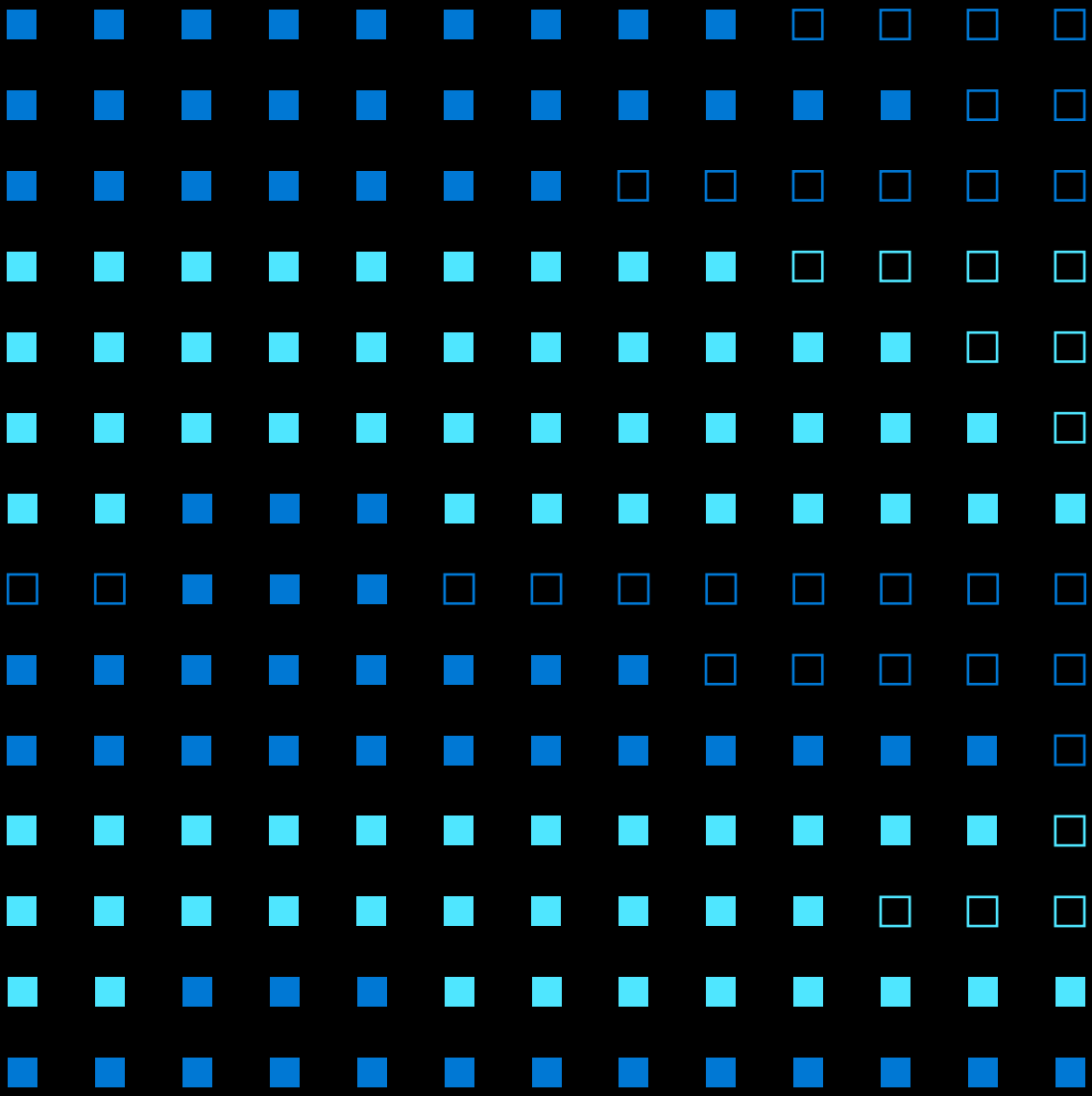
Microsoft Danmark & Island
Juni 2021
Dansk version 4.0

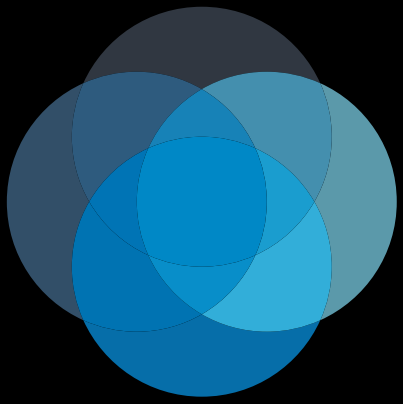
Microsoft

Cloud Governance.

Vejledning om hvordan sikkerhed, privatlivsbeskyttelse, compliance og risici kan vurderes og optimeres gennem ibrugtagning af Microsoft Cloud tjenester.



Dette whitepaper giver vejledning ift det der betegnes som Hyper Scale Cloud Computing (HSCC), og det er vigtigt at skelne denne form for cloud computing fra andre variationer[1], som tilbydes organisationer i dag – til markedsføringsformål vil mange udbydere navngive deres platform som Cloud Computing, mens den faktiske platform ofte vil mangle mange af de skaleringsmæssige, operationelle og økonomiske fordele sammenlignet med HSCC.



Indhold

00 / Opsummering

I løbet af de sidste 5-10 år har de fleste organisationer, herunder i den offentlige sektor og andre regulerede brancher, på et tidspunkt evalueret, om og i hvilket omfang de kan drage fordel af at bruge cloud-baserede løsninger og teknologier. Regeringer og tilsynsmyndigheder over hele verden har anerkendt potentialet i at udnytte dette teknologiparadigme, indføre "Cloud First"-lovgivning[1] og overordnet give vejledning i, hvordan man bedst evaluerer og implementerer cloud-baserede løsninger. Cloud computing er i nogen grad allerede blevet normen, ikke undtagelsen, når organisationer vælger platforme og løsninger til at understøtte og sikre deres evne til at drive forretning på en effektiv og modstandsdygtig måde i dag og i de kommende år.

Cloud computing defineres på følgende måde:

"Cloud computing er en model til at muliggøre allestedsnærværende, praktisk, on-demand netværksadgang til en delt pulje af konfigurérbare computerressourcer (f.eks. netværk, servere, storage, applikationer og tjenester), der hurtigt kan klargøres og frigives med minimal ledelsesindsats eller interaktion mellem tjenesteudbydere..."[2]

Dette whitepaper giver vejledning ift det der betegnes som Hyper Scale Cloud Computing (HSCC), og det er vigtigt at skelne denne form for cloud computing fra andre variationer[3], som tilbydes organisationer i dag - til markedsføringsformål vil mange udbydere navngive deres platform som Cloud Computing, mens den faktiske platform ofte vil mangle mange af de skaleringsmæssige, operationelle og økonomiske fordele sammenlignet med HSCC.

I de seneste år er bekymringerne i EU om, hvordan man etablerer og opretholder et passende databeskyttelsesniveau, og tilliden til udbyderne af Hyper Scale Cloud Computing-platformene vokset. EU-lovgivningen i form af en generel databeskyttelsesforordning (GDPR) er dog stadig helt klar og fastlægger de obligatoriske skridt, som enhver dataansvarlig og databehandler skal følge, for at beskytte og behandle personoplysninger. GDPR sammen med yderligere nationale databeskyttelseslove og EU-Domstolens Schrems II afgørelse den 16. juli 2020 (Schrems II) og EU's standardkontraktbestemmelser (udgivet af EU Kommissionen) udgør det juridiske grundlag, som al behandling af personoplysninger kan baseres på, uanset den valgte teknologiske platform. Dette dokument indeholder de detaljerede oplysninger, der er nødvendige for at alle organisationer kan vurdere, om og hvordan Microsoft HSCC Services (f.eks. Azure, O365, M365, D365, Power Platform).

1 New Zealand Cloud First strategi som et eksempel: https://www.digital.govt.nz/standards-and-guidance/technology-and-architecture/ cloud-tjenester

2 For flere detaljer om definitionen af cloud computing, se Mell, Peter og Grance, Timothy, 2011: NIST Definition af Cloud Services Computing, NIST Special Publication 800-145: https://aka.ms/NISTccDefinition

3 Yderligere oplysninger om variationerne findes i bilag A til dette dokument.

Vi mener, at konklusionerne er meget klare – Microsoft Hyper Scale Cloud Computing Services kan (og er allerede) tages i anvendelse til behandling og fuldt ud tilstrækkelig beskyttelse af personoplysninger.

Det er naturligt at udføre den nødvendige due diligence og sikre at HSCC-kunder i deres rolle som dataansvarlig kan bevare tilstrækkelig kontrol med de personoplysninger, som de registrerede har betroet dem, og denne hvidbog har til formål at beskrive en generisk proces hen imod en evaluering af om og hvordan tilstrækkelig privatlivs-, datasikkerheds-, juridisk og lovgivningsmæssig overholdelse kan etaleres.

Det er ikke i alle tilfælde en triviel opgave at etablere korrekt brug af Cloud Computing-tjenester. Passende risikovurderinger, supplerende foranstaltninger og styringsstrukturer (governance) skal gennemføres og vedligeholdes over tid – men de fordele, der venter, opvejer langt de ressourcer, der er nødvendige for denne rettidige omhu, både med hensyn til let adgang til innovativ ny teknologi, næsten uendelig skalerbarhed, gavnlig ændring af omkostningsstruktur og stærkt forbedret modstandsdygtighed over for et cybertrusselsmiljø i hastig udvikling.

Desuden er solid risikostyringspraksis ikke ny eller specifik for indførelsen af Cloud Computing, men har altid været nødvendig for vurdering og ibrugtagning af lovlig og tilstrækkelig sikkerhed og beskyttelse i både nye og eksisterende systemer i det lokale miljø (on-premises).

Denne hvidbog beskriver ikke kun modeller for, hvordan man etablerer det informerede og dokumenterede grundlag for denne tilstrækkelige beskyttelse, risikostyring, tillid og kontrol, men giver også vejledning i, hvordan man bedst udfører den krævede juridiske og sikkerhedsmæssige due diligence-proces, etablerer løsningsdesign og bedste praksis for styring af sikker og complianct brug af HSCC.

Introduktion- og læsevejledning

Digital transformation sker hver dag, overalt i verden. Det giver organisationer mulighed for at samarbejde med deres kunder eller partnere på nye måder og omdanne, tilpasse og innovere deres produkter, tjenester og forretningsmodeller. De kan optimere deres drift og samtidig styrke deres medarbejdere. Fremme af teknologier på den digitale arbejdsplads, forretningsapplikationer, data, maskinlæring og kunstig intelligens giver organisationer i alle størrelser mulighed for at gøre tingene fundamentalt anderledes og optimalt ift. markedet. På grund af den digitale transformations indvirkning på vores økonomi, samfund, regeringer og kultur beskrev World Economic Forum[4] dette som den fjerde industrielle revolution.

Digital transformation udmønter sig i mange forskellige scenarier, hvor en stigende mængde data skal behandles. Især inden for områder som Tingenes internet (IoT), big data, kunstig intelligens og maskinlæring genereres, genereres, lagres, behandles og analyseres, hvilket kræver skalerbar datacenterkapacitet og dynamisk adgang til ressourcer som compute-power, lagring og netværk. Forretningsinnovation nyder stor gavn af evnen til hurtigt at teste og implementere nye funktioner uden at pådrage sig omkostningerne ved at indkøbe, etablere og vedligeholde ny dyr infrastruktur. Efterhånden som organisationer omdannes til mere digitaliserede virksomheder, bliver teknologien mere og mere grundlæggende og afgørende for at understøtte processerne i organisationen, og det deraf følgende behov for kapacitet, smidighed og økonomiske fordele driver en stærk efterspørgsel efter Cloud computing. On-demand-tilgængelighed af store mængder ressourcer og innovative tjenester, der imødekommes af "betal-kun- for-hvad-du-bruger"-finansieringsmodeller – Cloud computings kerneegenskaber – giver attraktive muligheder for de fleste.

Bekymringer om tab af kontrol, privatliv, compliance, sikkerhed og pålidelighed kan dog stadig bremse organisationer fra fuldt ud at omfavne potentialet i HSCC onlinetjenester.

Det er klart, at organisationer bliver mere afhængige af deres it-infrastruktur og de leverandører som anvendes. Ligeledes bliverde typer data, der behandles, ofte mere kritiske eller følsomme, f.eks. intellektuel ejendomsret, personoplysninger, finansielle data eller sundhedsjournaler. Derfor bliver mange ikke-funktionelle krav til it, såsom tilgængelighed, kvalitet, privatliv og sikkerhed, udbredte:

"Virksomheder og brugere vil kun bruge teknologi, hvis de kan stole på den."[5]

Derfor er det vigtigt, at organisationer praktiserer due diligence ved at evaluere og vurdere disse ikke-funktionelle krav, typisk gennem en grundig risikovurderingsproces, hvor mange elementer generelt allerede er på plads, da vurderingen af it-risiko ikke er noget nyt i sig selv.

4 se: https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/
5 https://news.microsoft.com/2015/11/17/satya-nadella-and-julia-white-government-cloud-forum/

Tillid

Tillid er en sindstilstand, og uden tillid fungerer vores samfund ikke. Når man bruger cloudtjenester, indgår man reelt et partnerskab med cloudtjenesteudbyderen, og – som med ethvert partnerskab – er det bydende nødvendigt, at begge parters ansvar i dette forhold er klart defineret, og at tilliden kan verificeres (Trust, but verify!).

Så for at opbygge dette betroede forhold har kunderne brug for sikkerhed og indsigt i skyens pålidelighed for at fastslå, at cloud-tjenesten er designet og drevet sikkert og overholder alle gældende love og bestemmelser. Det krævede sikkerhedsniveau er for det meste klart defineret og håndhævet af juridiske og lovgivningsmæssige krav (f.eks. GDPR) og kan styres af sikkerhedskontrolrammer som ISO 27001 og revideres af tredjeparter ved hjælp af en international standard som SSAE/SOC 2.

Samtidig er det ikke muligt at drive en virksomhed uden at løbe nogen risiko, men organisationer skal have en solid forståelse af disse risici, så de kan træffe informerede beslutninger om deres risikoreduktionsstrategi: dvs. accept af risiko, overførsel af risiko eller reduktion af risiko til acceptable niveauer, som defineret af virksomheden, ved evt. at vælge passende supplerende kontroller.

Læsevejledning

Udgangspunktet for denne hvidbog er, hvordan Microsoft som cloududbyder håndterer det behandlingsansvar, der følger af, at kunder vælger at bruge Microsofts cloudbaserede tjenester, specifikt:

Online Service	Microsoft Trust Center	Yderligere detajer i specifikt whitepaper pr service
Microsoft 365: (inkl. O365)	https://aka.ms/MScloudtrust365	https://aka.ms/MSM365DataResidency Whitepaper som frigives i første halvår af 2021
Dynamics 365: (inkl. Power Platform)	https://aka.ms/MScloudtrustDynamics	https://aka.ms/MSD365DataResidency Whitepaper som frigives i første halvår af 2021
Microsoft Azure:	https://aka.ms/MScloudtrustAzure	https://aka.ms/MSAzureDataResidency

Du kan finde en overordnet beskrivelse af Microsoft Cloud Compliance, herunder et detaljeret whitepaper https://aka.ms/mscloudcompliance

Indholdet i dette dokument udvælges på grundlag af erfaringer opsamlet gennem talrige dialoger med private og offentlige organisationer i hele Europa. Oplysningerne i dokumentet er således relevante for både offentlige og private organisationer, der overvejer eller allerede bruger Microsoft Online Services.

Resten af hvidbogen er opdelt i følgende syv hovedafsnit:

01 / Juridiske rammer for cloud

02 / Cloud roller og fælles ansvar

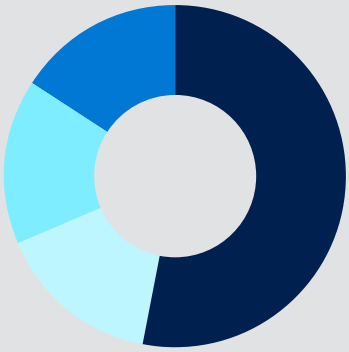
03 / Risikobaserede evalueringer

04 / Cloud Governance – bedste praksis

05 / Spørgsmål til cloud-udbyderen:
61 udvalgte spørgsmål om kontrakter, reerhedskontrol, underleverandørstyring, bæredygtighed, beredskabsplaner osv.

06 / Spørgsmål til din egen organisation:
18 udvalgte spørgsmål om strategi, forretningsplaner, risikovurdering, generel compliance, organisation, kompetencer og implementeringsplaner

07 / Appendix:
Detaljer om de samlede ejeromkostninger, Cloud Computing - Service- og leveringsmodeller, EDPB Udkast til anbefalinger, Specifikke nationale regler, Risikovurdering & Microsoft Cloud Assurance-proces, liste over de øvrige whitepapers, der henvises til, og en oversigt over de 79 spørgsmål og svar.



Dette papir er helt sikkert omfangsrigt og forsøger at dække alle scenarier og emner, der kan være af interesse. Læseren bør ikke afskrækkes af den store mængde information, men i stedet bruge den som reference ved blot at søge efter det specifikke emne af interesse. F.eks. en PDF-søgning efter udtrykket "underdatabehandlere", som vil guide direkte til to Q&A's som beskæftiger sig med dokumentation og vejledning om netop dette emne.

01 / Juridiske rammer for cloud

Generelt er al lovgivning teknologisk set agnostisk, og har altså ikke specifikt til formål at regulere Hyper Scale Cloud Computing (HSCC). Cloud-tjenesteudbydere påtager sig naturligvis rollen og ansvaret som databehandler. Det inkluderer udarbejdelse af detaljeret dokumentation, som er tilgængelig for den dataansvarlige (lovpligtigt) for, hvordan tjenesterne drives og sikres. I de senere år er der juridisk blevet rejst spørgsmål om, hvorvidt det er muligt lovligt at anvende HSCC, især for organisationer indenfor EU/EØS's geografiske område.

Flere officielle vejledning whitepapers er blevet offentliggjort i de seneste år for at hjælpe organisationer overveje, om og hvordan man bedst kan gå i gang med en rejse mod at udnytte HSCC og drage fordel af dette revolutionerende computing paradigme, samtidig med at man styrer fri af farer.

De retslige rammer for indsamling, opbevaring, behandling og deling af personoplysninger fra EU/EØS består primært af EU's databeskyttelsesforordning (GDPR) af 25. maj 2018 og de nationale databeskyttelseslove som fulgte i mange EU-medlemsstater. EU-Domstolen (CJEU) tilføjede den 16. juli 2020 i den såkaldte "Schrems II"-afgørelse, at "karakteren af dataoverførsler uden for EU/EØS" skal tages i betragtning i enhver vurdering.

Ingen af elementerne i de retslige rammer er specifikt skrevet til eller begrænset til brugen af teknologi – de har til formål at optimere sikkerhed og privatlivsbeskyttelse for alle personoplysninger, der indsamles i EU / EØS, uanset hvor eller af hvem personoplysninger indsamles, lagres eller behandles.

Generel databeskyttelsesforordning (GDPR)

Grundlaget for GDPR er 99[6] artikler, der præciserer alt fra omfang, formål, lovlighed af behandling, krav til dataoverførsler uden for EU/EØS, de registreredes, den dataansvarliges og databehandlerens roller, til det der kræves i en databehandleraftale mellem en dataansvarlig og en databehandler.

Microsoft forpligtede sig meget tidligt[7] til både at være GDPR-kompatibel i vores rolle som dataansvarlig (primært for forbrugertjenester som fx. Xbox) og databehandler og fortsætter med at sikre de nødvendige juridiske rammer, dokumentation og assistance til at hjælpe kunder med at implementere platformens produkter og tjenester på en GDPR-kompatibel måde.

6 https://gdpr-info.eu/
7 https://aka.ms/MSGDPR

Dette whitepaper er ikke ment som en guide til GDPR[8] som sådan, men det er vigtigt at påpege, at centrale elementer relateret til emnet Cloud Governance, er spredt ud over de følgende 30 artikler:

- Lovligheden af behandlingen (artikel 6)
- Den registreredes rettigheder (artikel 12-23)
- Den dataansvarliges og databehandlerens ansvar (artikel 24-43)
- Overførsel af personoplysninger til tredjelande eller internationale organisationer (artikel 44-50)

Gennem disse artikler og GDPR i almindelighed, er et par meget relevante og bemærkelsesværdige begreber:

- **Risikobaseret fremgangsmåde;** I hele GDPR opfordres organisationer, der kontrollerer behandlingen af personoplysninger, til at gennemføre beskyttelsesforanstaltninger som er passende ift risikoniveauet for deres databehandlingsaktiviteter, og mange databeskyttelsesmyndigheder har gennem årene offentliggjort specifik vejledning[9] om, hvordan disse udføres. Dette vil vi undersøge meget mere detaljeret i dette afsnit og også give eksempler til inspiration.

- **Proportionalitet/afbalanceret fremgangsmåde;** I henhold til GDPR kræves der en klar 'use case' for behandling af personoplysninger. I sin enkleste form betyder det, at personoplysninger i kundedata ikke kan behandles, medmindre det er nødvendigt for at opfylde et specifikt kundekrav (~dataminimering) og med databeskyttelsesforanstaltninger, der er proportionale med risiciene ved behandlingsscenarierne (~tilstrækkelighed). Dette vil vi også undersøge meget mere detaljeret i Q &A delene af dette whitepaper.

- **Gennemsigtighed og ansvarlighed;** Den dataansvarlige skal kunne påvise, at personoplysninger behandles på en gennemsigtig måde i forhold til den registrerede. Disse gennemsigtighedsforpligtelser begynder på dataindsamlingstidspunktet og gælder i hele behandlingscyklussen (~ansvarlighed). Databehandleren (f.eks. Microsoft som databehandler, når der gøres brug af Microsoft HSCC Online Services) har en klar rolle at spille her. På grund af karakteren af HSCC er mange af de implementerede sikkerheds- og privatlivskontroller i databehandlerens kontrol og skal dokumenteres, så den dataansvarlige kan vurdere og revidere (~gennemsigtighed) – men nogle af kontrollerne forbliver i hænderne på den dataansvarlige (se Roller & fælles ansvar nedenfor) og skal vurderes, implementeres og dokumenteres for at bringe den samlede risiko ned på et acceptabelt niveau. Disse to specifikke elementer er hovedparten af Q&A-afsnittene senere i dette dokument.

8 https://aka.ms/MSGDPROverview

9 Et eksempel er den vejledning om risikovurdering og konsekvensanalyse af privatlivets fred, som Datatilsynet har offentliggjort på https://aka.ms/DKGDPRvejledninger

På nuværende tidspunkt har der på grund af Schrems II-dommen været stor fokus på kapitel 5 i GDPR, hvori det specificeres, at dataoverførsler uden for EU/EØS kun lovligt kan finde sted, hvis følgende to betingelser er opfyldt:

01 / Et retsgrundlag for dataoverførsel skal fastlægges i aftalen mellem parterne som beskrevet i artikel 44 - 47 i GDPR. Det kan f.eks. være EU's standardkontraktbestemmelser, hvilket typisk er tilfældet for leverings-/ databeskyttelsesaftaler for HSCC tjenester.

02 / Der skal fastsættes og dokumenteres et tilstrækkeligt sikkerhedsniveau ("Passende sikkerhedsforanstaltninger") i forhold til den risikovurdering, som den dataansvarlige er ansvarlig for at udføre.

Generelt er artiklerne i GDPR fokuseret på begreber som "Proportionalitet", "risikobaseret tilgang" og "passende" – vigtige elementer, der på mange måder overlader det til den dataansvarlige at vurdere, træffe beslutning om en fremgangsmåde og gennemføre løbende styring.

I nogle tilfælde kan det under vurderingen af dataoverførsler være relevant også at tage hensyn til artikel 49 – 1d ("*overførslen er nødvendig af vigtige hensyn til almenvellet*") og senere artikel 49-4 ("*Den offentlige interesse, der er omhandlet i stk. 1, første afsnit, litra d), anerkendes i EU-retten eller i lovgivningen i den medlemsstat, som den dataansvarlige er underlagt.*")

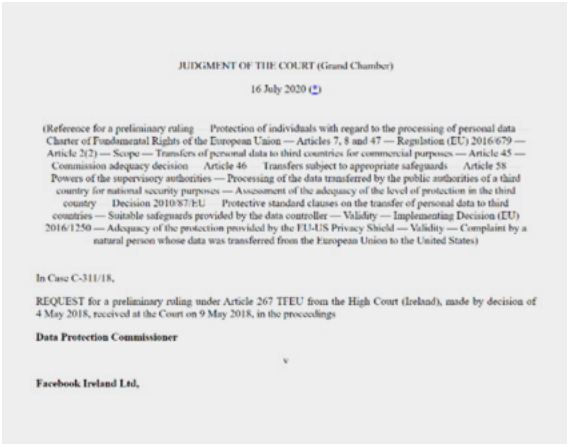
Den Europæiske Unions Domstol (EU-Domstolen): Schrems II afgørelse 16. juli 2020

Dette whitepaper vil naturligvis ikke gentage den fulde ordlyd af10 afgørelsen, men alene fremhæve et par vigtige elementer, af særlig interesse, når man vurderer HSCC platforme - især:

- Dommen er baseret på en klage over, at en udbyder af sociale medier fysisk overfører personlige data i bulk til servere i USA med Privacy Shield som det juridiske grundlag.

- EU-Domstolen ugyldiggør Privacy Shield som en validt overførselesgrundlag - genfortolkning af GDPR-artikel 45 i kontekst af Schrems II sagen.

- EU-Domstolen bekræfter også, at EU-Kommissionens standardkontraktbestemmelser (SCC) fortsat er et gyldigt juridisk grundlag for dataoverførsler uden for EU/EØS i henhold til artikel 46.



JUDGMENT OF THE COURT (Grand Chamber)

16 July 2020 (*)

(Reference for a preliminary ruling – Protection of individuals with regard to the processing of personal data – Charter of Fundamental Rights of the European Union – Articles 7, 8 and 47 – Regulation (EU) 2016/679 – Article 2(2) – Scope – Transfers of personal data to third countries for commercial purposes – Article 45 – Commission adequacy decision – Article 46 – Transfers subject to appropriate safeguards – Article 58 – Powers of the supervisory authorities – Processing of the data transferred by the public authorities of a third country for national security purposes – Assessment of the adequacy of the level of protection in the third country – Decision 2010/87/EU – Protective standard clauses on the transfer of personal data to third countries – Suitable safeguards provided by the data controller – Validity – Implementing Decision (EU) 2016/1250 – Adequacy of the protection provided by the EU-US Privacy Shield – Validity – Complaint by a natural person whose data was transferred from the European Union to the United States)

In Case C-311/18,

REQUEST for a preliminary ruling under Article 267 TFEU from the High Court (Ireland), made by decision of 4 May 2018, received at the Court on 9 May 2018, in the proceedings

Data Protection Commissioner

v

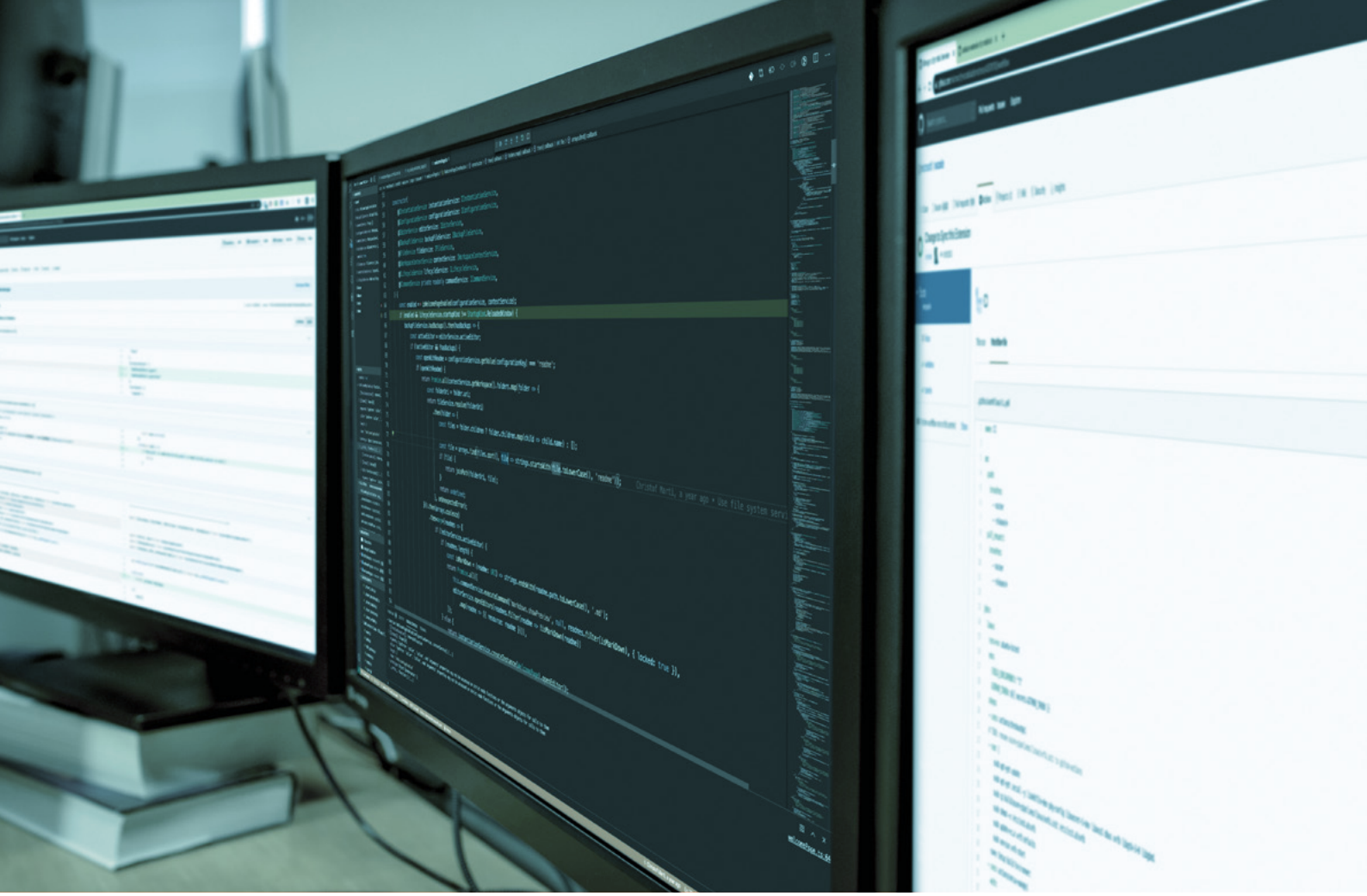
Facebook Ireland Ltd,

- EU-Domstolen gør det klart, at de dataansvarlige …
  - *skal altid tage hensyn t*il »Omstændighederne af overførslen«,
  - *skal* have en risikobaseret tilgang &
  - *i nogle tilfælde* skal der tilføjes supplerende foranstaltninger til EU's SCC for at sikre tilstrækkelig beskyttelse.

Endelig anfører EU-Domstolen, at amerikanske overvågningslove ikke giver tilstrækkelig databeskyttelse til de registrerede, idet de grundlæggende vurderer, at USA er et usikkert tredjeland[11]- som så mange andre i EU-lovgivningens øjne.

10 https://aka.ms/SchremsIIverdict

11 EU's afgørelse om tredjelandes tilstrækkelighed: https://aka.ms/EUSafe3rdCountries
A. https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/recommendations-012020-measures-supplement-transfer_en
b https://edps.europa.eu/press-publications/press-news/press-releases/2021/edpb-edps-adopt-joint-opinions-new-sets-sccs_en



Vurdering af relevant amerikansk lovgivning

Denne vurdering gav anledning til, at det amerikanske handelsministerium i september 2020 på vegne af den amerikanske regering at udstede et whitepaper[12] for *"…. at give en detaljeret diskussion af amerikanske love og praksis vedrørende regeringens adgang til data til nationale sikkerhedsformål …"* - samlet for at sikre baggrunden for og målene med amerikanske overvågningslove var klart forstået og ikke overdrevet.

Derudover er det vigtigt når man vurderer den amerikanske lovgivning, at tage hensyn til perspektiver fra disse to dokumenter:

- en vurdering[13] af den amerikanske CLOUD Act udstedt af IDC i november 2018, der har til formål at aflive eventuelle myter om rækkevidden og effekten af denne specifikke lovgivning,
- en ordre[14] fra det amerikanske justitsministerium fra december 2017 om "Seeking Enterprise Customer Data Held by Cloud Service Providers", der giver klar vejledning om, hvordan og hvornår man skal anmode om data fra dataansvarlige og ikke Cloud-tjenesteudbydere.

12 https://aka.ms/USDocDatatransfers
13 https://aka.ms/IDCCloudAct
14 https://aka.ms/USDOJSeekingEnterpriseData

Microsofts forpligtelse til overholdelse kræver opdateringer efter Schrems II-dommen

Dommen tilføjer yderligere perspektiv til fortolkningen af GDPR-artikel 45, og som følge heraf har Microsoft efterfølgende to gange foretaget ændringer i databeskyttelsesaftalen[15] om databehandling på Microsoft HSCC platforme - dette er de vigtigste ændringer, som er introduceret:

- **den 21. juli 2020, forsikrer kunder ift. grænseoverskridende[16] datastrømme**:
  - Privacy Shield bruges IKKE af Microsoft som den juridiske ramme for eventuelle dataoverførsler, når du bruger onlinetjenester, der er underlagt DPA. Microsoft vil dog fortsat overholde Privacy Shields principper om beskyttelse af personlige oplysninger.
  - EU's standardkontraktbestemmelser (SCC) bekræftes som den juridiske ramme for at beskytte data når/hvis de overføres uden for EU/EØS, ifm. brug af onlinetjenester omfattet af DPA.
- **den 9. december 2020**:
  - Tilføjede et tillæg 3 til EU›s SCC, det såkaldte "Additional Safeguards Addendum"[17], som
    - Forpligter sig til, at Microsoft vil anfægte enhver regerings anmodning om adgang til kundedata fra offentlige og private organisationer – fra enhver regering – hvor der er et lovligt grundlag for at gøre det.
    - Holder de registrerede skadesløs for enhver materiel eller ikke-væsentlig skade på den registrerede som følge af Microsofts videregivelse af personoplysninger om den registrerede, der er blevet overført i henhold til SCC, som svar på en ordre fra et statsligt organ eller en retshåndhævende myndighed uden for EU/EØS.
  - Understreger det mangeårige engagement[18] Microsoft har givet for at beskytte kundernes rettigheder til deres data, f.eks. ved at bruge stærk kryptering af kundedata både i hvile og i transit. Understreger også Microsofts principielle håndtering af, gennemsigtighed omkring og historisk succes med at beskytte rettigheder ved at udfordre alle tredjepartsanmodninger om adgang til kundedata.

15 https://aka.ms/DPA
16 https://aka.ms/MSXbDF
17 https://aka.ms/MSDyD
18 https://www.microsoft.com/en-us/trust-center/privacy

Yderligere opdateringer af databeskyttelsesaftalen (DPA) kan blive introduceret på grund af fremtidige ændringer i lovgivningen, og disse er simpelthen de seneste i en lang række trin, microsoft har taget for at give kunderne flere oplysninger og flere valgmuligheder og for at fortsætte vores bestræbelser på at beskytte kundernes data og rettigheder. Microsoft var den første store virksomhed, der frivilligt[19] offentligt gav fuld støtte til GDPR og til den stærkest mulige beskyttelse af personlige oplysninger til kunder over hele verden.

Microsoft vil fortsat konstant overvåge situationen og foretage[20] opdateringer, når det er nødvendigt, så kunderne kan fortsætte med at anvende Microsoft HSCC Services [21] på compliant vis.[22]

EU-kommission - Standardkontraktbestemmelser

Det er mere end 10 år siden, at EU-Kommissionen godkendte de såkaldte standardkontraktbestemmelser (SCC). Disse er siden i GDPR-artikel 46 – 2d blevet anset for at være en gyldig mekanisme til "passende beskyttelse" af PII ved overførsel af PII til et tredjeland. Som nævnt i ovenstående afsnit bekræftede EU-Domstolens Schrems II-dom gyldigheden af EU's SCC i juli 2020.

EU's SCC er og har længe været en integreret del af Microsoft Online Services – Data Protection Addendum (databeskyttelsesaftale som defineret i GDPR-artikel 28-3 red.) og for indblik i alle de forpligtelser, der følger af EU's SCC, henvises til den faktiske tekst i DPA. Nedenfor følger en hurtig oversigt over de forpligtelser, der er af særlig betydning for dataoverførsler, som allerede **er på plads i databehandleraftalen, når du bruger Microsoft HSCC Online Services**:

- EU's SCC pålægger Microsoft (som »importør«) at underrette kunden (»eksportøren«), hvis behandlingen ikke kan finde sted i overensstemmelse med de aftalte vilkår og EU's SCC.
- EU's SSC pålægger også Microsoft at vurdere, om der er gældende lovgivning (eller ændringer i lovgivningen), der forhindrer importøren i at opfylde aftalte vilkår – herunder EU's SCC.
- EU's SCC kræver, at Microsoft gennemfører tekniske og organisatoriske foranstaltninger for at sikre data inden overførslen.
- EU's SCC pålægger Microsoft at underrette kunden (»eksportøren«) om alle tilfælde af uautoriseret eller utilsigtet adgang.

19 https://aka.ms/MSGDPRCommitments
20 https://aka.ms/msdatalaw
21 https://aka.ms/mstechfit4europe
22 https://aka.ms/msdatalaw

Nye EU-standardkontraktbestemmelser

EU-Kommissionen offentliggjorde den 12. november 2020 et udkast til[23] og opdateret udgave af "standard-kontraktbestemmelserne for overførsel af personoplysninger til ikke-EU-lande". Høringsperioden sluttede i december 2020, og der forventes en endelig version i 202,1 med en efterfølgende gennemførelsesperiode, før den nuværende version er forældet.

Selv om det endelige indhold naturligvis er ukendt på nuværende tidspunkt, skal der bemærkes et par elementer – især at udkastet nævner:

- *"... bør navnlig tage hensyn til de særlige omstændigheder ved overførslen (f.eks. kontraktens indhold og varighed, arten af de overførte data, modtagerens type, formålet med behandlingen ...",*

- *"... og alle relevante praktiske erfaringer som viser, at der foreligger eller ikke foreligger forudgående tilfælde af anmodninger om offentliggørelse fra offentlige myndigheder, som dataimportøren har modtaget for den overførte type data) ..." og*

- *"Dataimportøren bør underrette dataeksportøren, hvis han efter at have accepteret klausulerne har grund til at tro, at han ikke er i stand til at overholde standardkontraktbestemmelserne. Hvis dataeksportøren modtager en sådan anmeldelse eller på anden måde bliver opmærksom på, at dataimportøren ikke længere er i stand til at overholde standardkontraktbestemmelserne, bør han identificere passende foranstaltninger til at håndtere situationen, om nødvendigt i samråd med den kompetente tilsynsmyndighed. Sådanne foranstaltninger kan omfatte supplerende foranstaltninger vedtaget af dataeksportøren og/eller dataimportøren, f.eks.*

Alt i alt har udkastet til nye SCC'er ligesom GDPR- og Schrems II-dommen altså en risikobaseret tilgang, hvor relevante og proportionale supplerende foranstaltninger skal sikre, at både eksportøren (Kunden) og importøren (Microsoft) kan implementere passende sikkerheds- og fortrolighedsforanstaltninger, og ikke mindst at kunden også skal vurdere risikoen, for at importøren ikke er i stand til at håndtere og dokumentere tredjepartsanmodninger om personoplysninger på passende vis.

Microsoft har offentligt forpligtet sig til at implementere de nye SCC senest 27. september, 2021.

23 https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12741-Commission-Implementing-Decision-on-standard-contractual-clauses-for-the-transfer-of-personal-data-to-third-countries

Finansielle tjenesteydelser

Cloud computing er også hurtigt ved at blive normen, ikke undtagelsen, for organisationer i den finansielle sektor (FSI) i EU. Sektoren er underlagt en lang række regler i EU og de enkelte medlemsstater (ud over naturligvis den generelle databeskyttelsesforordning), og det er derfor ofte et vigtigt aspekt af en risikovurdering eller evaluering af cloud-adoption at tage fat på bekymringer ift. compliance. Listen nedenfor præsenterer nogle af de mest almindelige regler, der også påvirker 'outsourcing' til cloud-udbydere til FSI:

- MiFID Org Regulation
- Solvency II Directive 2009/138/EC
- Solvency II Commission Delegated Regulation (EU) 2015/35
- European Bankers Association (EBA)'s endelige rapport om anbefalinger om outsourcing til cloudtjenesteudbydere EBA/REC/2017/03
- EBA Generelle retningslinjer for outsourcing EBA/GL/2019/02

EBA's anbefalinger om outsourcing til cloudtjenesteudbydere har skabt den nødvendige klarhed for FSI-kunder, der ønsker at implementere og høste fordelene ved cloud computing, samtidig med at det sikres, at risici identificeres og håndteres korrekt. Microsoft har været involveret i de drøftelser med EBA, der har ført til denne positive udvikling. Denne konstruktive måde at samarbejde på mellem Microsoft og FSI-tilsynsmyndigheder, som allerede startede i 2010, viser Microsofts engagement i effektivt at muliggøre en compliant anvendelse af moderne teknologier for kunder i denne regulerede sektor.

