal

Automatisk genereret beskrivelse

*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 System-Generated Logs, 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.[[26]](#footnote-26) 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.

## Microsoft Irelands databehandleraftale

### 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”.[[27]](#footnote-27)

“Product” er defineret på følgende måde i Microsoft Irelands databehandleraftale:

*“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 4.2 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 System-Generated Logs og Diagnostic Data, som gennemgås nedenfor i afsnit 5.3:

**Personal data**

**Customer Data**

**Professional Services Data**

**“Data generated, derived, or collected by Microsoft.”**

### 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. […]”*

### 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[[28]](#footnote-28):

*“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   1. 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](https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/reference-connect-sync-attributes-synchronized" \l "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.”*

### 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:[[29]](#footnote-29)

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

*Customer authorizes Microsoft:*

1. *to create aggregated statistical, non-personal data from data containing pseudonymized identifiers (such as usage logs containing unique, pseudonymized identifiers); and*
2. *to calculate statistics related to Customer Data or Professional Services Data*

*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)*”.

## Microsofts business operations white paper

Microsoft Ireland har, som beskrevet ovenfor i afsnit 5.1, 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[[30]](#footnote-30), 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.

Microsoft Ireland bruger overordnet set tre typer data, herunder personoplysninger, til forretningsaktiviteter: i) Diagnostic Data, ii) System-Generated Logs og iii) oplysninger *om* Customer Data.[[31]](#footnote-31) Der henvises i øvrigt til Microsoft Danmarks beskrivelse af Diagnostic Data og System-Generated Logs i besvarelse af 2. april 2024 (Bilag I), som beskrevet ovenfor i afsnit 5.1.

**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*”.

**System-Generated Logs** 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. System-Generated Logs 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]](#footnote-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 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.“*

System-Generated Logs genereres derimod i forbindelse med brug af cloudtjenester og sker således inden for Microsofts sfære.

System-Generated Logs 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]](#footnote-33)

Om formålet med at danne System-Generated Logs 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).”*

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.”* System-Generated Logs 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.”*

System-Generated Logs 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]](#footnote-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.”*

System-Generated Logs, der indeholder ikke-pseudonymiserede personoplysninger, behandles i henhold til Microsofts business operations white paper som Customer Data.[[35]](#footnote-35)

Pseudonymiserede System-Generated Logs 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]](#footnote-36) Flytningen sker som oplyst på møde med Microsoft Danmark inden for Microsoft Irelands sfære og således ikke til Microsoft Corporations sfære. Dette er ligeledes søgt illustreret ved figuren i afsnit 4.3. 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]](#footnote-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.

Efter flytningen af de relevante Diagnostiske Data og pseudonymiserede System-Generated Logs 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]](#footnote-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]](#footnote-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]](#footnote-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.*

*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. Microsoft har illustreret processen i figuren i afsnit 4.3.

De fire formål til forretningsaktiviteter (business operations), der er fastlagt i Microsoft Irelands databehandleraftale, og som er gengivet ovenfor i afsnit 5.2.4, er også nærmere beskrevet i Microsofts business operations white paper:

1. I relation til ”Customer Billing and Account Management”[[41]](#footnote-41) behandles de aggregerede data outputs dels til at fakturere services, der forbrugsafregnes, og dels til at få et overblik over de enkelte 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]](#footnote-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]](#footnote-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*”.

### 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 5.3. Diagnostic Data kan[[44]](#footnote-44) indeholde Personal Data, som skal behandles i overensstemmelse med Microsoft Irelands databehandleraftale. Der findes både valgfrie og obligatoriske Diagnostic Data. Om de obligatoriske skriver Microsoft Corporation følgende på sin hjemmeside[[45]](#footnote-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]](#footnote-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.”*

Listen af data, der indsamles om desktopapplikationerne og brugen heraf er lang[[47]](#footnote-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.