Microsoft giver yderligere vejledning og tjeklister til kunder, der hjælper med at håndtere risici og matche lovmæssige krav med Microsofts kontraktbestemmelser og -rammer. Desuden indeholder den seneste version af "Financial Services Amendment" yderligere kontraktmæssige commitment fra Microsoft til FSI-kunder til støtte for overholdelse af retningslinjerne fra EBA, EIOPA og ESMA. FSI amendment omhandler krav som f.eks.:

- Finanstilsynsmyndighedens ubegrænsede undersøgelses- eller revisionsrettigheder
- Forretningskontinuitet efter indgriben fra myndighed eller "Customer Transfer of Rights"
- Reaktion på lovgivningsmæssige ændringer

Du kan finde flere oplysninger, der er specifikke for FSI, på Microsoft Services Trust Center [24] og især i denne hvidbog om FSI-vejledning[25] som har til formål at matche (EBA Guidelines on) FSI Compliance-krav til Microsofts kontraktlige forpligtelser og bestemmelser.

24 https://aka.ms/STP
25 https://aka.ms/MSFSIComplianceGuide

Opsummering af de relevante juridiske rammer

Kort sagt har de retslige rammer (GDPR + EU-Domstolens domme + nationale databeskyttelseslove + EU's databeskyttelseslovgivning og særlige krav til FSI) alle en risikobaseret tilgang, hvor de søger proportionalitet mellem identificerede risici, passende og supplerende foranstaltninger, omstændighederne ved behandlingen/overførslerne og acceptable resterende risici samt proportionalitet mellem de behandlede Personoplysninger og formålet med en sådan behandling.

Formålet med de følgende sider er at vejlede om modeller og indhold/dokumentation, der er nødvendig for at udføre de lovpligtige vurderinger på vej henimod at kunne anvende HSCC – en vej som inkluderer vurderinger af, om, hvornår, for hvad og hvordan man bedst udnytter HSCC, styrer den optimale databeskyttelse og overholdelse af dokumentationskrav.

02 /
Cloud roller & fælles ansvar

Brug af cloud computing introducerer en 'Shared Responsibility'-model[26], som er vigtig at forstå for alle, der bruger HSCC. Den grundlæggende forudsætning for modellen er, at cloud computing er et partnerskab, der resulterer i fælles eller delte ansvarsområder.

Både HSCC-kunden og cloud-tjenesteudbyderen skal overholde love og regler, begge har ansvar for sikkerhed, kontinuitet og privatlivsbeskyttelse. Dermed er omfanget og rækkevidden af kontroller, serviceleverancemodel-lerne, grundlæggende og af største vigtighed når adskillelsen af ansvar og ansvarlighed mellem kunden og cloud-udbyderen fastlægges – og dermed vigtig af en cloudevalueringsproces.

Billedet nedenfor illustrerer modellen med delt ansvar for sikkerhedsdomænet, og modellen kan nemt replikeres til andre domæner.

26 https://aka.ms/SharedResponsibility

Modellen illustrerer blandt andet, at cloud-udbyderen er ansvarlig for at styre nogle af sikkerhedslagene, men aldrig den fulde 'stak', delvist på grund af dataansvarlige versus databehandleransvar som defineret i loven (GDPR), men også med baggrund i den serviceleverancemodel, som kunden beslutter at tage i brug.

Derudover er det vigtigt at forstå de forskellige cloud-implementeringsmodeller (private, hybride, offentlige) og serviceleveringsmodeller, da de danner grundlaget for det "fælles ansvarsparadigme", som igen udgør det centrale fundament for sikkerhedsmodellen. Tillæg A beskriver modellerne i detaljer i overensstemmelse med NIST SP 500-292 Cloud Computing Reference Architecture.[27]

Som tidligere beskrevet vil dette dokument fokusere på HSCC (kendt som 'offentlig sky'), hvor standardiserede isolerede tjenester leveres til cloud-kunder af cloud-udbyderen (CSP), en separat organisation, der ejer og vedligeholder den underliggende delte infrastruktur.

"Cloud computing er et partnerskab, der resulterer i fælles ansvar."

Kunden skal derfor selv etablere og konfigurere kontroller/foranstaltninger for de resterende lag af ansvaret (gennem konfiguration af cloudplatformene, implementeringsprocesser eller eventuelt tilføjelse af yderligere teknologiløsninger), så de passer til enhver regulering, risikovurdering og politikker, der er defineret af deres egen organisation. Distributionen og omfanget af den portefølje af værktøjer, som udbyderen stiller til rådighed for kunden, afhænger af den valgte platform og den type cloud-leveringsmodel, som en given løsning anvender.

Det er vigtigt at være opmærksom på, at en cloudtjenesteudbyder også kan levere valgfrie kontroller, som kan hjælpe kunden med at løfte deres ansvar. Ud over microsoft-administreret kryptering leverer Microsoft f.eks. yderligere omfattende datakrypteringsteknologier som en valgfri del af sine tjenester, og disse kan hjælpe kunderne med at håndtere yderligere databeskyttelseskrav, hvis de er identificeret igennem risikovurderingen.

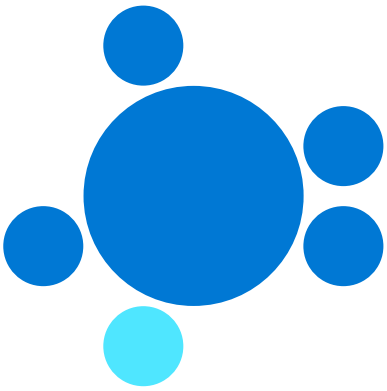
27 https://www.nist.gov/publications/nist-cloud-computing-reference-architecture

Samlet set opdeler modellen kontrolelementerne i tre kategorier:

A. Cloudtjenesteudbyder (CSP) administrerer og driver kontroller.
B. Kunden styrer og driver kontroller.[28]
C. Både kunden og CSP administrerer relevante kontrolelementer.

Så en cloud-tjenesteudbyder skal implementere, betjene og vedligeholde mange grundlæggende kontroller (de mørke bokse i illustrationen "Share Responsibility" ovenfor) og kan hjælpe kunden med yderligere, valgfrie kontroller til at håndtere det fulde sæt af kundens ansvarsområder. Selvfølgelig vil der altid være områder, hvor cloud-tjenesteudbyderen har ringe eller ingen indflydelse – fx. den måde hvorpå kunden konfigurerer, bruger og indlejrer cloud-tjenester i kundens processer.

Bemærk også, at end-to-end ansvarlighed for overholdelse forbliver i mange tilfælde hos kunden (defineret ved regulering som GDPR), så for at etablere den førnævnte grundlæggende tillid skal kunden være i stand til at kontrollere, om cloud-tjenesteudbyderen kan levere på tilstrækkeligt niveau - dette er en væsentlig del af "assuranceprocessen", der vil blive diskuteret yderligere i dette whitepaper.



28 Der er mange kontroller, hvor CSP leverer og driver teknologien til kontrollen, men kunden administrerer konfiguration og drift. Disse kontroller hører imidlertid under kundens overordnede ansvar. Microsoft kan f.eks. tilbyde multifaktorgodkendelse som en mulighed i Microsoft 365, men det er den enkelte kunde, der skal aktivere/administrere den (via konfiguration). Dette er adskilt fra f.eks. fysiske kontroller i Microsoft Datacentre, hvor kontroller både drives og administreres fuldt ud af Microsoft. Kunden har naturligvis stadig ansvaret for at kontrollere, om Microsoft-kontrolelementer er tilstrækkelige til kundens specifikke scenarie, f.eks. ved at evaluere tredjepartsrevisionsrapporter og certificeringer.

03 / Risikobaseret evaluering

Begrebet risikostyring er vigtigt for de fleste organisationer, fordi det hjælper med at definere og afbalancere målene for fremtiden.

Der er mange risikotyper og funktioner: strategisk, operationel, finansiel, sikkerhed (herunder it-sikkerhed) og compliance/juridisk risiko.

I forbindelse med dette whitepaper, der har til formål at sikre compliant vurdering, indførelse og anvendelse af teknologi og cloudtjenester i organisationers digitale transformation, er det afgørende at tage fat på it-sikkerhed, privatlivsbeskyttelse og compliance/juridisk risiko.

(...) risikostyring er målrettet personer, der skaber og beskytter værdi i en organisation ved at styre risici, træffe beslutninger, fastsætte og nå mål og forbedre ydeevnen (...)

ISO 31000:2009

Integration af forskellige risikoprogrammer og discipliner i en organisation, undertiden kaldet 'integreret sikkerhed', er et vigtigt emne, men det er uden for rammerne af dette whitepaper. Som en arbejdsdefinition af risiko[29] er det bredt accepteret at beskrive risiko som sandsynligheden for, at der sker noget, der fører til en faktisk negativ indvirkning.

29 https://www.merriam-webster.com/dictionary/risk

Illustrationen nedenfor beskriver it-sikkerhedsrisiko, men kan også gælde for andre former for risiko.

Afvejning af risiko og muligheder

Generelt opfattes risiko som noget der skal elimineres, da risikoen i definitionen vedrører sandsynligheden for et negativt resultat. Det er imidlertid vigtigt at forstå, at det generelt er afgørende for at en organisation kan vokse og trives, at der anlæggess en afbalanceret risikobaseret tilgang. Kun således kan den rigtige proces etablere afbalancerede muligheder fra en given aktivitet, med det rigtige niveau af risikostyring og naturligvis fuld compliance.

Dette indgår også i høj grad som et grundlæggende princip i de relevante retslige rammer, som beskrevet i ovenstående kapitel om GDPR, Schrems II-dommen osv.

Al databehandling indebærer risici, uanset arkitektur, leveringsmodel osv. Formålet med at foretage en risikovurdering af enhver form for dataindsamling, -lagring og -behandling er således IKKE at eliminere risici, men at vurdere, minimere og styre risiciene løbende. En nulrisikotolerance hindrer udførelsen af organisationens målsætninger, mens solid risikostyring kan understøtte organisationens vækst og samtidig give mulighed for optimal databeskyttelse.

Som det fremgår af eksempler i dette dokument, vil de fleste organisationer gennem udførelse af risiko-vurderinger finde temmelig store forbedringer i deres risikostyring, når de sammenligner nuværende lokale løsninger med HSCC-løsninger.

Risikovurderingsmodeller

I HSCC's verden er ISO/IEC 27001-standarden for informationssikkerhedsstyringssystemer afgørende og vil altid være i centrum for enhver compliance dokumentation en Cloud Service Provider, skal kunne levere til deres kunder (se afsnittet Q&A i dette whitepaper for ISO og mange andre standardcertificeringer, der tilbydes af Microsoft Online Services-platformen). ISO/IEC 27005 er derudover en standard, som udelukkende er dedikeret til risikostyring af informationssikkerhed – hvilket er meget nyttigt, hvis der er behov for dybere indsigt i risikovurdering af informationssikkerhed og behandlingsrisikobegrænsende foranstaltninger.

For en dataansvarlig under GDPR (alias: cloud-kunden) som påtager sig risici der skal identificeres, vurderes og potentielt afbødes, er det oftest ISO27001-standarden, rettet mod driften af en HSCC som er relevant, men kan også med den relativt nye ISO27701[30] Privacy Information Management System-standard få yderligere kontroller, af relevans for GDPR-overholdelse, (ISO27701 kan betragtes som implementeret, som den tilbydes af Microsoft HSCC Online Services, men bemærk at standarden indeholder en række kontroller fokuseret på implementering hos den data ansvarlige). Compliance porteføljen som CSP'en stiller til rådighed er et godt springbræt for kunden og giver indsigt i, hvordan den grundlæggende sikkerhed og privacy ifm. drift og vedligehold er etableret og konstant revideres af tredjepart.

Mange nationale[31] databeskyttelsesmyndigheder i EU har offentliggjort specifikke retningslinjer for de to typer risikovurderinger, dataansvarlige kan forventes at udføre, og under hvilke omstændigheder hver enkelt skal anvendes.

Nedenstående illustration er den samlede risikovurderingsmatrix der oftest tages udgangspunkt i. Den viser klart, at en nulrisikotilgang ikke er målet. Restrisici vil næsten altid eksistere og bør bevidst accepteres, håndteres og overvåges for eventuelle fremtidige ændringer.

Sandsynlighed	Konsekvenser				
	1 Ubetydelig	2 Mindre	3 Alvorlig	4 Meget alvorlig	5 Katastrofale
5 Ofte	5	10	15	20	25
4 Sansynlig	4	8	12	16	20
3 Sjælden	4	6	9	12	15
2 Usansynlig	2	4	6	8	10
1 Meget usansynlig	1	2	3	4	5

30 https://aka.ms/MScloudISO27701

31 Datatilsynets vejledning om risikovurderinger og konsekvensanalyser af databeskyttelse, herunder eksempler på inspiration, kan findes på https://aka.ms/DKGDPRVejledninger

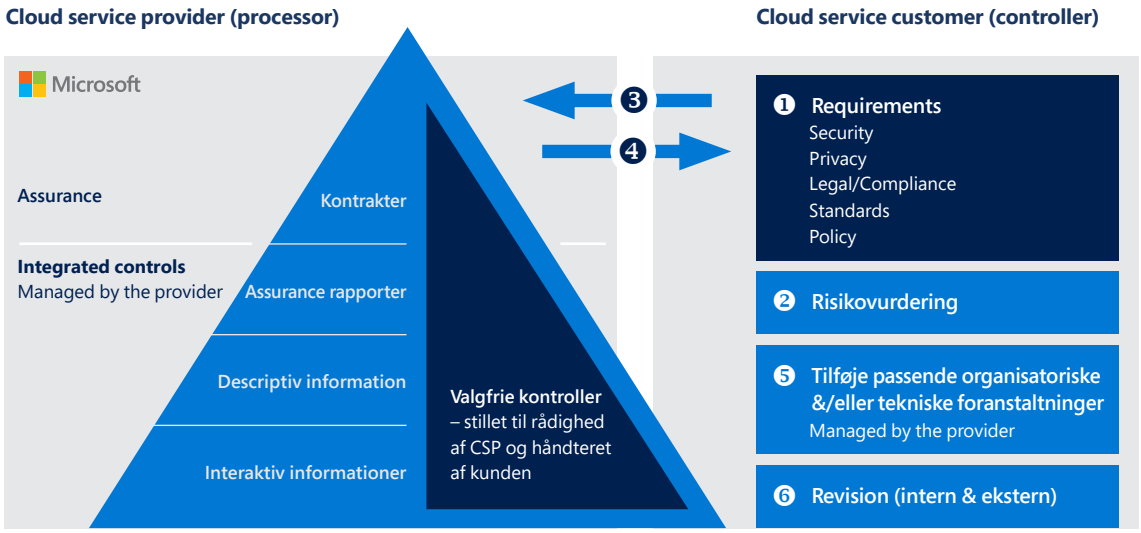
For at sænke den samlede risiko fremgår det af matrixen, at der kan træffes foranstaltninger for at sænke enten en eller begge faktorer (Konsekvens og Sandsynlighed).

For eksempel kan en identificeret risiko for, at personoplysninger falder i hænderne på en uønsket tredjepart på grund af medarbejderens fysiske tab af deres digitale enhed, flyttes fra en score på 3-5 i både sandsynlighed og konsekvens til en 2-3, hvis 'supplerende foranstaltninger' såsom stærk adgangskodebeskyttelse, multifaktorgodkendelse eller lignende implementeres. Og hvis fuld enhedskryptering og muligvis evnen til at fjernsletning af en enhed implementeres, kan det vurderes til at flytte begge ned til en score på 1, hvilket således minimerer den samlede restrisiko til det laveste punkt og klart til et acceptabelt niveau.

Hvilke af disse foranstaltninger der er passende for en given organisation og proportionale med den faktiske risiko, kommer altid an på risikovurderingens datatyper, relevante scenarier etc. - og hver dataansvarlig er i sidste ende ansvarlig for at udføre vurdering og dokumentation af tilstrækkelighed og accept af restrisiko.

Med andre ord vil de identificerede risici altid omfatte scenarier, der involverer den dataansvarlige og deres medarbejdere/processer samt scenarier, der involverer juridisk commitment, teknologi, proces og organisation hos CSP'en. Og foranstaltningerne (eller mere præcist sikkerheds- og privatlivskontrollerne) vil alle falde i en eller flere af de 3 kategorier, der diskuteres i afsnittet "Cloud roles and Shared Responsibilities" ovenfor – og dermed kan de implementeres og administreres af den dataansvarlige, databehandlere eller begge. Hele processen kan opsummeres i illustrationen nedenfor, som i trin 1 - 4 viser, hvordan Microsoft leverer flere lag af sikkerhedsdokumentation for de kontrolelementer, Microsoft administrerer, som input til kundens risikovurdering og dokumentation. I trin 5 evaluerer kunden yderligere "kundeadministrerede" kontrolelementer og kan senere validere resultatet gennem regelmæssige interne eller eksterne revisionsprocesser:

Customer Risk Assessment Process



Eksempler på risikovurdering

Kunder over hele EU udfører disse risikovurderinger efter forskellige modeller, som dog alle netop identificerer et udvalg af risici og passende foranstaltninger (jura, teknologier og processer) som kan minimere Sandsynlighed og/eller Konsekvens for disse risici. Da hver dataansvarlig naturligvis vil indsamle, opbevare og behandle de personoplysninger, de er ansvarlige for, vil det aldrig være muligt 100% at overføre den enkelte risikovurdering til andre scenarier. Microsoft har dog sammen med 3 kunder og KPMG i 2020-2021 udført og anonymiseret risikovurderinger, som kan bruges som inspiration for andre kunder ifm. deres risikovurderinger:

- **Office 365:** https://aka.ms/O365Risikovurderinger
- **Azure:** https://aka.ms/AzureRisikovurdering

Al dokumentation vedrørende kontrollerne og forpligtelserne for Microsoft som CSP i disse eksempler på risikovurderinger kan findes i Q&A-sektionen i dette whitepaper, og som sådan er det beregnet til at blive inkluderet som et værktøj til at levere dokumentation, når du udfører både risikovurderinger og eventuelle konsekvensanalyser.

Microsoft Cloud kontrakter og dokumentation

I processen med at opbygge den nødvendige forståelse og indsigt, som udgør udgangspunktet for at demonstrere regulatorisk compliance, er det vigtigt at kende den overordnede struktur i Microsoft Cloud-aftaler, dokumentation, vejledning og ikke mindst certificeringer og revisionsrapporter. Dette "Assurance Framework" matcher de forskellige lag i den overordnede risikovurderingsproces gennemgået ovenfor og illustrationen nedenfor giver et overblik over elementerne og de overordnede indgange til de relevante elementer online.

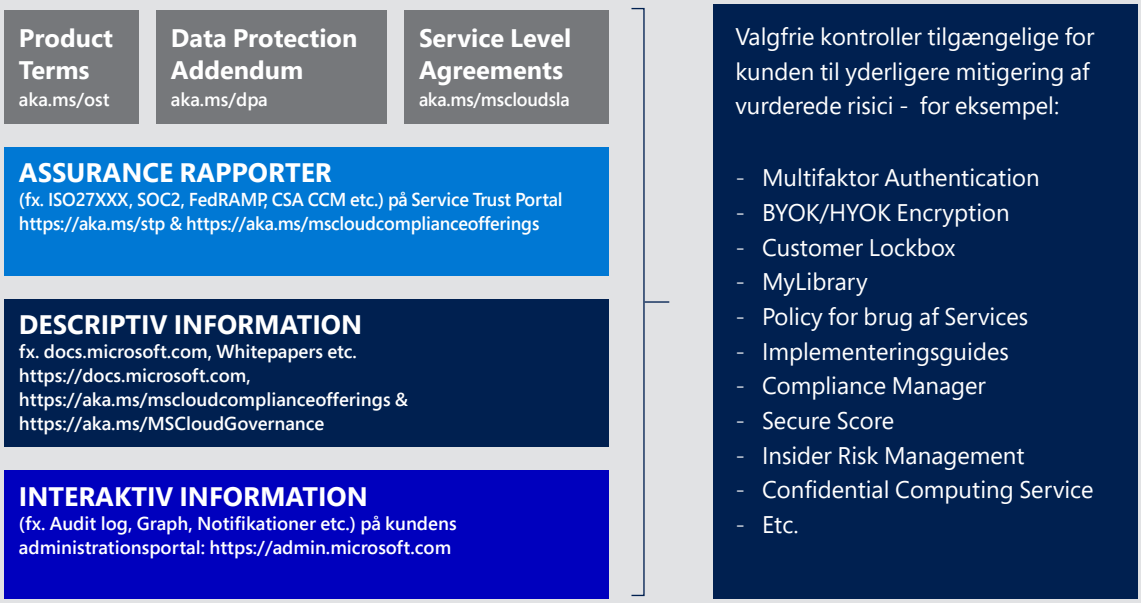


Illustration af "Microsoft Assurance Framework"

1. Det øverste niveau er juridiske aftalegrundlag, hvor bl.a. databehandleraftalen (for Microsoft HSCC kaldet Data Protection Addendum) og SLA'erne er vigtige dele.

2. For at forbinde de vilkår der opstilles i det juridiske aftalegrundlag, til den praktiske implementering og test af hvorledes Microsoft lever op til disse, anvendes det næste lag af 'Assurance rapporter'. Her findes adgang til alle 3. parts revisionsrapporter, certificeringsbeviser, SOA etc..

3. Tredje element udgøres af Microsoft vejledninger og beskrivelser af konkrete funktioner, features, processer o.lign. er tilgængelige. Herunder også en række whitepapers som dette dokument.

4. Endelig har kunden også løbende dokumentation og oplysninger specifikt om deres egen brug af Microsoft Cloud-tjenester, som er tilgængelige via deres administrationsportal for den enkelte ydelse, for eksempel overvågnings-/aktivitetslogfiler, hændelseslogger og diagnostik.

For alle disse fire (4) niveauer af 'Assurance dokumentation', er der yderligere funktioner, tjenester og processer til rådighed for implementering af den enkelte kunde. Disse kan anvendes på baggrund af den generelle risikovurdering af løsningens anvendelse og datastrømme gennem løsningen og kan derfor indgå i en afbødningsplan i forhold til de identificerede risici, beslutter kunden at afbøde. I figuren ovenfor vises flere af de mest almindelige i boksen til højre, og flere beskrives yderligere i dette dokument, når det er relevant for et givet risikodomæne.

Microsoft Online Tjenester – Data definitioner

I det juridiske aftalegrundlag, indgår en række data definitioner, som er væsentlige at kende til og kunne adskille helt klart, især når der foretages risikovurderinger. Nedenfor illustreres hvilke data definitioner der indgår i Microsoft aftalegrundlaget.

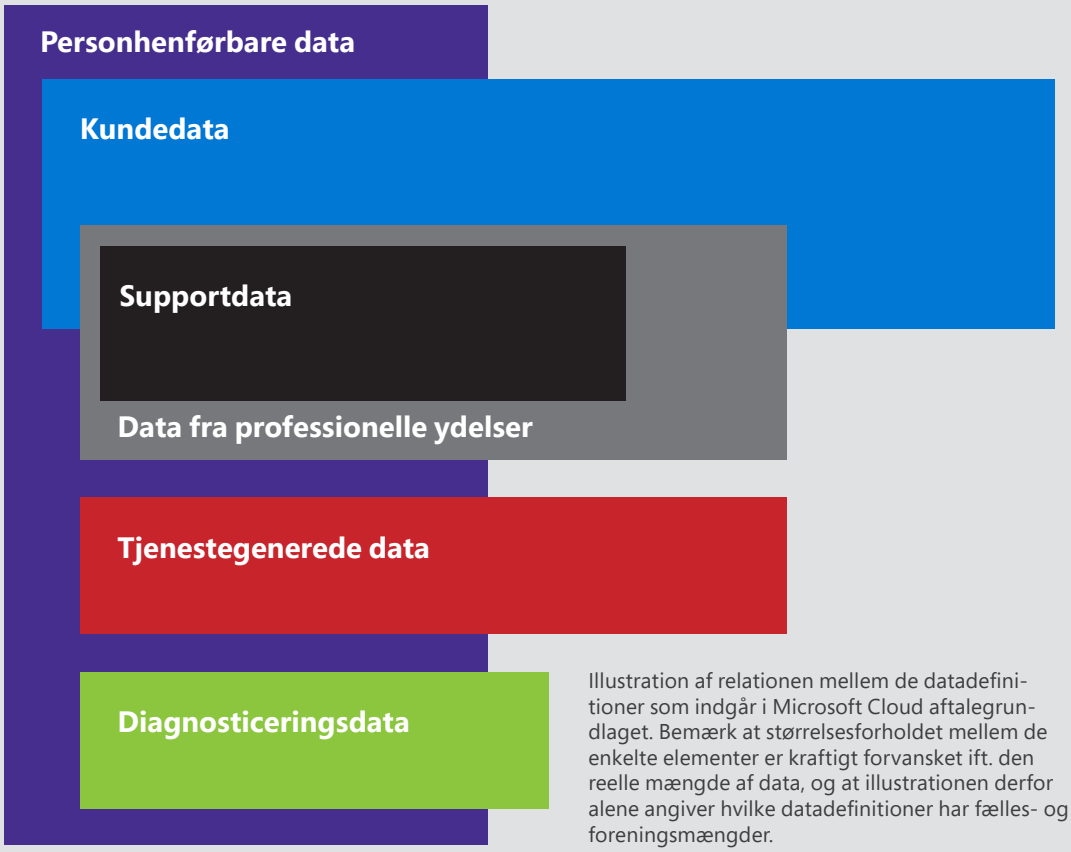


Illustration af relationen mellem de datadefinitioner som indgår i Microsoft Cloud aftalegrundlaget. Bemærk at størrelsesforholdet mellem de enkelte elementer er kraftigt forvansket ift. den reelle mængde af data, og at illustrationen derfor alene angiver hvilke datadefinitioner har fælles- og foreningsmængder.

For nærmere beskrivelse af de enkelte data definitioner, henvises til https://aka.ms/DPA side 4

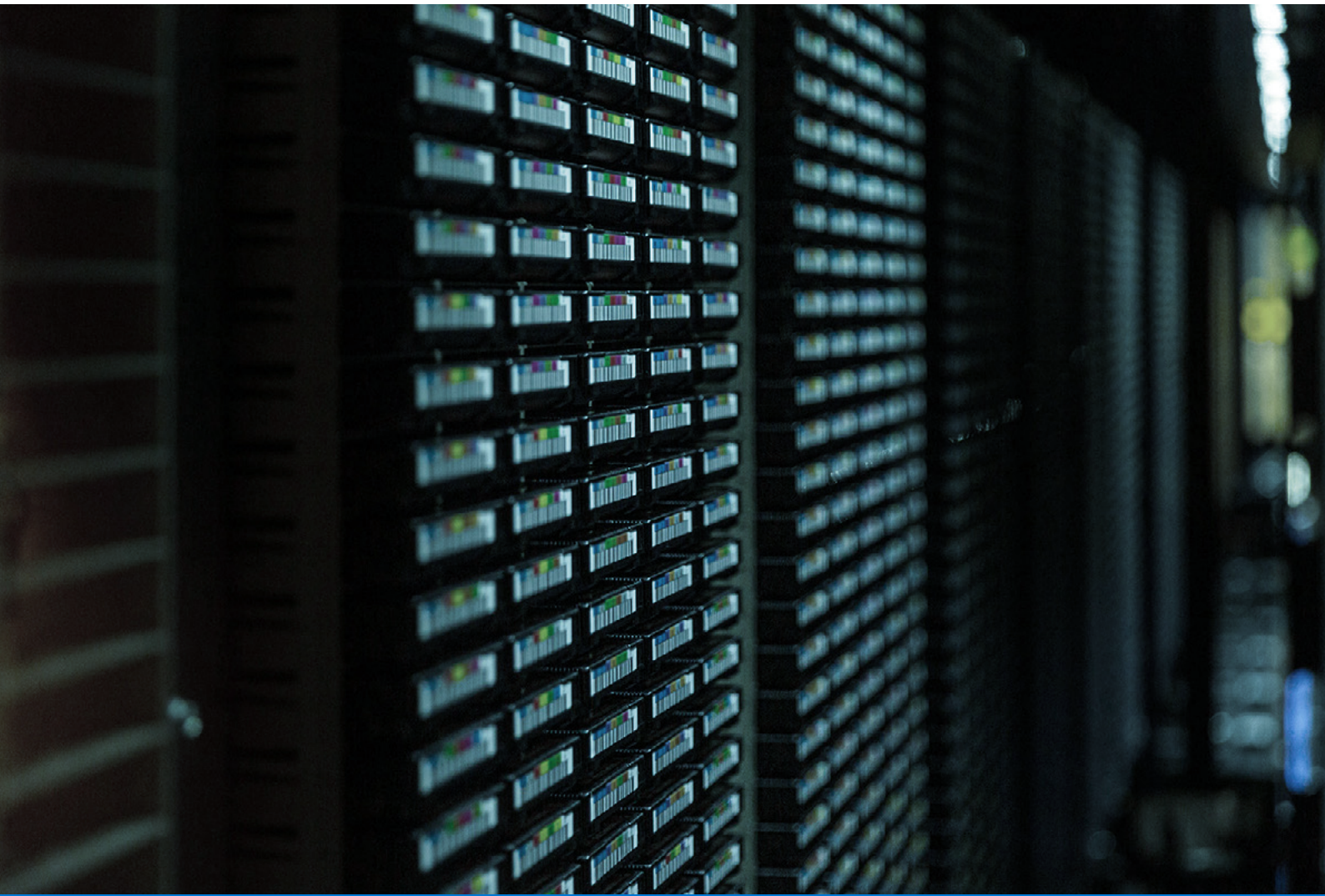
Illustration af relationen mellem de datadefinitioner som indgår i Microsoft Cloud aftalegrundlaget.

Risikovurdering – herunder overførsler til lande uden for EU/EØS

Med det øgede fokus på dataoverførsler fra EU/EØS efter Schrems II-dommen (se afsnittet om juridiske rammer ovenfor) er det også naturligt i dette dokument at give indsigt i, hvilke scenarier der kan føre til overførsel af personoplysninger, når man anvender Microsoft HSCC-platformen, under hvilke omstændigheder og hvilke kontrolmuligheder man som kunde opretholder.

I henhold til Schrems II-dommens tekst skal en række elementer være kernen i enhver vurdering af omstændighederne ved sådanne overførsler: data definitioner, hyppighed/sandsynlighed for overførsler, gennemførte supplerende foranstaltninger, overførselstype etc.

Microsoft er naturligvis dedikeret til at give kunderne et fuldt overblik over disse scenarier, omstændigheder og enhver anden detaljeret dokumentation, der er nødvendig at medtage for vurderinger af dataoverførsler. Disse oplysninger findes i Q&A afsnittet nedenfor, og beskrivelserne vil løbende blive mere detaljerede i de kommende måneder – dette whitepaper indeholder således links til disse beskrivelser, som opdateres over tid.



04 /
Cloud Governance
– bedste praksis

Sætte det hele sammen

Der er generelt flere forskellige trin involveret i en grundig cloud assurance-evaluering. Dette afsnit indeholder en oversigt over den fremgangsmåde, der er beskrevet ovenfor, og som kræver seks væsentlige aktiviteter. Flere detaljer til hvert af trinnene findes i appendix om "Microsoft Cloud Assurance – Proces".

Bemærk, at en organisation i praksis kan medtage flere trin i deres proces baseret på deres specifikke behov og krav. Procesbeskrivelsen i dette dokument har ikke til formål at være fuldstændig udtømmende, men tager udgangspunkt i de aktiviteter, der anses for væsentlige i en risikostyringsproces. Desuden har mange organisationer sandsynligvis allerede implementeret lignende processer og behøver muligvis kun at tilpasse evalueringen til nogle af de specifikke egenskaber ved HSCC.

De vigtigste skridt er ...

01 / Dokumentations- & kravs-indsamling.
02 / Vurdere krav.
03 / Anmod om dokumentation fra cloud-tjenesteudbyder.
04 / Vurder dokumentation og vurder (rest)risiko.
05 / Adressere risiko ved at evt at implementere yderligere/supplerende foranstaltninger/kontroller.
06 / Demonstrere compliance & reevaluere løbende.

Den løbende reevaluering af alle seks trin er nødvendig for at give organisationen mulighed for løbende at forblive compliant og tilbyde den bedst mulige og passende databeskyttelse. Når en af faktorerne ændrer sig (f.eks. en ny potentiel trussel, ændringer i mængden eller følsomheden af de personoplysninger, der indsamles, lagres og/eller behandles osv.), skal processen genstartes – naturligvis ikke fra bunden, men ved at ændre de forandre elementer og reevaluere om kontroller og processer (tekniske og organisatoriske foranstaltninger) imødekommer ændringerne og sikrer fortsat overholdelse og optimal databeskyttelse i forhold til de identificerede risici.

Alt dette fører til etablering af optimal cloud governance i organisationen – en proces som kræver, at en organisation har en struktureret intern tilgang – flere detaljer om dette kan findes i det sidste Q&A-afsnit i dette whitepaper.

Før du går i gang med Q&A-afsnittene i dette whitepaper, hvor de vigtigste emner af interesse i cloud-tjenesteudbyderens dokumentation af tilstrækkelig databeskyttelse findes, afsluttes introduktionen med et kig på en definition af Cloud Governance.

Cloud Governance

Cloud governance definerer, hvordan risici ifm. anvendelse af Cloud Computing håndteres og er væsentlig for alle typer af Cloud Computing (altså ikke alene for HSCC). Grundlæggende handler det om at administrere de tidligere nævnte trin og er af stor betydning for enhver organisations evne til at forblive kompatibel. Det drejer sig med andre ord ikke blot om at vurdere, hvilke sikkerheds-, privatlivs- og overholdelseskontroller og -aktiviteter der er behov for på et bestemt tidspunkt, men også om at etablere den organisation og de processer, der er nødvendige for at gentage trinene, når det er nødvendigt.

Overordnet Governance kan opdeles i to dimensioner:

- Regulatorisk cloud governance
- Cloud governance/Online Service Management.

I begge dimensioner er det vigtigt at inddrage flere discipliner i evalueringen og implementeringen af god cloud governance.

Regulatorisk cloud governance

Regulatorisk cloud governance sikrer, at organisationen har den nødvendige kontrol over brugen af cloud computing:

- I cloud computing opnås og dokumenteres 'at være i kontrol' gennem **forståelse og indsigt**.
- Den **indledende vurdering** af betingelser og certificeringsniveauer vil resultere i en forståelse af, hvilke processer der **løbende skal følges for** at kunne dokumentere, at organisationen har den nødvendige kontrol over brugen af Cloud og de involverede risici.

Cloud governance/Online Service Management

Dette står i kontrast til den regulatoriske cloud governance, og er i princippet en mere IT-relateret opgave. De fleste cloududbydere leverer Cloud Service Management-portaler til deres kunder, gennem hvilke kunden kan håndtere denne opgave, overvåge og vurdere de risici, der er forbundet med den daglige brug af HSCC-tjenesterne.

Nogle kundespecifikke konfigurationer kan vælges af lovgivningsmæssige årsager, andre baseret på virksomhedens egne politikker, men alle har typisk til hensigt at tilføje grader af "hærdning" af løsningen for at imødekomme den ovennævnte risikovurdering udført af kunden / den dataansvarlig.

Cloud-kundens totale kontrol over data og cloud løsningen sker i samspillet mellem regulatorisk cloud governance og Online Service Management. Cloud-kunder bør derfor sikre, at ejerskabet af alle disse processer altid er forankret i deres organisation.

Cloud-egenskaber, der kræver kundens implementering af cloud governance

Uanset om cloud governance behandles ud fra et regulerings- eller Online Service Management perspektiv, er det ofte ikke nok blot at anvende en cloud-udbyders administrationsmetode, da den samme cloududbyder ofte har forskellige betingelser og certificeringsniveauer for unikke cloudtjenester. Derfor bør der også foretages en vurdering baseret på de involverede datatyper, den nuværende teknologi/tjeneste som anvendes og løbende udvikles, efterhånden som en given tjeneste modnes, og dermed potentielt kan ændre compliance-status.

Cloud-udbydere kan ikke indgå unikke/ad hoc-databehandleraftaler med hver HSCC-kunde og har ikke specifik indsigt i, hvordan cloud-tjenesten bruges af kunden, eller hvilke data der behandles inden for tjenesten. Derfor skal HSCC's kunde/dataansvarlige dokumentere deres forståelse af cloud-udbyderens databehandleraftale og implementere de nødvendige processer, der sikrer løbende kontrol.

Det betyder, at regulering af cloud governance normalt ikke kun er én afdelings ansvar, men omfatter processer, der bør inkludere flere enheder i organisationen. IT kan være det daglige forankringspunkt, men bør koordineres nøje med de berørte forretningsområder og den øverste ledelse.

Det er afgørende at kunne adskille kundedata fra de andre typer data, og i hvilke (få og begrænsede) tilfælde, at kundedata er inkluderet i andre datadefinitioner – fællesmængden er ofte ret begrænset, ofte uden personoplysninger og ikke mindst underlagt strenge krav til, hvordan databehandling kan finde sted og på hvilke betingelser. Senere i dette whitepaper vil detaljer om vilkår, betingelser m.v. til databehandling af de enkelte datadefinitioner blive gennemgået i afsnittene 'Q&A'.

Specifik dokumentation for roller i kundens organisation

Den dokumentation, Microsoft tilbyder ifm. 'cloud assurance', er skræddersyet til forskellige roller i kundeorganisationen. Tabellen nedenfor opsummerer de enkelte roller og den tilgængelige dokumentation:

Rolle	Ansvar	Dokumentation
Risiko- og compliance-medarbejdere	Styring af risici og sikring af, at virksomheden overholder eksterne lovkrav og interne politikker.	Specifikke oplysninger, der er målrettet mod denne rolle, kan findes i Microsoft Trust Center. Disse oplysninger vil hjælpe med at dokumentere overholdelse af globale standarder og regler, hvordan datasikkerhed og databehandlings compliance administreres, og hvordan Microsoft hjælper med at beskytte data. *Herunder indsigt i tredjepartsrevisionsrapporterne*. Se https://aka.ms/mscloudcompliance
Sikkerheds-ansvarlige og arkitekter	Teknisk udformning af sikkerhedskontrollen	For sikkerhedsansvarlige og arkitekter er indhold også tilgængeligt i Microsoft Trust Center https://aka.ms/mscloudcompliance Desuden oprettes såkaldte 'control companions' på Service Trust Platform for at finde funktioner, der knytter sig til specifikke sikkerheds- og compliancekontroller ved hjælp af standarder som ISO og FEDRAMP. Endelig tilbyder Microsoft Learning portal https://learn.microsoft.com tilbyder mange gratis online kurser med henblik på at opkvalificere disse roller om relevante emner, såsom: - Få mere at vide om, hvordan Microsoft beskytter kundedata: https://docs.microsoft.com/en-us/learn/paths/audit-safeguard-customer-data/ - Administrere identitet og adgang i Azure Active Directory: https://docs.microsoft.com/en-us/learn/paths/manage-identity-and-access/ - Administrere sikkerhedshandlinger i Azure: https://docs.microsoft.com/en-us/learn/paths/manage-security-operations/ - Og mange flere

Rolle	Ansvar	Dokumentation
Privacy Officers / Ansvarlige for beskyttelse af personlige oplysninger	Håndtering af risici og forretningsmæssige konsekvenser af love og politikker om beskyttelse af personlige oplysninger.	I forbindelse med denne rolle indeholder Microsoft Trust Center også separate sektioner, som giver et godt udgangspunkt for at hjælpe med at forstå, hvordan Microsoft implementerer og vedligeholder beskyttelse af dine data, og de politikker – herunder politikker vedrørende dataopbevaring, suverænitet og adgangskontrol – der understøtter beskyttelsen af personlige oplysninger i Microsofts Online Tjenester: https://aka.ms/mscloudprivacy. På samme måde er flere relevante ressourcer[32] også tilgængelige på Service Trust Portalen.[33] For eksempel er der adgang til ISO 27001- og 27018-revisionsrapporter, for gennemgang og vurdering af Microsoft Cloud Governance og praksis for beskyttelse af personlige oplysninger samt en række GDPR Controls Mapping-dokumenter tilgængelige for kundens Privacy Officers evaluering. Endelig tilbyder Microsoft Learning portal https://learn.microsoft.com mange gratis online kurser med henblik på opkvalificering om relevante emner også for denne rolle, såsom: - Forstå Microsoft 365 Privacy: https://docs.microsoft.com/en-us/learn/modules/audit-privacy/ - Introduktion til databeskyttelses- og privatlivsbestemmelser: https://docs.microsoft.com/en-us/learn/modules/intro-to-data-protection-privacy/ - Undersøg standarder for beskyttelse af personlige oplysninger, overholdelse af angivne standarder og databeskyttelse på Azure: https://docs.microsoft.com/en-us/learn/modules/examine-privacy-compliance-data-protection-standards/ - Og mange flere

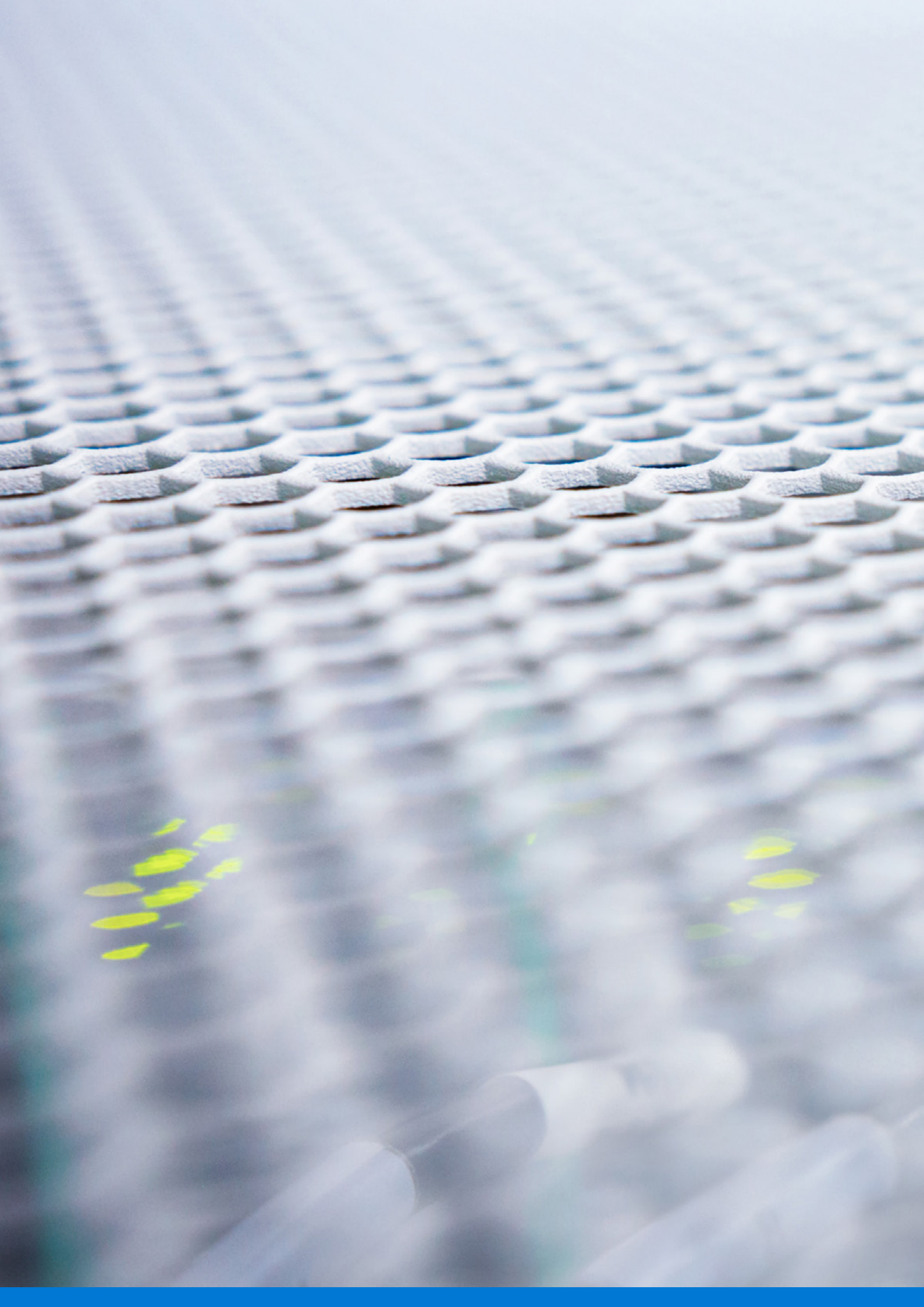
32 https://www.microsoft.com/en-us/trust-center/privacy/resources
33 https://aka.ms/STP

Rolle	Ansvar	Dokumentation
Legal Officer	Håndtering af juridiske risici ved at rådgive virksomhedens andre medarbejdere om eventuelle større juridiske og lovgivningsmæssige spørgsmål.	Hyppigst anvendte lovbestemmelser: - Online Produktvilkår[34] - Microsoft Online Services – Data Protection Addendum (databehandleraftale)[35] - Service Level aftaler[36]

Disciplinen data governance

... er en specifik delopgave under cloud governance og er uden for dette whitepapers anvendelsesområde, men behandles i stedet mere detaljeret i dette separate whitepaper: https://aka.ms/msdatagovernance

34 https://aka.ms/ost
35 https://aka.ms/dpa
36 https://aka.ms/mscloudsla



05 /

Gode spørgsmål til cloud-udbyderen

I forbindelse med vurdering af en given cloud computing-platform eller -service, som en organisation overvejer at tage i anvendelse, kan en lang række spørgsmål med fordel stilles til leverandøren. Det er reelt ikke muligt at udtømme listen over mulige spørgsmål, men nedenstående er de hyppigst forekommende og alle yderst relevante.

Er man bekendt med Cloud Security Alliance[1] Cloud Controls Matrix[2], vil man kunne genkende de bærende grupperinger af spørgsmålene, men en række spørgsmål er af mere generisk karakter og tilføjes derfor i en afsluttende 'Diverse'-gruppe.

1 https://cloudsecurityalliance.org/
2 https://cloudsecurityalliance.org/research/working-groups/cloud-controls-matrix

Revisionssikring og compliance

Definition og dokumentation på Microsoft Cloud

Q&A

1 Data-ejerskab; er der en tydelig definition og aftale ift. kundens ejerskab af egne data?

I Microsoft Online Services Data Protection Addendum (DPA)[3] defineres dette på side 6 i "Databehandlingens art; ejerskab" som: *"Microsoft vil kun bruge og på anden vis behandle Kundedata og Personoplysninger i overensstemmelse med Kundens dokumenterede instruktion og som beskrevet i og i henhold til de begrænsninger, der er angivet herunder (a) for at levere Onlinetjenester til Kunden og (b) i forbindelse med Microsofts legitime forretningsaktiviteter vedrørende levering af Onlinetjenesterne til Kunden. Som mellem parterne, beholder Kunden alle rettigheder, ejendomsret og interesse i og til Kundedata. Microsoft erhverver ingen rettigheder til Kundedata, bortset fra de rettigheder, som Kunden tildeler Microsoft i dette afsnit."*

Efterlevelsen af denne politik dokumenteres af Microsofts adoption af den internationale standard "ISO/IEC 27018 Code of Practice for Protecting Personal Data in the Cloud" – flere detaljer her: https://aka.ms/msiso27018 og her: https://aka.ms/mscloudprivacystandards

Bemærk, at Microsoft også var en af de første Cloud-tjenesteudbydere, der er blevet certificeret mod ISO/IEC27701, "Privacy Information Management System", der ligner mange af kravene fra GDPR: https://aka.ms/msiso27701. Og at den 20. maj, 2021 kunne Microsoft annoncere at Microsoft i sin drift af Online Services til fulde efterlever den nye EU Cloud Code of Conduct[4].

I afsnittet "**Behandling i forbindelse med Microsofts legitime forretningsaktiviteter**" (LBO) på side 7 i DPA, defineres en række scenarier, hvor Microsoft på grundlag af GDPR-artikel 6 f har et lovligt behandlingsgrundlag og påtager sig de yderligere ansvarsområder, som en dataansvarlig har, i forbindelse med at levere onlinetjenesterne. I afsnittet defineres scenarierne som *"... består "Microsofts legitime forretningsaktiviteter" af følgende, der hver især medfølger ved levering af Onlinetjenesterne til Kunden: (1) fakturering og kontoadministration; (2) aflønning (f.eks. beregning af medarbejderprovision og partnerincitamenter); (3) intern rapportering og forretningsmodellering (f.eks. udarbejdelse af prognoser, omsætning, kapacitetsplanlægning, produktstrategi); (4) bekæmpelse af svindel, internetkriminalitet eller internetangreb, der kan påvirke Microsoft eller Microsofts Produkter; (5) forbedring af kernefunktionaliteten i forhold til tilgængelighed, beskyttelse af Personoplysninger eller energioptimering og (6) økonomisk rapportering og overholdelse af juridiske forpligtelser (i henhold til begrænsningerne for videregivelse af Personoplysninger, der gennemgås herunder).*

Microsoft vil ikke bruge eller på anden vis behandle Kundedata eller Personoplysninger ved behandling

3 https://aka.ms/dpa
4 https://aka.ms/AzureEUCloudCoC

i forbindelse med "Microsofts legitime forretningsaktiviteter", når det gælder: (a) brugerprofilering, (b) annoncering eller lignende kommercielle formål eller (c) alle andre formål på nær i forbindelse med de formål, der er angivet i dette afsnit."

DPA sætter klare begrænsninger for, til hvilket formål LBO-data kan behandles, og er også underlagt alle databeskyttelsesbetingelser, der er fastsat i DPA (herunder Microsoft Security-politikkerne (Appendiks A), GDPR-vilkår (tillæg 3) og EU's SCC (tillæg 2), herunder appendix 3 til EU SCC kaldet "*Additional Safeguards Addendum*").

Det er også vigtigt at forstå, at Microsoft kun behandler data for LBO-data i forbindelse med leverancen af de tjenester, som kunden har indgået kontrakt med Microsoft. Det betyder, at Microsoft ikke opnår adgang til nogle kunde- eller personlige data til LBO'er for tjenester, som kunden ikke udtrykkeligt har indgået kontrakt med Microsoft.

Alle data, som Microsoft behandler for LBO indsamles eller genereres alene baseret på Microsofts rolle som databehandler. Desuden minimeres LBO-dataene (som krævet i GDPR), pseudonymiseres og behandles overvejende kun på et aggregeret niveau. Det er ikke muligt for dette whitepaper at gennemgå alle LBO-scenarierne (hvis det er nødvendigt, kan kunderne kontakte Microsoft for yderligere oplysninger), men til illustration, er her inkluderet to eksempler:

- **Kundefakturering**; Microsoft fakturerer for online tjenester baseret på brug. Microsoft skal bruge data, der er genereret eller modtaget, mens onlinetjenesterne faktureres nøjagtigt. For nøjagtig fakturering af online tjenester "pr. bruger" har Microsoft behov for at kunne tælle det unikke antal brugere. Data som disse er pseudonymiserede og brugeridentiteten er ikke tilgængelig (irrelevant) for de systemer/handlinger, der behandler data.

- **Microsoft Intern rapportering og forretningsmodellering**; Microsoft bruger aggregerede data til intern rapportering og forretningsmodellering til formål som prognoser, kapacitets- og forretningsplanlægning og produktstrategi. Hvis Microsoft f.eks. frigiver en ny funktion, kan Microsoft bruge aggregerede brugsdata til at afgøre, om kunderne bruger funktionen og får værdi ud af den. Det kan igen hjælpe Microsoft med at investere i forbedring af funktioner for at gøre dem mere nyttige. Data som disse aggregeres baseret på pseudonymiserede brugsdata, uden adgang til at se enkeltpersoners brug (eller mulighed for at identificere enkeltpersoner fra pseudonymiserede identifikatorer) eller adgang til indholdet af kundedata, herunder personoplysninger i kundedata.

Q&A **2** **Datalokation; fremgår det til enhver tid, hvor kundens data opbevares og hvor leverandørens datacentre befinder sig?**

I juridiske spørgsmål vedrørende levering af online tjenester og dataplaceringer er det vigtigt at understrege, at Microsoft kontraktligt forpligter sig til at overholde alle relevante regler. I de tilfælde, hvor dette vedrører databeskyttelseslovgivningen, gjorde Microsoft dette meget eksplicit i den seneste version af databehandleraftalen (DPA): "*Microsoft overholder alle love og reguleringer, der er gældende for leveringen af Onlinetjenesterne, herunder lov om information vedrørende sikkerhedsbrud og Krav til databeskyttelse ...)*" og "*(...) Microsoft er underlagt kravene i databeskyttelseslovgivningen i det Europæiske Økonomiske Samarbejdsområde og Schweiz vedrørende indhentning, brug, overdragelse, opbevaring og andre former for behandling af Personlige data fra det Europæiske Økonomiske Samarbejdsområde, Storbritannien og Schweiz. Alle overførsler af Personoplysninger til et tredjeland eller en international organisation underlægges passende beskyttelsesforanstaltninger som beskrevet i Artikel 46 i GDPR, og sådanne overførsler og beskyttelsesforanstaltninger skal dokumenteres i henhold til Artikel 30(2) i GDPR. (...)*".

Selvom Microsoft udtrykkeligt giver kontraktlige forpligtelser over for kundedata i hvile, gælder Microsofts generelle kontraktlige forpligtelser over for personoplysninger på tværs af kundedata, diagnosticeringsdata, servicegenererede data og professionelle tjenester for enhver form for behandling. Afsnittet "Dataoverførsler og -placering" i DPA, side 10, beskriver dette. Yderligere - og mere

specifikke - kontraktlige forpligtelser vedrørende dataopbevaring er specificeret her: https://aka.ms/OnlineServicesPrivacySecurityTerms

Kunden kan konfigurere deres brug af Microsoft-skytjenester til kun at gemme data inden for EU. I alt tilbydes der i sin nuværende form mere end 60 regioner, herunder mange inden for EU/EØS. Du kan finde en komplet oversigt over placeringen af Microsoft HSCC Data Centre på disse interaktive kort: https://aka.ms/azuredataresidency, for Office 365 her: https://aka.ms/o365dataresidency og for Dynamics365 her: https://aka.ms/D365dataresidency.

De fleste af de tilgængelige cloudtjenester tilbyder dataplacering inden for EU, og kunden kan kontrollere tilgængeligheden af en given tjeneste her: https://aka.ms/mscloudregions og for Office 365 Services her: https://aka.ms/mso365datalokation.
Denne webside indeholder desuden specifikke oplysninger om dataopbevaring for M365 inden for EU: https://aka.ms/M365EUDatalocations. Microsoft 365-kunder kan også validere dataplaceringer via deres Microsoft 365 Administrationsportal ved at navigere til Settings | Org settings | Organization Profile | Data Location.

For Microsoft Azure vises en liste over alle tjenester, der tilbydes ud af EU-regionerne, her: https://aka.ms/mscloudEUregions og forpligtelserne til dataopbevaring kan findes her: https://aka.ms/AZUREDatalocations.

Yderligere oplysninger om **dataopbevaring** kan findes i følgende whitepapers:

- Microsoft Azure: *h*ttps://aka.ms/AzuredataresidencyWP
- *Microsoft Dynamics:* https://aka.ms/d365dataresidencyWP

Nogle "**ikke-regionale tjenester**" tilbydes efter design og funktion uden forpligtelse til dataopbevaring inden for den valgte geo – som beskrevet i whitepaperet "Azure data residency" ovenfor. Kunderne med specifik interesse i Azure Active Directory Service (AAD), som er afgørende for mange onlinetjenesters løsninger – kan finde en beskrivelse af Microsofts forpligtelser vedrørende dataplacering for denne tjeneste her: https://aka.ms/msaaddatalocation. Kunderne bør også være opmærksomme på arten af data i AAD, som er dokumenteret her: https://aka.ms/aadattributessync.

For nogle online tjenester henviser Microsoft til eller "inkluderer" dele af Microsoft Trust Center for yderligere oplysninger om dataopbevaring pr. tjeneste. Da Microsoft Online Services består af flere specifikke tjenester, og nye (under)tjenester kan tilføjes over tid, bruger Microsoft denne mekanisme til at henvise til trust center for up-to-date oplysninger om faktiske dataplaceringer. Det er vigtigt at bemærke her, at selv om Microsoft kan ændre indholdet af disse websider fra tid til anden, så committer online tjenesternes privacy & security vilkår (se https://aka.ms/OnlineServicesPrivacySecurityTerms) udtrykkeligt, at: "(...) Microsoft will not add exceptions for existing Services in general release (...)" og DPA tilføjer desuden: "(...) Når Kunden fornyr eller køber et nyt abonnement på en Onlinetjeneste, gælder de på tidspunktet gældende Vilkår for "Tillæg om databeskyttelse", og den ændres ikke under Kundens abonnement på Onlinetjenesten (...) "

Yderligere **kundeadministrerede kontrolelementer** er tilgængelige med relevans for dataplacering:

- Ved hjælp af **"Azure-politikker"**[5] kan **kunden** definere sine egne politikker for f.eks. overholdelse og generelle sikkerhedsindstillinger. På denne måde kan de minimumskrav, der skal opfyldes i forbindelse med implementering og brug af en tjeneste, defineres – f.eks. datalagringsplacering, antal privilegerede konti, firewallindstillinger osv.
- "**Azure** Blueprints" gør det også muligt for kunden fx. at blive sikret mod idriftsættelse af tjenester, der ikke tilbydes med datalagring i det valgte område[6].
- Den organisatoriske kontrol "Customer **Lockbox"** sikrer at kunden skal give den endelig godkendelse[7] af scenarier som potentielt kan eksponere kundedata for en Microsoft drifts eller support medarbejder – scenarier som i sjældne kan medføre overførsel til tredjelande udenfor EU/EØS i form af "fjernadgang". I dette tilfælde anbefaler Microsoft, at kunden foretager en risikovurdering

5 https://aka.ms/azurepolicies
6 https://aka.ms/azureblueprints
7 https://aka.ms/msazurelockbox

for hver enkelt request/hændelse og medtager effekten på alle Service Level Agreements. Selvom sådanne tilfælde er yderst sjældne, skal dette gøres, for fuldstændigt at kontrollere (stoppe eller udsætte) udførelsen af opgaven baseret på "fjernadgang" med potentiel adgang til Kundedata.

- Flere detaljer og kundeadministrerede kontrolelementer er tilgængelige i spørgsmål 48 & 51 senere i dette afsnit.

Dataoverførsels-scenarier og -vurderinger:
Schrems II-dommen (se afsnittet ovenfor om "Juridiske rammer for cloud computing") har givet anledning til yderligere at vurdere det lovlige grundlag for dataoverførsler, de risici, der er forbundet med dataoverførselsscenarier, og de "supplerende foranstaltninger", der er implementeret for at minimere sådanne risici. EDPB har udarbejdet en "Sekstrinsvejledning" om, hvordan man griber dette ind (se bilag C for at få yderligere oplysninger eller find en oversigt her: https://aka.ms/EDPB6Steps).

Nedenstående tabel er et eksempel på, hvordan en sådan vurdering kunne udføres i fald man anvender Microsoft Azure Services.**Data transfer scenarios and assessments**:

STEP	VURDERING
Overførsels scenarie	Microsoft initierede operationelle vedligeholdelse og fejlfindingsopgaver. **Omstændigheder/arten af overførslen**: Fjernadgang med rettigheder, der potentielt kan udsætte kundedata for vedligeholdelses- og fejlfindingstekniker. **Hyppighed/sandsynlighed:** Langt de fleste operationelle opgaver automatiseres, uden at der finder overførsler sted. Af og til kan vigtige opgaver ikke automatiseres, og kræver derfor at en driftstekniker engageres – langt de fleste af sådanne scenarier kræver ikke rettigheder med adgang til kundedata og en endnu mindre delmængde af disse sjældne tilfælde, hvor sådanne rettigheder er påkrævet, kan så inkludere fjernadgang fra lande uden for EU/EØS. **Lande, hvorfra fjernadgang i sjældne scenarier kan forekomme**: USA, Australien, Japan, Canada, Indien, Irland, Israel, Tjekkiet, Tyskland, Serbien, Holland & U.K. **Formålet med behandlingen/overdragelsen**: Som defineret på side 6 i DPA er behandlingsformålet med en onlinetjeneste "... at levere kunden onlinetjenesterne", som består af: Levering af funktionsmuligheder som licenseret, konfigureret og anvendt af Kunden og dennes brugere, herunder levering af tilpassede brugeroplevelser. Fejlfinding (forhindre, konstatere og afhjælpe problemer) og Løbende forbedring (installation af de seneste opdateringer og forbedring af brugerproduktivitet, driftssikkerhed, effektivitet og sikkerhed). Microsoft vil ikke bruge eller på anden vis behandle Kundedata eller Personoplysninger ved levering af Onlinetjenester i forbindelse med: (a) brugerprofilering, (b) annoncering eller lignende kommercielle formål eller (c) markedsundersøgelse, 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.
Transfer tool (juridisk ramme for regulering af vilkår for overførsel)	Alle potentielle dataoverførsler, der kan forekomme i Microsoft HSCC Online Services, er underlagt EU's standardkontraktbestemmelser som defineret i DPA – i overensstemmelse med GDPR, artikel 46 .

STEP	VURDERING
Effektiviteten af Transfer tool	I henhold til Schrems II-dommen anses EU's SCC for ikke at være effektiv nok specifikt i tilfælde af dataoverførsler til/fjernadgang fra USA, og lande, som EU-Kommissionen ikke anså for sikre tredje lande. Passende supplerende foranstaltninger anses derfor for nødvendige i tilfælde af sådanne overførsler/ fjernadgang og vil blive overvejet nedenfor.
Kan der træffes supplerende foranstaltninger	Ja – både af dataansvarlig/eksportør og databehandler/importør.
Passende supplerende foranstaltninger	**Af Microsoft som databehandler:** Ud over de kontrolelementer, der er defineret i databehandleraftalen (Microsoft-sikkerhedspolitikker (appendiks A), GDPR-termer (tillæg 3) og EU SCC (tillæg 2) inklusiv appendix 3 "Additional Safeguards Addendum")), for operationelle opgaver er følgende kontrolelementer på plads: - Produktionsadgang er begrænset til isolerede identiteter og stærkt kontrollerede arbejdsstationer. - Adgang, der er tildelt på basis af rollebaseret adgangskontrol. - Der kræves godkendelse med Multiple faktorer. - Just-In-Time "JIT" sikrer, at forhøjet adgang er midlertidig og 'least-privilege'. - Adgangsanmodninger, der revideres, logføres, overvåges og der udstedes automatisk advarsler om risikofyldte tildelinger af privilegier. - Overvågning 24x7x365 via Microsoft Cyber Defense Operations Center. - Alle data krypteres i hvile og i transit. I henhold til DPA, Microsoft *"(...)vil ikke levere følgende til tredjemand: (a) direkte, indirekte eller fri adgang til Behandlede data, (b) platformskrypteringsnøgler til beskyttelse af Behandlede data eller mulighed for at bryde en sådan kryptering eller (c) adgang til Behandlede data, hvis Microsoft ved, at dataene skal bruges til andre formål end angivet i anmodningen fra tredjemand"*. **Af Microsoft som 'EU SCC Importer:** Microsoft Corporation har en mangeårig forpligtelse til databeskyttelse og privacy: https://aka.ms/MSCloudPrivacy. Microsoft har gennem mange år været en stærk fortaler for og kæmpet juridiske kampe for at sikre kunderne ret til deres egne data og ret til gennemsigtighed om juridiske anmodninger om dataadgang (f.eks.: https://aka.ms/MSSecrecyOrders). Efter Schrems II-dommen meddelte Microsoft yderligere tilsagn om at 'Defend Customer Data' (https://aka.ms/MSdyd) og har efterfølgende føjet disse forpligtelser til databehandleraftalen. Importørens proces og historik i forbindelse med håndtering af 3.partsanmodninger om kundedata er tilgængelig på https://aka.ms/MSLERH og https://aka.ms/MSLERR - på grundlag af disse rapporter kan det vurderes, at disse supplerende foranstaltninger fra importørens område effektivt begrænser sandsynligheden for, at adgang til kundedata ved hjælp af Microsoft Azure Services er "tæt på nul" /'på et acceptabelt lavt niveau". **Af den dataansvarlige/'EU SCC exporter:** - Azure Customer Lockbox Service. Før der tildeles rettigheder, der giver potentiel adgang til kundedata, skal en dertil af kunden udpeget entitet godkende tildeling. Flere oplysninger på https://aka.ms/msazurelockbox - Azure Policy Service. Effektiv begrænsning af tilgængeligheden af onlinetjenester til dem, der tilbyder f.eks. dataopbevaring inden for EU's geografi. - Azure monitoring service. Loganalyse og meddelelse om dataadgang.

STEP	VURDERING
Reevaluere	Der er indført en governance struktur og teknologier til støtte for at reevaluere alle ovennævnte elementer, herunder, men ikke begrænset til: - Automatisk meddelelse om ændringer af dokumentation, overvågning, certificering og aftaler ved hjælp af funktionen MyLibrary på Microsoft Services Trust Portal. - Azure Customer Lockbox, for at tillade vurdering fra sag til sag af dataoverførselsscenarier under vedligeholdelses-, fejlfindings- og supportforekomster. - Azure Policy Service på for online service abonnement for at sikre politikdrevet konfiguration og tilgængelighed for kun relevante tjenester. - Monitoring af Customer Audit logs. - Det bemærkes iøvrigt at Microsoft i Maj 2021 annoncerede projektet EU Data Boundary (https://aka.ms/MSEUDataBoundary) og dermed forventes det, at senest pr. 1. januar, 2023 vil alle ovenstående overførselsscenarier være elimineret.

For flere detaljer om "tredjepartsanmodninger om dataadgang", se spørgsmål#35.

Answering Europe's Call: Storing and Processing EU Data in the EU

On May 6th, 2021, Microsoft President and Chief Legal Officer Brad Smith announced8 the initiative **EU Data Boundary for the Microsoft Cloud**, which will go beyond the existing data storage commitments Microsoft is giving. This will enable customers to both process and store all your data in the European Union (or in Norway or Switzerland, Member States of the European Free Trade Association where we have datacenters). This commitment will apply across Microsoft's main cloud services—Azure, Microsoft 365, and Dynamics 365. Microsoft have already begun the engineering work necessary to implement this new initiative and will complete that by the end of the year 2022. With this new pledge, Microsoft will be the only hyperscale cloud provider to offer this level of data residency in the region.

We would like to call your attention to three important points:

- Today, Microsoft cloud services already comply with or exceed the requirements of EU data protection laws. We were the first major technology company to affirm our compliance with the GDPR. More recently, we responded to the *Schrems II* decision with our Defending Your Data[9] initiative.
- Microsoft already provide commercial and public sector customers the choice to have data stored in the EU, and many of our cloud services can already be configured to process data in the EU[10] as detailed elsewhere in this whitepaper. Nonetheless Microsoft recognize that some cloud customers want even greater data residency commitments and more transparency and are with this initiative responding to those needs.
- Microsoft will build these EU Data Boundary solutions into the core cloud services to enhance the current offerings for customers and, where needed, will reflect that in standard contract terms in the future.

Building upon an already strong portfolio of solutions and commitments to protect customer data, Microsoft are taking this additional step to support the success of our European customers and as part of our commitment to Europe more generally. Our EU Data Boundary for the Microsoft Cloud will be powered by the already substantial and planned investments in an expansive European datacenter infrastructure spanning 13 European countries. These datacenters power cloud services that help European customers realize their ambitions to achieve digital transformation and increase their competitiveness with the assurance that they can operate in compliance with all applicable laws and regulations.

8 https://aka.ms/MSEUDataBoundary
9 https://aka.ms/MSDyD
10 https://azure.microsoft.com/en-us/global-infrastructure/data-residency/

Beyond that, as the EU pursues its vision for a "Europe Fit for the Digital Age," Microsoft recognize and enthusiastically embrace our responsibility to build what we call "Tech Fit 4 Europe"[11]. Microsoft believe that "EU Data Boundary for the Microsoft Cloud" is an important additional step in that direction, and we will continue to consult with customers and regulators about this plan and move forward in a way that responds to that feedback.

In the fall of 2021 Microsoft will conduct an EU Cloud Customer Summit to share more about this work.

All information provided in the paper you are reading now, is describing the setup and operations as they exist today. Over the months from the announcement on May 6th, 2021, until the end of 2022, the "EU Data Boundary" initiative, will migrate Microsoft internal systems (for processing of Legitimate Business Operations – see a description of these in the introduction to this paper), Microsoft engineering, troubleshooting, maintenance, and support organization, to enable full EU/EEA data processing.

The detailed plans are yet to be confirmed as they are being formed based on e.g., collaboration with and feedback from EU/EEA customers and authorities. While the changes will most likely not affect the day-to-day delivery or operations of customers solutions, all customers with subscriptions in EU/EEA will benefit from the initiative, as plans are executed throughout the months until completion by the end of 2022.

Microsoft recommend performing the assessments today, based on the detailed information as provided by this paper, and making a note about the expected coming changes to the data transfer scenarios as the EU Data Boundary initiative is executed.

11 https://aka.ms/MSTechFit4Europe

Q&A

3 Hvordan håndteres ændringer i sikkerheds-, privacy og compliance-dokumentation, liste med underleverandører, generelle vilkår, etc.?

Overordnet er vilkår mm. defineret i aftalegrundlaget (primært DPA og OST) og al dokumentation publiceres desuden på Microsoft Services Trust Portal12, og kunden kan via funktionen MyLibrary udvælge specifikke dokumenter, certifikater, audit-rapporter etc., som kunden ønsker ændringsnotifikation om: https://aka.ms/MScloudMyLibrary

Q&A

4 Har kunden adgang til at foretage egne inspektioner ledet af kunden eller en af kunden bemyndiget revisor?

Ja.

Baseret på udtalelser fra det Danske Datatilsyn[13] og det Europæiske Article 29 Data Protection Working Party[14] (nu EDPB), henvises kunden som udgangspunkt til at foretage sin inspektion gennem adgang til Microsoft Audit Reports, som er tilgængelige via Microsoft Services Trust Portal[8]

I DPA[3] defineres implementeringen i afsnittet '*Overholdelse af kontrol*' på side 9.

Her specificeres ydermere hvorledes og under hvilke forudsætninger kunden kan gennemføre en særlig 3. parts revision.

Q&A

5 I hvilket omfang og hvordan har kunden adgang til log og revisionsrapporter?

Enhver kunde i Microsoft Cloud har adgang til dokumentation på Service Trust Portal[8]
Kunden kan via funktionen MyLibrary udvælge specifikke dokumenter, certifikater, audit-rapporter etc., kunden ønsker ændringsnotifikation om: https://aka.ms/MScloudMyLibrary

I DPA[3] beskrives adgangen i afsnittet *'Overholdelse af kontrol'*

Q&A

6 Hvorledes sikres logs - og hvor ofte, samt hvordan, gennemgås de for at sikre mod uopdagede sikkerhedshændelser?

Microsoft leverer monitorerings- og logteknologier for at give kunder maksimal gennemsigtighed i aktiviteten på deres cloudbaserede netværk, applikationer og enheder, så kunder kan identificere potentielle sikkerhedshuller. Onlinetjenesterne indeholder funktioner, der gør det muligt for kunderne at begrænse og overvåge deres medarbejderes adgang til tjenesterne, herunder Azure AD Privileged Identification Management system og multi-faktor-autentificering.

Derudover omfatter onlinetjenesterne indbyggede, godkendte Windows PowerShell-scripts, som minimerer adgangsrettighederne og dermed muligheden for fejlkonfiguration.

12 https://aka.ms/stp
13 https://aka.ms/dpao365decision
14 Cloud leverandørs brug af uafhængig tredjepart til inspektion / audit af Cloud tjenester (4.2 Third Party Data Protection Certification) https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf

Microsoft giver kunderne mulighed for at logge adgang til og brug af informationssystemer, der indeholder kundedata, registrering af adgangsID, tidspunkt, tilladelse, der er givet eller nægtet, og andre relevante aktiviteter.

Et internt, uafhængigt Microsoft-team overvåger logs mindst en gang i kvartalet, og kunderne har adgang til disse overvågningslogfiler.

Derudover gennemgår Microsoft jævnligt adgangsniveauer for at sikre, at kun brugere med passende berettigelse har adgang.

Q&A

7 Er leverandøren tydeligt forpligtet til at efterleve regulering/lovgivning om databeskyttelse?

Ja.

DPA[3] definerer i afsnittet "*Overholdelse af lovgivning*" på side 6 at: "*Microsoft overholder alle love og reguleringer, der er gældende for leveringen af Onlinetjenesterne, herunder lov om information vedrørende sikkerhedsbrud og Krav til databeskyttelse.*"

I samme DPA i afsnittet " Behandling af Personoplysninger, GDPR" på side 7-8 beskrives Microsofts særlige GDPR-forpligtelser som databehandler, specifikt Artikel 28, 32 og 33, herunder f.eks. definitionen af roller og ansvar for både den dataansvarlige og databehandleren og "Rettigheder i forhold til registrerede" som fx. "hjælp til anmodninger" og Microsofts rolle med hensyn til at bistå de dataansvarlige med at håndtere disse. Ligesom den fulde tekst fra GDPR af relevans for Microsoft som databehandler, indgår som "*Tillæg 3 – Vilkår i EU's Databeskyttelsesforordning*".

Microsoft har desuden gentagne gange officielt givet fuldt commitment[15] til at efterleve fx GDPR og assistere Microsofts kunder med at leve op til deres ansvar for databeskyttelse.

Ydermere er det defineret i samme afsnit, at Microsoft for visse datatyper (ikke kundedata) er en uafhængig dataansvarlig under GDPR og derfor for disse data har ansvaret for beskyttelsen.

Q&A

8 Overholder databehandleraftalen de nødvendige minimumskrav?

Ja.

For at hjælpe kunder med at matche fx det Danske Datatilsyns forslag til en skabelon for databehandleraftaler har Microsoft Danmark udarbejdet denne vejledning: https://aka.ms/dpamapping.
Desuden tilpasser Microsoft regelmæssigt databehandleraftalen baseret på feedback fra kunder og tilsynsmyndigheder. Fx baseret på en omfattende konsekvensanalyse foretaget af Det Hollandske justitsministerium (resultaterne er blevet gjort bredt tilgængelige for kunder over hele verden: https://aka.ms/DutchPrivacyDPIA og Microsoft efterfølgende udvidede aftalen for alle kunder for at imødekomme bl.a. disse resultater https://aka.ms/PrivacyTransparency.

---

15 https://aka.ms/MSGDPRefterlevelse

Q&A **9** **Inkluderes GDPR-artikler om databehandleransvar i databehandleraftalen eller inkluderes på anden vis i aftalen?**

Ja, defineres overordnet på side 7 i DPA[3] i afsnittet "*Behandling af Personoplysninger, GDPR*" og flere gange undervejs i aftalen, hvor det er relevant. Fx om GPDR Artikel 33 i afsnittet "*Security Incident Notification*".

Derudover inkluderer DPA[3] i "*Tillæg 3 – Vilkår i EU's Databeskyttelsesforordning*" alle Microsofts GDPR-forpligtelser fra artikel 28, 32 og 33.

Q&A **10** **Hvilke værktøjer stiller leverandøren til rådighed for den dataansvarlige til at levere og assistere med opbygning af den nødvendige compliance-dokumentation?**

Alle cloudkunder vil have adgang til en række specifikke værktøjer, som kan assistere med denne opgave enten i kombination eller individuelt. Deriblandt "Compliance Manager"[16] inklusiv "Secure Score"[17] og "Regulatory Compliance Score"[18].

Derudover har cloudkunden adgang til alle Microsoft Cloud Audit, ISO, PCI-rapporter etc. via Service Trust Portal[8]. En omfattende oversigt over Compliance-vejledningen fra Microsoft 365 kan findes her: https://aka.ms/M365ComplianceOverview

Ligeledes er der på STP adgang til en række 'mapping dokumenter', hvor de 1.000+ sikkerheds- og privacykontroller i Microsoft Cloud, mappes op imod de forskellige standarder (som ISO, NIST) og krav fra regulering (som GDPR).

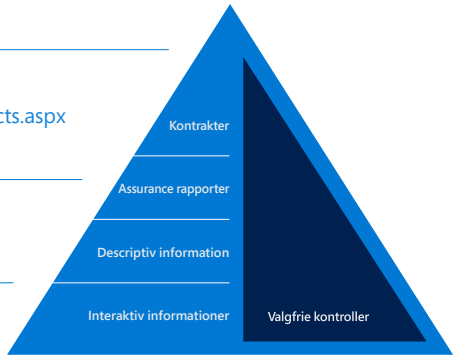
Til brug for cloudkundens compliance og risikovurderinger er alle disse værktøjer yderst relevante.

F.eks. når Security Center[19] på et Azure-abonnement er aktiveret, er Azure Security Benchmark[20] automatisk tildelet det pågældende abonnement. Dette bredt respekterede benchmark bygger på the Center for Internet Security (CIS21) og National Institute of Standards and Technology (NIST22) med fokus på cloud-centreret sikkerhed.

For at få et overblik over den foreslåede proces med at etablere den nødvendige overensstemmelses- og sikkerhedsoversigt kan det være nyttigt at læse afsnittet om "Microsoft Assurance Framework" i indledningen af denne hvidbog. Se også referenceoversigten på næste side:

16 https://aka.ms/mscompliancemanager
17 https://aka.ms/mssecurescore for SaaS og https://aka.ms/azuresc for IaaS & PaaS.
18 https://aka.ms/MSComplianceScor
19 https://aka.ms/azuresccd
20 https://aka.ms/AzureSecurityBenchmarkDoc
21 https://www.cisecurity.org/benchmark/azure/
22 https://www.nist.gov

Stakken af Microsoft assessment information



Kontrakt	Product terrms, Data Protection Addendum & SLA https://www.microsoft.com/en-us/Licensing/product-licensing/products.aspx https://aka.ms/dpa	
Platform	Service Trust Portal; assurance rappoter https://aka.ms/stp	
Dokumentation	Trust Center & docs.microsoft.com; assurancedokumentation https://aka.ms/mscloudtrust & https://docs.microsoft.com	
Proces	Microsoft Lockbox & Zero Standing Access https://aka.ms/zerostandingaccess	
Tjenester	Azure Customer Lockbox https://aka.ms/msazurelockbox	M365 Customer Lockbox https://aka.ms/o365CustomerLockbox
	Azure Advisor https://azure.microsoft.com/en-us/services/advisor/	M365 Security Score https://securescore.office.com/
Dyb	Azure Security Center https://azure.microsoft.com/en-us/services/security-center/	M365 Security & Compliance Centers https://aka.ms/m365seccenter & https://aka.ms/m365complcenter
Dybere	Azure Monitor https://azure.microsoft.com/en-us/services/monitor/	M365 Compliance Manager https://aka.ms/mscompliancemanager
Dybest	Rå Logs https://azure.microsoft.com/en-us/services/log-analytics/	Rå Logs https://protection.office.com/

Beredskabsplaner og operationel modstands-dygtighed

Definition og dokumentation på Microsoft Cloud

Q&A **11** **Kan leverandøren understøtte en kundes eventuelle "Exit strategi"? Hvordan?**

Ja.

Ved udløb eller opsigelse kan kunden udtrække sine data. Som fastsat i DPA[3] vil Microsoft beholde kundedata lagret i onlinetjenesten i en funktionsmæssigt begrænset version af tjenesten i 90 dage efter udløb eller opsigelse af kundens abonnement. Kunden kan dermed udtrække dataene. Når opbevaringsperioden på 90 dage udløber, deaktiverer Microsoft kundens konto og sletter kundedata. Microsoft deaktiverer kontoen og sletter kundedata fra tjenesten højst 180 dage efter udløb eller opsigelse af kundens brug af en onlinetjeneste.

De 90 dage efter udløb eller opsigelse er ment som et "sikkerhedsnet" for eventuelle resterende data. Når en kunde har brug for eller planlægger at afslutte, bør et af de første trin i en struktureret exitplan ikke være blot at opsige abonnementet. I stedet skal kunden starte en koordineret dataudtræksproces, når der er oprettet en ny destination for dataene. Microsoft tilbyder flere muligheder ud over den standardmekanisme til udtrækning af kundedata, der er integreret i Microsoft Online Services. Bemærk, at i henhold til DPA: *"I hele den periode, hvor Kundens abonnement er aktivt, har Kunden mulighed for at få adgang til og udtrække og slette Kundedata, der er gemt på hver Onlinetjeneste."*

Ejerskab af dokumenter, optegnelser og andre data forbliver hos kunden og overføres på intet tidspunkt til Microsoft eller anden part, så det behøver ikke at blive behandlet ved afslutning.