## 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.

# roller i forbindelse med behandlingen af personoplysninger

## De Dataansvarliges rolle som selvstændigt dataansvarlige

I databeskyttelsesforordningens artikel 4, nr. 7, er den dataansvarlige defineret 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 en behandling af personoplysninger lever op til reglerne i databeskyttelsesforordningen.

Der er flere forskellige aktører involveret i den behandling af personoplysninger, der sker i forbindelse med anvendelse af de udvalgte applikationer og cloudtjenester i Microsoft 365. Det er derfor centralt at fastlægge, hvilke aktører der er ansvarlige for de enkelte dele af behandlingen af personoplysninger.

De Dataansvarlige er hver især selvstændigt dataansvarlige for deres respektive behandling af personoplysninger ved brug af Microsoft 365 og de udvalgte applikationer og cloudtjenester. Det gælder for den behandling, der foretages af brugere hos De Dataansvarlige fra det øjeblik, de modtager personoplysninger fra borgere og ansatte via en af de anvendte applikationer eller cloudtjenester, eller når De Dataansvarlige selv indtaster tidligere indsamlede oplysninger heri. Ligeledes gælder det, når Microsoft Ireland som databehandler behandler personoplysninger på vegne af hver af De Dataansvarlige.

Der gælder ikke et fælles dataansvar for De Dataansvarlige. Når De Dataansvarlige via Outlook/Exchange Online eller Teams udveksler personoplysninger med medarbejdere i andre myndigheder, der selv er dataansvarlige, behandler parterne personoplysninger som selvstændige dataansvarlige, og der er således tale om videregivelser mellem De Dataansvarlige.

## Statens It’s rolle som databehandler

I forbindelse med Statens It’s varetagelse af adgangsstyring, behandler Statens It personoplysninger som databehandler på vegne af hver af De Dataansvarlige. Der er indgået databehandleraftaler mellem De Dataansvarlige hver især og Statens It for denne behandling af personoplysninger.

## Microsofts databeskyttelsesretlige rolle

Som nærmere begrundet i det følgende er det vurderingen, at for så vidt angår Microsoft Irelands behandling af personoplysninger til brug for levering af produkterne og services til De Dataansvarlige vil Microsoft Ireland agere som databehandler for hver af De Dataansvarlige.

Det vurderes endvidere, at Microsoft Ireland alene er dataansvarlig for selve anonymiseringen af de pseudonyme personoplysninger, som Microsoft har indsamlet/genereret som databehandler, men hverken databehandler eller dataansvarlig efter databeskyttelsesforordningen for så vidt angår den efterfølgende brug af de anonymiserede oplysninger til Microsofts egne forretningsaktiviteter (business operations), da databeskyttelsesforordningens regler ikke finder anvendelse for så vidt angår denne efterfølgende brug af de nu anonyme oplysninger.

### 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 databehandlere, 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]](#footnote-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]](#footnote-49) Kvalifikationen som dataansvarlig eller databehandler skal vurderes med hensyn til hver specifik databehandlingsaktivitet.[[50]](#footnote-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]](#footnote-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]](#footnote-52) På linje hermed anføres det i den daværende Artikel 29-Gruppes udtalelse 05/2012 vedrørende cloud computing, afsnit 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]](#footnote-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]](#footnote-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 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 figuren i afsnit 4.3, 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.

Et billede, der indeholder tekst, skærmbillede, Font/skrifttype, Brand

Automatisk genereret beskrivelse

Om Microsoft Irelands rolle i forbindelse med levering af produkter og services, som er beskrevet ovenfor i afsnit 5.2.3, 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 5.2.3, 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.”*

### 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 5.2.4, 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 5.1 og 5.3. 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[[55]](#footnote-55):

*”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.)

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 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.