Endelig har Microsoft produceret en vejledning i udformning af en "Exit Strategi" som kan findes her under menupunktet "*FAQ and White Papers*" på Service Trust Portalen: https://aka.ms/MSCloudExit.

Q&A **12** **Foreligger der dokumentation for, hvordan platformen driftes, sikres og vedligeholdes?**

Kunder har altid adgang til en opdateret portefølje af 3. partscertificeringer og revisioner beskrevet bl.a. i svaret på spørgsmål 5 og 10 ovenfor.

Derudover beskrives i et offentligt brief[23], hvorledes Microsoft Ireland Operations Limited (MIOL) sikrer platformens høje pålidelighed og sikkerhed.

23 https://aka.ms/mscloudoperations

Dokumentet er globalt dækkende og omfatter både det fysiske beredskab, robuste processer for håndtering af hændelser, servicesupport, sikkerhed, change management, compliance, opbygningen af datacenterhardware, netværk, software og strategi for bæredygtighed.

Endelig driftes MIOL datacentre desuden efter konceptet "Operational Security Assurance[24]" (OSA), som sikrer indlejring af al unik erfaring om cybersikkerhedstrusler, som Microsoft opsamler gennem bl.a. SDL (se yderligere detaljer i spørgsmål 16), Microsoft Security Response Center[25], herunder Microsoft Cyber Defence Center[26].

OSA minimerer derigennem risici, fordi det sikres, at igangværende operationelle aktiviteter følger strenge sikkerhedsretningslinjer og validerer ydermere, at retningslinjerne rent faktisk følges effektivt. Opstår problemer, hjælper en etableret feedback-loop med at sikre, at fremtidige revisioner af OSA indeholder afhjælpninger for at løse dem. OSA udvikles således konstant for på tidssvarende vis at afspejle det til enhver tid gældende globale trusselsbillede.

En nærmere beskrivelse af MIOL Information Security Management System (ISMS) som certificeret gennem ISO (27001) er tilgængelig her: https://aka.ms/MSISMS

Endelig indeholder Microsoft Azure Security Fundamentals[27] oplysninger om de funktioner, der er indbygget i platformen, og en cloud-tjeneste-tjeklisteramme, der tilpasser klausul for klausul med de internationale standarder for cloud-serviceaftaler (standarder som f.eks. ISO/IEC 19086, med reference til ISO/IEC 19941).

NB! For MS HSCC-kunder fra EU vil modparten i licensaftalen være Microsoft Infrastructure Operations Ireland (MIOL), der opererer ud af adressen: One Microsoft Place, South County Business Park, Leopardstown, Dublin 18.

Q&A

13 Hvorledes vurderes leverandørens soliditet, finansielle stabilitet og commitment til i overskuelig fremtid at kunne vedligeholde, videreudvikle og fastholde minimums-compliance på platformen?

Mange af verdens førende virksomheder bruger Microsoft cloudtjenester. Casestudier vedrørende brugen af Microsofts cloudtjenester kan findes på https://customers.microsoft.com

Disse løsninger har opnået myndighedsgodkendelser (hvor krævet) for brug af onlinetjenester i alle regioner på kloden, herunder Asien, Nordamerika, Latinamerika, Europa, Mellemøsten og Afrika. Microsoft Office 365 (SaaS) er vokset til at have over 100.000.000 brugere, herunder nogle af verdens største organisationer indenfor alle brancher - private såvel som offentlige.

Microsoft Corporation er offentligt noteret i USA og har siden år 2000 været blandt verdens største virksomheder målt på "market capitalisation" (pt. omkring USD $2.000.000.000.000). Microsofts finansielle stabilitet har vist en stærk track-record af overskud.

Fuld firmaprofil er tilgængelig her: https://microsoft.com/en-us/investor/ og de årlige finansielle rapporter kan findes her: https://microsoft.com/en-us/Investor/annualreports.aspx

Microsofts cloudtjenester er baseret på ISO/IEC27001 og ISO/IEC 27018-standarderne, - et stringent sæt globale standarder, der dækker fysiske og logistiske proces- og forvaltningskontroller. Microsoft tilbyder og videreudvikler endvidere det mest omfattende sæt standardcertificerede og auditerede tjenester ift. enhver anden cloududbyder.

En liste over de aktuelle certificeringer kan findes på denne adresse:
https://aka.ms/mscloudcomplianceofferings

24 https://aka.ms/msopsec
25 https://aka.ms/mssrc
26 https://aka.ms/mscdoc
27 https://aka.ms/azurefundamentalsecurity

Den relativt nyelig publicerede ISO27701[28]-standard for PIMS (Personal Information Management System) bygger ovenpå ISO27000-serien og er designet til at hjælpe dataansvarlige og databehandlere med at forene forskellige lovkrav, herunder GDPR, i operationelle kontroller, der kan implementeres og revideres på en konsekvent måde. Kort sagt er formålet med designet at komme tæt på en GDPR certificering[29] (fastsat i artikel 42) og andre regler, og ultimativt etablerer en omfattende dokumentation for efterlevelse.

Microsoft har som én af de første virksomheder gennemgå denne revisionsproces for Microsoft cloudtjenester, og kunne 13. januar, 2020 annoncere[30] den endelige certificering. Ydermere kunne Microsoft i Maj 2021 meddele fuld overholdelse af det netop verificerede EU Cloud Code of Conduct[4].

Integritet er desuden en kerneværdi for Microsoft[31], som er gennemgående for alle dele af Microsofts forretning og en del af den interne kultur. Medarbejdere såvel som partnere trænes og måles med jævne mellemrum i efterlevelse. Læs evt. mere her: https://aka.ms/MSIntegrity

Samlet set bør kunder således ikke have nogen betænkeligheder mht. Microsofts finansielle styrke eller commitment til fortsat at drive, videreudvikle og fastholde det høje sikkerheds- og compliance-niveau.

Q&A

14 I hvilket omfang sikres modstandsdygtigheden geografisk?

Microsoft cloudinfrastruktur er delt op med leverance i (pt.) 58 regioner, hvor hver region består af mindst to datacentre, der er geografisk adskilt for sikring mod udefrakommende, ikke-digitale, trusler.

Kundedata lagres inden for den region, kunden vælger, men data replikeres mellem to separate lokationer inden for samme region. Primær afvikling sker så i et center med redundant (hot) fail-over i et andet datacenter i regionen. Inden for mange regioner eksisterer mere end to datacentre, hvorfor nogle tjenester kan tilbydes dedikeret fra disse og dermed yderligere øge modstandsdygtigheden baseret på geografisk lokation.

Microsoft forpligter sig løbende til yderligere at udvide antallet af tilgængelige regioner globalt set og specielt indenfor EU/EØS. Alene i løbet af de seneste 12 måneder er der blevet bebudet ny kapacitet og nye regioner i EU/EØS-geografien i bl.a. Sverige[32], Danmark[33], Italien[34], Østrig[35] og Grækenland[36].

En meget mere detaljeret beskrivelse af, hvordan man muliggør og sikrer dataopbevaring i Microsoft Azure regioner, findes i hvidbogen[37] "Enabling Data Residency and Data Protection in Microsoft Azure Regions" publiseret i April 2021. Dette dokument indeholder de oplysninger og værktøjer, der er nødvendige for at optimere og kontrollere datalokation og adgang, herunder dybdegående kontrol med Azures regionale infrastruktur, optimering af arkitekturmæssige beslutninger, etablering af datalokationssgarantier pr. tjeneste, etc. Så man som cloud kunde kan fastholde og administrere dataplacering og adgang.

Det nævnte whitepaper indeholder også oplysninger om den såkaldte ExpressRoute service[38], som giver kunderne mulighed for at udvide lokale netværk til Microsoft-skyen via en privat forbindelse, der er faciliteret af en netværksudbyder. Forbindelsen kan være fra et IP VPN-netværk (any-to-any), et punkt-til-punkt Ethernet-netværk eller en virtuel krydsforbindelse via en netværks/internetudbyder på en co-lokations facilitet. ExpressRoute-forbindelser går ikke over det offentlige internet. Dette gør det muligt for ExpressRoute-forbindelser at tilbyde ensartet latency, større pålidelighed, generelt hurtigere hastigheder og højere sikkerhed end typiske forbindelser over internettet.

---

28 https://aka.ms/PIMS3pager
29 https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201801_v3.0_certificationcriteria_annex2_en.pdf
30 https://aka.ms/azureiso27701
31 https://www.microsoft.com/en-us/about/corporate-values
32 https://aka.ms/DigitalLeapSv
33 https://aka.ms/DigitalLeapDenmar
34 https://aka.ms/DigitalLeapIt
35 https://aka.ms/DigitalLeapAu
36 https://aka.ms/DigitalLeapGr
37 https://aka.ms/AzureDataResidencyWP
38 https://aka.ms/expressroute

Serviceforandrings-kontrol og konfigurations-håndtering

Definition og dokumentation på Microsoft Cloud

Q&A **15** **Hvorledes håndterer leverandøren ændringer i platformen, fx nye service-funktioner, software-opdateringer etc.?**

Generelt følger Microsoft og MIOL NIST vejledning om sikkerhedsovervejelser ifm. softwareudvikling, og disse er således indlejret i SDL (se spørgsmål 16 for detaljer).

I Cloud Security Alliance, Cloud Control Matrix[39] (CSA CCM), afsnittet "*Change Control & Configuration Management*" fra side 19 og frem, beskrives indgående de processer og kontroller, der indgår.

39 https://aka.ms/csamatrixazure for Azure & Dynamics. https://aka.ms/csamatrixo365 for Microsoft Office 365

Datasikkerhed og informations-livscyklushåndtering

Definition og dokumentation på Microsoft Cloud

Q&A **16** **Har leverandøren en klar beskrivelse af 'Information Lifecycle Management'-processer?**

Microsoft har besvaret CSA CCM[23] og dokumenterer her fra side 23 og frem, hvorledes '*Data Security & Information Lifecycle Management*'-kontroller er implementeret på tværs af cloudplatformen (Azure, Office 365 og Dynamics 365).

Ligeledes er driftsprincipperne beskrevet i '*Operational Security Assessment*'[40] (OSA), som inkorporerer viden opnået gennem en række funktioner, der er unikke for Microsoft, herunder "*Microsoft Security Development Lifecycle*"[41] (SDL), "*Microsoft Security Response Center*"-programmet[42] og gennemgående bevidsthed om og håndtering af cybersikkerhed i et globalt trusselslandskab.

SDL er en omfattende sikkerhedsproces, der kontrollerer hvert trin i design, udvikling og udrulning af Microsofts cloudtjenester. Gennem designkrav, referencespørgsmål/krav, vejledning og analyse af angrebsoverflade- og trusselsmodellering, hjælper SDL Microsoft med at forudsige, identificere og afbøde sårbarheder og trusler fra før en tjeneste lanceres og gennem hele produktets produktionslivscyklus.

Q&A **17** **Hvorledes håndteres data retention?**

Beskrives i CSA CCM[23], afsnittet "*Data Governance*".

Specifikt for Office 365 kan med fordel læses: https://aka.ms/o365drdd
Bemærk, at kunden har omfattende kontrol over opbevaring af data i Microsoft Online Services.
Se https://aka.ms/M365DataGovernance for Microsoft365.
Se https://aka.ms/AzureDataGovernance for Microsoft Azure.

Harddiske genbruges eller repareres ikke.

40 https://aka.ms/msopsec
41 https://aka.ms/mssdl
42 https://aka.ms/mssrc

Applications- og interfacesikkerhed

Definition og dokumentation på Microsoft Cloud

Q&A **18** **I hvilket omfang scannes kildekode for sårbarheder? Er processen dokumenteret og standardiseret?**

SDL (se svaret på spørgsmål 16) er rammeværktøjet for sådanne 'Security reviews' af alt design, arkitektur og kode, der udrulles på platformen. SDL er desuden udgivet i Open Source, og ligger frit tilgængeligt[43] for enhver for implementering eller 'revision'.

Microsoft Government Security program[44] (GSP) tilbydes offentlige entiteter, som har til formål at håndtere den nationale cybersikkerhed og giver deltagerne adgang til fortrolige sikkerhedsoplysninger og ressourcer fra Microsoft.

GSP-deltagere omfatter i øjeblikket over 45 lande og internationale organisationer repræsenteret af mere end 90 agenturer.

Deltagelse muliggør kontrolleret adgang til kildekode, udveksling af trussels- og sårbarhedsoplysninger, inddragelse af teknisk indhold om Microsofts produkter og tjenester og adgang til fem globalt distribuerede gennemsigtighedscentre.

Gennem GSP opnår både de deltagende landes tjenester det indblik, de skal bruge for at kunne have tillid til Microsofts produkter og tjenester, ligesom de gennem programmet er forpligtet til at dele evt. viden om sårbarheder el.lign., de måtte finde, med Microsoft.

Q&A **19** **Sikres det at al kode i produktion på platformen følger samme sikkerheds-standarder?**

Se spørgsmål 15-17.

Q&A **20** **Gennemføres dataintegritets-tjek?**

CSA CCM[23], afsnittene "*Application and Interface Security*" og "*Data Security and Information Lifecycle Management*", beskriver de tilstedeværende kontroller for sikring af dataintegritet.

43 https://aka.ms/mssdl
44 https://aka.ms/msgsp

Q&A

21 Gennemføres penetrationstests på både netværk og applikationer?

Ja.

Microsoft gennemfører regelmæssigt penetrationtests for at muliggøre løbende forbedring af den generelle sikkerhed og 'Incident Response'-procedurer. Disse interne tests hjælper Microsoft Cloud Services' sikkerhedseksperter med at skabe en metodisk, gentagelig og optimeret trinvis responsproces og automatisering.

Penetrationstestrapporter offentliggøres på Service Trust Portalen under fanen "Pentest and Security Test" i afsnittet 'Data Protection'.

Ydermere driver Microsoft Red Teaming 'live' site penetrationstests mod Microsoft Managed Cloud-infrastrukturtjenester og -programmer. De simulerer 'breaches' i den virkelige verden, udfører løbende sikkerhedsovervågning og 'incident respons'-øvelser for at validere og forbedre sikkerheden i Microsoft Azure og Office 365.

Disse erfaringer med sikkerhedsprocedurer giver kunder et godt grundlag at bygge på for at implementere og administrere cloudbaserede løsninger på en sikker måde. Læs mere om RedTeam her: https://aka.ms/MSRedTeam

Q&A

22 Kan cloudkunden gennemføre egne penetrations-tests?

Ja.

Microsoft forstår, at sikkerhedsvurderinger også er en vigtig del af kunders applikationsudvikling og udbredelse. Derfor har Microsoft etableret en politik for kunder til at udføre autoriserede penetrationstests på deres applikationer hostet i Azure. Da sådanne tests ikke kan skelnes fra et rigtigt angreb, er det afgørende, at kunderne kun foretager penetrationstests i overensstemmelse med *'Microsoft Online Services – Data Protection Addendum' (DPA*[3]) aftale og *'Rules of Engagement'*, som kan findes her: https://aka.ms/MSpenTestROE

Q&A

23 Hvordan sikres det, at kunden kan genskabe sine data i tilfælde af fejl eller tab?

Kundedata replikeres kontinuerligt og placeres i geografisk spredte Microsoft-datacentre for at give mulighed for datagendannelse i tilfælde af fejl i denne lokale infrastruktur.. Kunderne er ansvarlige for at tage videre skridt til at give yderligere fejltolerance, fx skabe historiske sikkerhedskopier af kundedata, gemme sikkerhedskopier af kundedata uden for miljøet, implementere redundante 'Compute instanser' i og på tværs af datacentre eller sikkerhedskopiere 'state' og data i en virtuel maskine.

Microsoft giver kunden mulighed for selv at opbygge denne funktion over toppen af bl.a. Azure Storage. For at hjælpe med due diligence, er det værd at bemærke, at CSA CCM[23] Control ID DG-04 Data Governance-Retention Policy kræver følgende:

"Policies and procedures for data retention and storage shall be established and backup or redundancy mechanisms implemented to ensure compliance with regulatory, statutory, contractual or business requirements. Testing the recovery of disk or tape backups must be implemented at planned intervals."

I Microsofts svar, som kan findes i dokumentet "Microsoft Azure standard Response to RFI – Security & Privacy[45]", angives følgende:

"Data retention policies and procedures are defined and maintained in accordance to regulatory, statutory, contractual or business requirements.

The Microsoft Azure backup and redundancy program undergoes an annual review and validation. Microsoft Azure backs up infrastructure data regularly and validates restoration of data periodically for disaster recovery purposes.

Microsoft Azure includes replication features detailed below to help prevent loss of customer data in the event of failures within a Microsoft data center.
...

"Information back-up" is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 10.5.1. For more information, review of the publicly available ISO standards we are certified against is suggested."

Yderligere er Geo-replikering fastsat for at sikre data i tilfælde af et større datacenter katastrofe eller forbigående hardwarefejl. Kunden har tre muligheder for at replikere data:

- **Locally redundant storage (LRS)** *is replicated three times within a single datacenter. When you write data to a blob, queue, or table, the write operation is performed synchronously across all three replicas. LRS protects your data from normal hardware failures*
- **Geo-redundant storage (GRS)** *is replicated three (3) times within a single region, and is also replicated asynchronously to a second region hundreds of miles away from the primary region. GRS keeps an equivalent of six (6) copies (replicas) of your data (three in each region). GRS enable Microsoft to failover to a second region if we can't restore the first region due to a major outage or disaster. GRS is recommended over locally redundant storage*
- **Read-access geo-redundant storage (RA-GRS)** *provides all of the benefits of geo-redundant storage noted above, and also allows read access to data at the secondary region in the event that the primary region becomes unavailable. Read-access geo-redundant storage is recommended for maximum availability in addition to durability."*

Vejledning i opbygning, vedligeholdelse og test af en plan for sikkerhedskopiering og gendannelse af Azure-tjenester, der passer til den enkelte kundes tolerance over for reduceret funktionalitet under en katastrofe, er tilgængelig på http://aka.ms/MSAzureBackAndRecovery.

For SaaS-løsninger som M365 har platformen i sig selv indbygget datarobusthed46 Kunden bør dog overveje, hvordan de bedst beskytter deres data mod moderne trusler (f.eks. Ransomware-angreb), ved hjælp af Threat Protection47 løsninger, genskabelses[48] løsninger og konfigurering af backup af den pågældende service (fx. Exchange Online[49]).

45 https://aka.ms/MSazurecsa
46 https://aka.ms/M365DataResiliency
47 https://aka.ms/M365threatprotection
48 https://aka.ms/M365RansomwareRecovery
49 https://aka.ms/M365ExchangeBackup

Fysisk datacentersikkerhed

Definition og dokumentation på Microsoft Cloud

Q&A **24** **Hvilke kontroller og beredskab er på plads for at sikre kunden mod udefra-kommende påvirkning (fx naturkatastrofer) af det enkelte datacenters sikkerhed?**

Microsoft går meget langt for at minimere risiko for afbrydelser i driften af online tjenester, inkl. fysisk redundans (harddiske, NIC, strøm, serverniveauer, indholds-replikering, backup, fail over, realtidsmonitorering, automatiseret håndtering af hændelser, kontinuerlig læring gennem post-hændelsesproces etc.), men deler ikke alle detaljer af Microsoft Disaster Recovery og Business planer med andre end auditors.

Microsoft anbefaler kunder at gennemgå den tekniske vejledning, som er tilgængelig her: https://aka.ms/MScloudBizCon og/eller Microsoft HSCC Enterprise Business Continuity Management plan som kan findes her: https://aka.ms/MSEBCMguidance.

In-scope Microsoft OnlineTjenester er certificeret i forhold til ISO22301, som er den internationale standard for administration af forretningskontinuitet: https://aka.ms/msISO22301.

Q&A **25** **I hvilket omfang er der redundans i driften af data-centre ift. elektricitet, netværk etc.?**

Se ovenfor.

Microsoft vedligeholder fysisk redundans på serveren, datacenteret og serviceniveauerne. Dataredundans med robuste fail over-funktioner. Funktionel redundans sikres med offline funktionalitet. Microsofts redundante Storage, og procedurer for genskabelse af data, er designet til at forsøge at rekonstruere kundedata i sin oprindelige eller sidst-replikerede tilstand fra før den tid, data blev tabt eller ødelagt.

For at fremme datas modstandsdygtighed, tilbyder Microsoft Online Services aktiv load-balancing, automatiseret fail over og menneskelig backup samt Recovery tests på tværs af fejlede domæner. Fx leverer Azure Traffic Manager load-balancing mellem forskellige regioner, og kunden kan bruge virtuelle netværksenheder i sin Azure Virtual Netværk til funktioner til Application Delivery Controllers (ADC/Load Balancing)-funktionalitet.

Load-balancing leveres også af Power BI-tjenester, gatewayen og Azure API Management-roller.

Q&A

26 Hvilken Recovery time objective (RTO) for systemer eller applikationer outsources til leverandøren?

RTO for hver Microsoft onlinetjeneste er angivet i service level-aftalen (SLA) som kan findes her:
http://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=3&DocumentTypeId=37

Kryptering og nøglehåndtering

Definition og dokumentation på Microsoft Cloud

Q&A **27** **I hvilket omfang anvendes kryptering på platformen, hhv. når data er i hvile og i transit?**

Som beskrevet i DPA, *"(...) Kundedata (herunder alle inkluderede Personoplysninger), som er i færd med at blive overført via offentlige netværk mellem Kunden og Microsoft, eller mellem Microsofts datacentre, er som standard krypterede.*

Derudover krypterer Microsoft inaktive Kundedata i Onlinetjenesterne. I tilfælde af Onlinetjenester, hvor Kunden eller en tredjemand handler på Kundens vegne og må udvikle applikationer (f.eks. visse Azure-tjenester), krypteres visse data, som er lagret i disse applikationer, muligvis efter Kundens skøn og ved hjælp af ekspertise fra Microsoft eller en af Kundens samarbejdspartnere. (...)"

Kundedata i Microsofts Enterprise Cloud-tjenester er beskyttet af en lang række teknologier og processer, herunder forskellige former for kryptering. Microsoft tilbyder en række indbyggede krypteringsfunktioner, der hjælper med at beskytte data:

- For Office 365 følger Microsoft branchens kryptografiske standarder som TLS/SSL og AES for at beskytte fortroligheden og integriteten af kundedata. For data i transit forhandler alle servere med kundemøder en sikker session ved at bruge TLS/SSL med klientmaskiner til at sikre kundedata. For data i hvile, installerer Office 365 BitLocker med AES 256-bit-kryptering på servere, der holder alle meddelelsesdata, herunder mail- og chatsamtaler samt indhold, der er lagret i SharePoint Online og OneDrive for Business. I nogle scenarier har Microsoft desuden brugerkryptering på filniveau.
- For Azure hjælper teknologiske sikkerhedsforanstaltninger såsom krypteret kommunikation og driftsprocesser med at holde kundernes data sikre. Microsoft giver også kunderne fleksibilitet til at implementere yderligere kryptering og administrere deres egne nøgler. I forbindelse med data i transit bruger Azure branchestandardiserede, sikre transportprotokoller, fx TLS/SSL, mellem brugerenheder og Microsoft-datacentre. For data i hvile tilbyder Azure mange krypteringsmuligheder, såsom støtte til AES-256, hvilket giver kunderne fleksibilitet til at vælge det datalagringsscenarie, der bedst opfylder kundens behov.

Microsoft bruger nogle af de stærkeste, mest sikre krypteringsprotokoller, der er tilgængelige til at skabe barrierer mod uautoriseret adgang til kundedata. Korrekt nøgleadministration er også et vigtigt element i optimale krypteringsløsninger, og Microsoft arbejder på at sikre, at alle Microsoft-administrerede krypteringsnøgler er korrekt sikret.

Uanset kundens konfiguration, er kundedata lagret i Microsofts Enterprise Cloud-tjenester, der er beskyttet ved hjælp af én eller flere krypteringsformer. Validering af Microsoft krypteringspolitik og dens håndhævelse er uafhængigt verificeret af flere tredjepartsrevisorer, og rapporter om disse revisioner er tilgængelige på Service Trust Portal, som tidligere er blevet nævnt.

På Office365 tilbydes desuden såkaldt "Customer Key Encryption" som på applikationsniveau tilføjer yderligere et krypteringslag: https://aka.ms/o365CustomerKey

Særlige white papers med overblik over kryptering:

- hvordan Microsoft Cloud platform overordnet set anvender kryptering: https://aka.ms/Mscloudkryptering
- Microsoft Azure-kryptering: https://aka.ms/msazureencryption
- Microsoft O365-kryptering: https://aka.ms/o365contentencryption & https://aka.ms/o365IntroTilKryptering
- Mailkryptering: https://aka.ms/o365kryptering

Video-beskrivelser leveret af Microsoft Security er også tilgængelige hvis man har brug for en hurtig introduktion til mange af disse emner:

- M365 Encryption of data-at-rest: https://www.youtube.com/watch?v=Dk380mk-xh0&t=41s
- Azure Data Protection: https://www.youtube.com/watch?v=dRgZJpKj7hU&t=818s

Q&A

28 I hvilket omfang har kunden adgang til at tilføje krypterings-teknologier inkl. BYOK o. lign.?

Microsoft administrerer nøgler til den stærke standardkryptering, der er etableret i miljøet, men kunderne kan også anvende deres egen kryptering.

Microsoft tilbyder en række løsninger (inkl. BYOK) som beskrives i detaljer i disse seperate white papers:

På Office 365: https://aka.ms/mscloudCMkryptering
På Azure: https://aka.ms/msazureprotection

I disse dokumenter er det vigtigt at bemærke en væsentlig detalje mht. forvaltning af nøgler, når en kunde anvender/tilføjer egen kryptering:
"*Encryption and authentication do not improve security unless the keys themselves are well protected. It is generally considered a critical IT security task to manage key lifecycles, as proper key management is important to maintaining high security, high reliability, and low overhead.*"

Bring-Your-Own-Key/Hold-Your-Own-Key (BYOK/HYOK) kryptering

Azure Key Vault[50] er en skytjeneste til sikker opbevaring og adgang til hemmeligheder. En hemmelighed er alt, hvad du vil kontrollere adgangen til, f.eks. Det giver organisationer af enhver størrelse mulighed for især at gemme og bruge - i overensstemmelse med boksens adgangspolitik - deres egne nøgler med ekstrem sikkerhed takket være dens afhængighed af branche bevist, FIPS-kompatible hard-waresikkerhedsmoduler (HSM'er) fra en række HSM-leverandører[51]. It tilbyder BYOK-funktionen, der giver disse organisationer mulighed for at generere og importere deres lokale nøgle og uddelegere brugsrettigheder til brug til et stigende antal Microsoft HSCC-tjenester (f.eks. Office 365 og en række Azure Services) som supporterer integration med Azure Key Vault for server-side kryptering, client-side kryptering og/eller indholdskryptering for at beskytte data.

50 https://aka.ms/AzureKeyVault
51 https://aka.ms/MSAKVHSM

Løsningen er udviklet til at sikre, at Microsoft ikke kan se eller udtrække kundenøglerne.

En dybere beskrivelse af, hvordan man planlægger og implementerer brugen af Azure Key Vault, kan findes her: https://aka.ms/azurekeyvaultplanning

Som en relativt ny tjeneste tilbyder Microsoft også såkaldt "Double Key Encryption" (https://aka.ms/dke) hvor Microsoft gemmer en nøgle i Microsoft Azure, og kunden har den anden nøgle. Kunden bevarer fuld kontrol over en af kundenøglerne ved hjælp af tjenesten Dobbeltnøglekryptering. Med dette kan beskyttelsen anvendes ved hjælp af Azure Information Protection unified labeling client, på de data man klassificerer som meget følsomme.

Bemærk venligst!
BYOK/HYOK løsninger (som DKE) er kun beregnet til de mest følsomme data, der er underlagt de strengeste beskyttelseskrav. DKE kan ikke anbefales at anvende for alle data, da der er nogle konsekvenser både med hensyn til omkostninger, kompleksitet, nye sikkerhedsrisici (potentielt tab af tilgængelighed af data) og ikke mindst lejlighedsvise funktionelle begrænsninger!
Generelt bør kunderne kun bruge dobbeltnøglekryptering til at beskytte en lille del af den samlede mængde data. Due dilligence bør udføres så man identificerer de rigtige data til anvendelse af sådanne løsninger, før implementering af DKE eller en anden BYOK/HYOK-løsning. I nogle tilfælde kan det være nødvendigt at begrænse omfanget af data og gøre brug af andre løsninger til beskyttelse af den største datamængde – fx., løsninger som Microsoft Information Protection med Microsoft-administrerede nøgler eller BYOK. Disse løsninger er sandsynligvis tilstrækkelige til de fleste dokumenter/data, som ikke er underlagt skærpede beskyttelse og lovmæssige krav.

Ligeledes, kan BYOK/HYOK løsninger umuliggøre brug af de mest kraftfulde Office 365-tjenester og funktioner. Følgende er tjenester, der ikke fuldt ud kan udnyttes med DKE-krypteret indhold:

- Transportregler, herunder anti-malware og spam, der kræver synlighed i de vedhæftede filer.
- Microsoft Delve[52] og MyAnalytics.
- eDiscovery[53].
- Indholdssøgning og indexering.
- Office Web Apps inklusiv 'samtidig redigeringsfunktionalitet'.

Eksterne programmer eller tjenester, der ikke er integreret med DKE (ved hjælp af Microsoft Information Protection[54]), kan ikke udføre handlinger på de krypterede data.

Videos er tilgængelige for en hurtig introduktion til mange af disse emner, fx:

- M365 Double Key Encryption: https://www.youtube.com/watch?v=0d-A4OYxaEA&t=2s.
- MyAnalytics: https://www.youtube.com/watch?v=43i-lXo4wN8.

52 https://aka.ms/MSDelveDoc
53 https://aka.ms/MSeDiscoveryDoc
54 https://aka.ms/MSIPdoc

Governance- og risikohåndtering

Definition og dokumentation på Microsoft Cloud

Q&A **29** **Hvorledes foretager leverandøren risikovurdering på platformen?**

I Microsofts SSAE 18 SOC 2 Type II rapport[55], som er tilgængelig på Services Trust Portalen, fremgår det af afsnittet '*OIS: Organization of Information Security*'.

55 https://aka.ms/mscloudsoc

Human resources

Definition og dokumentation på Microsoft Cloud

Q&A

30 Hvilke sikkerheds- og privacykontroller har leverandøren implementeret ift. egne og under-leverandørers personale?

For visse kernetjenester i Office 365 og Azure er personale (herunder medarbejdere og underleverandører) med mulig adgang til kundedata underlagt baggrundsscreening, sikkerhedstræning og adgangsgodkendelser som tilladt af gældende lov (se afsnit om juridiske opmærksomhedspunkter i indledningen).

Baggrundsscreening finder sted før, det kan komme på tale at give medarbejderen tilladelse til i sjældne tilfælde at få mulig adgang til kundedata. I det omfang straffesager, der involverer uærlighed, tillidsbrud, hvidvaskning af penge eller jobrelateret afgivelse af urigtige oplysninger, forfalskning eller udeladelse af faktiske forhold, kan det diskvalificere en kandidat fra ansættelse, eller kan, hvis personen har beskæftigelse, medføre opsigelse af ansættelsesforhold.

Se desuden CSA Cloud Control Matrix[56], side 40-46 "*Human Resources: Controls*".

56 https://aka.ms/csamatrixazure for Azure & Dynamics. https://aka.ms/csamatrixo365 for Microsoft Office 365

Identitets- og adgangskontrol

Definition og dokumentation på Microsoft Cloud

Q&A

31 Hvorledes håndterer leverandøren identitets- og adgangskontrol?

Alle Security Measures er en del af Microsofts kontrolset, som auditeres i SSAE 18 SOC 1 Type II og SSAE 18 SOC 2 Type II-rapporterne[57]

Microsoft har implementeret en række kontroller påkrævet under standarden ISO/IEC 27002:2013 "*Information Technology – Security techniques – Code of Practice for Information Security Controls*". Nedenfor et overblik (en mere detaljeret beskrivelse af kontrollerne kan desuden findes i CSA Cloud Control Matricerne[24]):

Adgangstilladelse

- **Microsoft vedligeholder og opdaterer** en fortegnelse over medarbejdere, der er autoriseret til at få adgang til Microsoft-systemer, som indeholder kundedata
- **Microsoft deaktiverer godkendelseslegitimationsoplysninger**, der ikke er blevet brugt i en periode på højst seks måneder
- **Microsoft identificerer** de medarbejdere, der kan give, ændre eller annullere autoriseret adgang til data og ressourcer
- **Microsoft sikrer**, at hvis mere end én person har adgang til systemer, der indeholder kundedata, har personerne separate identifikationer/logins
- **Mindste privilegium / "Least Privilege"**
- **Teknisk support-personale er kun tilladt at have adgang til kundedata**, når det er absolut nødvendigt
- **Microsoft begrænser kun adgangen til kundedata** til de personer, der har brug for en sådan adgang til at udføre deres jobfunktion

Mht. Microsoft-understøttelse af kundens egen Identity Management-strategier, gør Azure Active Directory[58] det muligt for kunder at administrere adgang til deres cloudinstanser. Multi-faktor-autentificering[59] og adgangsovervågning-tjenester60 tilbyder derudover øget sikkerhed.

Læs desuden evt. Microsofts gode råd om identitets- og adgangskontrol på: https://aka.ms/MScloudidam

57 https://aka.ms/mscloudsoc
58 https://aka.ms/azureAD
59 https://aka.ms/azureADMFA
60 https://aka.ms/azureADmonitorering

Infrastruktur og virtualiseringssikkerhed

Definition og dokumentation på Microsoft Cloud

Q&A **32** **Hvordan håndterer leverandøren adskillelse af kundedata i multi-tenant miljø?**

For alle onlinetjenester isolerer Microsoft logisk kundedata fra de andre data, som Microsoft opbevarer. Datalagring og behandling for hver lejer er opdelt i en "Active Directory"-struktur, som isolerer kunder ved hjælp af sikkerhedsgrænser ("siloer"). Siloerne beskytter kundens data, så dataene ikke kan tilgås eller kompromitteres af andre kunder på platformen.

Se denne dokumentation for en forklaring på isolationsmetoden i Microsoft Azure: https://aka.ms/AzureIsolation.

Se denne dokumentation for en forklaring på isolation indenfor Microsoft365: https://aka.ms/M365Isolation.

Se evt. CSA CCM-kontrol "AAC-03.1", "IVS-08.3", "IVS-09.4".

Q&A **33** **Kan kunden håndtere egne backups off-site?**

Ja, se svaret på spørgsmål 23 ovenfor.

Q&A **34** **Kan kunden genskabe virtuelle maskiner til et tidligere tidspunkt/'stage'?**

Ja.
Microsoft Cloud tilbyder både backup og genskabelse: https://aka.ms/azurebackuprestore

Interoperabilitet og portabilitet

Definition og dokumentation på Microsoft Cloud

Q&A **35** **Hvorledes håndteres myndigheders anmodning om dataadgang/udlevering af data?**

Microsoft har i årevis arbejdet på at bevare tidløse værdier og fremme den offentlige sikkerhed og samtidig sikre, at folk kan stole på teknologi, der forbedrer deres liv. Vi håber, at vores bidrag kan føre til moderne love, der fungerer for alle. se: https://aka.ms/datalaw.

Hos Microsoft mener vi, at kunderne fortjener at kende vores politikker for at kunne besvare regeringens anmodninger om deres data. Denne gennemsigtighed hjælper også med at informere de politiske beslutningstagere, når de arbejder på at modernisere love, der påvirker vores kunder.

Microsoft er af den overbevisning, at kunderne har ret til at være beskyttet af deres egne love. Desuden mener Microsoft, at de formulerede principper repræsenterer universelle rettigheder og grundlæggende minimumskrav, der bør gælde for retshåndhævelsesadgang til data i vores moderne tidsalder. Anvendelsen af disse principper kan variere fra land til land, men de underliggende principper om kontrol og balance, ansvarlighed og gennemsigtighed forbliver gyldige også når vi opererer globalt.

Microsoft har en principfast og stringent tilgang til behandling af offentlige anmodninger om adgang til kundedata i Microsofts varetægt. De centrale politikker, vi overholder på tværs af vores tjenester, er:

- Microsoft giver ikke nogen regering direkte og uhindret adgang til vores kunders data, og vi giver ikke nogen regering vores krypteringsnøgler eller evnen til at bryde vores kryptering.
- Hvis en regering ønsker kundedata, skal den følge gældende juridisk proces. Det skal tjene os med en kendelse eller retskendelse for indhold, eller en stævning for abonnent oplysninger eller andre ikke-indholdsdata.
- Alle anmodninger skal målrettes mod bestemte konti og identiteter.
- Microsofts juridiske team gennemgår alle anmodninger for at sikre, at de er gyldige, afviser dem, der ikke er gyldige, og leverer kun det absolutte minimum af data når lovgivning beviseligt kræver det.

Processen er beskrevet i detaljer her: https://aka.ms/MSLERH.

En del af Microsofts arbejde med anmodninger fra myndighederne omfatter offentliggørelse af "rapporter om anmodninger om retshåndhævelse" hvert halve år for at sikre gennemsigtighed i omfanget og arten af disse hændelser. Rapporterne kan findes her: https://aka.ms/MSLERR og kan bruges til at hjælpe med at gennemføre den lovpligtige risikovurdering.

Til brug i den krævede vurdering af risikoen for, at myndigheder søger adgang til kundedata i forbindelse med efterforskning af alvorlig (og ofte global) kriminatitet, kan det være relevant at tage hensyn til de

faktuelle tal på omfanget fra Microsoft Law Enforcement Request-rapporterne, der er tilgængelige fra linket ovenfor.

Nedenstående tabel indeholder tallene fra 2020 og en lignende periode i 2018 til reference og klar angivelse af udviklingen:

Tidsperiode	Anmodninger Globalt	... heraf relateret til virksomheder	Direkte afvist eller omdirigeret til kunden	nogle meta-data udleveret	Noget indhold udleveret	Associeret med US LE	Heraf data lagret udenfor USA
Jul-Dec 2018	21433	61	39 af 61 ~63,9%	7 af 22 ~31,8%	N/A	8 of 15 ~53,3%	1 af 8
- oOo -							
Jan-Jun 2020	24093	91	42 af 91 ~46,2%	25 af 49 ~51,0%	24 af 49 ~49,0%	20 of 24 ~83,3%	2 af 20
Jul-Dec 2020	24798	109	69 af 109 ~63,3%	21 af 40 ~52,5%	19 af 40 ~47,5%	10 of 19 ~52,6%	1 af 10

Naturligvis kan stigningen i det samlede antal anmodninger (herunder forbrugertjenester) samt den relativt større stigning i virksomhedsrelateret anmodning forklares på mange måder, og det er umuligt at sige, hvilken er de nøjagtige forklaringer. Den samlede brug af digitale tjenester er bestemt steget i løbet af de sidste 3 år, både blandt forbrugere og virksomheder. Omfanget af kriminelle aktiviteter globalt kan også være steget i antal såvel som i omfang og rækkevidde, og myndighedernes brug af anmodninger om dataadgang kan også ganske enkelt være steget.

abellen og de underliggende anmodningsrapporter viser, at Microsoft kun modtog 1 anmodning (kendelse) fra retshåndhævelsesmyndigheder i USA for kommercielle virksomhedskunder, som resulterede i udlevering af indholdsdata relateret til ikke-amerikanske virksomhedskunder, hvis data var lagret udenfor USA. Enhver anmodning skal som minimum være specifik på en person og uden fare for kompromitering af efterforskningen, kunne fremfindes eller anmodet udleveret fra den dataansvarlige organisation selv.

Med det anslåede antal virksomhedskonti i Microsoft HSCC Online Services, fremgår det klart af tallene ovenfor, at ...

- sandsynligheden for, at en given Enterprise-kunde (privat så vel som offentlig) er målet for en sådan anmodning, er minimal
- sandsynligheden for, at en sådan anmodning IKKE afvises eller omdirigeres, er endnu mindre, og
- sandsynligheden for en sådan anmodning om data, der er gemt uden for anmodningens oprindelsesland og IKKE afvises eller omdirigeres, er ca 1 i forhold til det samlede antal offentlige og kommercielle kunder der anvender MS HSCC Online Services.