Inddelingen i databeskyttelsesretlige roller ser herefter således ud:

Tabel I 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 II 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. |

# Microsofts placering af data og tredjelandsoverførsler

Det følger af Microsoft Irelands databehandleraftale[[56]](#footnote-56), 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”.[[57]](#footnote-57)

Alle cloudtjenester omfattet af konsekvensanalysen undtagen Exchange Online Protection er ”EU Data Boundary Online Services”.[[58]](#footnote-58)

Desktop-applikationerne Word, PowerPoint, Excel, Outlook og Teams app er *ikke* omfattet af begreberne ”Core Online Services” eller ”EU Data Boundary Online Services” og kan ikke placeres i EU Data Boundary.[[59]](#footnote-59) Som beskrevet ovenfor i afsnit 5.3 er det dog til brug for nærværende konsekvensanalyse oplyst af Microsoft Danmark, at Database Storage, hvortil Diagnostic Data og pseudonymiserede System-Generated Logs flyttes efter indsamling og generering, er placeret inden for EU/EØS på samme måde som kundens tenant.

Om EU Data Boundary Services fremgår følgende af Microsoft Product Terms[[60]](#footnote-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.”*

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”[[61]](#footnote-61)* (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.

# Vurdering af nødvendigheden og proportionaliteten

Det er et krav efter databeskyttelsesforordningens artikel 35, stk. 7, at De Dataansvarlige foretager en vurdering af lovligheden og nødvendigheden af behandlingsaktiviteterne i de udvalgte applikationer og cloudtjenester i Microsoft 365, herunder i forhold til eventuelle videregivelser af personoplysninger til Microsofts egne formål. Det skal også vurderes, om behandlingsaktiviteterne er rimelige set i forhold til formålet med behandlingen. Vurderingen skal bl.a. medvirke til at sikre, at der kun behandles personoplysninger, der er nødvendige, og som kan rummes inden for formålet med behandlingen. Behandlingen må ikke gå videre end det, der kræves for at opfylde de formål, som De Dataansvarlige er berettigede til at forfølge.

## De grundlæggende principper

### 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[[62]](#footnote-62):

*”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 8.2.2 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 8.2.3.

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 ved indsamling og generering af personoplysninger, herunder Diagnostic Data, System-Generated Logs og personoplysninger, der indtastes af brugerne samt genereres, sker hovedsageligt automatisk i systemet og således ens for alle de registrerede. Af Microsoft Danmarks svar af 2. april 2024 (Bilag I) side 4, anføres også, at behandlingen sker på tværs af kunder og derfor typisk ikke er relateret til én kunde men ens for flere:

*“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 vedrører ifølge præambelbetragtningen navnlig den dataansvarliges opfyldelse af oplysningspligten efter artikel 13 og 14 samt af den registreredes indsigtsret efter artikel 15.

Det må i dag anses for forventeligt for alle i Danmark, herunder både borgere og ansatte, at deres personoplysninger i forbindelse med myndigheders lovbestemte opgaver, herunder sagsbehandling og personaleadministration, behandles ved hjælp af applikationer som Word, Excel, Outlook, PowerPoint og i et vist omfang også Teams. På samme måde må det anses for forventeligt for systembrugere, at der i forbindelse med deres anvendelse af applikationer samt cloudtjenester indsamles systemgenererede personoplysninger såsom diagnostiske data og genereres logs om systembrugerens brug af applikationer og cloudtjenester. I et vist omfang anvender systembrugerne selv disse oplysninger undervejs i arbejdet, f.eks. for at se, om et dokument er tjekket ind eller ud, samt til hvem og hvornår der sidst er redigeret i dokumentet o.l. Ligeledes må det anses for at være almindeligt kendt i dag, at det er væsentligt at have et indblik i den brug, der sker, for at være i stand til at yde supporthjælp samt håndtere sikkerhedshændelser. Sådanne tekniske foranstaltninger, herunder logning, er i dag også anset for at være en væsentlig sikkerhedsforanstaltning.

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.