Baseret på disse rapporter, en forståelse af den principfaste proces og historikken for Microsofts beskyttelse af kundernes ret til privatlivsbeskyttelse, bør det være muligt at udføre en risikovurdering, der viser sandsynligheden og efterfølgende den samlede risiko, fra 3.lands Retshåndhævelsesanmodninger, at være absolut minimal til ikke-eksisterende.

Bemærk, at forskellen i antal mellem anmodninger om forbrugerkonti i forhold til virksomhedskonti også afspejler formelle retningslinjer fra det[61] amerikanske justitsministeriums afdeling for computerkriminalitet og intellektuel ejendomsret, som råder anklagere til at gå direkte til virksomheder, når de søger adgang til deres data, når det er praktisk muligt, og hvornår det ellers ikke ville bringe undersøgelsen i fare i stedet for at forsøge at gå gennem cloud-tjenesteudbydere.

61 https://aka.ms/USDoJSeekingEnterpriseData

Fra retningslinjerne:

> *"(...) Prosecutors should seek data directly from the enterprise, rather than its cloud-storage provider, if doing so will not compromise the investigation. (...) Working with counsel and the enterprise's information technology staff, law enforcement can identify and seek disclosure of relevant information. (...) If law enforcement has developed reasons to believe that the enterprise will be unwilling to comply or if the enterprise itself is principally devoted to criminal conduct, seeking disclosure directly from the cloud provider may be the only practical option. (...) Therefore, for any large enterprise, especially one held to high professional standards, it would be difficult for law enforcement to argue [(MSFT): before an independent U.S. judge] that specific facts exist that notification would compromise the investigation."*

Schems II-dommen nævner specifikt de amerikanske overvågningslove som begrundelse for at vurdere USA som et usikkert land med 3. Mens Microsoft har en lang historie med både[62] at

- udfordre anmodninger, de procedurer, 63 der vedrører sådanne anmodninger,
- som kategorisk fastslår, at ingen tredjepart har (eller nogensinde har haft) nogen uhindret adgang til hverken data- eller krypteringsnøgler,
- forbedring af de[64] beskyttelsesmekanismer, der anvendes i Microsoft HSCC-infrastrukturen,
- kræve reformer af[65] overvågningspraksis og ikke mindst
- kæmpet for at kunne skabe den bedst mulige gennemsigtighed med hensyn til[66] omfanget og resultaterne af sådanne anmodninger,

så er der ingen vej uden om, at fuld gennemsigtighed af hensyn til den nationale sikkerhed i øjeblikket ikke er juridisk mulig at give.

De rapporter, som Microsoft kan offentliggøre om disse anmodninger baseret på den amerikanske overvågningslovgivning, indeholder dog lige nok data til at kunne vurdere risiciene for en bestemt virksomhedskunde ved at få deres data til at være mål for en sådan anmodning. Som med anmodninger om retshåndhævelse er den samlede sandsynlighed (dermed risikoen) klart på et absolut minimum i en grad, hvor de fleste sikkerhedsfolk ville anse det for acceptabelt, hvis ikke ubetydeligt. De rapporter, som Microsoft lovligt kan offentliggøre, findes her: https://aka.ms/MSLERNSO.

Bemærk, at Microsofts processer og kontraktlige forpligtelser til at reagere på regeringens anmodninger også gælder for anmodninger vedrørende den nationale sikkerhed.

Microsoft interagerer dagligt med kunder og regeringer over hele verden og danner de internationale juridiske rammer for at løse disse kritiske problemer. Som en vejledning i dette arbejde har Microsoft udgivet seks principper, som også er baseret på løbende bestræbelser på at beskytte Microsoft-kunders data og forbedre deres privatliv:

"SEKS PRINCIPPER FOR INTERNATIONALE AFTALER OM RETSHÅNDHÆVELSE ADGANG TIL DATA": https://aka.ms/MS6dataaccessPrinciples.

Microsoft forpligter sig desuden kontraktligt til sit ansvar for denne håndtering som specifikt er defineret i Microsoft DPA[3] under "*Videregivelse af behandlede data",* på side 7, og som nævnt i introduktionen, efter Schrems II afgørelsen, yderligere til at udfordre enhver 3. parts anmodning om adgang til kunders data. Dette er tilføjet den standardiserede Microsoft Data Processing Addendum, som styrer al virksomhedsbrug af Microsoft HSCC Online Services.

62 https://aka.ms/MSSecrecyOrdersHistory
63 https://aka.ms/MSSecrecyOrders2021
64 https://aka.ms/MSProtectingDataFromGovernments
65 https://aka.ms/MSReformGovernmentSurveillance
66 https://aka.ms/MSSecrecyOrders

Q&A

36 Har leverandøren programmer eller procedurer for efterretningstjenesters indblik i platformen?

Ja, se svaret på spørgsmål 18 ovenfor.
I forbindelse med anvendelse af Public Cloud løsninger er der et forståeligt fokus på, hvilke internationale og nationale lovgivninger der kan regulere adgangen til kundedata – og ofte nævnes U.S. CLOUD Act. Desværre nævnes ofte en række alvorlige misforståelser omkring denne lovgivning, som måske til dels har rod i navngivningen, som kan skabe den fejlopfattelse at den specifikt omhandler Cloud Computing. CLOUD Act er en forkortelse for "Clarifying Lawful Overseas Use of Data Act" og som navnet indikerer, er formålet at sætte rammerne for hvorledes myndighederne i USA kan indgå aftaler med andre lande og regioner om, under hvilke forudsætninger data kan udveksles.

CLOUD Act giver således ingen yderligere bemyndigelse til at tilgå eller kræve data udleveret, men alene en ramme for hvorledes aftaler om udveksling kan indgås. UK og US indgik den første af sådanne aftaler som fx kan studeres her: https://aka.ms/ukuscloudactagreement og EU forhandler i øjeblikket en lignende aftale.

Disse aftaler regulerer således adgang til at kræve data udleveret både fra og til USA, således at også de ikke-amerikanske myndigheder kan aftale forudsætninger for, at efterforskningsenheder kan få adgang til data lagret i USA.

For en fuld beskrivelse af CLOUD Act, og hvorledes Microsoft forholder sig specifikt til denne del af lovgivningen, kan man med fordel studere dette notat: https://aka.ms/mscloudactguidance

Derudover eksisterer talrige eksempler på 3.parts vurderinger af CLOUD Act, som med fordel kan studeres. Fx denne artikel fra advokatfirmaet Hogan Lowells https://aka.ms/CloudActDM og denne analyse foretaget af analysefirmaet IDC: https://aka.ms/IDCCloudAct.

Q&A

37 I hvilket omfang kan virtuelle maskiner downloades og porteres til en anden leverandør?

I CSA CCM[23] afsnit "*Interoperability and Portability*" beskrives hvorledes API'er, standarder (fx for virtualisering for portability til 3. part) og services management understøtter dette.

Azure Migrate Dokumentation giver vejledning og værktøjer til at understøtte mange forskellige migreringer til Microsoft Azure; se https://aka.ms/AzureMigrateVM. Denne dokumentation indeholder vejledning i eksport af VM'er fra Azure: https://aka.ms/AzureExportVM

Q&A

38 Hvor bred er understøttelsen af programmerings-sprog, applikations-platforme etc.?

Microsoft tilbyder et omfattende sæt udviklingsværktøjer til enhver udvikler – ved hjælp af en platform eller et sprog – til at levere cloudprogrammer.

Udviklere kan vælge det ønskede sprog (ASP.NET; PYTHON; JAVA; JAVASCRIPT; PHP; C; C#, SWIFT etc.) og drage fordel af komplette integrerede udviklingsmiljøer (IDEs) og editorer med avancerede fejlfindingsfunktioner og indbygget Azure-support.

Det samme gør sig gældende for services, applikationsplatforme o.lign.: Kubernetes, Cosmos DB, MySQL SAP, Red Hat OpenShift, Xamarin etc.

Senest i efteråret 2019 annoncerede Microsoft, at også værktøjer til driftsovervågning og sikkerhed inkluderer mulighed for at integrere på tværs af ikke bare MS Cloud og on-premise-løsninger, men 3. partscloudløsninger.

Sikkerhed omkring mobilitet

Definition og dokumentation på Microsoft Cloud

Q&A **39** **Er anvendelse af mobile enheder tilladt i leverandørens lokationer?**

Nej.
Beskrives i CSA CCM[23] afsnit "*Mobile Security*".

Q&A **40** **Hvilke sikkerheds-løsninger specifikt rettet mod kundens brug af mobile klienter er tilgængelig på platformen?**

Microsoft-platformen indeholder en række løsninger til sikring af data, identiteter og enheder - også i mobile scenarier.

Samlet identitets-, enheds- og datasikkerhedshåndtering kan opnås gennem "Enterprise Mobility + Security"[67].

Såkaldt "Skygge-IT" indgår også i løsningen med en"Cloud Access Security Broker (CASB)[68]"-løsning kaldet "Cloud App Security", som giver mulighed for analyse af brugernes autoriserede såvel som uautoriserede anvendelse af cloudtjenester, og deraf følgende evt. risici for data og generel regulatorisk compliance.

Generelt anbefales det at lade mobile scenarier indgå i den generelle risikovurdering[69] og deraf træffe beslutning om, hvilke foranstaltninger må anses for at være tilstrækkelige for organisationen.

67 https://aka.ms/msemsdk
68 https://aka.ms/o365cas
69 https://aka.ms/msrisikomitigering

Håndtering af sikkerhedshændelser

Definition og dokumentation på Microsoft Cloud

Q&A **41** **Er leverandørens 'incident håndtering' klart beskrevet, inkl. evt. nødvendig notifikation af den dataansvarlige?**

Første element er Microsoft DPA[3], hvor ansvaret for '*Security Incident Notification*" beskrives i detaljer, inkl. notifikation af den dataansvarlige.

Andet element er selve hændelseshåndtering processen omkring:

a. Hvis der registreres en sikkerhedshændelse eller en overtrædelse, underretter Microsofts kundeservice og supportere kunderne ved at opdatere Dashboardet for tjenestetilstand. Kunder vil have adgang til Microsofts dedikerede supportmedarbejdere, der har dybt kendskab til tjenesten.

b. Microsoft leverer RTO-forpligtelser (se spørgsmål 26).

c. Efter hændelsen giver Microsoft en grundig Post-Incident Review Report (PIR), som indeholder:
- En hændelsesoversigt og hændelsestidslinje
- Bred kundepåvirkning og analyse af grundlæggende årsager
- Der træffes foranstaltninger til løbende forbedring

Hvis kunden påvirkes af en servicehændelse, deler Microsoft anmeldelsen efter hændelsen med dem. Adgang til en specifikt beskrivelse af Administration af sikkerhedshændelser i Azure Security Center her: https://aka.ms/MSSecurityIncidentManagement.

Læs flere detaljer om processen på: https://aka.ms/mscloudbreachnotification for Azure og Dynamics 365, på: https://aka.ms/o365breachnotification og for Office 365 og generelt for GDPR relaterede notifikationer på: https://aka.ms/MSGDPRBreachNotification.

Det tredje element, er et sæt af robuste procedurer og organisationer, der er implementeret som beskyttelse mod, håndtering af og ikke mindst rettidig opdagelse af sikkerhedshændelser og evt. brud på data (FIT ~ Fortrolighed, Integritet og Tilgængelighed):

d. 24-timers overvågning af fysisk hardware. Datacenteradgang er begrænset alle døgnets 24 timer efter jobfunktion, så kun vigtigt personale har adgang til kundeapplikationer og -tjenester. Fysisk adgangskontrol vha. flere godkendelses- og sikkerhedsprocesser, herunder badges og chipkort, biometriske scannere, lokale sikkerhedsofficerer, kontinuerlig videoovervågning, og to-faktor-autentificering.

e. "prevent, detect & mitigate breach"-strategi, som er en defensiv strategi, der har til formål at forudsige og forhindre et sikkerhedsbrud før, det sker. Dette indebærer løbende forbedringer af indbyggede sikkerhedsfunktioner, herunder port-scanning og afhjælpning, perimeter-sårbarhedsscanning, OS-rettelser til de seneste sikkerhedsopdateringer, DDOS- (distribueret Denial-of-Service) afsløring og forebyggelse på netværksniveau gennem trafikbegrænsning, og multi-faktor-autentificering for adgang til tjenesten. Desuden har Microsoft anti-malwarekontrol for at hjælpe med at undgå at skadelig software får uautoriseret adgang til kundedata.

Endelig foretages vedligehold af et sæt sikkerhedsregler for administreret kode for at hjælpe med at sikre, at der registreres information om afværgede trusler, før koden implementeres.

f. Microsoft beskæftiger nogle af verdens førende eksperter inden for cybersikkerhed, cloudcompliance og generel regulering.

Microsoft Digital Crime Unit[70] beskæftiger fx cybereksperter, hvoraf mange tidligere arbejdede for retshåndhævelse og bruger de mest avancerede værktøjer til at opdage, beskytte og reagere på cyberkriminelle. Sammen med sikkerhedseksperter fra hele Microsoft hjælper de med at beskytte, registrere og reagere 24/7 på sikkerhedstrusler mod Microsofts og kunders infrastruktur og onlinetjenester i realtid.

g. Risikovurdering gennemføres mindst én gang om året for at identificere interne og eksterne trusler og tilknyttede sårbarheder i cloudmiljøet. Oplysninger indsamles fra en lang række datakilder i Microsoft via interviews, workshops, dokumentationsgennemgang og analyse af empiriske data. Vurderingen følger en dokumenteret proces for at producere konsistente, gyldige og sammenlignelige resultater år for år.

h. Når det er muligt, erstattes menneskelig indgriben af en automatiseret, værktøjsbaseret proces, herunder rutinemæssige funktioner som installation, fejlfinding, diagnosticering og genstart af tjenester. Microsoft investerer fortsat i systemautomatisering, der hjælper med at identificere unormal og mistænkelig adfærd og reagere hurtigt for at afbøde sikkerhedsrisici. Microsoft udvikler løbende et yderst effektivt system til automatiseret patch-udrulning, der genererer og implementerer løsninger af problemer, der identificeres af overvågningssystemerne — alt sammen uden menneskelig indgriben. Dette forbedrer i høj grad sikkerheden og omstillingsparatheden af tjenesten.

i. 24-timersovervågning vedligeholdes af alle onlinetjenester, og alle brud på sikkerheden registreres. For brud på sikkerheden, som resulterer i ulovlig eller uautoriseret adgang til Microsofts udstyr, faciliteter eller kundedata, giver Microsoft meddelelse om berørte parter uden urimelig forsinkelse. Microsoft foretager en grundig gennemgang af alle oplysninger om sikkerhedshændelser. Læs evt. yderligere om Microsoft Sikkerhedsorganisationens arbejde her: https://news.microsoft.com/on-the-issues/topic/cybersecurity/

Specifikt for håndtering af notifikationer ifm. GDPR relevante sikkerhedshændelser, sikrer Microsoft som databehandler på Office 365, at kunderne bliver i stand til at opfylde GDPR's krav om underretning om brud som dataansvarlige. En nærmere beskrivelse af vore forpligtelser og deraf følgende investeringer kan findes her: https://aka.ms/o365GDPRDataBreach og https://aka.ms/mscloudbreachnotification.

Hændelseshåndtering indgår desuden også i CSA CCM[23] i afsnittet "*Security Incident Management, E-Discovery and Accountability*".

70 https://aka.ms/msdcu

Supply Chain Management, transparency, and accountability

Definition og dokumentation på Microsoft Cloud

Q&A **42** **Hvordan sikrer leverandøren hele leverancekæden på platformen i det tilfælde, at hardware, software eller operationelle procedurer håndteres eller leveres af 3. part?**

Beskrives i CSA CCM[23] afsnittet "*Supply Chain Management, Transparency and Accountability*".

Q&A **43** **Benyttes under-leverandører til opgaver, som kræver en risikovurdering? Og hvis ja, under hvilke konditioner benyttes disse under-leverandører og til hvad?**

Data Protection Addendum (DPA[3]) beskriver i afsnittene " *Meddelelse og kontrolfunktioner angående brug af Underdatabehandlere*", hvordan Microsoft håndterer underleverandører og bl.a. notificerer kunder om evt. ændringer i porteføljen af underleverandører.

På Services Trust Portalen (https://aka.ms/stp) vedligeholdes listen, inkl. hvilke services de leverer, deres hovedkontors lokation, i hvilken grad og under hvilke forudsætninger de *kan* have adgang til kundedata: https://aka.ms/mscloudsubprocessors.

NB! Som følge af Schrems II afgørelsen har Microsoft igangsat en udvidelse af listen over underleverandører, således at også den faktiske databehandlingslokation, vil indgå, ligesom de faktiske datastrømme i løbet af 2021 vil blive publiceret på Microsoft Cloud Trust Center[71]. Bemærk også at det som en del af EU Data Boundary projektet annonceret i Maj 2021, er Microsofts hensigt at sikre at al databehandling senest 1/1/2023 vil foregå indenfor EU/EØS og målsætningen at begrænse mængden af 'Contract Staff' underdatabehandlere gående mod 0. Læs mere om EU Data Boundary projektet i spørgsmål #2 ovenfor.

Konditionerne for brugen af underleverandører og dataadgang findes I databehandleraftalen (DPA) og korte læsevejledninger kan findes her: https://aka.ms/msclouddataaccess, for Azure Services her: https://aka.ms/AzureDataAccess og for O365 Services her: https://aka.ms/o365dataaccess.

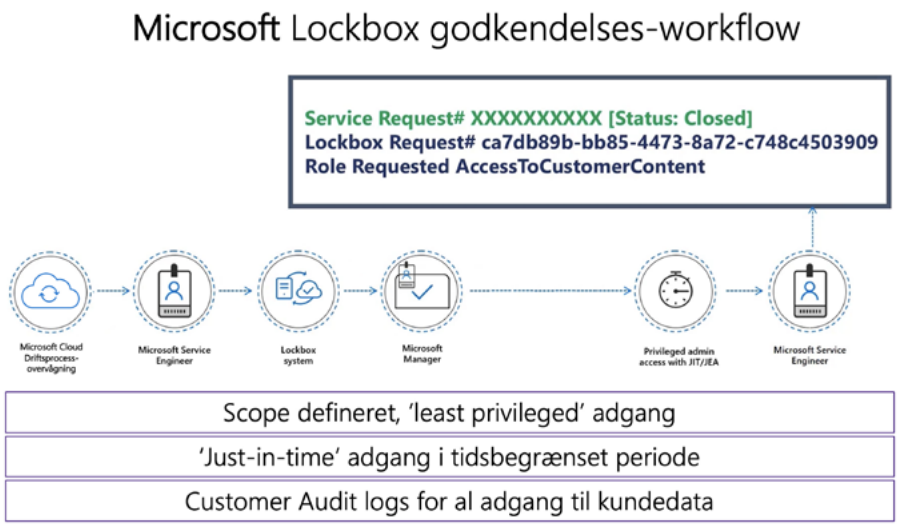
Det beskrives heri hvilke bl.a. krav Microsoft stiller til underleverandøren og at Microsoft er ansvarlig for at underleverandører lever op til alle krav, som er en del af Microsoft Online Services – Data Protection Addendum (incl GDPR).

Hverken Microsoft eller underleverandører har stående administrativ adgang til kundedata eller kundeløsninger. Microsoft Cloud opererer med såkaldt "Zero standing ADMIN" a.k.a. "Least Priviledge",

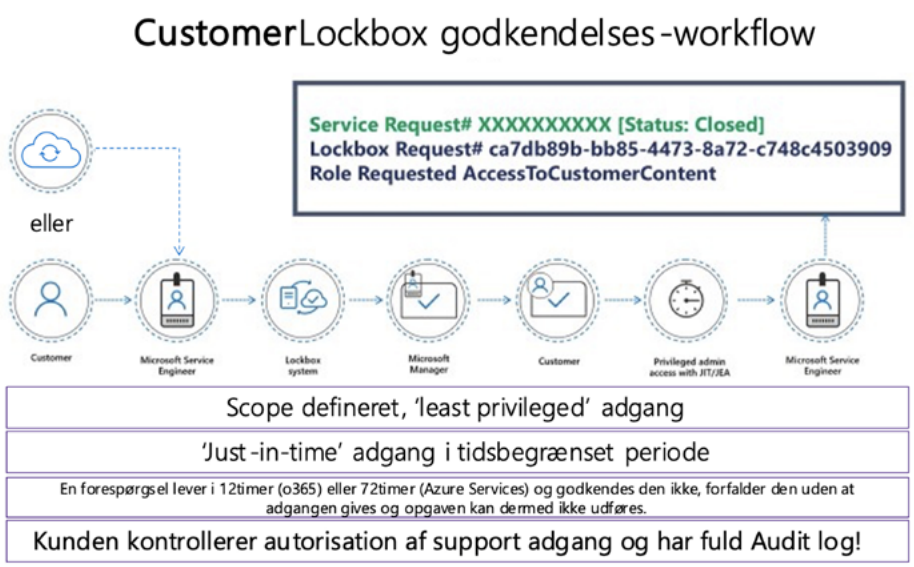
71 https://aka.ms/mscloudtrust

hvor administrativ adgang kontrolleres af en godkendelsesprocedure (kaldet "Lockbox") fx i tilfælde af at kunder instruerer Microsoft om at foretage en supportopgave, som kræver at medarbejderen får privilegier som *kan* give adgang til at kunne se kundedata. Tildelingen af administrativ adgang skal således igennem flere ledelseslag, time-boxes og fuld log etableres – og hvis kunden ønsker det, kan det ydermere inkludere endelig godkendelse hos kunden, gennem etablering af en udvidet "lockbox" proces, kaldet "Customer Lockbox".

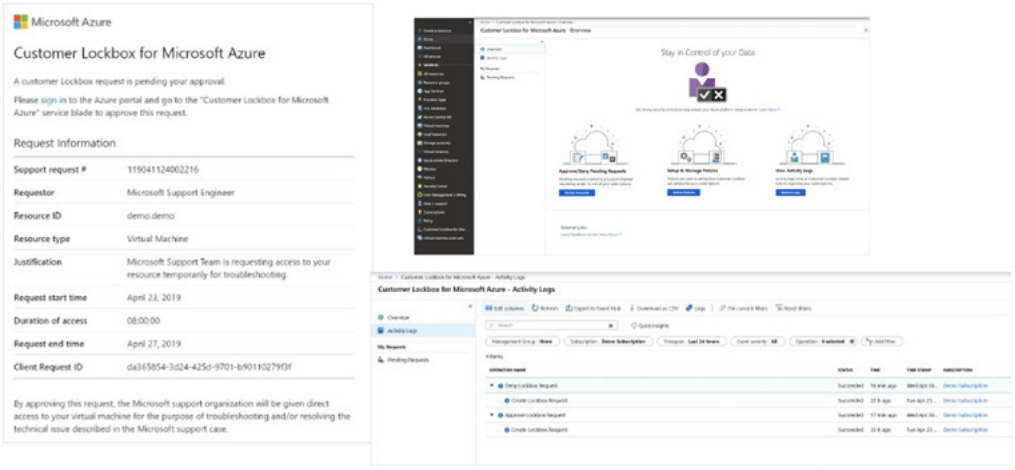
Nedenstående illustrerer de to procedurer:



Lockbox, kan udvides med kundens endelige godkendelse:



Som præsenterer kunden for valget om at få gennemført opgaven som beskrevet:



Læs evt. yderligere om "Customer Lockbox" kontrollerne …

- For Azure Services: https://aka.ms/msazurelockbox og
- For O365 her: https://aka.ms/o365CustomerLockbox

Emnet behandles yderligere i det følgende afsnit '06 / Spørgsmål til egen organisation', da det helt naturligt er et element, som kræver implementering hos den dataansvarlige.

Trussels- og sårbarhedshåndtering

Definition og dokumentation på Microsoft Cloud

Q&A **44** **Hvordan og hvor hurtigt/ofte håndterer leverandøren trusler og sårbarheder som malware, vira, patching etc.?**

Beskrives i CSA CCM[23] afsnittet "*Threat and Vulnerability Management*".

Information om Microsofts generelle løsninger til håndtering af denne type trusler hos den dataansvarlige er desuden tilgængelig her: https://aka.ms/mstrusselsstyring

Omfanget og udvalget af løsninger til håndtering af udefrakommende trusler er afhængigt af både den dataansvarliges risikovurdering (se evt. afsnittet '06 / Gode Spørgsmål til egen organisation') og hvilken Cloud Leverancemodel, der er tale om (se evt. indledningens afsnit '02 / Cloud Roller & fælles ansvar', hvor 'Shared Responsibility'-konceptet gennemgås.

Diverse og bredere, ikke domænespecifikt

Definition og dokumentation på Microsoft Cloud

Q&A **45** **I hvilken grad understøttes internationale sikkerheds-standarder?**

Microsoft Cloud tilbyder et unikt udgangspunkt, der kan hjælpe kunder med at opfylde deres forpligtelser i forbindelse med overholdelse af angivne standarder. Det er det bedste udgangspunkt for at beskytte følsomme og vigtige forretningsmæssige oplysninger.
Den samlede liste af standarder Microsoft Cloud er certificeret i kan findes her: https://aka.ms/mscloudcomplianceofferings

Udgangspunktet er helt naturligt ISO27001-certificering[72] med overbygninger som ISO27018[73] (PII in Cloud) og ISO27701[74] (Privacy Information Management System eller PIMS). Microsoft anmodede umiddelbart efter frigivelsen af ISO27701 i August 2019 om, at certificering kunne påbegyndes og kunne 13. januar, 2020 annoncere at certificeringen var gennemført. Bemærk her, at ISO27701 standarden introducerer en række nye kontroller for håndtering af "PIMS", som fordeler sig over både den dataansvarlige og databehandlere.

Den 20. maj, 2021 kunne Microsoft ydermere annoncere at Microsoft i sin drift af Online Services til fulde efterlever den nye EU Cloud Code of Conduct[75].

Q&A **46** **I hvilken grad understøttes internationale privacy-standarder?**

I 2014 blev ISO/IEC 27018:2014 vedtaget som et tillæg til ISO/IEC 27001 og blev dermed det første internationale '*Code of Practice*' for cloudprivacy. Baseret på EU's databeskyttelseslovgivning, giver den specifik vejledning til cloudtjenesteudbydere (CSPs), der fungerer som databehandlere af personligt identificerbare oplysninger (PII), om vurdering af risici og gennemførelse af state-of-the-art kontrol for at beskytte PII.

Microsoft var den første større udbyder af Hyper Scale Cloud Computing, som søgte og opnåede ISO27018-certificeringen.

72 https://aka.ms/mscloudiso
73 https://aka.ms/msiso27018
74 https://aka.ms/PIMS3pager
75 https://aka.ms/AzureEUCloudCoC

Mindst en gang om året revideres Microsoft Cloud Platform ift. at overholde ISO/IEC 27001 og ISO/IEC 27018 af et akkrediteret tredjeparts certificeringsorgan, der giver en uafhængig validering af, at gældende sikkerhedskontrol er på plads og fungerer effektivt.
Som led i denne overholdelsesverifikationsproces, validerer revisorerne i deres '*statement of applicability*', at Microsofts cloudtjenester og kommercielle tekniske supporttjenester har inkorporeret ISO/IEC 27018-kontrolelementer til beskyttelse af PII. For at forblive kompatibel skal Microsoft cloudtjenester være underlagt årlige anmeldelser fra tredjeparter.

Læs evt. flere detaljer på https://aka.ms/MSComplianceDokumentation og https://aka.ms/mscloudprivacystandards

Generelt overblik over certificeringsstatus på Microsoft Cloud platformen finder man her: https://aka.ms/mscloudcomplianceofferings

---

Q&A **47** **Hvorledes assisterer leverandøren den dataansvarlige i forbindelse med henvendelser fra datasubjekter?**

Som en del af Microsofts årelange commitment til fuld efterlevelse af GDPR, er processen og værktøjer beskrevet i detaljer her: https://aka.ms/GDPRDSR

En specifik proces er etableret for at behandling af datasubjekters anmodninger om data fra Microsoft Support og professional servicedata, som er beskrevet her: https://aka.ms/MPSDSR.

Q&A **48** **I hvilket omfang foretages dataoverførsel til lande udenfor EU/EØS, og hvilke foranstaltninger er til rådighed for den data-ansvarlige til at risikovurdere og dokumentere evt. overførsel?**

DPA[3] definerer i afsnittet *'Dataoverførsler og -placering'* i hvilke tilfælde, overførsel (i juridisk forstand) kan forekomme. Se evt. svaret på spørgsmål 2 om datalokation tidligere i dette dokument.

Den helt almindelige drift af Azure Core Online Services, kræver som udgangspunkt ikke privilegier som giver adgang til kundedata. Microsofts egne politikker fordrer at tildeles en sådan adgang, og kunden har tilføjet "Customer Lockbox" funktionen, kræver det kundens accept. Uanset om "Customer Lockbox" er tilføjet, vil alle tilfælde af sådanne ydelser på kundens tenant, være en del af kundens almindelige revisionslog og dermed kunne indgå i evt. nødvendig comliance dokumentation.

BEMÆRK!
Som beskrevet i indledningen af dette dokument, er den nuværende situation således, at der juridisk ikke er hindringer for, at man kan foretage behandling af både persondata og særlige persondata uden for EU/EØS.

To forudsætninger (beskrevet i det indledende afsnit om 'Tidligere juridiske udfordringer') skal opfyldes for, at denne behandling/overførsel kan ske, og begge er til fulde opfyldt på Microsoft Cloud platformen.

Der er i den Danske Databeskyttelseslov en særlig paragraf 3, stk.9 som gælder for et specifikt antal systemer af interesse for 'Nationens Sikkerhed' for hvilke man begrænset til at skulle drive selve serveren som løsningen kører på, i Danmark. Flere detaljer i appendix D om særlige nationale reguleringer.

Har man alligevel et ønske om at undgå eller yderligere kontrollere hvornår, hvorledes og under hvilke forudsætninger, data behandles udenfor EU/EØS, anbefaler Microsoft at den dataansvarlige overvejer følgende elementer af kontrol med overførsler til 3. lande:

- notér, om der er lovlighed i overførselsgrundlag ift. GDPR-artikel 45 og 46 og det Danske Datatilsyns vejledning om dataoverførsel til 3. lande (https://aka.ms/dkgdprvejledninger). Findes

i DPA[3] - Tillæg 2 – The Standard Contractual Clauses (Processors) (https://aka.ms/dpa)

- Vurdér, og følg løbende, Microsoft Cloud compliance niveau via gennemgang af fx revisionsrapporter og standardcertificeringer (https://aka.ms/stp). Af særlig interesse for danske organisationer er nok beskrivelsen af sikkerhedsforanstaltninger i MS DPA[3] - Appendix A – Sikkerhedsforanstaltninger. Adgang til specifikt ISO (https://aka.ms/mscloudiso) og SOC rapporter (https://aka.ms/mscloudsoc)
- vurdér, hvorledes der i Microsoft Cloud udøves kontrol med alle med potentiel dataadgang eller eksponering for kundedata:

  a. CSA CCM afsnittet "*Human Ressource*" (https://aka.ms/csamatrixazure og https://aka.ms/csamatrixo365).

  b. Microsoft Supplier Security and Privacy Assurance Program: https://aka.ms/mssspa.

  c. Læs evt. denne nærmere beskrivelse af hvorledes dataadgang håndteres i Microsoft Cloud: https://aka.ms/azuredataaccess & https://aka.ms/o365dataaccess.

  d. Endelig vurdér mulighederne for notifikation og håndtering af hændelser, som bl.a. beskrives her: https://aka.ms/MSCloudIncidentDescription & i CSA CCM afsnit "*Security Incident Management, E-Discovery and Accountability*".

- sæt notifikation på fx underleverandørliste, relevante certificeringer og revisionsrapporter: https://aka.ms/MSCloudMylibrary
- hvis man alene ønsker data opbevaret i EU, så vælg services, der har datalokation i EU, Nord- eller Vesteuropa: https://aka.ms/mscloudregions og https://aka.ms/mscloud datalocation
- lås organisationens adgang til alene at kunne anvende cloudservices, som opfylder egne krav til lokation, opsætning etc.: https://aka.ms/msazurepolicies og evt. https://aka.ms/msazureblueprints.
- tilføj Customer Lockbox, for endelig godkendelse af support med potentiel overførsel (Bemærk at for Azure Services er Customer Lockbox slået til pr default!): https://aka.ms/msazurelockbox og https://aka.ms/o365CustomerLockbox
- risikovurdér case by case, ift. supportlokation, opgave, datatype og sandsynlighed for risiko ved dataadgang (https://aka.ms/msriskoanalyse og se desuden gerne afsnittet '03 / Risikobaserede evalueringer' i indledningen, hvor yderligere inspiration er at finde) og tag efterfølgende beslutning om go/no go og re-direct til anden supporter/lokation. Inkludér vurdering af effekt på SLA op imod risikovurdering
- vurdér kryptering leveret af leverandøren (https://aka.ms/msazuredataatrest og https://aka.ms/mscloudkryptering), og overvej egen kryptering af data ift. risikovurdering (https://aka.ms/msazureencryption og https://aka.ms/mscloudcmkryptering)
- opsæt proces for log-gennemgang ift. risikovurdering: https://aka.ms/azurelogaudit og https://aka.ms/o365log

Krypter data i microsoft cloud, mens data er i brug!

Ved hjælp af 'Confidential Computing'[76] kan Microsoft fra foråret 2020, gøre det muligt for kunder fuldt ud at beskytte fortroligheden og integriteten af deres data, mens data er i brug.

Azure er den første Hyper Scale Public Cloud, der tilbyder en virtualiseringsinfrastruktur til fortrolig databehandling, gennem brug af hardwarebaserede miljøer til 'trusted execution' ('Trusted Execution Environments' ~TTE). For en dybdegående beskrivelse af konceptet kan anbefales at læse denne offentligt tilgængelige e-bog af Microsoft Azure CTO Mark Russinovich m.fl.: https://aka.ms/CCCatACM.

Azure Confidential Computing beskytter den på 'run-time', hvilket bringer Intel SGX og Virtualization Based Security til skyen. Confidential Computing er med til at sikre, at også når data er "i klar form" (ukrypterede) for effektiv behandling, er dataene fortsat beskyttet inde i en TEE

TEEs hjælper med at sikre, at ingen på ydersiden kan se data eller operationer inde i TEE, selv med et fejlfindings-program/debugger (selv ikke cloud administratorer eller datacenter operatører med fysisk adgang til serverne, kan få adgang til TEE-beskyttede data). Mens data behandles, gennemtvinger TEE disse beskyttelser mod visning og ændring, herunder adgang for Microsoft-medarbejdere. Dette er også med til at sikre, at kun autoriseret kode har adgang til data. Hvis koden ændres eller ændres, afvises handlingerne, og miljøet deaktiveres. For at bruge Confidential Computing vælger kunden DCsv-2series, som understøttes af den nyeste generation af Intel XEON E-2288G-processorer med SGX-teknologi.

Reelt fjerner dette således enhver bekymring om potentiel tredjeparts adgang til data i skyen og det gør det muligt at bruge cloud computing til højrisikodata (f.eks. følsomme IP- eller nationalsikkerhedsdata) og også deling af data på tværs af organisationer, f.eks. at træne Machine Learning-modeller uden at afsløre selve dataene ('Confidential Multi-party Computation'[77]).

Q&A **49** **Hvilke(n) Service Level Agreement(s) indgår?**

Oppetidsgarantien, Microsoft stiller, omfatter langt de fleste onlineservices, som defineret i det separate Service Level Agreement (SLA)-dokument: https://aka.ms/msosla

Hvis ikke Microsoft opnår og opretholder serviceniveauerne for hver tjeneste, som beskrevet i denne SLA, kan kunden være berettiget til at få fratrukket et beløb fra den månedlige tjenestegebyr/faktura. Vilkårene i SLA kan ikke ændres inden for den oprindelige løbetid af abonnementet. Hvis abonnementet fornyes, vil den version af SLA, som er aktuel på fornyelsestidspunktet, som udgangspunkt også gælde i hele fornyelsesperioden, og Microsoft giver besked mindst 90 dage i forvejen i forbindelse med væsentlige ændringer i SLA. For vilkår i øvrigt og specifikke oppetidsgarantier for hver enkelt online service, se ovennævnte dokument.

76 https://aka.ms/azurecc
77 https://aka.ms/cmpc

Q&A

50 Hvilke muligheder eksisterer for at tilføje yderligere supportaftaler?

Microsoft Unified Support[78] (MUS).

Forrester Research udgav i 2018 en rapport[79] som opsummerer værdien (såkaldt 'Total Economic Impact') af at tegne en MUS-aftale. Den positive effekt på mængden af nedetidshændelser, medarbejderproduktivitet og ikke mindst kompetenceløft, giver MUS-kunder en klar fordel i kvaliteten af deres cloudimplementering.

Microsoft Partner-netværk[80] tilbyder derudover kunder en portefølje af højt kvalificerede, certificerede partnere, som bl.a. kan supportere strategiudvikling, arkitektur, etablering/migrering, risikovurdering, drift og udvikling på Microsoft Cloud-platformene (Azure, M365 og Dynamics365).

Q&A

51 Hvilke værktøjer til 'procurement', 'deployment', 'migrering' og til sikring af compliant anvendelse er tilgængelige?

EKSISTERENDE KUNDECASES:'

Millioner af kunder i alle industrier verden over anvender i dag de mange tilgængelige Microsoft cloudservices – for inspiration kan kunder med fordel gå på opdagelse i de mange casebeskrivelser tilgængeligt online her: https://aka.ms/msazurecases

Overordnet giver portalen https://azure.microsoft.com/da-dk/industries/government/ hovedindgangen til et væld af informationer omkring løsninger specifikt rettet mod udvalgte industrier (fx Offentlig sektor[81]), teknisk og compliancedokumentation, udviklerværktøjer, træning[82] for både udviklere, driftsfolk og brugere etc..

Og tilsvarende materiale er tilgængeligt for både Office 365, Microsoft 365 og Dynamics 365.

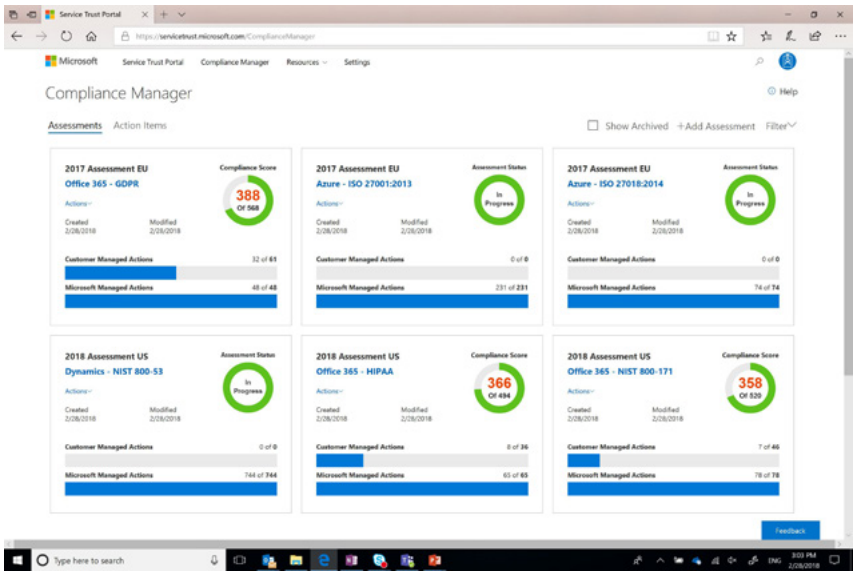
VURDERING AF CLOUD OMKOSTNINGSNIVEAU:

Microsoft konfigurations- og prisberegningsportal[83] giver kunder mulighed for at estimere og forecaste omkostninger ved ibrugtagning og drift af alle Cloud Services.

78 https://www.microsoft.com/da-dk/enterprise/services/unified-support-solutions
79 https://aka.ms/unifiedsupport/forrester_wp
80 https://www.microsoft.com/da-dk/solution-providers/home
81 https://azure.microsoft.com/da-dk/industries/government/
82 https://docs.microsoft.com/da-dk/learn/azure/
83 https://aka.ms/MSCloudTCO

VURDERING AF & STYRING AF COMPLIANCE OPGAVEN:

Microsoft Compliance Manager[84], der forenkler opgaven med at udføre risikovurderinger af Microsofts cloudtjenester. Compliance Manager kan bruges til at administrere organisationens complianceaktiviteter fra implementering til rapportering/fortegnelse. Compliance manager linker desuden til hele kataloget af Microsoft Cloud Standard-certificeringer og revisionsrapporter, helt ned på den enkelte sikkerhedskontrol/foranstaltning og giver dermed både kunden overblik over, hvilke kontroller Microsoft som databehandler har etableret og ift. gældende rådgivning eller valgt standard/regulering (GDPR, ISO27001, PCI, FedRAMP etc.) - rådgivning om hvilke tiltag, er at anse som Best Practice at implementere.