### 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 4.3 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 5.1, 5.3 og 6.3.2 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 6.3.2, 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 cloudtjenester 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.

### Princippet om dataminimering

Personoplysninger skal være tilstrækkelige, relevante og begrænset 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 nærværende paraply-konsekvensanalyse med en vurdering af princippet om dataminimering, herunder at der kun indsamles, behandles og opbevares personoplysninger, der er nødvendige i overensstemmelse med det formål, hvortil de er indsamlet, herunder også for at overholde de forvaltningsretlige principper. De Dataansvarlige supplerer således også nærværende konsekvensanalyse med eventuelle foranstaltninger såsom interne retningslinjer om, hvad der må indsamles, registreres, beriges og opbevares af personoplysninger i forbindelse med sagsbehandling og personaleadministration, herunder om der er personoplysninger, der ikke må anvendes i forbindelse med Teams og Outlook.

For så vidt angår den behandling af personoplysninger som Microsoft Ireland foretager som databehandler for De Dataansvarlige, iagttages princippet om dataminimering ved dannelse af System-Generated Logs, 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 8.1.2 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 8.1.2, 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 System-Generated Logs, 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[[63]](#footnote-63). 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 Cybersikkerheds trusselsvurdering af cybertruslen mod Danmark af 8. maj 2023.[[64]](#footnote-64) 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).

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 System-Generated Logs)]:*

*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 8.1.2 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 8.1.2 for at være inden for rammerne af databeskyttelsesforordningens artikel 5, stk. 1, litra c.

### 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.

### 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 System-Generated Logs)]:*

*[…]*

*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 System-Generated Logs 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.

### 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 9.3, 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[[65]](#footnote-65), 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 8.1.6.1-8.1.6.3 nedenfor, med en beskrivelse af de væsentligste tekniske, organisatoriske og kontraktuelle foranstaltninger, som gælder generelt for De Dataansvarlige, herunder sikkerhedsforanstaltninger implementeret af Microsoft.

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 Irelandss databehandleraftale gennemført en risikovurdering før påbegyndelse af behandlingen af De Dataansvarliges oplysninger. Videre følger det af Microsoft Irelands databehandleraftale[[66]](#footnote-66), 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[[67]](#footnote-67) 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[[68]](#footnote-68). 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.[[69]](#footnote-69) 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.

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[[70]](#footnote-70):

”*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[[71]](#footnote-71). 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[[72]](#footnote-72).

##### Fastsat af Microsoft

**Kryptering**

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

*“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 System-Generated Logs (brugsoplysninger, herunder aktivitetslogs) pseudonymiseres. Dette er endvidere kontrolleret af revisionsfirmaet Ernst & Young, idet der henvises herom til revisionserklæringen omtalt i afsnit 5.3.

**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)[[73]](#footnote-73). 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.

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.

## Hjemmelsgrundlag

### 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 sådan 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 8.2.2 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.

### Vurdering af grundlaget for behandling til De Dataansvarliges formål

Som beskrevet ovenfor i afsnit 8.2.1.1 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 5.2.3 og afsnit 6.3.1 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 System-Generated Logs. 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 8.1.3 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 5.2.3 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.

### Vurdering af grundlag for aggregering og efterfølgende behandling til Microsofts forretningsaktiviteter

Som beskrevet ovenfor i afsnit 5.2.4 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 6.3.2 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.

## De registreredes rettigheder

### 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.

### 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 system-generated logs 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 System-Generated Logs)]:*

*[…]*

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 8.1.5, være muligt for De Dataansvarlige at slette personoplysninger, hvor det er relevant og i overensstemmelse med databeskyttelsesforordningens artikel 17.

#### Øvrige

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.

## 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 beskyttelses- niveauet 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.

## 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 System-Generated Logs kan der henvises til ”System-generated logs 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 System-Generated Logs 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 system-generated logs 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 5.1 og 5.3.

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.