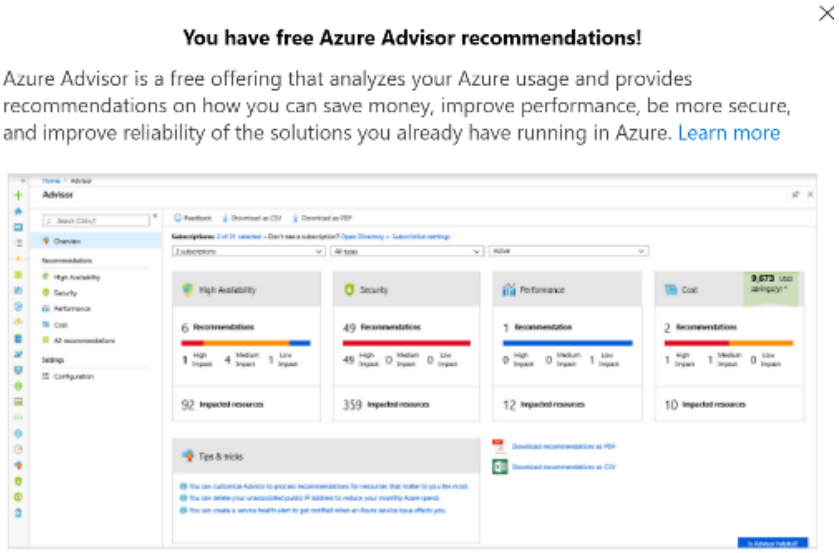


OPTIMERING AF CLOUD IMPLEMENTERING:

Azure Advisor[85] er en personlig cloudkonsulent, der hjælper dig med at følge bedste praksis for at optimere dine Azure-implementeringer. Den analyserer ressource-konfiguration og anvendelse og anbefaler derefter løsninger, der kan hjælpe med at forbedre omkostningseffektiviteten, ydeevnen, den høje tilgængelighed og generelle sikkerhed.

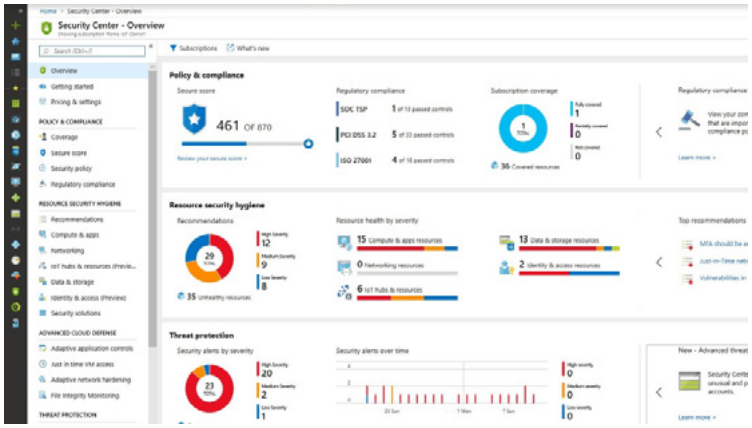
MONITORERING OG OPTIMERING AF SIKKERHED & COMPLIANCE:

Sikkerheds- og Compliance Dashboard i Security Center[86]



84 https://aka.ms/mscompliancemanager
85 https://aka.ms/msazureadvisor
86 https://aka.ms/azuresc

Med bl.a. Secure Score (se spørgsmål 10 i dette afsnit) giver dashboard hurtigt et overblik over cloudimplementeringens sikkerhed og Best Practice-anbefalinger til prioritering af yderligere tiltag.

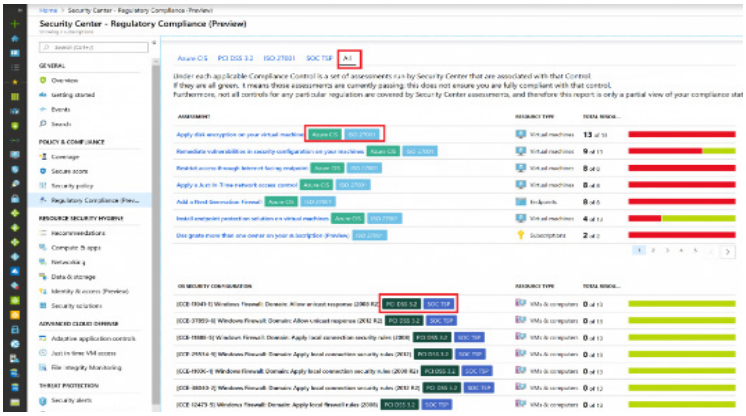


- For Azure Infrastructure as a service (IaaS) og platform as a service (PaaS)-ressourcer eksponerer Dashboardet almindeligt forekommende fejlkonfigurationer, som fx:
  - Manglende implementering af system-opdateringer på virtuelle maskiner (VM'er)
  - Unødig udsættelse for internettet via Public Facing-endpoints
  - Ikke-krypterede data i transit eller under lagring

- For M365 kan der fra et centralt dashboard i Microsoft 365-sikkerhedscenteret findes anbefalinger om beskyttelse mod trusler. Fx gennem monitorering og generel konfigurering af sikkerheden af deres Microsoft 365-identiteter, apps og enheder. Secure Score hjælper organisationer via:
  - Rapporter om den aktuelle tilstand af organisationens eksponering.
  - Forbedring deres sikkerhedskonfiguration gennem eksponering af fejlkonfigurationer, synlighed ift sårbarheder, mulige ekponeringer gennem brugeradfærd, generel vejledning og kontrol.
  - Sammenligninger med benchmarks, og fastlæggelse af KPI'er (Key Performance Indicators).

Organisationer får desuden adgang til robuste visualiseringer af målinger og tendenser, integration med andre Microsoft-produkter, scoresammenligning med lignende organisationer og meget mere. Scoren kan også afspejle, når tredjepartsløsninger har adresseret anbefalede handlinger.

Regulatorisk Compliance



M365 Compliance Center[87]giver detaljeret indsigt i den overordnede compliance88 baseret på løbende vurderinger af implementeringen. Security center analyserer risikofaktorer i et (potentielt også hybridt) cloud-miljø i henhold til bedste sikkerhedspraksis. Dashboardet viser status for alle vurderinger, der er relateret til en bestemt standard og/eller regulering. Hvis anbefalingerne89 og risikofaktorerne i konfigurationen reduceres, forbedres den overordnede compliance.

Security Center kan desuden integrere styring af sikkerhedsstillinger og trusselsbeskyttelse til andre cloudløsninger og VM'er i det lokale miljø, samt klargøre serveragenter til at køre i det lokale/on-premise-miljø. Ligeledes kan der oprettes forbindelse til eksisterende værktøjer og processer, såsom sikkerhedsoplysninger og hændelsesstyring (SIEM), eller integrere partner-sikkerhedsløsninger.

87 https://aka.ms/m365ComplianceCenter
88 https://aka.ms/MSComplianceDashboard
89 https://aka.ms/azureseccd

Azure Sentinel[90] tilføjer dynamikken og funktionalitet fra Online Services domænet til SIEM domænet, som historisk ofte har været svært integrerbart med kompleks signaludveksling mellem platforme og systemer. Sentinel tilføjer desuden orkestrering af automatiserede responsfunktioner og leverer intelligent sikkerhedsanalyse og trusselsintelligens i hele virksomheden, på tværs af platforme og miljøer. Det giver en enkelt løsning til advarselsregistrering, trusselssynlighed, proaktiv jagt på angribere, trusselshåndtering og respons.

- Indsamler data i skyskala på tværs af alle brugere, enheder, applikationer og infrastruktur, både lokalt og på tværs af cloud platforme.
- Registrer tidligere uopdagede trusler, og minimer både falske positive og minimerer falske negative ved hjælp af Microsofts Machine Learning analyser og best-in-class trusselsefterretninger.
- Undersøger trusler med kunstig intelligens, og jagt efter mistænkelige aktiviteter i stor skala, bl.a. gennem at anvende viden fra mange års arbejde med cybersikkerhed hos Microsoft globalt.
- Håndtér hændelser hurtigt med indbygget orkestrering og automatisering af almindelige opgaver, for at optimere brugen af ressourcer og hastigheden hvormed hændelser håndteres.

SIKRING AF OPTIMAL IMPLEMENTERING & KONFIGURATION:

Azure Blueprints[91] og **Azure Policy**[92]

Azure Blueprints er cloud-baserede ressourcer, der hjælper med a opbygge og lancere cloudbaserede programmer under hensyntagen ti den dataansvarliges regler og standarder. De omfatter:

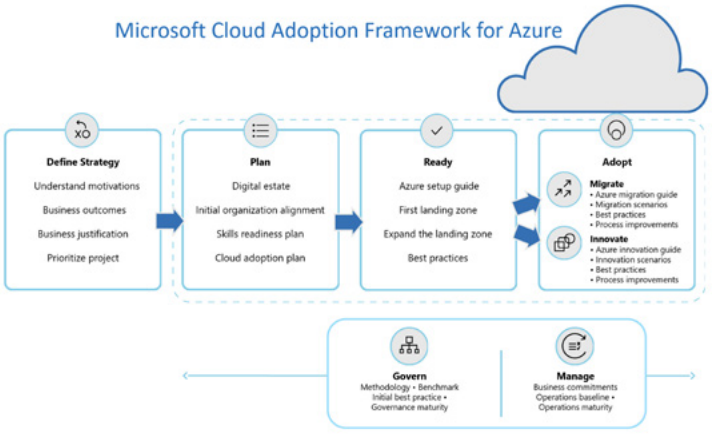
- Branchespecifikt overblik og vejledning
- Matrix for kundeansvar
- Referencearkitekturer med trusselsmodeller
- Kontrol af implementeringsmatricer
- Automatisering til implementering af referencearkitekturer

Azure Policy er en tjeneste i, som kan bruges til at oprette, tildele og administrere politikker. Disse politikker gennemtvinger valgte regler for de anvendte ressourcer i løsningen, så disse ressourcer overholder virksomhedsstandarder, compliancepolitikker og serviceniveauaftaler. Azure Policy opfylder dette behov ved at evaluere ressourcerne for manglende overholdelse af tildelte politikker. Fx kan en politik definere, at der kun tillades en bestemt SKU-størrelse på virtuelle maskiner i miljøet. Når denne politik er implementeret, evalueres nye og eksisterende ressourcer for overholdelse og dermed bringes til compliance/overensstemmelse med organisationens valgte politikker og standarder.

90 Service: https://aka.ms/AzureSentinel & Description: https://aka.ms/MSAzureSentinel
91 https://aka.ms/azureblueprints
92 https://aka.ms/msazurepolicies

VEJLEDNING TIL IBRUGTAGNING AF CLOUD:

Microsoft Cloud Adoption Framework[93] (CAF) er den samlende Microsoft-vejledning til adoption og implementering af Azure. CAF konsoliderer og deler bedste praksis fra Microsoft selv, partnere og kunder. Det giver kunderne et sæt værktøjer og vejledning, der hjælper med at forme teknologi, forretning og ressourcestrategier og dermed drive de ønskede forretningsmæssige resultater gennem cloudanvendelsen. Vejledningen er afstemt i en række faser i livscyklussen for cloud-ibrugtagning, hvilket sikrer nem adgang til den rette vejledning på det rigtige tidspunkt: Strategi, Planlægning, Klargøring, Migrering, Udvikling, Governance og Drift.



Azure Migration Service[94] hjælper med at vurdere, planlægge, overføre, optimere og administrere migrering til cloudmiljøet. Her er der adgang til alle nødvendige værktøjer og ressourcer[95] i det valgte tempo og uden unødvendige bekymringer.

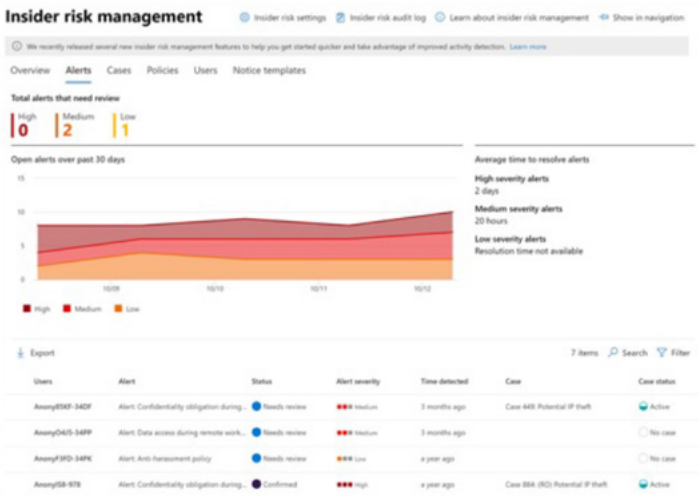
For partnere tilbyder Microsoft desuden den såkaldte Cloud Migration Playbook[96], som tilbyder assistance og rådgivning ifm. migrering af work loads eller modernisering af ældre programmer/løsninger til Microsoft Cloud. Lignende vejledninger findes for specifikke løsningsområder som AI, IoT, Operations, Cloud App udvikling etc.

Ovenstående funktioner og løsninger er gennemgående anvendelige på tværs af Microsoft Cloud-tjenesterne. For enkelte tjenester, findes yderligere værktøjer til at skabe overblik over og anbefale handlinger til at forbedre regulatorisk compliance og den generelle sikkerhed. Fx på Microsoft 365 platformen:

- Microsoft Secure Score: https://aka.ms/m365secscore
- Office 365 Security & Compliance Center: https://aka.ms/m365seccomplcenter.

Insider risk management

Microsoft 365 Insider Risk Management[97] hjælper med at minimere interne risici ved at give dig mulighed for at registrere, undersøge og håndtere ondsindede og utilsigtede aktiviteter i organisationen. Politikker for insider risici giver dig mulighed for at definere de typer risici, der skal identificeres og registreres i organisationen, herunder at handle i sager og eskalere sager til Microsoft Advanced eDiscovery, hvis det er nødvendigt. Risikoanalytikere i organisationen kan hurtigt træffe passende foranstaltninger for at sikre, at brugerne overholder organisationens overholdelsesstandarder.



93 https://aka.ms/MScaf
94 https://aka.ms/azuremigrering
95 https://aka.ms/azuremigrationtools
96 https://assets.microsoft.com/en-us/mpn-playbook-cloud-migration.pdf
97 https://aka.ms/M365InsiderRisk

Q&A

52 I hvilket omfang er der mulighed for etablering af hybrid-cloudscenarier?

Microsoft tilbyder hybrid-cloudløsninger med det formål, at kunder kan migrere til en 'multi-tenant'-cloud, som matcher deres funktions, ressources, arkitekturs og/eller compliances ønsker i det ønskede tempo.

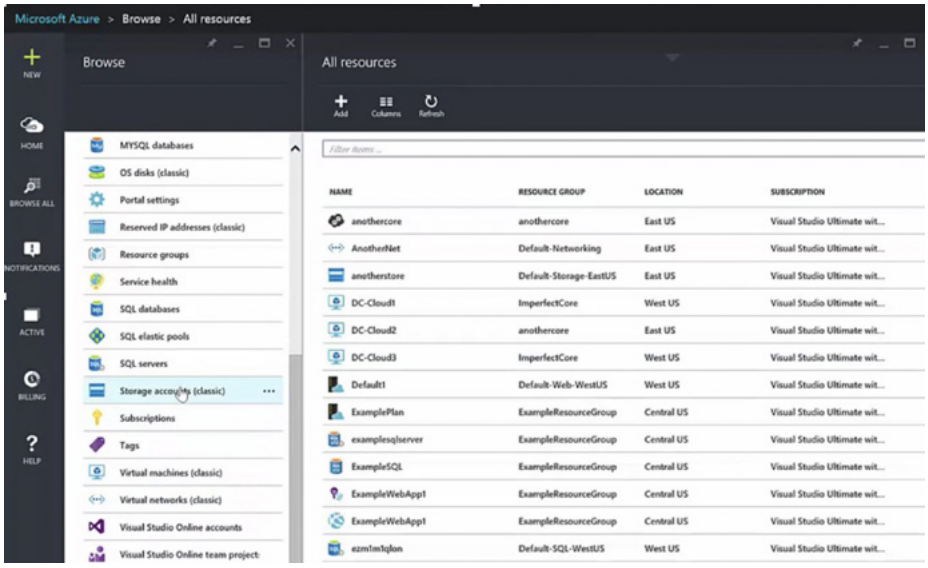
Dataklassificering kan fx afgøre brug af en arkitektur, som inkluderer delvis/udvalgt lagring og databehandling på on-premisehardware og -software.

En hybridinstallation som fx gennem anvendelse af **Office 365 connectors**[98], **Exchange Server hybrid**[99] og/eller **Azure AD Hybrid**[100] giver organisationer mulighed for at udvide den funktionsrige oplevelse og administrative kontrol, de har med deres eksisterende lokale miljø, til skyen. Og samtidig kan en hybrid installation fungere som et mellemliggende trin til at flytte helt til en Cloud Computing baseret løsning.

Gennem anvendelse af **Azure Stack**[101] kan også Azure-tjenesterne og -egenskaberne udvides til et miljø efter eget valg – fra datacentret til placeringer på grænseenheder (Edge Locations) og andre lokationer udenfor organisationens hovedkontor. Med Stack kan skabes, udrulles og driftes hybride løsninger på en ensartet måde på tværs af lokationsgrænser. Det giver fuld valgfrihed i - og fleksibilitet til - at håndtere den moderne organisations mange forskelligartede work loads.

Gennem **Azure Arc Service**[102] er der yderligere muligheder for at kontrollere og sikre de tiltagende komplekse miljøer som de hybride scenarier skaber. Scenarier som inkluderer flere data centre i lokale miljøer, flere clouds og ikke mindst Edge computing. Hvert miljø og hver cloud har ofte sit eget sæt af ukoblede managementværktøjer som man skal at konfigurere og anvende. Azure Arc simplificerer denne governance håndtering og muliggør een konsistent og samlet tilgang til administration af forskellige miljøer ved hjælp af robuste, etablerede funktioner (fx velkendte stærke Azure management muligheder for Linux såvel som Windows servers og Kubernetes clustere på enhver platform) som Azure Resource Manager, Microsoft Azure cloud shell, Azure Portal, API og Microsoft Azure Policy.

Med Azure Arc kan udviklere oprette 'containeriserede apps' med værktøjer, de selv vælger, og IT-teams kan sikre, at apps implementeres, konfigureres og administreres ensartet ved hjælp af GitOps-baseret Konfigurationsstyring. Endelig gør Azure Arc det endnu nemmere at implementere cloudsikkerhed på tværs af miljøer med centraliseret, rollebaseret adgangskontrol og sikkerhedspolitikker.



98 https://aka.ms/o365hybrid
99 https://aka.ms/exchangehybrid
100 https://aka.ms/aadhybrid
101 https://aka.ms/azurestackdk
102 https://aka.ms/azurearcservice

Derudover er en række integrationsfunktioner beskrevet bl.a. ifm. svaret på spørgsmål 51 ovenfor.

Det er dog ikke målet for dette whitepaper, at beskrive en udtømmende liste for hybride scenarier, men blot slå fast at det er muligt og en ofte benyttet strategi, specielt for organisationer med større og mere kompleks infrastruktur og løsningsportefølje.

Q&A

53 Hvor veletableret og mangfoldigt er økosystemet af organisationer, som allerede i dag anvender platformen?

Microsoft Cloud-platforme (Azure, Microsoft 365/Office 365 & Dynamics 365) anvendes i dag af millioner af kunder verden over. Omkring 90% af verdens største virksomheder anvender Microsoft Cloud.

For specifikke casebeskrivelser i alle relevante industrier/sektorer, se evt.
https://azure.microsoft.com/da-dk/overview/

Q&A

54 I hvilken grad understøttes Tilgængeligheds-standarden EN 301 549?

Microsoft lister her alle tilgængelige tilgængelighedsrapporter pr. produkt:
https://aka.ms/en301549conform

Generelt om Microsoft-understøttelse af tilgængelighed: https://aka.ms/MSCloudAccessibility

Udover EN301549 inkluderer Microsoft commitment til understøttelse af tilgængelighedsstandarder også U.S. Section 508 & WCAG 2.1 (ISO/IEC 40500).

Q&A

55 Hvordan er leverandørens beredskabsplaner beskrevet?

Gennem Microsoft Enterprise Business Continuity Management program[103] (EBCM) sikres, at der foreligger effektive, pålidelige, velafprøvede planer, systemer og processer, som kan fungere også under en udefrakommende indgribende begivenhed (fx pandemien kendt som 'COVID-19' i foråret 2020).

Microsoft Cloud kunder kan på Service Trust Portalen (STP) få adgang til en beskrivelse og en valideringsrapport af EBCM. I disse dokumenter opsummeres de foranstaltninger, Microsoft har truffet for at reagere på større eller betydelige forretningsforstyrrelser med en effektiv og omfattende forretningskontinuitet.

På Service Trust Portalen er validerings og test rapporter[104] tilgængelige sammen med Microsoft EBCM planer[105].

Ydermere vedligeholder Microsoft som inspiration for kunder som skal etablere eller videreudvikle eget Enterprise Business Continuity Management program, en række vejledninger om emnet: https://aka.ms/MSEBCMguidance

Endelig er Microsoft Online Services certificeret som ISO22301[106], hvilket er den primære anerkendte internationale standard for styring af forretningskontinuitet.

---

103 https://aka.ms/MSEBCM
104 https://aka.ms/EBCMTesting
105 https://aka.ms/MSEBCMValidation
106 https://aka.ms/msISO22301

Bæredygtighed

Bæredygtighed har som domæne normalt ikke været i fokus, når man ser på sikkerhed og compliance ift. cloud computing. Bæredygtighed fortjener dog separat behandling. Fx bør den eksponentielle udvidelse af cloudbaserede IT-infrastrukturer give anledning til at vurdere også de miljømæssige effekter, og det er således oplagt at lade dette punkt indgå, når man er i overvejelser om at tage cloud computing i anvendelse.

I marts 2021 offentliggjorde IDC en rapport[1] med den overordnede konklusion, at "*Cloud Computing kunne eliminere en milliard tons CO2-udledning i løbet af de næste fire år og muligvis mere.*", hvilket gør bæredygtighed til en indlysende faktor i enhver vurdering af, hvorfor og hvordan man gør brug af Hyper Scale Cloud Computing.

I denne hvidbog fokuseres i tabellen nedenfor alene på, hvilke informationer man kan afkræve cloudleverandøren. Ligeledes bør man vurdere disse informationer op imod en vurdering af og viden om de miljømæssige alternativomkostninger, som følger af **ikke** at tage cloud computing i anvendelse i en form for miljømæssig business-case.

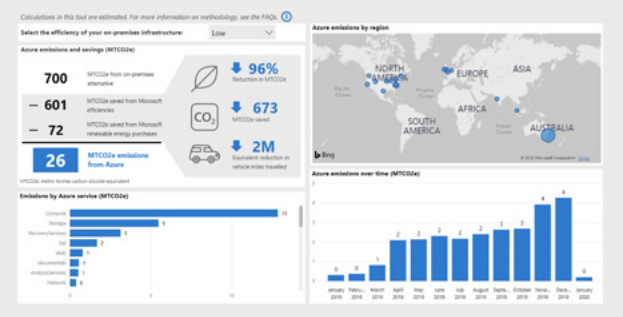
1 https://aka.ms/IDCCloudComputingReport2021

Bæredygtighed

Definition og dokumentation på Microsoft Cloud

SPØRGSMÅL

56 I hvor høj grad er cloud-platformen CO2-neutral?



Microsoft har siden 2009 på globalt plan målrettet arbejdet for at reducere vores carbonudledning og har siden 2012 opereret 100% carbon-neutralt.
Microsoft er også medunderskriver af klimaløftet[2].

Endelig er Microsoft forpligtet til at udvikle og stille værktøjer til rådighed for vores kunder og partnere for at hjælpe dem med at vurdere bæredygtighedseffekten af deres nuværende aktiviteter sammenlignet med virkningen af at bruge et Hyper Scale Cloud Computing-miljø, f.eks. Microsoft Azure. Det første sådant værktøj blev udgivet i 2020, kaldet Azure Carbon Calculator.
Dette værktøj hjælper med at beregne både de aktuelle og forventede CO2-emissioner, der er forbundet med Azure, besparelser ved at bruge Azure sammenlignet med det lokale miljø og omsætte emissionsbesparelser til faktiske forretningsgevinster. Værktøjet leverer også emissionsdata relateret til Azure, der er klar til at blive føjes til enhver rapport om virksomhedens bæredygtighed[3].

SPØRGSMÅL

57 Hvilke planer har leverandøren for evt. yderligere reduktion af CO2 (og anden GHG)-udledning?

Microsoft arbejder fortsat med ambitiøse målsætninger om konstant reduktion af negativ miljøpåvirkning og har således længe arbejdet frem mod målsætningen om yderligere 75% reduktion i vores carbonudledning inden 2030.

Igennem dette arbejder er omfanget og hastigheden af verdens miljøændringer blevet mere om mere åbenlyse og det er et problem, der vil få katastrofale konsekvenser for alle på kloden. Som de fleste CO2-neutrale virksomheder har Microsoft opnået CO2-neutralitet primært ved at investere i kompensationer som kvoter, der primært undgår emissioner i stedet for at fjerne kulstof, der allerede er udledt.

2 https://www.theclimatepledge.com/
3 https://aka.ms/CarbonCalculator

Det er derfor, vi skifter fokus. Kort sagt er neutral ikke nok til at imødekomme verdens behov og vi har besluttet at Microsoft skal gøre mere!
I starten af 2020, annoncerede[4] Microsoft derfor at vi som organisation i 2030

1. ikke alene vil være carbon-neutrale, men carbon-negative
2. vil være 'vand positive' og
3. vil opnå 'zero waste' i vores produktion og drift.

Udover disse 2030 mål, har Microsoft sat det mål, at vi senest i 2050 vil have elimineret vores totale historiske carbon-aftryk!

Microsoft commitments

i 2030 *i 2050*

Reducere samlet med 50% i Scope1-2-3 + producere overskud af vedvarende energi

Bevare, beskytte og genopfylde vandkilder + øge tilgængelighed

I direkte drift, produkter og indpakning. Fx. 'Circular Centers' for at genbruge og forny.

Udledt enten direkte eller via forbrug af electricitet siden 1975

Ydermere har Microsoft oprettet en Klima Innovations fond på $1mia, som skal fremskynde udviklingen af teknologier til fremme af kulstofreduktion og eliminering, såvel som adressere de bredere klimafokuserede områder.

Mange initiativer[5] er sat i gang for at opnå disse målsætninger, inklusiv vores fulde 'forsyningskæde' for dermed at adressere ikke blot Scope 1 og 2, men i høj grad også Scope 3, fx gennem vore partnere og underleverandører i alle dele af Microsofts mange forretningsområder.

4 https://aka.ms/MSSustainabilityPlan2020
5 https://aka.ms/MSSustainability

SPØRGSMÅL **58**

I hvor høj grad anvendes genanvendelige energiformer frem for fossile brændstoffer?

I 2018 nåede Microsoft målsætningen om, at 50% af den energi, som forbruges i vores cloudinfrastruktur, skal være vedvarende.

Dette mål er opnået bl.a. gennem investeringer i talrige projekter[6] til produktion af vedvarende energi.

I 2020 annoncerede Microsoft at alle nye Datacentre alene vil anvende genanvendelige energiformer.

SPØRGSMÅL **59**

Hvilke planer har leverandøren for evt. yderligere anvendelse a genanvendelige energiformer frem for fossile brændstoffer?

Målet er, at 60% skal komme fra vedvarende energikilder tidligt i 2020'erne, 70% i 2023 og 100% i 2025.

Vi vil ydermere senest i 2030 have elektrificeret hele vores globale flåde af køretøjer på vore 'campus'.

I 2019/2020 byggede Microsoft desuden de første europæiske datacentre (i Sverige[7]), som baseres 100% på vedvarende energi og annoncerede planer om at udvide vores commitment for TechFit4Europe[8], gennem at bygge yderligere Hyper Scale data centre i Italien[9], Polen, Finland, Østrig[10], Grækenland[11], Frankrig og i Danmark[12].

SPØRGSMÅL **60**

Hvilke 3. partscertificeringer eller audits har leverandøren på området?

I fravær af officielle kilder til certificering, er det nødvendigt at se efter andre kilder til information og vurdering på området.

Accenture udgav i 2010 en rapport[13] med vurdering af de bæredygtighedsmæssige fordele af at anvende cloud computing.

Og i maj 2018 udgave Microsoft en rapport[14], som i detaljer dokumenterer strategien for bæredygtighed på cloudplatformen. Rapporten er udarbejdet af det globale konsulentfirma WSP, som har ekspertise inden for miljø- og bæredygtighedsspørgsmål. WSP opstiller i rapporten deres model for den miljømæssige påvirkning ved at bruge Microsofts cloudtjenester i stedet for on-premise-miljøer. Til at foretage teknisk review af rapporten indgik Dr. Jonathan Koomey, der er ekspert i IT-bæredygtighed og Compute Energy fra Stanford Universitet.

6 https://aka.ms/MSCleanEnergy
7 https://aka.ms/MSSwedishDC
8 https://aka.ms/MSTechFit4Europe
9 https://aka.ms/DigitalLeapIt
10 https://aka.ms/DigitalLeapAu
11 https://aka.ms/DigitalLeapGr
12 https://aka.ms/DigitalLeapDenmark
13 Cloud Computing and Sustainability: The Environmental Benefits of Moving to the Cloud, Accenture, November 2010
14 Rapporten kan downloades her: https://aka.ms/mscloudsustainability

Og endelig udgav Microsoft i 2020 vores første årlige rapport[15] om miljømæssig bæredygtighed, hvor vi ser tilbage på, hvordan og hvorfor vi har indgået vores bæredygtighedsforpligtelser, oplysninger om disse forpligtelser, vores fremskridt til dato og vigtige erfaringer, vi har lært. Det er vores hensigt ikke kun at dele vores succeser, men også dele vores udfordringer, hvilket er grunden til, at vi i hvert afsnit af rapporten også har inkluderet yderligere oplysninger og ressourcer for at hjælpe andre med at fremskynde deres fremskridt i retning af en velstående, retfærdig og miljømæssigt stabil fremtid.[16]

SPØRGSMÅL

61 Udover cloudplatformen, har leverandøren så andre bæredygtighedselementer på øvrige dele af deres forretning?

Microsoft nåede globalt set carbon-neutralitet i 2012 på tværs af alle forretningsenheder.

Vand er blevet tilføjet til vores mangeårige forpligtelser om reduktion af carbon og generelt energiforbrug. Microsoft har således lanceret en ny "vandgenopfyldningsstrategi", hvor vi inden 2030 vil erstatte, hvad vores aktiviteter forbruger i vand-stressede regioner.

Derudover fokuseres på at bygge, renovere og drive vores mange bygninger og kontorer rundt om i verden på en måde, der mindsker vores påvirkning af miljøet:

- Mængden af carbon, der er forbundet med byggematerialerne i vores nye bygninger, reduceres med mindst 15% med et mål om at nå 30%.

- Bygninger drives uden anvendelse af fossile brændstoffer og på 100% carbon-fri elektricitet.

Verdens behov for bæredygtige løsninger stiger, og Microsoft arbejder derfor tæt sammen med kunder og partnere om at bruge digital teknologi og fx kunstig intelligens til at imødegå udfordringerne.

Disse projekter hjælper dem til at drive effektivitet, omdanne deres virksomheder og skabe egne løsninger for at skabe en mere bæredygtig planet. Vi kalder denne infusion af teknologi for "*Tech Intensity*[17]" og vi ser det bidrage til bæredygtig vækst rundt om i verden.

Virksomheder som **Ecolab**[18] og **Ørsted**[19] forbedrer vandbesparelser og effektiviteten af vedvarende energiløsninger gennem anvendelse af Microsoft Azure, IoT og kunstig intelligens.

Siemens Gamesa Renewable Energy[20] har implementeret en digital løsning kaldet "Hermes", hvor autonome droner inspicerer turbiner og bygger nu på dette med Azure Cognitive Services for at forbedre driften yderligere og hjælpe med at gøre vedvarende energi mere omkostningsmæssig overkommelig og i fremtiden endnu mere bæredygtig.

Endelig har Microsoft i 2017 grundlagt programmet '*AI for Earth*[21]', som har til formål at lokalisere og støtte data/teknologibaserede bæredygtighedsprojekter. Data kan fortælle os om planetens sundhed, herunder tilstanden af vores luft, vand, jord og dyreliv. Men der er brug for teknologiens hjælp til at fange denne enorme mængde data og omdanne den til handlingsrettede intelligens. Medio 2019 deltog 230 projekter[22] i programmet.

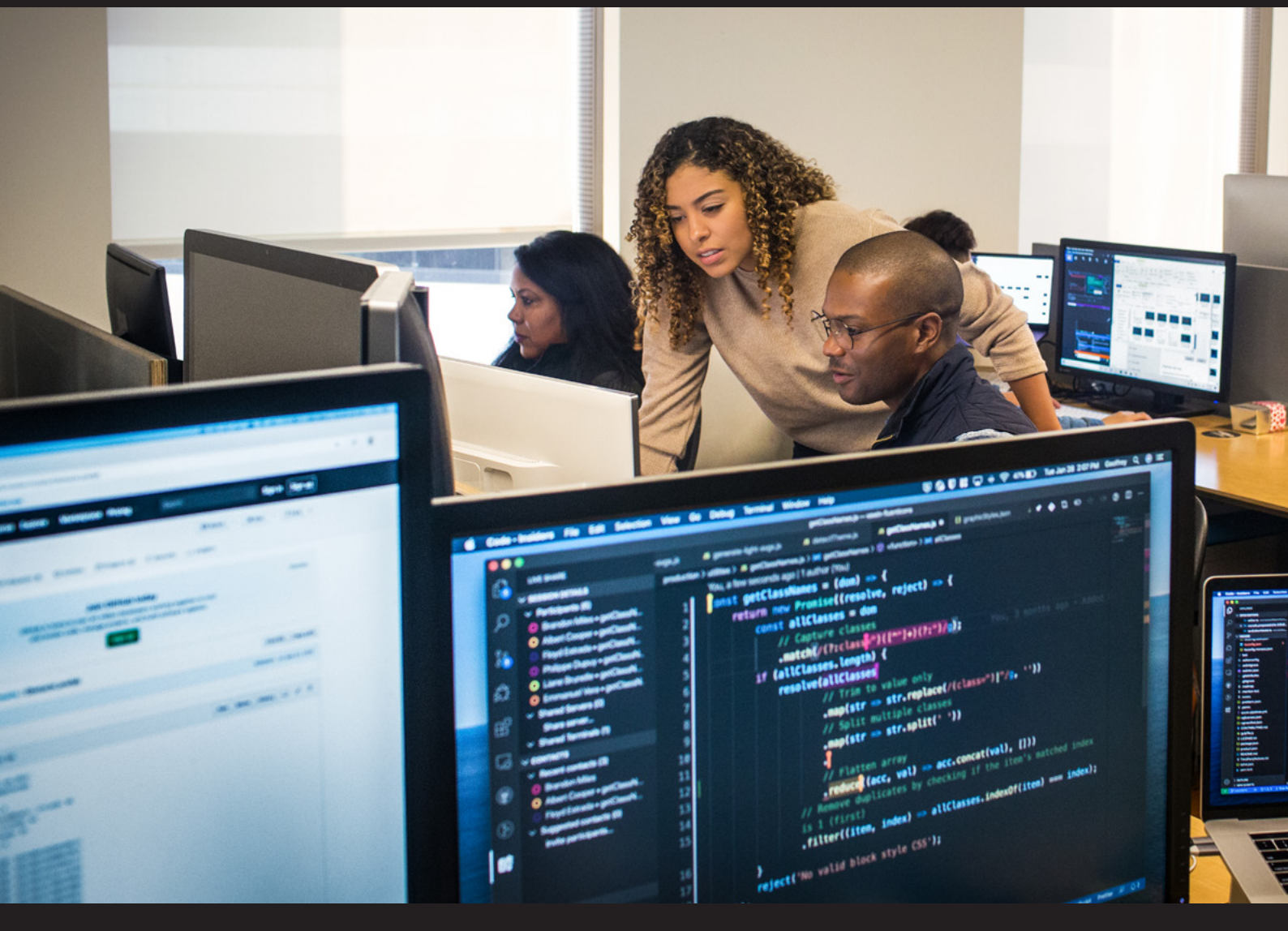
15 https://aka.ms/MSFTSustainabilityreport2020
16 https://aka.ms/MSFTsustainabilityreport2020
17 https://www.linkedin.com/pulse/necessity-tech-intensity-todays-digital-world-satya-nadella/
18 https://news.microsoft.com/transform/ecolab-and-microsoft-team-to-face-water-shortage-challenges/
19 https://news.microsoft.com/transform/videos/orsted-greener-world-offshore-wind-digital-technology/
20 https://news.microsoft.com/transform/siemens-gamesa-renewable-energy-wind-power-ai-cloud/
21 https://www.microsoft.com/en-us/ai/ai-for-earth
22 https://aka.ms/AIforEarthGrants

06 /

Gode spørgsmål til egen organisation

Som beskrevet ovenfor, vil enhver anvendelse af cloud computing stille krav ikke alene til leverandørens håndtering af platformen, men i nogen grad også til kunden, kundens konfiguration af cloud services og ikke mindst organisering, procesimplementering og dokumentation. Det er altså ikke umiddelbart nok at anvende fx Digitaliseringsstyrelsens tekniske minimumskrav[1], selvom de alle er udmærkede krav at stille både til leverandører og egen drift. På sidste side i dette dokument linkes til yderligere tekniske og governance-baserede anbefalinger fra den New Zealandske regering i forbindelse med etableringen af deres 'Cloud First'-strategi - de kan være et udmærket sted at søge yderligere inspiration.

1 https://aka.ms/DIGSTtekniskeminimumskrav



I tabellen nedenfor opstilles en ikke udtømmende liste spørgsmål til disse cloud governance-opgaver, som Microsoft mener en kunde som minimum bør overveje. Igen er de forsøgt grupperet efter en række hoveddomæner som fx Strategi, Økonomi, Compliance etc..

For at forenkle den overordnede proces begynder vi dette afsnit med en 8-trins Faststart-vejledning:

FASTSTART til EU Cloud Compliance & Governance

1. **Kend dine data** – hvilke kategorier af data du skal behandle i løsningen, og hvem der er de registrerede?
2. Dokumenter, hvilke **krav du beslutter, skal være** retningsgivende for dataindsamling, -lagring og -behandling.
   a. Lovgivningen er naturligvis GDPR, herunder relevante domme, præcedens, fortolkninger osv. (såsom EU-Domstolens Schrems II-afgørelse – se indledningen for en beskrivelse af denne) og enhver national databeskyttelseslov af relevans - hvilke krav stiller de for din behandlings- og sikkerhedskonfiguration,
   b. Sikkerhedspolitikker og politikker for beskyttelse af personlige oplysninger i din egen organisation, som kan føjes til kravene,
   c. Standarder som ISO27001, NIS osv.
3. Skab overblik over **datastrømme** i din indsamling, lagring og behandling af data – herunder flow i organisationen, f.eks. medarbejdernes adgang til og/eller kopiering af data på egne enheder.
4. **Specielt for cloud:**
   a. Forstå alle elementer i modellen for **Delt ansvar**, som beskrevet i indledningen '**02 / Cloud Roller** og **Delt ansvar**'.
   b. Tag aktiv stilling til de elementer i modellen, hvor ansvaret for implementeringen/udførelsen forbliver hos den dataansvarlige, og i hvilket omfang cloud-udbyderen stiller valgfrie værktøjer til rådighed for den dataansvarlige til at håndtere disse dele af ansvaret (dataklassifikation, RBAC osv.).
   c. Gør dig bekendt med detaljerne i HSCC-udbydernes sikkerhedsdokumentation – til Microsoft HSCC:
      i. MBSA, Produktvilkår og SLA'er – f.eks.
      ii. DPA, herunder EU's SCC og Microsoft's sikkerhedspolitikker – der f.eks. definerer databeskyttelsesbetingelser.
      iii. Microsoft Service Trust Portal og MyLibrary – leverer detaljeret compliance - revisionsdokumentation, som bør være kernen i HSCC kundens leverandørstyrings- & tilsyns-proces, hvilket giver mulighed for løbende revurderinger af sikkerheden og overholdelsen i databehandlingen.
      i. En oversigt over rollespecifik vejledning findes i 04/ Cloud Governance – bedste praksis ovenfor.