# Identifikation og evaluering af risici samt foranstaltninger til at håndtere risici

## 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.[[74]](#footnote-74)

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.

## Valg af evalueringskriterier for sandsynlighed og konsekvens

I denne konsekvensanalyse anvendes følgende evalueringskriterier for sandsynlighed:

Tabel 1 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). |
| **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[[75]](#footnote-75):

Tabel 2 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:

**Figur 3 Risikokort**

Et billede, der indeholder tekst, skærmbillede, Font/skrifttype, nummer/tal

Automatisk genereret beskrivelse

## 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.

### 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 8.3.2 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 (System-Generated Logs), er dog som beskrevet ovenfor i afsnit 5 relativ kompleks.

Som beskrevet ovenfor i afsnit 8.1.1 og 8.1.2 kan det være svært at gennemskue den behandling, som Microsoft Ireland foretager på vegne af De Dataansvarlige ved generering af System-Generated Logs 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 5.1 ”*[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 8.1.2.

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***.

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

#### Beskrivelse

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 8.1.2 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.

### Risiko nr. 3: Microsoft indsamler og genererer for mange personoplysninger om de registrerede i forbindelse med Diagnostic Data og System-Generated Logs (manglende iagttagelse af dataminimeringsprincippet)

#### Beskrivelse

Microsoft indsamler mange datapunkter, hvoraf flere udgør pseudonymiserede personoplysninger, når Microsoft indsamler Diagnostic Data og System-Generated Logs om brugerne (de ansatte), som nærmere beskrevet ovenfor i afsnit 5.3.

Microsoft oplyser, at alle handlinger, foretaget af en bruger, logges. Som beskrevet ovenfor i afsnit 8.1.3 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 System-Generated Logs. 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.[[76]](#footnote-76) 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 System-Generated Logs, særligt også henset til det formål hvortil de behandles.

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 System-Generated Logs samt til hvilke konkrete formål, ved selv at trække en oversigt over disse for tenanten og spørge Microsoft ind til dette ved audits.

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

#### Beskrivelse

Som nærmere beskrevet i afsnit 5.1 og afsnit 6.3.2 skaber Microsoft Ireland aggregerede, statistiske ikke-personhenførbare personoplysninger (anonyme data) fra pseudonyme personoplysninger fra Diagnostic Data og System-Generated Logs, hvilket er blevet bekræftet i en revisorerklæring fra revisionsfimaet Ernst & Young. Derudover vil Statens It løbende foretage audits af, hvorvidt der er foretaget en effektiv anonymisering.

Risikoen består i, hvis denne anonymisering ikke er tilstrækkeligt effektivt, såfremt Microsoft selv måtte have midlerne til at bryde anonymiseringen.

Det vurderes, at konsekvenserne for de registrerede af, at oplysningerne ikke vil være helt eller delvist anonyme, vil være, at der af Microsoft foretages yderligere behandlinger af pseudonymiserede personoplysninger til Microsofts egne forretningsmæssige aktiviteter (business operations). Som begrundet ovenfor i afsnit 8.2.3 vurderes det imidlertid, at selv hvis det – imod Microsofts, Statens It’s og Økonomistyrelsens opfattelse – måtte lægges til grund, at Microsoft ikke foretager en aggregering af de pseudonymiserede personoplysninger til et niveau, der udgør anonyme data, vil der være hjemmel til en sådan videregivelse af pseudonyme, ikke-følsomme personoplysninger i databeskyttelsesforordningens artikel 6, stk. 1, litra e, 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 5.1.

## 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 1 og 2 i afsnit 9.2 ovenfor. De identificerede risici er uddybende beskrevet og evalueret ovenfor i afsnit 9.3. Resultatet af denne vurdering fremgår af risikokortet i figur 4 straks nedenfor.

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

Et billede, der indeholder tekst, skærmbillede, Font/skrifttype, nummer/tal

Automatisk genereret beskrivelse

### Overblik over evaluering og håndtering af risici

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

Tabel 3 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 9.3.1.1 | 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 System-Generated Logs (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

Et billede, der indeholder tekst, skærmbillede, Font/skrifttype, nummer/tal

Automatisk genereret beskrivelse

### Samlet residualrisiko

Som det fremgår af figur 4 i punkt 9.4.1 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.

# 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 9.4.2, 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.

# Dokumentation af DPO’ens synspunkter

Her indføres udtalelse fra den dataansvarliges databeskyttelsesrådgiver (DPO).

# Ledelsens godkendelse af konsekvensanalysen

Konsekvensanalysen har været forelagt ledelsen hos Økonomistyrelsen.

Ledelsen har besluttet følgende vedrørende konsekvensanalysen:

Tabel 5 Ledelsens godkendelsesskema

|  |  |  |
| --- | --- | --- |
| Beslutning | Beskrivelse | Sæt kryds |
| **Godkendt** | Behandlingen kan herefter påbegyndes, såfremt de i konsekvensanalysen mitigerende foranstaltninger bliver implementeret. | X |
| **Betinget godkendt** | Behandlingen kan alene påbegyndes, såfremt 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.

# Vedligeholdelse og ajourføring af konsekvensanalysen

De Dataansvarlige skal regelmæssigt gennemgå konsekvensanalysen vedrørende databeskyttelse og de databehandlingsaktiviteter, som vurderes i denne, jf. databeskyttelsesforordningens artikel 35, stk. 11.

Denne konsekvensanalyse vedrørende anvendelse af udvalgte applikationer og cloudtjenester i Microsoft 365 samt supportydelser i forbindelse hermed vil blive revideret en gang årligt eller ved væsentlige ændringer og hændelser.

Konsekvensanalysen ajourføres af databeskyttelsesenheden i Statens Indkøb og Jura.