5. Foretag en **risikovurdering (**se 03/ Risikobaserede evalueringer)
   a. Find inspiration i fx. https://aka.ms/O365RisikoVurderinger & https://aka.ms/AzureRisikoVurdering.
   b. Husk at vurdere den faktiske sandsynlighed og konsekvens og inkludere allerede etablerede supplerende (formildende) foranstaltninger (f.eks. MS-sikkerhedspolitikker).
   c. Medtag **dataoverførsler** til tredjelande som en separat risiko (se eksempel i *'05/ Gode spørgsmål - til cloud-udbyderen'* – spørgsmål #2) og se 6step-vejledningen, der inkluderer:
      i. Kend dine overførsler – herunder hyppighed, mængde data, datatyper, formålet med overførslen, placering, overførselstype (fysisk, fjernadgang osv.) og andre omstændigheder såsom implementerede sikkerheds- og privatlivskontroller.
      ii. Sikre, at der er et retsgrundlag for overførslen – f.eks. EU's SCC
      iii. Vurdere, om der i alle tilfælde af overførsler ydes tilstrækkelig databeskyttelse i det land, hvortil overførslen finder sted/fra hvilket der foretages fjernadgang.
      iv. Hvis der ikke kan ydes tilstrækkelig databeskyttelse i alle tilfælde i det pågældende land, skal du identificere de "supplerende foranstaltninger", der skal indføres for i tilstrækkelig grad at reducere risikoen i forbindelse med overførsel til et acceptabelt niveau.
   d. Fastsætte en hyppighed for revurdering og definere, hvilke hændelser der skal indlede en ekstraordinær revurdering (f.eks. større ændringer i truslerne, x% stigning i mængden af data og/eller ændringer i datatyper, der behandles).

6. Vurdér, om der skal udføres en **Konsekvensanalyse (dPIA).**
   a. Vejledning om dette kan findes i GDPR-artikel 35 og fra en lang række europæiske databeskyttelsesmyndigheder, herunder det danske Datatilsyn[2].
   b. Dokumentation er tilgængelig på alle dele af Microsoft HSCC Online Services (se Spørgsmål #18 i dette afsnit).

7. Overvej eventuelt at gennemføre yderligere **foranstaltninger** for risici, der ikke anses for at være på et acceptabelt niveau for både risikovurderingen (herunder dataoverførselsscenarier) og konsekvensanalysen af databeskyttelse – disse omfatter for Microsoft HSCC tjenester f.eks. Compliance Score, Secure Score, Azure Policies, Azure blueprints, MFA, DKE, AKV osv., detaljer om, hvilke der alle kan findes i afsnittet '05/ Gode spørgsmål til cloud-udbyderen'.

8. Planlæg kompetenceopbygning, migrering, omkostningsstyring, strategi for HSCC udnyttelsegrad & udnyttelsesscenarier, exit strategi etc.

2 https://aka.ms/DKGDPRVejledninger

Strategi

Definition og dokumentation på Microsoft Cloud

SPØRGSMÅL **1** **Er der etableret en cloudstrategi, hvori organisationen klart definerer, i hvilket omfang, hvordan og til hvad, man ønsker at anvende cloudteknologier?**

Svarene på spørgsmål 51 i *'05/ Gode spørgsmål - til cloud-udbyderen'* ovenfor lister en række inspirationskilder og værktøjer, som kan assistere med udarbejdelsen af både den underliggende forretningsstrategi og de tilhørende afhængigheder af teknisk, juridisk eller sikkerhedsmæssig karakter.

SPØRGSMÅL **2** **Indeholder strategien målsætninger for anvendelsen af cloud – som fx at nå nye markeder, øge produktiviteten, reducere 'time-to-market' for systemændringer eller introduktion af nye systemer, reducere IT-vedligeholdelses-omkostninger, øge den samlede bæredygtighed, udvikle nye produkter, ydelser etc.?**

Koblingen til den overordnede forretningsstrategi er et væsentligt element for de kunder, som bringer cloud i anvendelse, ikke alene ud fra et omkostnings-besparelsesperspektiv, men som en mulighed for at udbytte de potentielle transformerende effekter, som cloud ofte kan bibringe organisationen. Dermed sikres en forankring, ikke blot i ledelsen, udvikling eller IT-afdelingen, men på tværs af organisationen til gavn for den maksimale udnyttelse.

For konkrete værktøjer, se igen svarene på spørgsmål 51 i *'05/ Gode spørgsmål - til cloud-udbyderen'* ovenfor.

Økonomi

Definition og dokumentation på Microsoft Cloud

SPØRGSMÅL **3** **Inkluderer den udarbejdede business case alternativ-omkostninger i tilfælde af en 'no-cloud'-beslutning og evt. afskrivning af eksisterende investeringer i udstyr, kompetencer etc. i tilfælde af en 'go-cloud'-beslutning?**

I det indledende afsnit om TCO og uddybningen i appendix til dette dokument, bliver vigtigheden af at bygge en TCO-model for organisationen gennemgået. Helt kort kan det her bemærkes at Microsoft stiller et TCO-værktøj til rådighed for denne opgave: https://aka.ms/MSCloudTCO

Elementerne, som udvælges til at indgå, og deres vægtning, er typisk individuelle fra organisation til organisation – dog er det af hensyn til specielt sikkerheden i løsningen og muligheden for på længere sigt at kunne understøtte organisationens behov for tidssvarende løsninger væsentligt at inkludere alternativomkostningerne, som organisationen står overfor, i fald man vælger IKKE at tage cloud computing i anvendelse. Dette er udgangspunktet for overhovedet at overveje anvendelsen, som ligger bag bl.a. de offentlige strategiske overvejelser, som præsenteres i appendix D.

SPØRGSMÅL **4** **Er der udarbejdet en plan for at sikre, at alle relevante niveauer af organisationen er klar til at realisere fordelene ved implementering af strategien?**

En lang række værktøjer til kompetenceopbygning (gratis og professionelle tilbud om træning og certificering) er tilgængelig for alle dele af Microsoft Cloud-platformen. Fx

Hyper Scale Cloud Computing Services:	**Træning, Learning Paths & Certificeringer:**
Microsoft Azure	https://docs.microsoft.com/en-us/learn/azure/ for eksempel: https://docs.microsoft.com/en-us/learn/paths/az-900-describe-cloud-concepts/
Microsoft 365 (incl. O365)	https://docs.microsoft.com/en-us/learn/m365 og Office Apps træning på: https://support.office.com/en-us/office-training-center
Microsoft Dynamics 365	https://docs.microsoft.com/en-us/learn/browse/?products=dynamics-365 – fx: https://docs.microsoft.com/en-us/learn/modules/introduction-dynamics-365

Oveni er en lang række partnerløsninger ligeledes i markedet for at sikre kompetenceopbygning for alle dele af organisationen, uanset om det gælder strategi, arkitektur, udvikling, drift, anvendelse eller andet.

Compliance

Definition og dokumentation på Microsoft Cloud

SPØRGSMÅL **5** **Hvorledes sammenlignes egne eksisterende eller nødvendige fremtidige implementeringer af sikkerheds- og privacy-kontroller i eksisterende infrastruktur og løsningsportefølje med det setup, som tilbydes (default) gennem anvendelsen af den vurderede cloudteknologi/platform?**

I afsnit '*05 / Spørgsmål til cloud-udbyderen*' ovenfor er gennemgået det relativt store katalog af sikkerheds- og privacy foranstaltninger som Microsoft implementerer, drifter og auditeres i. Disse udvikles konstant i takt med trusselsbilledet, regulatoriske krav og vores erfaring og tilbyder således altid en tidssvarende platform til cloudkunden.

Seneste mapping af fx Office 365 security kontroller (192 stk) op imod GDPR, kan findes på Service Trust Portalen her: https://aka.ms/o365GDPRAudited

Dette skal naturligvis holdes op imod en risikovurdering for den enkelte organisation, som udover eksterne forhold inkluderer organisationens viden om relevante dataklassifikationer, reguleringer og love samt eksisterende systemportefølje og brugsscenarier m.v..

Følgende kan være til yderligere hjælp med

- Risikoanalyse: https://aka.ms/msrisikoanalyse
- Risiko-mitigerende foranstaltninger: https://aka.ms/msrisikomitigering. Dette whitepaper beskriver desuden de tilgængelige værktøjer ifm. Mitigering af risici bl.a. i afsnittet '05/ Gode spørgsmål - til cloud-udbyderen' i spørgsmål #48 & #51.
- Cloud Compliance & sikkerhedsmæssigt overblik for Juridiske og Compliance professionelle: https://aka.ms/mscloudsecurity

SPØRGSMÅL **6** **Er der etableret et fuldt overblik over indgåede databehandleraftaler og dertilhørende kontrol med efterlevelse hos databehandleren?**

Det danske Datatilsyn har udgivet en række vejledninger[3] om bl.a. GDPR-compliance, som med fordel kan indgå i vurderingen.

Ligeledes har tilsynet udgivet en skabelon for Databehandleraftaler, (frivilligt at anvende) som inspiration til hvad en dækkende aftale skal indeholde. Microsoft har sammenlignet de krav skabelonen indeholder med

3 https://aka.ms/dkgdprvejledninger

Microsoft Online Services Terms og Microsoft Online Services – Data Protection Addendum, så man kan dokumentere[4] overholdelse.

Bemærk i øvrigt at både det Europæiske Databeskyttelseskontor, det Danske Datatilsyn og Cloud Vejledningen fra Digitaliseringsstyrelsen og Center for Cybersikkerhed, anerkender at de standardaftaler som fx cloud-udbydere tilbyder, af naturligt praktiske årsager ikke er til forhandling, men netop standardaftaler som er ens for alle kunder.

Alle pointerer de så ligeledes, at det påhviler den Dataansvarlige at sikre at standardaftalen overholder reguleringen og at etablere netop den rette governance for at kunne følge op på og føre kontrol med aftalernes overholdelse. Det er således nødvendigt at den Dataansvarlige har sat sig ind i detaljerne i databehandleraftalen – her påhviler det naturligvis Databehandlere at assistere den dataansvarlig og netop det er en stor del af grundlaget for og målet med dette whitepaper.

SPØRGSMÅL **7** **Er interne processer etableret ift. fx notifikationer fra databehandleren, governance omkring hvilke cloudservices, der kan tages i anvendelse, og hvorledes de services, som anvendes, konfigureres?**

Se svarene i afsnittet '*05/ Gode spørgsmål - til cloud-udbyderen*', bl.a. spørgsmål 2, 3, 10, 48 og 51.

SPØRGSMÅL **8** **Er der etableret en klar standard og proces for egen iterativ-risikovurdering, uanset valg af arkitektur, leverandør etc.?**

ISO27005-standarden for information security risk management er en mulighed, men den enkelte kunde bør naturligvis foretage den nødvendige udvælgelse og anvendelse af en model for risikovurdering.

Microsoft stiller bl.a. dette dokument og TrustCenter-dokumentation[5] til rådighed for gennemførelsen. På TrustCenter findes fx en 'Risk Assessment Checklist' baseret på NIST Cybersecurity Framework (CSF) og er specielt rettet mod organisationer i Financial Services Industrien, men som kan være til udmærket hjælp for kunder i alle typer af organisationer.

SPØRGSMÅL **9** **Er der en forståelse af det generelle instruksbegreb, generel godkendelse af underleverandører etc., som følger med anvendelsen af cloud computing?**

Instruksbegrebet defineres i den indgåede Databehandleraftale ved anvendelse af Microsoft Cloud Services (MS Online Services - Data Protection Addendum), specifikt i den engelske udgave afsnittet 'Nature of Data Processing' og i den danske udgave '*Databehandlingens art; ejerskab*' på side 6 og frem.

4 https://aka.ms/dpamapping
5 https://aka.ms/mscloudrisikovurdering

Organisering

Definition og dokumentation på Microsoft Cloud

SPØRGSMÅL **10** **Er det vurderet, hvorledes evt. nødvendige ændringer til organisationen skal implementeres?**

Microsoft Services og/eller Partnere kan assistere med planlægning og gennemførsel af denne implementering. Se evt. svar på spørgsmål 48 og 50 i afsnittet '*05/ Gode spørgsmål - til cloud-udbyderen*'.

SPØRGSMÅL **11** **Er der udarbejdet en plan for at sikre de nødvendige medarbejderkompetencer?**

Se svar i ovenstående spørgsmål 4 i dette afsnit '*06/ Gode spørgsmål til egen organisation*'.

SPØRGSMÅL **12** **Er ansvaret for fremtidig compliancevurdering af evt. nye services eller anvendelse af eksisterende services klart placeret og kommunikeret?**

Se svar i ovenstående spørgsmål 10 i dette afsnit og evt. svar på spørgsmål 48 i afsnittet: '*05/ Gode spørgsmål - til cloud-udbyderen*'.

Implementering, plan og proces

Definition og dokumentation på Microsoft Cloud

SPØRGSMÅL **13** **Med baggrund i risikovurderingens resultater, er der etableret klar stillingtagen til og plan for, hvorledes en risiko håndteres og evt. mitigeres organisatorisk eller teknisk?**

Til inspiration ifm. risikovurdering har Microsoft Danmark publiceret dette whitepaper, som i afsnittet '*03/ Risikobaserede evalueringer*' gennemgår nogle af de risici, som er væsentlige at vurdere ift. sandsynlighed/konsekvens og matchet med en række af tilgængelige – og ofte cloudbaserede – værktøjer: https://aka.ms/msrisikomitigering. I samme afsnit findes en række eksempler på virkelige (dog anonymiserede) risikovurderinger udført i 2020, som ydermere kan fungere som inspiration.

I afsnittet '*05/ Gode spørgsmål - til cloud-udbyderen*' kan findes detaljer om hvordan Microsoft som standard har implementeret en lang række juridiske, tekniske, organisatoriske og processuelle supplerende foranstaltninger for at mitigere identificerede risici. Det kan anbefales at søge efter en term/risiko i dette whitepaper (PDF), fx 'underdatabehandler', 'tredjelandsoverførsel', 'kryptering' eller lignende, og på den måde hurtigt finde frem til beskrivelsen af og dokumentationen for de implementerede kontroller som behandler/beskytter data.

Ligeledes vil en Microsoft Cloud kunde have adgang til værktøjer, som kan give yderligere vejledning om optimal konfiguration og brug af den pågældende cloud tjeneste. Se evt spørgsmål #51 i afsnittet i '*05/ Gode spørgsmål - til cloud-udbyderen*' for at finde detaljer om de enkelte værktøjer. Eksempler på værktøjer som kan nævnes her, er den såkaldte 'Secure Score' funktion, som yderligere kan vejlede specifikt ift. den eksisterende Cloud konfiguration og anvendelse: https://aka.ms/m365secscore og det så kaldte 'Insider Risk Management' værktøj, som giver mulighed for gennem etablering af en række politikker at opdage, undersøge og tage direkte action på risikabel adfærd i organisationen: https://aka.ms/m365irm

SPØRGSMÅL **14** **Er der etableret proces for evt. at føre register over datatyper, som uploades i cloudservices inkl. de valgte konfigurationer?**

Microsoft Cloud inkluderer en række værktøjer og inspirationskilder til at håndtere dataklassifikation:

- Data Classification Service: https://aka.ms/azuredataclass
- Azure Information Protection Service: https://aka.ms/o365aip
- Indbygget i Microsoft 365 og Office 365: https://aka.ms/m365dataclassification
- Overblik over MIOL[6]-anvendte dataklassifikationer i forbindelse med Microsofts egne data (NB! Ikke lig med de 'Data Definitioner' som anvendes i databehandleraftalen): https://aka.ms/msclouddataclassification[7]

6 MIOL = Microsoft Ireland Operations Limited, hvilket er den organisation som drifter Microsoft HSCC Online Services og dermed modpart på databehandleraftalen med kunder, som vælger at placere deres løsning/data i en Data center region indenfor EU/EØS.

7 Klassifikationen anvendt af MIOL er ikke et fuldstændigt match med 'Data Definitioner' som anvendes i DPA – for detaljer om dette se afsnittet "03/ Risikobaserede evalueringer"

SPØRGSMÅL **15** **Er der etableret en revisionsproces - via gennemgang af uvildig revisors revisionsrapport af cloudservicen - med henblik på kontinuerligt at sikre cloudleverandørens fortsatte evne til at implementere de kontraktuelt lovede tekniske og organisatoriske foranstaltninger?**

Kunder har via Service Trust Portalen[8] adgang til alle revisionsrapporter og anden dokumentation af relevans for denne proces, uanset hvilke dele af Microsoft Cloud Platformen, der anvendes.

SPØRGSMÅL **16** **Er der etableret proces for at håndtere evt. notifikationer om ændringer i leverandørens dokumentation, brug af underleverandører etc.? Og inkluderer den alle relevante data, som fx anvendt overførselsgrundlag i tilfælde af 3. landes overførsel?**

Se svarene i afsnittet *'05/ Gode spørgsmål - til cloud-udbyderen', bl.a. spørgsmål 3, 10, 48 og 51, for anbefalinger om værktøjer som kan assistere med denne opgave.*

SPØRGSMÅL **17** **Er der etableret en proces for og/eller nødvendige teknologiske midler til løbende at foretage risikovurderinger og dokumentation af regulatorisk compliance og efterlevelse af beskrevne interne politikker?**

Se svarene i '*05/ Gode spørgsmål - til cloud-udbyderen',* bl.a. spørgsmål 2, 3, 10, 48 og 51.

Microsoft anbefaler at den dataansvarlige, bl.a. etablerer en proces for løbende som minimum at gennemføre funktionerne

- 'Secure Score' https://aka.ms/m365secscore og
- 'Compliance Score' https://aka.ms/MSComplianceScore

Da begge disse funktioner, giver adgang til Microsofts umiddelbare vurdering af sikkerheds- og compliancemæssige eksponering og ikke mindst vejledning om hvilke tiltag der med fordel kunne gennemføres, med sigte på at høje sikkerhed og/eller compliance.

En del af denne vejledning vil naturligvis omhandle de større opgaver som håndtering af 'Privileged Accesss Mananagement', Retention politikker etc..

Dokumentation og vejledning kan naturligvis også findes online uden brug af de nævnte 'score' funktioner, fx

- 'Privileged Access Management': https://aka.ms/o365PAM,
- 'Retention politikker': https://aka.ms/mscloudretentionpolicies,
- 'Forsvar mod Ransomware': https://aka.ms/azureransomwaredefense og https://aka.ms/m365ransomwaredefense,
- 'Establish Zero Trust Model': https://aka.ms/mszerotrust
- Etc.

8 https://aka.ms/stp

SPØRGSMÅL **18** **Er alle nødvendige informationer til rådighed for at kunne gennemføre 'Konsekvensanalyser' (DPIA) for de dataflows hvor det er relevant?**

GDPR artikel 35 definerer i hvilke tilfælde det er påkrævet, at gennemføre en Konsekvensanalyse.

Der findes flere modeller for hvorledes en sådan analyse kan gennemføres og endda en ISO standard (https://www.iso.org/standard/62289.html) ISO/IEC 27134, men det kan klart anbefales at gennemlæse det Danske Datatilsyns specifikke vejledning om emnet: https://www.datatilsynet.dk/media/6563/konsekvensanalyse.pdf

Microsoft assisterer naturligvis med relevante informationer for udarbejdelsen af konsekvensanalyser i forbindelse med anvendelsen af HSCC Online Services:

- Overordnet: https://aka.ms/MSCloudDPIA
- For Microsoft Azure: https://aka.ms/azuredpia
- For Microsoft Office 365: https://aka.ms/o365dpia
- For Microsoft Dynamics 365: https://aka.ms/d365dpia
- For Microsoft Professional Services: https://aka.ms/mpsdpia

Yderligere perspektivering

Ønsker man yderligere inspiration til rammeværktøjer, gode spørgsmål etc. ifm. vurdering af anvendelsen af cloud computing, kan det nævnes, at den New Zealandske Offentlige sektor, i 2019 har lanceret deres såkaldte 'Cloud First'-strategi.

I den forbindelse har man udarbejdet en portefølje af skabeloner og standarder, som skal assistere organisationerne og give dem det bedste grundlag for at vælge cloud computing der, hvor det giver mening, er sikkert og med fuldt privacy.

Strategien og dertilhørende værktøjer kan findes her:
https://www.digital.govt.nz/standards-and-guidance/technology-and-architecture/cloud-services/

Derudover publicerede Ponemon Institute [1] i Januar 2020, resultaterne af en undersøgelse af

- organisationers bevæggrunde for ibrugtagning af Cloud Computing,
- hvilke udfordringer de typisk har ift. sikkerhed og privatlivsbeskyttelse og
- hvilke skridt de så har taget for at håndtere Cloud compliance.

Rapporten opsummerer endelig top 10 anbefalinger om hvordan man kan forbedre compliance og databeskyttelse i sin anvendelse af Cloud computing.

1 https://aka.ms/mscloudponemon

Anerkendelser

Forfatter
Ole Kjeldsen, Teknologi- & Sikkerhedsdirektør, Microsoft Danmark ApS.
https://aka.ms/olekbio

Martin Vliem, National Sikkerhedsdirektør, Microsoft Holland
https://www.linkedin.com/in/mvliem

Bidragsydere
Jørgen Hallengren, Cloud Strategy & Compliance Advisor, Microsoft Denmark ApS
Sandra Elvin, National Security Officer, Microsoft Sweden
Daniel Akenine, National Technology Officer, Microsoft Sweden
Juha Karppinen, National Technology Officer, Microsoft Finland
Dave Sloan, Chief Technology Officer, Global Market Development,
Worldwide Public Sector, Microsoft

Forretningsansvarlige
Maria Damborg Hald, Direktør for Public Sector, Microsoft Danmark ApS
Peter Quarfort Skov, Direktør for Enterprise Commercial, Microsoft Danmark ApS

Microsoft

Disclaimer

Denne hvidbog indeholder alene information, som repræsenterer, hvordan Microsoft Danmark ApS anskuer Cloud Governance på publikationsdatoen.

Fordi Microsoft konstant må reagere på ændringer i markedsvilkår og lovgivning, kan informationen ikke udgøre et endeligt commitment fra Microsoft og er således kun beregnet til orientering og overordnet vejledning. Indholdet må ikke bruges som juridisk rådgivning eller til at afgøre, hvordan GDPR eller andre lignende krav kan være gældende for dig og din organisation. Vi anbefaler i stedet, at du i samarbejde med en juridisk kvalificeret person diskuterer GDPR og anden relevant lovgivning specifikt for din organisation, og hvordan du bedst kan sikre overholdelse af den.

Vi anbefaler ligeledes, at du i samarbejde med Microsoft og/eller en af vores mange partnere diskuterer, hvordan du og din organisation bedst kan implementere den relevante Cloud Governance, cloudstrategi og ikke mindst forretningsplan for evt. anvendelse af cloud.

For at få adgang til den seneste version af hvidbogen, kontakt forfatteren eller hent den på her: **https://aka.ms/MSCloudGovernance**

Publiceret Juni 2021
Version 4.0
© 2021 Microsoft. Alle rettigheder forbeholdes

07 /
Appendix

Appendix / **Indhold**

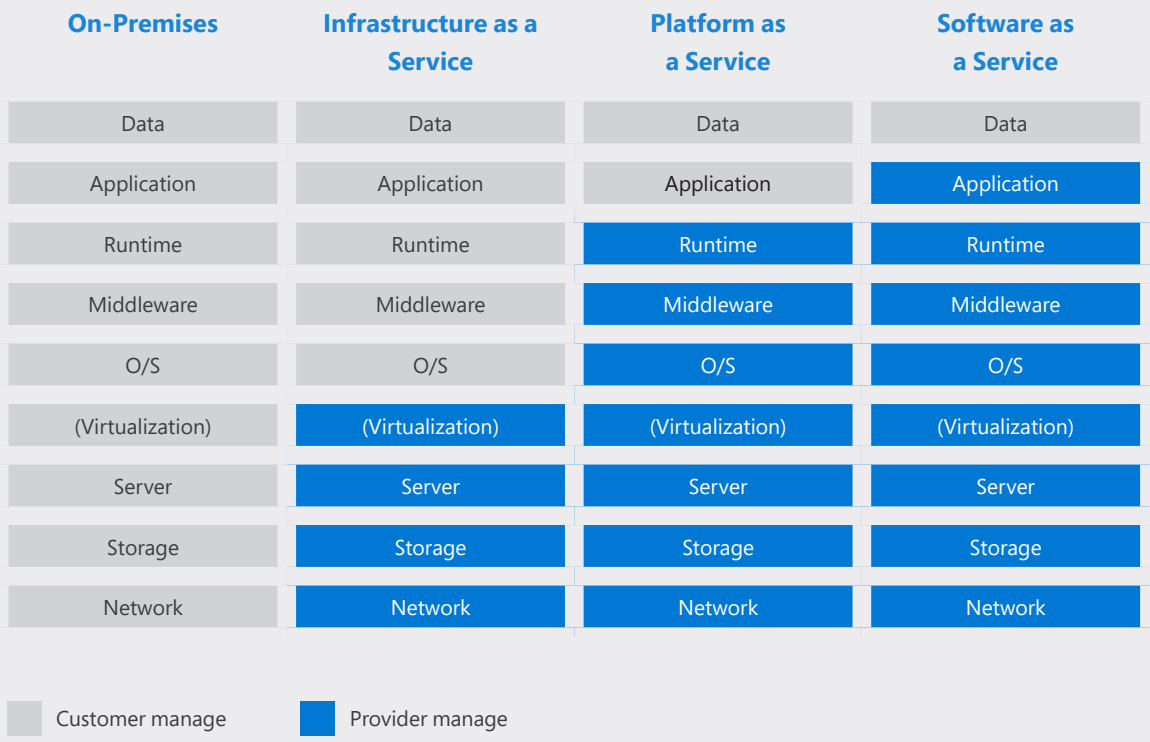
A. Cloud computing – service- og leverancemodeller

Service- og leverancemodeller beskriver, hvordan man får sin cloud leveret og med hvilken opgave- og ansvarsfordeling mellem kunde og leverandør.

Servicemodeller

Et væsentligt element i cloud computing er de servicemodeller, der danner grundlag for cloud governance (Infrastructure as a Service, Platform as a Service og Software as a Service) og den afledte ansvarsfordeling. I modellen nedenfor illustreres det, hvordan opgavesplittet mellem leverandør og kunde varierer afhængigt af servicemodel.

Ansvarsfordelingen[1] afspejler foruden governance en allokering af risici og omkostninger mellem kunden og leverandør.



1 Yderligere detaljer om ansvarsfordelingen kan findes i dette whitepaper: https://aka.ms/MSSharedResponsibility

Leverancemodeller

Et andet væsentligt element i NIST-definitionen af cloud computing er de såkaldte 'Leverancemodeller' (Private, Community, Public & Hybrid).

Denne hvidbog behandler alene den såkaldte 'Public Cloud', hvilket reelt er defineret ved såkaldt 'Hyper scale Cloud', fordi det til forskel fra Private, Community og Hybrid understøtter én af de TCO-mæssigt og sikkerhedsmæssigt væsentligste kendetegn: *Den fulde fleksible skalerbarhed uden begrænsninger defineret i cloud-anvenderens egen organisation.*

Under de tre øvrige leverancemodeller er man fortsat afhængig af egen it og it-sikkerhedsafdelingens kompetencer, adgang til ressourcer til opbygning af nødvendig kapacitet og modstandsdygtighed over for trusler. Dermed afskærer man sig reelt fra en række af de dimensioner af omkostningsreduktion og øget servicekvalitet, som udgør en væsentlig del af TCO-beregningen ved valget af cloud computing (som gennemgået i afsnittet Total Cost of Ownership).

Der kan være flere scenarier, hvor man i sin vurdering af cloud computing bør overveje andre leverance-modeller end Hyper Scale Cloud. Ønsker man fx, at dele af de data, som indgår i løsningen, alene lagres i egen infrastruktur, kan Hybrid Cloud modellen med fordel anvendes.

Valget af løsning påvirker naturligvis den samlede vurdering (TCO).

Ovenfor er illustreret Microsoft Cloud Services nuværende 60 datalagringsregioner[2]

Microsoft Azure og leverancemodeller - Global tilstedeværelse

Denne globale tilstedeværelse giver både adgang til trussels- og hændelsesinformation, som kommer alle cloud-anvendere til umiddelbar gavn i form af større og hurtigere modstandsdygtighed, fordi man får adgang til de mest avancerede sikkerhedskompetencer og teknologisk innovation. Funktioner som fx Advanced Threat Protection[3] og Web Application Firewall[4], der er bygget ovenpå det meget store omfang af trusselsintelligens, giver adgang til højt sofistikerede modeller til at identificere og mitigere tidligere ukendt malware. Det giver kunden adgang til analyse af og værktøjer til yderligere at indarbejde informations- og databeskyttelse i løsningen.

Hybrid Cloud i Microsoft Azure

Ved ønsket om Hybrid Cloud kan fx benyttes en såkaldt 'Azure Stack'[5]-løsning, som kombinerer Hyper Scale Cloud med on-premises-løsninger. Man udvider med dette setup det lokale miljø med adgang til Azure Hyper Scale Cloud-tjenester og -funktionalitet og kan udvikle, udrulle og håndtere hybride cloudprogrammer og grænseprogrammer på en ensartet måde.

Man kan også konfigurere 'Azure Stack' til at være en egen autonom cloud, der ingen forbindelse har, eller kun har en delvis forbindelse til internettet og Hyper Scale Cloud. Uanset hvilken løsning man vælger, er det alene cloudkunden, som kontrollerer adgangen til data.

2 https://azure.microsoft.com/da-dk/global-infrastructure/regions/
3 https://aka.ms/o365atp
4 https://aka.ms/azurewaf
5 https://aka.ms/azurestackdk

B. Total Cost of Ownership sammenligning

Elementer i en TCO-beregning

Uanset om organisationen allerede anvender eller er i færd med at flytte til cloud computing, er forståelse af kompleksiteten ved at bygge og vedligeholde en skalerbar, sikker og omkostningseffektiv infrastruktur afgørende for at kunne lægge en strategi for, hvorledes man bedst udnytter de muligheder, cloud computing tilbyder. En TCO-baseret vurdering involverer som minimum følgende fire dimensioner:

- Omkostninger til etablering, drift og sikring
- Fleksibilitet og innovation
- Skalering til fortsat data-eksplosion
- Optimal udnyttelse af energi (bæredygtighed)

Ad. 1: Omkostninger forbundet med at:

- sikre, at organisationen kan holde trit med det hurtige tempo, hvormed infrastrukturen ændrer sig
- sikre, at organisationen kan administrere det store antal leverandører og processer til køling strøm, netværk, elektricitet, fail over, disaster recovery etc. (cloud computing-leverandøren håndterer denne kompleksitet for cloudkunden)
- den enorme investering og risiko er involveret i opbygningen og vedligeholdelsen af et robust og tidssvarende fysisk og logisk sikkerhedsprogram

Ad. 2: Fleksibilitet og innovation – organisationen skal:

- være i stand til at implementere programmer og tjenester overalt i verden
- etablere fleksibiliteten ved at have flere muligheder for forretningskontinuitet
- overholde skiftende krav til dataopbevaring og datasikkerhed
- have muligheden for at skalere op, ud og tilbage – alt efter behov
- hurtigt kunne udnytte nye tjenester og teknisk innovativ

Ad. 3: Data-eksplosion – løsningen skal kunne håndtere, at:

- mængden af data, der skal administreres, vokser med hidtil uset hastighed
- den dataansvarlige ikke alene skal sikre, at der er hardware- og netværkskapacitet til at understøtte behovet, men også sikre, at data er umiddelbart tilgængelige

Ad. 4: Bæredygtighed:

- Mange organisationer har målsætninger om bæredygtighed som skal opfyldes, og anvendelse af cloud computing kan resultere i en betydelig reduktion i energiforbruget. Analyser6 viser, at man opnår op til en 90% reduktion i emissionerne ved at flytte fra det lokale miljø til Microsoft cloud computing

6 https://aka.ms/mscloudsustainability

Gevinster ved cloud computing

Gevinsterne ved cloud computing omfatter såkaldte "hårde omkostningsbesparelser" (it-afdelinger, som kan undgå at skulle investere i servere, lagringskapacitet, fysiske lokationer, køling etc.).

Herudover bør organisationer inddrage gevinsterne ved at have en kortere og mere effektiv reaktion ved understøttelse af forretningsmæssige forandringer.

Cloud computing-løsninger muliggør umiddelbar tilgang til tidssvarende og fuldt skalerbar kapacitet samtidig med, at det daglige ansvar for vedligeholdelse af IT-driften kan flyttes til en erfaren cloududbyder. Dette inkluderer bl.a. håndtering af datalagring, "disaster recovery", fysisk sikkerhed, patch-håndtering og generel tilgængelighed etc.. Hermed frigøres tid og ressourcer i en organisations interne it-team til at fokusere på mere strategiske initiativer, dvs. til understøttelse af organisationens nuværende og fremtidige forretningsmæssige behov.

Andre fordele ved cloudbaserede løsninger i forhold til en typisk on-premise-løsning omfatter bl.a. følgende:

- **Complianceværktøjer** stiller leverandøren oftest til rådighed således, at cloudkunden har adgang til data, dokumentation og funktioner, som forenkler complianceopgaven

- **Bæredygtigheden** af at anvende cloud computing kan ofte bidrage positivt til organisationens miljømæssige aftryk – særligt hvis leverandøren har fokus på netop bæredygtighed – fordi stordrifts-fordelene muliggør, at cloudleverandøren kan innovere og implementere grønnere løsninger både inden for GHG[7], vand og generelt energiforbrug og brug af genanvendelige energiformer

- **Modstandsdygtigheden** over for nye, hastigt udviklende cybertrusler er ofte langt højere i en cloud-løsning af den simple årsag, at leverandøren har det som en kerneydelse konstant at monitorere det globale trusselsbillede og professionelt håndtere behov for patching, nye processer, forsvarsteknologier etc.. Cloudkunden 'låner' således leverandørens sikkerhedskompetencer, reaktionshastighed og overblik over det til enhver tid gældende globale trusselsbillede og får hermed større og hurtigere modstandsdygtighed, end hvis de selv skulle holde sig på omgangshøjde med globale trusler og nødvendige modtræk

7 GHG ~ Green House Gases

Alternativomkostninger

Enhver TCO-beregning skal opstilles ud fra en specifik model for, hvorledes de enkelte omkostninger vægter for den pågældende organisation. Fx varierer prioriteringen af bæredygtighed fra organisation til organisation. Uanset den valgte model, bør en sammenligning af cloud computing med en traditionel on-premise-platform indeholde de reelle omkostninger forbundet med de ressourcer, organisationen bruger internt.

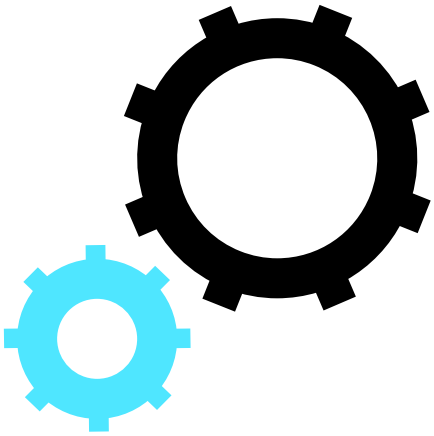
Disse omkostninger omfatter bl.a. følgende:

- Nødvendige fremtidige investeringer i og implementeringen af hardware, så organisationen også på sigt effektivt kan drifte nuværende og evt. kommende løsninger
- Løbende udgifter til drift af datacenter – køling, energi, plads
- Vedligehold, afskrivninger, support på og opgradering af både hardware og software
- Patching, logning og overvågning af infrastrukturs modstandsdygtighed over for aktuelle cybertrusler og generelle sikkerhedsrisici, samt beredskab overfor hændelser (disaster recovery, backup etc.)
- Nedetid eller omkostning ved at have en 'hot failover' kørende som matcher et cloud setup

Omkostninger til datamigrering

Ligesom der eksisterer en række omkostningsmæssige fordele ved at migrere til cloud computing eller bygge og anvende en ny løsning, udgør datamigrering en ny omkostning, der skal medregnes ved vurdering af cloud computing.

De fleste leverandører af cloud computing stiller værktøjer til rådighed,8 som hjælper med denne opgave og holder omkostningen på et relativt lavt niveau.



8 https://aka.ms/MScloudMigration

Øvrige omkostninger

En række øvrige omkostninger bør vægtes og beregnes ved vurdering af cloud computing over for traditionel on-premise-drift:

- Generelle miljø- og bæredygtighedsomkostninger
- Kompetenceopbygning og vedligehold af samme
- Tilpasning af løsninger/applikationer
- Bruger- og enhedshåndtering, identitets- og adgangskontrol, arkivering og dataklassifikation
- Enhedshåndtering og håndhævelse af organisationens sikkerhedspolitikker over for brugerne

Beregningen af de samlede omkostninger forbundet med valget af en IKT-løsning er komplekst, men nødvendigt for at opnå et sammenligneligt grundlag for at træffe en informeret beslutning.

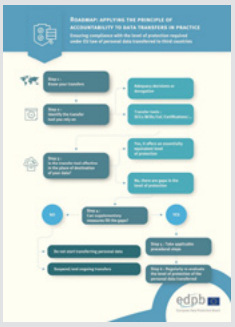
Det er således ikke tilstrækkeligt at vurdere en løsning alene ud fra indkøbspris samt hardware- og softwareomkostninger. Beregningen bør inkludere løbende træning af medarbejdere, husleje, elektricitet, samlet bæredygtighed, audits, it-sikkerhed og backup-løsninger etc.. Endelig skal den kvantificerede forretningsværdi, der kan skabes ved, at organisationen henlægger hele eller dele af sin infrastruktur til cloud computing, ligeledes indgå.

C. Det Europæiske Databeskyttelsesråds udkast til anbefalinger af 11. november, 2020

I modsætning til alle elementer i lovgivningen om behandling af personoplysninger (se afsnit 01, Juridiske rammer for cloud computing, tidligere i dette dokument) anlægger EDPB i deres udkast til supplerende foranstaltninger en no-risk-baseret tilgang, hvor alle dataoverførsler uanset omstændighederne, juridiske, tekniske eller organisatoriske foranstaltninger skal betragtes som utilstrækkelige og dermed enhver restrisiko som uacceptabel.

Denne konflikt eller ubalance mellem lovgivningen og udkastet fra EDPB er emnet for mange webinarer og drøftelser rundt omkring i EU/EØS-landene i tiden efter november 2020. Det har efterladt mange EU/EØS-organisationer – i nogle tilfælde organisationer der allerede har taget Hyper Scale Cloud Computing-løsninger til sig - i tvivl om der er en vej frem mod compliant brug af HSCC, og hvis der er, hvilke skridt de skal tage nu og her.

- *Pressemeddelelse* https://edps.europa.eu/press-publications/press-news/press-releases/2021/edpb-edps-adopt-joint-opinions-new-sets-sccs_en.
- *Seks trins vejledning* (se Q&A afsnit 1 og 2, hvor eksempler på anvendelse af de seks trin i vejledningen kan findes).
- EU's SCC v2 er stærk og sikrer harmonisering.
- opfordrer til yderligere klarhed omkring dataoverførsler.
- Anmoder om ændringer for at sikre den "praktiske anvendelighed" & "tilsvarende beskyttelse".
- Anmoder om ad hoc-foranstaltninger og med reference til EDPBs udkast til "supplerende foranstaltninger" – "i visse tilfælde"!
- De endelige henstillinger kan ændres "på grundlag af resultatet af den offentlige høring"!
- Ingen dato for, hvornår de endelige anbefalinger vil blive offentliggjort – den aktuelle forventning er før 1. juli, 2021 og EDPB har planlagt møde 19. maj, 2021, hvor bl.a. dataoverførsler og supplerende foranstaltninger er på agenda'en. Endnu er det naturligvis uvist hvad det møde leder frem til.



- Microsoft har i sagens natur ikke eksplicit foretaget tilretninger til disse anbefalinger – fordi
  1. der er tale om draft og EDPB har givet klar besked om at de endelige anbefalinger vil være modificeret,
  2. der i draft anlægges en no-risk-baseret tilgang, hvilket bryder med al gældende lovgivning og har store praktiske og økonomiske konsekvenser for enhver organisation som følger draft vejledningerne – uanset om de anvender cloud computing eller ej,
  3. der ikke i draft tages hensyn eller stilling til de allerede implementerede supplerende foranstaltninger og endelig
  4. har Microsoft allerede som følge af CJEU Schrems II afgørelsen to gange opdateret databehandleraftalen for at imødekomme afgørelsen (se afsnit 01 i dette dokument) og igangsat produktion af yderligere gennemsigtigheds dokumentation, for dermed at assistere kunder som anvender Microsoft HSCC online services, med fortsat at kunne dokumentere fuld compliance med lovgivning og tilstrækkelig databeskyttelse.