1. Microsoft data protection and security terms for products and services: Business operations, side 13. [↑](#footnote-ref-1)
2. Microsoft data protection and security terms for products and services: Business operations, side 13. [↑](#footnote-ref-2)
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). [↑](#footnote-ref-3)
4. For et eksempel på en kongelig resolution kan der henvises til bekendtgørelse nr. 110 af 4. februar 2020. [↑](#footnote-ref-4)
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. [↑](#footnote-ref-5)
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). [↑](#footnote-ref-6)
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). [↑](#footnote-ref-7)
8. Lov nr. 410 af 27. april 2017 om retshåndhævende myndigheders behandling af personoplysninger (med senere ændringer). [↑](#footnote-ref-8)
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. [↑](#footnote-ref-9)
10. ISO/IEC 29134:2023 ”Information technology — Security techniques — Guidelines for privacy impact assessment”. [↑](#footnote-ref-10)
11. Se Microsofts hjemmeside: [https://learn.microsoft.com/en-us/office365/servicedescriptions/office-applications-service-description/office-applications-service-description](https://learn.microsoft.com/en-us/office365/servicedescriptions/office-applications-service-description/office-applications-service-description%20)  (senest tilgået den 27. februar 2024) (Bilag H, side 395). [↑](#footnote-ref-11)
12. 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). [↑](#footnote-ref-12)
13. EU Data Boundary dokumentationen (“Microsoft 365 Applications”, “Research”). [↑](#footnote-ref-13)
14. EU Data Boundary dokumentationen (“Microsoft 365 Applications”, “Shared Channel Invitations”). [↑](#footnote-ref-14)
15. Microsofts hjemmeside: <https://learn.microsoft.com/en-us/office365/servicedescriptions/office-online-service-description/office-online-service-description> (senest tilgået den 27. februar 2024) (Microsoft 365 and Office 365 service descriptions side 409). [↑](#footnote-ref-15)
16. Microsofts hjemmeside: <https://learn.microsoft.com/en-us/office365/servicedescriptions/teams-service-description> (senest tilgået den 27. februar 2024) (Microsoft 365 and Office 365 service descriptions side 522). [↑](#footnote-ref-16)
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 27. februar 2024) (Microsoft 365 and Office 365 service descriptions side 463). [↑](#footnote-ref-17)
18. Datatilsynets afgørelse 2012-218-0006 af 17. januar 2013: Transmission af gudstjenester. [↑](#footnote-ref-18)
19. Justitsministeriets betænkning nr. 1565, del 1, side 31. [↑](#footnote-ref-19)
20. Microsoft Irelands databehandleraftale, side 4,” Definitions”. [↑](#footnote-ref-20)
21. Microsoft Irelands databehandleraftale, side 4,” Definitions”. [↑](#footnote-ref-21)
22. Microsoft Irelands databehandleraftale, side 4,” Definitions”. [↑](#footnote-ref-22)
23. Microsofts business operations white paper, side 4, ‘Overview of processing in the Microsoft cloud’, ‘Privacy by Design’. [↑](#footnote-ref-23)
24. Microsofts business operations white paper vol. 2, side 1. [↑](#footnote-ref-24)
25. Microsoft Irelands databehandleraftale, side 7, “Processing of Personal Data; GDPR”. [↑](#footnote-ref-25)
26. Microsofts business operations white paper, side 11, ’Details on the data used for business operations’. [↑](#footnote-ref-26)
27. Microsoft Irelands databehandleraftale, side 5, ”Scope”. [↑](#footnote-ref-27)
28. Microsoft Irelands databehandleraftale, side 6,” Processing to Provide Customer the Products and Services”. [↑](#footnote-ref-28)
29. Microsoft Irelands databehandleraftale, side 6, “Processing for Business Operations Incident to Providing the Products and Services to Customer”. [↑](#footnote-ref-29)
30. Microsofts business operations white paper, side 10, ‘Details on the data used for business operations’, ‘Overview’, samt side 14. [↑](#footnote-ref-30)
31. Microsofts business operations white paper, side 9 f., ’Details on the data used for business operations’. [↑](#footnote-ref-31)
32. Microsofts business operations white paper, side 9 f., ’Details on the data used for business operations’. [↑](#footnote-ref-32)
33. Microsofts business operations white paper vol. 2, side 1. [↑](#footnote-ref-33)
34. Microsofts business operations white paper, side 6, ’Overview of processing in the Microsoft cloud’. [↑](#footnote-ref-34)
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. [↑](#footnote-ref-35)
36. Vol. 2, side 6. [↑](#footnote-ref-36)
37. Microsofts business operations white paper, side 10, ’Details on the data used for business operations’. [↑](#footnote-ref-37)
38. Microsofts business operations white paper, side 11, ’Details on the data used for business operations’. [↑](#footnote-ref-38)
39. Se f.eks. Microsofts business operations white paper, side 13, ‘Details on each of the four business operations’. [↑](#footnote-ref-39)
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). [↑](#footnote-ref-40)
41. Microsofts business operations white paper, side 13, ’Customer Billing and Account Management’. [↑](#footnote-ref-41)
42. Microsofts business operations white paper, side 14, ’ Compensation’. [↑](#footnote-ref-42)
43. Microsofts business operations white paper, side 14, ’Microsoft Internal Reporting and Business Modelling’. [↑](#footnote-ref-43)
44. Microsofts hjemmeside: <https://support.microsoft.com/en-gb/office/diagnostic-data-in-microsoft-365-f409137d-15d3-4803-a8ae-d26fcbfc91dd>, under ”note” (senest tilgået 16. marts 2024). [↑](#footnote-ref-44)
45. Microsofts hjemmeside: <https://support.microsoft.com/en-gb/office/diagnostic-data-in-microsoft-365-f409137d-15d3-4803-a8ae-d26fcbfc91dd> (senest tilgået 16. marts 2024). [↑](#footnote-ref-45)
46. Microsofts hjemmeside: <https://learn.microsoft.com/en-us/deployoffice/privacy/required-diagnostic-data> (senest tilgået 16. marts 2024). [↑](#footnote-ref-46)
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 16. marts 2024). [↑](#footnote-ref-47)
48. EDPB, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 2.1, Adopted on 07 July 2021. [↑](#footnote-ref-48)
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. [↑](#footnote-ref-49)
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. [↑](#footnote-ref-50)
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. [↑](#footnote-ref-51)
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. [↑](#footnote-ref-52)
53. Artikel 29-Gruppen, udtalelse 05/2012 om cloud computing, WP 196, vedtaget den 1. juli 2012. [↑](#footnote-ref-53)
54. Journalnummer 2020-431-0061. [↑](#footnote-ref-54)
55. Datatilsynets udtalelse af 15. februar 2024 vedrørende Region Syddanmarks påtænkte brug af Microsoft 365, tilsynets j.nr. 2023-431-0012. [↑](#footnote-ref-55)
56. Microsoft Irelands databehandleraftale, side 9 (Bilag C), “Data Transfers and Location”. [↑](#footnote-ref-56)
57. Bilag B, side 20. [↑](#footnote-ref-57)
58. Bilag B, side 23. [↑](#footnote-ref-58)
59. EU Data Boundary dokumentationen, “On-premises software and client applications. [↑](#footnote-ref-59)
60. Side 23 f. [↑](#footnote-ref-60)
61. [https://learn.microsoft.com/en-us/privacy/eudb/eu-data-boundary-learn den 3](https://learn.microsoft.com/en-us/privacy/eudb/eu-data-boundary-learn%20den%203). marts 2024; *What is the EU Data Boundary?* [↑](#footnote-ref-61)
62. Journalnummer 2023-431-0001. [↑](#footnote-ref-62)
63. EDPB: Guidelines 3/2019 on processing of personal data through video devices, version 2.0, vedtaget den 29. januar 2020. [↑](#footnote-ref-63)
64. Fra CFCS’ hjemmeside her: <https://www.cfcs.dk/da/cybertruslen/trusselsvurderinger/cybertruslen-mod-danmark/> (senest tilgået den 23. maj 2024). [↑](#footnote-ref-64)
65. Microsofts hjemmeside: <https://learn.microsoft.com/en-us/microsoft-365/community/basic-security-set-up-for-microsoft-365> (tilgået 14. marts 2024). [↑](#footnote-ref-65)
66. Bilag C, side 8. [↑](#footnote-ref-66)
67. Bilag C, side 8-9 samt side 13-15. [↑](#footnote-ref-67)
68. Bilag C, appendix A, og bilag E, side 6. [↑](#footnote-ref-68)
69. Bilag E, side 6. [↑](#footnote-ref-69)
70. Bilag C, side 9. [↑](#footnote-ref-70)
71. <https://digst.dk/strategier/cyber-og-informationssikkerhed/national-strategi-for-cyber-og-informationssikkerhed-2015-2016/> (tilgået 14. marts 2024). [↑](#footnote-ref-71)
72. <https://sikkerdigital.dk/myndighed/tekniske-tiltag/tekniske-minimumskrav/tekniske-minimumskrav-2024> (tilgået 14. marts 2024). [↑](#footnote-ref-72)
73. Microsofts hjemmeside: <https://learn.microsoft.com/en-us/purview/customer-lockbox-requests> (senest tilgået den 22. marts 2024). [↑](#footnote-ref-73)
74. EDPB, WP 248, rev. 01, s. 7. [↑](#footnote-ref-74)
75. 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 19. juni 2024). [↑](#footnote-ref-75)
76. Microsofts business operations white paper, side 6, ’Overview of processing in the Microsoft cloud’. [↑](#footnote-ref-76)