Der kan naturligvis fortsat opstå situationer, hvor det er påkrævet at Microsoft opdaterer de juridiske aftaler og/eller dokumentation, for at imødekomme myndigheders fortolkninger og afgørelser – skulle det opstå vil Microsoft annoncere via bl.a. dette link: https://aka.ms/MSEUDataBlog

OPDATERING Juni 2021!

EDPB udgav 21. juni 2021 de endelige anbefalinger, som nu både inkluderer i vid udstrækning en risiko-baseret tilgang, men også umiddelbart samtidig en række scenarier, som kan medføre en kompleks og ressource-krævende række af vurderinger og dokumentationsopgaver for den dataansvarlige.

Microsoft analyserer i skrivende stund (5 dage efter EDPBs udgivelse) stadig de konkrete elementer af anbefalingerne og vil naturligvis forsøge at assistere HSCC kunder med de forestående opgaver, og derigennem sikre at de dataansvarlige fortsat kan anvende og drage fordel af HSCC services. Udover eventuelle nødvendige ændringer i det juridiske aftalegrundlag, som vil blive annonceret offentligt og det EU Data Boundary initiativ, som beskrives i detaljer i spgm#2 i dette whitepaper, vil man kunne holde sig opdateret i de kommende måneder gennem dette link, hvor vi vil publisere alle kommende ændringer og anbefalinger: https://aka.ms/mscloudgovernanceRoundtable2021

D. Særlig national regulering

Holland

Den private/kommercielle sektor
Inden for den Hollandske kommercielle sektor er opfattelsen af offentlig cloud computing generelt positiv. Der er ingen direkte hindringer fra specifikke Hollandske bestemmelser, der blokerer for adoption af offentlig cloud, og derfor gælder de generelle retlige rammer mellem EU og EØS, der er beskrevet i dette whitepaper, direkte for kommercielle organisationer i Holland. Inden for det Hollandske FSI-regulerede marked er de fleste krav også i nøje overensstemmelse med retningslinjerne fra EBA/EIOPA/ESMA. Det Hollandske FSI-tilsyn er generelt neutrale over for cloud computing, hvis regulerede organisationer kan påvise, at de har kontrol over risici.

Den offentlige sektor
Mange organisationer på tværs af den hollandske offentlige sektor tilpasser sig mange af anvisningerne og opfattelserne fra den hollandske centralregering vedrørende offentlig cloud computing.

Der er ingen formel politik i Holland, der hverken tillader eller forbyder brugen af offentlig HSCC i den hollandske centralregering. Nogle regeringsorganisationer kan stadig henvise til "parlamentsbrevet fra minister Donner" fra 2011[1], der hævdede, at den offentlige cloud ikke var tilstrækkelig moden. Men mange andre formelle dokumenter siden da viste en voksende ambition og appetit til at begynde at "eksperimentere" på grundlag af den forventede værdi den private sektor oplever ved cloud computing.[2]

Mest tæt på en politik er et vejledningsdokument fra "CIO Rijk"[3], der bruges i flere afdelinger, der giver en beslutningstabel for forskellige kategorier / klassifikationer af data i forhold til forskellige Cloud-leveringsmodeller. For data, der er klassificeret som "Departmentaal Vertrouwelijk – Dep.V." eller lavere, som dækker de fleste data fra den hollandske regering, kan den foreløbige politik sammenfattes som:[4]

1 Se: (Kamerstuk 26643, nr. 179 | Overheid.nl > Officiële bekendmakingen (officielebekendmakingen.nl)
2 Se: Eindrapport Tijdelijke 1984 19 IKT-projekten (kennisopenbaarbestuur.nl) Eindrapport Tijdelijke 1984 19 IKT-projekten (kennisopenbaarbestuur.nl) https://zoek.officielebekendmakingen.nl/kst-26643-573.pdf
3 se: notitie "verkenning Skybeleid voor de Nederlandse Rijksdienst"; Kenmerk 2019-0000642838; November 2019
4 Se de nederlandske retlige rammer for informationssikkerhed i centralregeringen "VIR-BI": https://wetten.overheid.nl/BWBR0033507/2013-06-01

Offentlig cloud computing er ikke tilladt, medmindre:

1. CISO eller CISO Rijk burde have foretaget en risikovurdering (BIO-assessment[5]/Privacy DPIA[6]) på de offentlige cloud tjenester, og resterende risici bør accepteres af CISO eller CISO Rijk.
2. Gennemføre yderligere relevante tekniske og organisatoriske foranstaltninger for at beskytte, opdage og reagere på APT'er og nationalstatstrusler.
3. "The Secretary General" (SG) bør give udtrykkelig tilladelse og acceptere risiciene.
4. "The Secretary General" (SG) bør i sin afgørelse følge rådene fra NBV (Nationaal Bureau voor Verbindingsbeveiliging). Denne rådgivning blev revideret i januar 2021 og giver neutral vejledning baseret på en risikovurdering fra sag til sag.[7]

Microsoft har arbejdet tæt sammen med flere offentlige myndigheder for at løse de fire krav fra den foreløbige Cloud-politik, hvilket resulterer i yderligere sikkerhed (anført nedenfor), som kunder i den hollandske centrale regering kan bruge til at ibrugtage Microsoft Cloud-tjenester på en compliant måde. *Resultaterne er også blevet anvendt med succes i andre segmenter af den offentlige sektor, f.eks. Regional og lokale regeringsorganisationer og bredt indenfor den hollandske uddannelsessektor.*

Privatlivsbeskyttelse, GDPR og DPIAs. Processen med det hollandske justitsministerium (MoJ) – Strategic Vendor Management (strategisch leveranciersmanagement Microsoft rijk) førte til en generisk godkendelse af beskyttelse af personoplysninger, hvis enhederne bruger de kontraktvilkår, Microsoft forhandlede med MoJ[8]. Dette blev delt med parlamentet i et brev: Verificatie op de uitvoering van het overeengekomen verbeterplan mødte Microsoft | Tweede Kamer der Staten-Generaal[9]. Selvom der fortsat er mange (geopolitiske) udviklinger vedrørende privatlivets fred, bør kunderne kunne indføre Microsofts onlinetjenester på en måde, der er i overensstemmelse med centralregeringens krav.[10]

Sikkerhed/BIO-vurdering. Microsoft har gennem KPMG fået udarbejdet en mapping som hjælper med at anvende Microsoft Online Services på en BIO "BBN2"[11] -compliant måde. Desuden giver Microsoft omfattende vejledning og sikkerhed (ISO27001, ISO27002, SOC2-Type II, ISO27701, ISO2000), som meget godt stemmer overens med kvalitets-/sikkerhedskrav fra den hollandske regering (https://aka.ms/stp).

"The Secretary General" (SG) tilladelse: I betragtning af den yderligere sikkerhed, der er stillet til rådighed, mener Microsoft, at en afdeling/organisation bør være i stand til at foretage en risikovurdering, der i tilstrækkelig grad adresserer eventuelle restrisici/bekymringer til et niveau, som en SG bør kunne acceptere. Microsoft samarbejder fortsat med den hollandske regering om at løse eventuelle nye eller udestående problemer.

---

5 Hollandsk baseline informationssikkerhedsregering, BIO. se: https://www.cip-overheid.nl/productcategorie%C3%ABn-en-worshops/producten/bio-en-thema-uitwerkingen/#bio-tekst

6 se: https://wetten.overheid.nl/BWBR0040940/2020-01-01

7 Se: Januari 2021: NBV standpunt offentligeskydiensten da Gerubriceerde gegevens (Januari 2021); Kenmerk 9242d00c-eller1-1,2

8 Dette gælder for alle Microsoft Commercial Online Services (herunder Azure og Dynamics365).

9 https://aka.ms/NLTweedeKamer01072019

10 De fleste af de kontraktlige forpligtelser fra MoJ er blevet gjort bredt tilgængelige i Microsofts standardkontrakter. Dette er nogle offentligt tilgængelige Microsoft blogs om det arbejde, vi gjorde med MoJ: https://blogs.microsoft.com/eupolicy/2019/11/18/introducing-privacy-transparency-commercial-cloud-customers/ & https://blogs.microsoft.com/eupolicy/2019/07/02/how-microsoft-works-with-customers-to-keep-their-trust-a-story-from-the-netherlands/

11 De fleste data, der behandles inden for den hollandske regering, klassificeres som DEP.V eller lavere. Derfor sigter Microsoft mod at yde et tilstrækkeligt beskyttelsesniveau til at behandle BBN2/DEP.V klassificerede data. BBN2 er det niveau, der kræves for at beskytte "Departementaal Vertrouwelijk – DEP.V" klassificerede oplysninger som defineret i forordningen "Besluit Voorschrift Informatie beveiliging Rijksdienst Bijzondere Oplysninger 2013 (VIRBI 2013)" https://wetten.overheid.nl/BWBR0033507/2013-06-01

Sverige

Microsoft Cloud Design for the Public Sector (MSMD) er en samling værktøjer, skabeloner, politikker, rapporter og kurser, der gør det lettere for den offentlige sektor i Sverige at bruge cloud tjenester i Microsoft Azure og Microsoft 365. Designet er specielt tilpasset organisationer, der har brug for at overholde de regler, krav og love, der gælder for den offentlige sektor i Sverige. MSMD tilbyder et cloud-miljø for it-tjenester med meget høj sikkerhed og indeholder samtidig flere værktøjer, der gør det lettere at overholde regler og love som f.eks. databeskyttelsesforordningen (GDPR) og OSL (Public Access and Secrecy Act). Microsoft Cloud Design for den offentlige sektor består af forskellige komponenter afhængigt af den type data, der håndteres i Microsoft-tjenester.[12]

Finland

Finansministeriets retningslinjer for den offentlige sektors brug af Cloud

Finansministeriet offentliggjorde sine retningslinjer for den offentlige sektors brug af cloud: "Guidelines for Public Sector on Data Communications" [13], i 2018. Senere i september 2020 offentliggjorde Finansministeriet yderligere retningslinjer om produktivitet gennem cloudtjenester: "A guide[14] to leveraging public administration cloud services and Guidelines[15] for the application of cloud services to public administration organizations.".

Disse retningslinjer fastlægger hovedprincipperne for brug af public cloud til offentlige formål og for fremme af sådanne anvendelser og påpeger de aspekter, der skal tages i betragtning ved planlægning af nye løsninger baseret på cloud computing-tjenester. Formålet med retningslinjerne er at støtte beslutningstagningen i centralregeringen, amterne og kommunerne, når de planlægger og indkøber nye IKT-tjenester.

Følgende politikker er defineret i retningslinjerne:

1. Cloud-tjenester skal behandles på samme måde som alle andre IKT-tjenester, der indkøbes eller ændres.
2. Når det drejer sig om cloudtjenester, skal der lægges særlig vægt på aftaler, der sikrer servicekontinuitet og adgang til data.
3. Cloud-tjenesten skal opfylde indkøbspartens krav til servicefordele og garantier.
4. Hvis en cloudtjeneste eller cloud-serviceteknologi giver den bedste servicefordel og garanti, og der ikke findes andre barrierer, bør den vælges som førsteprioritet.

12 Læs mere om Microsoft Cloud Design for Public Sector i Sverige: https://pulse.microsoft.com/sv-se/sustainable-futures-sv-se/na/fa1-offentlig-sektor-till-molnet-med-microsofts-nya-molndesign/
13 https://aka.ms/FI_PSDataCommServices
14 https://aka.ms/FI_PSCloudServices
15 https://aka.ms/FI_PSCloudServicesApplication

5. Servicefordelen og garantien for cloudtjenester skal evalueres med jævne mellemrum, og når der sker væsentlige ændringer i aftalevilkårene.
6. Behandlingen af offentlige data er ikke begrænset.
7. Ikke-offentlige data kan behandles i en public cloudtjeneste, når informations-sikkerhed & -beskyttelse er blevet korrekt implementeret og verificeret.

Værktøj til revision af informationssikkerhed for myndigheder

Kriterierne for national sikkerhedsrevision KATAKRI[16] er et værktøj til overvågning af informationssikkerhed for myndighederne.

Det bruges typisk til revision af datacenter, hvor myndighederne håndterer klassificerede oplysninger relateret til national sikkerhed. Som et revisionsværktøj for myndigheder kan KATAKRI bruges til at vurdere en organisations evne til at beskytte klassificerede oplysninger. KATAKRI selv angiver ikke obligatoriske krav til informationssikkerhed. Den samler de minimumskrav, der er baseret på national lovgivning og internationale forpligtelser om oplysningssikkerhed. I denne forbindelse er det vigtigste stykke national lovgivning "Regeringsdekretet om informationssikkerhed i centralregeringen", som vil blive omtalt som dekretet om informationssikkerhed, og som følges for at beskytte både nationale og internationale klassificerede oplysninger. En vigtig international kilde her er Rådets afgørelse om sikkerhedsregler for beskyttelse af EU-klassificerede oplysninger (2013/488/EU), som fastlægger de grundlæggende principper og minimumsstandarder for sikkerhed for beskyttelse af EU-klassificerede oplysninger (EUCI). Et KATAKRI vurderings-værktøj er tilgængeligt for download.[17]

Kriterier for sikkerhedsvurdering af cloudtjenester

Kriterier for vurdering af informationssikkerheden i Cloud Services (PiTuKri[18]) indeholder fortolkninger og retningslinjer for vurdering af risici i forbindelse med cloudtjenester. Formålet med kriterierne for vurdering af informationssikkerheden i cloudtjenester (PiTuKri) er at forbedre sikkerheden af myndighedernes oplysninger, der skal hemmeligholdes i situationer, hvor oplysningerne behandles i cloud computing-miljøer. Kriterierne er tænkt som et værktøj til sikkerhedsvurdering af cloud computing-tjenester. Kriterierne blev udarbejdet ud fra Finlands nationale behov. De nationale lovgivningsreformer er blevet taget i betragtning, så kriterierne også støtter den lovgivning, der blev revideret i begyndelsen af 2020. Et PiTuKri vurderings-værktøj er tilgængeligt for download.[19]

16 https://aka.ms/FI_Katakri
17 https://aka.ms/FI_KatakriToolkit
18 https://aka.ms/FI_PuTuKri
19 https://aka.ms/FI_PuTuKriToolkit

Danmark

Danske offentlige strategier og analyser har i mange år alle støttet og givet vejledning i, hvordan man kan vurdere og beslutte, hvordan og til hvilket formål HSCC-tjenester skal/kan anvendes.

Den fælles strategi for digitalisering i den offentlige sektor [20]

"Den offentlige sektor skal have mulighed for at bruge cloud computing, hvor det giver værdi og er sund, forretningsmæssig og sikkerhedsmæssigt".

Sammenhængsreformen for digital service i verdensklasse [21]

"[.] Der gøres en indsats for at fremme brugen af cloud-teknologi" og "Samtidig er adgang til cloud-teknologier i høj grad en forudsætning for yderligere arbejde med kunstig intelligens, da cloud-løsninger giver adgang til høj computerkraft og de nødvendige avancerede værktøjer."

Center for Cybersikkerhed ved Thomas Lund Sørensen [22]

"Nogle gange bør du overveje, om du hellere skal fokusere på, hvad du har været sat i verden for og derefter købe dig ind i tjenesten ud af byen [...] Jeg vil tro, at en stor procentdel [...] kunne være godt tjent med at gøre denne overvejelse ".

Officiel cloudvejledning i den offentlige sektor efter Schrems II

De fleste organisationer i den danske offentlige sektor søger tilpasning til officiel vejledning og opfattelser fra den danske stat om brug af HSCC online tjenester.

Selv om der ikke er nogen formel politik i Danmark, som hverken tillader eller forbyder brugen af public cloud tjenester i den danske stat, udsendte Digitaliseringsstyrelsen og Center for Cybersikkerhed i juli 2020 en opdatering til deres cloud-vejledningspapir direkte rettet mod offentlige myndigheder, og papiret giver både forretningsmæssige, juridiske og sikkerhedsmæssige overvejelser at medtage. Vejledningen har det erklærede formål, at støtte en beslutningsproces der fører til brug af cloudtjenester, så offentlige myndigheder kan fjerne enhver usikkerhed og hindringer for brugen af cloudtjenester.

20 https://aka.ms/DKdigitalstrategi
21 https://aka.ms/DKdigitalservice
22 https://aka.ms/cfcsStyrkItSikkerheden

"Cloud-tjenester kan bidrage til hurtigere it-udvikling, mere effektiv skalering og et højt sikkerhedsniveau. Cloud er baseret på fleksibel deling af ressourcer, hvor du kun betaler for det, du bruger. Det kan udnyttes, hvis du oplever udsving i belastningen på ens systemer. Derudover drives cloud ofte i meget stor skala, hvilket giver mulighed for etablering af totale sikkerhedsløsninger hos udbydernes datacentre."
...

"Det er nyttigt at finde inspiration i ISO 27701-standarden til at identificere relationer mellem bestemmelserne i databeskyttelsesforordningen og informationssikkerhed. Det kan også overvejes at kræve, at cloududbyderen bruger ISO 27001- og 27002-standarderne samt 27017 og 27018, som vedrører sikkerheden ved behandling af personoplysninger i cloudløsninger....

Hvis ovenstående punkter er afklaret, og udbyderen kan dokumentere overholdelse af relevante standarder, kan du generelt være sikker på, at informationssikkerheden er tilfredsstillende, og at behandlingen af personoplysninger er i overensstemmelse med relevant lovgivning. ...

Men den 16. Juli, 2020 afgjorde EU-Domstolen, at EU-USA Privacy Shield ikke yder tilstrækkelig beskyttelse, hvorfor det ikke længere kan bruges som overførselsgrundlag. Yderligere oplysninger kan fås ved at henvende dig til Datatilsynet. Denne vejledning vil blive opdateret, når andre konsekvenser af dommen er blevet afklaret ....

Risikovurderingen er et vigtigt værktøj til at bestemme de sikkerhedsrisici, som brugen af en it-løsning indebærer, uanset om løsningen bruger cloud-tjenester eller ej."

Uddrag fra vejledningen[23]

23 https://aka.ms/digstcloudvejledning

Baseret på dette (og de yderligere juridiske præciseringer, der følger nedenfor) kan de fleste organisationer gå videre med en reel vurdering af potentialet og målene for deres brug af cloud computing samt risikovurderingerne, der er beskrevet i hovedafsnittene i dette whitepaper.

Krigsreglen – omdøbt til 'Lokationskravet'

I juni 2019 færdiggjorde Justitsministeriet deres vejledning om 'Lokationskravet' (§3, stk 9 i databeskyttelsesloven), der præciserer de nye retslige rammer og erstatter den tidligere mere bredt definerede 'krigsregel' fra den nu forældede persondatalov.

I realiteten er omfanget af 'Lokationskravet' blevet reduceret til en liste, af meget få systemer, der er relevante for den nationale sikkerhed.

I vejledningen hedder det:

- Et meget begrænset antal systemer er og vil være på listen (i øjeblikket fem (5) systemer på listen).[24]
- Kun offentlige systemer, der er afgørende for "national sikkerhed", kan føjes til listen.
- Det er kun selve systemerne – den server, der styrer systemet – der skal forblive på dansk suveræn grund, så serveren/systemet kan beskyttes af det danske forsvar.
- Data fra disse servere/systemer kan behandles i henhold til alle de almindelige databeskyttelsesregler – GDPR – og kan derfor behandles eller indgå i løsninger i f.eks. HSCC.
- Vedligeholdelse og støtte fra lande uden for EU/EØS kan udføres på de systemer, der er opført på listen (etableret som "visning eller fjernadgang"), hvis der træffes supplerende sikkerhedsforanstaltninger for at beskytte dataene i disse systemer tilstrækkeligt.

Derfor er det blot et spørgsmål om placering for driften af kun en begrænset mængde servere/systemer, der er omfattet af 'Lokationskravet', og ikke data i disse systemer. Beskrivelsen indeholder også en liste over flere systemer, der anses for **ikke** at være med på listen, herunder SKAT's e-indkomstsystem, der indeholder indkomstdata om alle danskere, uanset indtægtskilden – en liste som giver mulighed for med nogen nøjagtighed at vurdere om et givet system er relevant at vurdere ift 'Lokationskravet'.

Alt i alt gør denne vejledning det fuldt ud muligt for ejere/dataansvarlige i de fleste offentlige systemer at foretage en klar vurdering af, om og hvordan cloud computing kan anvendes mere bredt, end det hidtil har været tilfældet.

24 https://aka.ms/3-9

Dansk Microsoft Datacenter Region

Den 7. december 2020 annoncerede[25] Microsoft desuden en investering i at opbygge en ny Microsoft Hyper Scale Cloud Computing datacenter region - i alt tre (3) datacentre, der alle ligger et sted på Sjælland - den faktiske Go Live-dato er endnu ikke annonceret, men baseret på tidligere erfaringer skal de være operationelle når som helst inden for op imod 36 måneder fra meddelelsen. Da disse datacentre vil være på dansk jord, og alle data kan lagres (herunder backup og failovers) i Danmark, bør det således være muligt at implementere selv systemer, der er underlagt ‹Lokationskravet› i denne del af Microsoft HSCC.

Investeringen i datacentre i Danmark[33] er en del af en større investering i det, der er indrammet i konceptet Microsoft TechFit4Europe[26], og omfatter også initiativer og investeringer i bæredygtighed og opkvalificering af den danske arbejdsstyrke.

Den private/kommercielle sektor

Den danske private sektor opfatter generelt HSCC som positiv, og brugen vokser hurtigt i mange brancher. I finanssektoren (FSI) er de danske FSI-myndigheder generelt neutrale med hensyn til cloud computing, hvis de regulerede FSI organisationer kan påvise, at de har kontrol med risici og kan dokumentere en række yderligere vurderinger og planer forud anvendelse af HSCC (f.eks. ved at dokumentere en exitplan for visse væsentlige systemer – få mere at vide om exitplaner i Microsoft HSCC i afsnittet '05/ Gode spørgsmål til cloududbyderen'), og de fleste af kravene er i nøje overensstemmelse med retningslinjerne fra EBA/EIOPA/ESMA.

Der er således ingen hårde blokeringer i specifikke danske regler, og som følge heraf gælder de generelle EU/EØS-retlige rammer, der er beskrevet i afsnit '01/' i dette whitepaper, umiddelbart for dansk erhvervsliv.

Vejledning fra Datatilsynet

Vejledning fra Datatilsynet har længe været tilgængelig[27] og reelt afklaret spørgsmålet om, hvorvidt der kan etableres et retsgrundlag for etablering af dataoverførsler uden for EU/EØS og hvordan. Hovedkonklusionen er, at dette kan gøres, hvis følgende to betingelser er opfyldt:

- Der skal skabes et retsgrundlag for dataoverførsel i aftalen mellem parterne som beskrevet i artikel 46 i GDPR. Det kan f.eks. være EU's standardkontraktbestemmelser, hvilket typisk er tilfældet for leverings-/databeskyttelsesaftaler om cloud computing-tjenester. Schrems II-dommen ændrer IKKE dette, den eliminerer blot brugen af Privacy Shield i henhold til artikel 46.
- Der skal fastsættes et tilstrækkeligt sikkerhedsniveau ("passende sikkerhedsforanstaltninger") i forhold til den risikovurdering, som den dataansvarlige er ansvarlig for at udføre.

25 https://aka.ms/DigitalLeapDenmark
26 https://aka.ms/MSTechFit4Europe
27 https://aka.ms/DKGDPRVejledning

Det Danske Datatilsyn har siden EDPB's udkast til anbefalinger (se ovenfor) offentliggjort at dataoverførsler til tredjelande som en naturlig konsekvens, vil være et af deres fokuspunkter i deres 2021-revisioner. [28]

Men de har også gjort det meget klart, at hvis de dataansvarlige ...

- har indgået og forstået juridisk forsvarlige databehandleraftaler,
- kender scenarierne og omstændighederne for evt. dataoverførsler og de retslige rammer for sådanne overførsler,
- udfører de obligatoriske risikovurderinger, herunder af dataoverførsler, og en vurdering af, om de gennemførte supplerende foranstaltninger er tilstrækkelige, og endelig
- kan dokumentere og demonstrere alle de ovennævnte ...

... overholdelseskrav er sandsynligvis opfyldt.

Myndigheden giver naturligvis ingen garantier for detaljerne i fremtidige revisioner, men på baggrund af de offentlige erklæringer skal danske organisationer være sikre på, at DPA vil fokusere på ovennævnte fire (4) punkter, når det drejer sig om dataoverførsler til lande uden for EU/EØS.

Microsoft Danmark giver lokale partnere vejledning i overholdelse og sikkerhed

Microsoft Public Sector Cloud Framework (MPCF) er et træningsprogram for lokale Microsoft-partnere, der har til formål at gøre det muligt for partnerne at bruge en række værktøjer, vurderinger, skabeloner, politikker, konfigurationer og kontrolelementer, der gør det lettere for den offentlige sektor i Danmark at bruge Microsoft HSCC-tjenester på en kompatibel og sikker måde. [29]

Rammen opdateres ofte, og flere partnere er om bord for at sikre en opdateret tilgang, der tager hensyn til både juridiske og tekniske markedsovervejelser/-anbefalinger samt ændringer af Microsoft HSCC-tjenester og -operationer.

28 Webinar af Den Danske Union IDA (16. marts 2021), hvor DPA klokken 1 time og 21 minutter giver perspektiver på Schems II, the EDPB og hvor DPA-revisionerne i 2021 vil fokusere på https://ida.dk/viden-og-netvaerk/videoer-fra-ida/how-to-3-cloud-compliance-i-praksis

29 https://aka.ms/mpcf

E. Risikobaseret tilgang – yderligere detaljer

Nøglen til risikostyring i forbindelse med indførelse af teknologi er at afveje fordele og værdi i forhold til de potentielle negative virkninger af gennemførelsen. Implementering af teknologi eller flytning til skyen har indflydelse på en virksomheds drift. Governance, risiko- og compliancefunktioner er ofte justeret i tre forsvarslinjer, hvor forretnings- eller procesejeren skal træffe foranstaltninger for at kontrollere risikoen, risikostyring understøtter virksomheden gennem risikostyringsprogrammer, og den tredje linje reviderer resultaterne. Risikostyringsprogrammer fokuserer effektivt på at identificere og vurdere mulige risici, evaluere mulige modforanstaltninger og kontrollere og afveje restrisiko, alt sammen afbalanceret i forhold til den forventede forretningsværdi. [30]

Baseret på branchen er en organisation en del af specifik lovgivning og regler kan også være relevant, som understøttes og implementeres gennem tilsynsvejledning og kontrol. Dette vil også påvirke den måde, hvorpå teknologirisici implementeres og vedligeholdes.

To fordele ved en risikobaseret tilgang

Der er to grundlæggende aspekter, der øger vigtigheden af risikobegrebet i evalueringen af cloud computing.

1. **Det hjælper med at bevæge sig væk fra en rent overholdelsesbaseret tilgang.**
   En sikkerhedsproces kan ende med blot at bruge tjeklister og basislinjer til at logge af på store lister over kontroller, som cloudtjenesteudbyderen kan vise sig at have implementeret. Selvom dette naturligvis kan bidrage til at reducere en vis risiko (primært for ikke at overholde visse standarder), og det er en væsentlig del af den faktiske sikkerhed, som cloud-tjenesteudbydere kan levere, betyder det ikke, at der tages højde for de vigtigste risici, der er specifikke for den pågældende organisation. Det er derfor vigtigt at vurdere, hvilken (yderligere) risiko der kan være involveret for en bestemt organisation, for den specifikke use case eller scenario, der behandler den specifikke type eller klassificering af data. Selvom den faktiske risiko kan håndteres (mere end) tilstrækkeligt, kan en ren overholdelsesbaseret tilgang kræve kontroller, der ikke er realistiske i et cloud computing-scenarie og kan forhindre organisationen i at realisere fordelene ved den pågældende cloudløsning. En compliance-tilgang, der er udvidet med et risikobaseret fundament, giver mulighed for en mindre stiv tilgang, der gør det muligt for virksomheden at drage fordel samt tackle trusler og bekymringer.

30 Se f.eks. https://www.isaca.org/Journal/archives/2011/Volume-5/Pages/The-Three-Lines-of-Defence-Related-to-Risk-Governance.aspx

2. **Det driver en afbalanceret og rationaliseret tilgang til bekymringer og trusler.**
   Især når overgangen til skyen evalueres, er der ofte (opfattede eller faktabaserede) bekymringer og diskussioner. Meget er baseret på et fatamorgana af mediehistorier, misforståelser og vandre-historier. Eksempler er det potentielle eller opfattede tab af (fysisk) kontrol af data og behand-lingsstederne, bekymringerne for, at udenlandske regeringer på en eller anden måde burde have upåvirket, ubegrænset og direkte adgang til data eller cloudtjenesteudbyderens sikkerhedsforsvar, der ikke leverer det krævede beskyttelsesniveau. Selvfølgelig skal disse bekymringer tages alvorligt, og I det væsentlige kræver HSCC, at en dataansvarlig har tillid til og verificerer cloud-tje-nesteudbyderen samt konfigurerer tjenesten, etablerer kontroller og ikke mindst en omfattende styringsmodel. Identifikation og beskrivelse af risiciene i form af faktiske (business &privacy) virkning / konsekvens og den faktiske sandsynlighed, vil bidrage til at afbalancere trusler mere rationelt med de potentielle fordele.

For en organisation til at gennemføre risikostyring er der mange dokumenterede praksis til rådighed. De kan være generaliseret praksis og standarder for risikostyring (som ISO 31000, ISO 27005 eller NIST 800-37 / RMF), men der er også mange flere specialiserede ressourcer til rådighed, der beskæftiger sig med for eksempel med specifikke opfattede trusler relateret til it-sikkerhed, cybersikkerhed eller cloud computing. Et meget tilgængeligt whitepaper er CSA's "Forræderiske 12", der beskriver de mest opfattede trusler i forhold til cloud computing og hvordan man vurderer og adresserer dem.[31]

Risikostyring er vigtig i sikkerhedsprocessen for at kunne gennemføre en mere rationaliseret tilgang og ikke alt for fokusere på overholdelse alene. Desuden, når det ses som en mulighed, bidrager det ikke kun til at beskytte værdi, men hjælper endda organisationer i deres udvikling og værdiskabelse.

At tage en risikobaseret tilgang er et af de grundlæggende principper i en cloud-sikkerhedsproces, men man kan argumentere for, at en organisation fra et juridisk overholdelsesperspektiv simpelthen skulle overholde. Når vi henviser til en risikobaseret tilgang til overholdelse, henviser vi generelt til, at retlige rammer ofte ikke specificerer, hvordan du kan overholde reglerne. F.eks. kan juridiske klausuler henvise til at træffe "passende tekniske og organisatoriske modforanstaltninger"; at bestemme, hvad der er "passende", er det sted, hvor risikobaseret kommer ind, da det ikke bør baseres på blot at bruge en tjekliste.

31 Den forræderiske 12 - Cloud Computing Top Trusler i 2016; https://cloudsecurityalliance.org/group/top-threats/#_overview

F. Microsoft Cloud Assurance - proces

Dette afsnit vil give et dybere niveau af en sikkerhedsproces, der kan tjene som en ramme for evaluering af teknologi og cloud computing og for at strukturere de ressourcer, Microsoft stiller til rådighed for sine kunder.

Der er generelt flere forskellige trin involveret i en grundig revisionsevaluering. I dette afsnit beskrives mere detaljeret de seks væsentlige aktiviteter. Bemærk, at en organisation i praksis kan medtage flere trin i deres proces baseret på deres specifikke behov og krav. Procesbeskrivelsen i dette dokument har ikke til formål at være fuldstændig udtømmende, men giver de aktiviteter, der anses for væsentlige i en bestemt sikkerhedsproces. Desuden har mange organisationer sandsynligvis allerede implementeret lignende processer og behøver muligvis kun at tilpasse sig nogle af de specifikke egenskaber ved evaluering af cloud computing.

Roller og ansvarsområder

På grund af princippet om fælles eller delt ansvar er det vigtigt at uddybe den grundlæggende forskel mellem cloud-udbyderens rolle (CSP) og cloud-kunden. I kommercielle cloudscenarier fungerer en organisation typisk som den cloud-forbruger, der giver og kontrollerer adgangen til sine medarbejdere, kunder eller partnere for de cloudtjenester, den forbruger, og licenser fra cloudtjenesteudbyderen.

I denne sammenhæng er det nyttigt også at knytte disse roller til de roller, der er defineret i GDPR. Databeskyttelses- eller privatlivskrav er ofte kernen i mange af de juridiske krav, der er relevante, når cloud computing evalueres, fordi de fleste scenarier på en eller anden måde involverer behandling af personlige oplysninger.

Definitionerne af roller i databeskyttelseslovgivningen er meget velegnede til de nævnte roller.

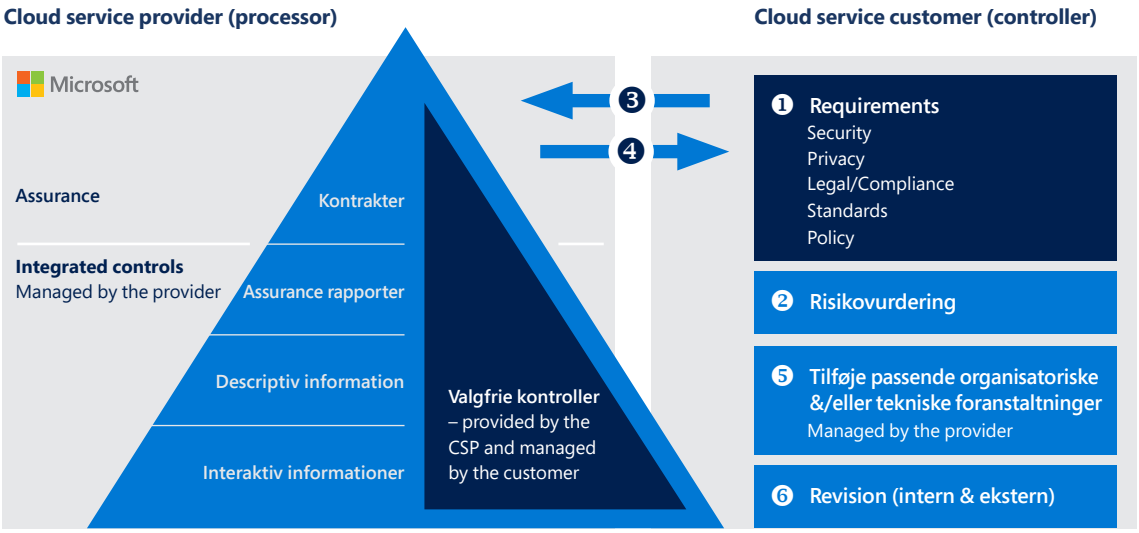
- "Emnet" er typisk den person, som personlige oplysninger er relateret til, og er ofte den faktiske forbruger af cloud-tjenesterne. I et virksomhedsskyscenscenario er emnerne typisk kunder eller medarbejdere i den organisation, der bruger skyen.
- "Registeransvarlig" i GDPR ": den fysiske eller juridiske person, den offentlige myndighed, agenturet eller et andet organ, som alene eller sammen med andre fastlægger formålet med og midlerne til behandling af personoplysninger". Dette er typisk den organisation, der indgår i cloud-tjenesterne.
- Ved registerfører forstås "en fysisk eller juridisk person, offentlig myndighed, agentur eller andet organ, der behandler personoplysninger på den registeransvarliges vegne". Cloudtjenesteudbyderen udfører typisk denne rolle.

Således er controlleren i forretningsscenarier typisk cloud-forbrugerorganisationen og er ansvarlig for formålet med og midlerne til behandling af personlige oplysninger. Controlleren kan vælge at behandle oplysningerne på deres egne systemer i deres egne datacentre (hvilket betyder, at de også er processoren), men de kan også bruge (cloud) tjenesteudbydere til at behandle oplysningerne baseret på deres instruktioner. Selvom den registeransvarlige i de fleste typer lovgivning er ansvarlig for at opfylde de (specifikke) lovkrav, der vedrører de oplysninger, der behandles, er der i henhold til GDPR – vedrørende behandling af personoplysninger – også direkte krav til databehandleren. I sikkerhedsprocessen starter kravindsamlingsfasen dog med cloud-forbrugerorganisationens syn på dens krav.

Rammerne for

Den risikobaserede ramme opregner seks aktiviteter, som ikke nødvendigvis udføres i rækkefølge, men som i vid udstrækning kan udføres parallelt. Processen vil være rekursiv, fordi det kræver mange discipliner i organisationen til at samarbejde, ofte afviger fra eksisterende og velkendte praksis, kræver en solid forståelse af nye begreber, og vedrører følsomme emner for driften af en organisation.

Customer Risk Assessment Process



1. Indsamling af oplysninger og krav

Som input til cloud-sikkerhedsprocessen skal en organisation have et godt overblik over de interne og eksterne krav. Det er vigtigt klart at identificere mål og krav, før man vurderer og sammenligner det serviceniveau, der tilbydes af cloud-tjenesteudbydere. Det krævede sikkerhedsniveau kan variere og skal analyseres fra mere end ét perspektiv, f.eks. Iso/IEC 19086-1-standarden kan hjælpe med at oprette en sådan visning på en struktureret måde, afhængigt af hvilken Microsoft har oprettet den nyttige Cloud Services Due Diligence-kontrolliste.[32] [33]

Tjeklisten opregner de vigtigste overvejelser, der er fordelt på fire temaer: ydeevne, service, datastyring og styring. Det kan bruges – sammen med vejledningen og en projektmappe – til at starte en diskussion om at flytte til skyen. Det vil understøtte en overgang til skyen fra et mere holistisk synspunkt og indlede en meningsfuld due diligence-evaluering.

Hvis tjeklisten hjælper med at identificere de vigtigste krav til en lang række ikke-funktionelle, skal organisationerne udvide dem, der har et godt syn på mere specifikke krav, der stammer fra lovgivning, sikkerhedspolitikker, standarder og informationspolitikker. Der henvises ofte til det sæt (ikke-funktionelle) sikkerhedskrav med udtrykket myndighedsdokumenter. Fra et cloud-sikkerheds- og privatlivsperspektiv er de fælles overholdelsesrammer, der ofte bruges, BSI C5, CSA's CCM, NIST 800-53r4 eller ISO 27002/17/18. Brug af disse kan fremskynde sikkerhedsprocessen betydeligt, fordi cloud-tjenesteudbyderen typisk kan afspejle krav, der stammer fra disse bredt accepterede standarder, fordi de allerede bruges til deres egne interne processer. Brugen af dem skal imidlertid afvejes med en risikobaseret proces, som vi tidligere har forklaret. Risikovurdering er en vigtig del af anden fase, hvor den faktiske cloudløsning vurderes i forhold til de identificerede krav og mål.

I denne første fase er det også vigtigt at indsamle den foreslåede indledende tekniske arkitektur i cloud-løsningen, især med hensyn til niveauet for, hvilken funktionalitet eller cloudplatforms byggesten der vil blive brugt, og hvordan de vil blive integreret i eksisterende it-infrastruktur og stillet til rådighed for brugerne. Desuden kan det hjælpe med at tilføje informations-/datastrømme og have en visning af typen og følsomheden af, hvilke data der skal behandles. De nødvendige oplysninger skal være i overensstemmelse med de cloud-servicemodeller (IaaS, PaaS, SaaS), der blev introduceret tidligere. For en SaaS-løsning betyder det typisk:

- En beskrivelse af de teknologifunktioner på SaaS-niveau, der vil blive evalueret; for eksempel kerne e-mail-tjeneste, e-mail arkivering, e-mail-sikkerhed og e-mail rengøring. Bemærk, at de underliggende infrastrukturkomponenter ikke behøver at indgå. det ville kun give mening (delvis), når for eksempel en IaaS-løsning ville blive evalueret.

32 En meget omfattende guide til evaluering af interne og eksterne krav kan findes her: http://download.microsoft.com/download/1/5/A/15ABB577-BD3C-4CC4-9AA2-0EE1337714DE/msft_SAFE_handbook.pdf

33 https://www.microsoft.com/en-gb/trust-center/compliance/due-diligence-checklist

- En beskrivelse af, hvordan SaaS-løsningen ville fungere sammen med eksisterende systemer. F.eks. med identitetstjenester, sikkerhedstjenester eller andre funktionelle byggesten.
- En beskrivelse af typen og følsomheden af de oplysninger, der skal behandles.
- En beskrivelse af, hvordan oplysninger flyder gennem de funktionelle komponenter.

2. Vurdering af krav

De fleste organisationer vil allerede have eksisterende processer til at vurdere it-risikoen ved at indføre teknologier, der fører til ændringer i driften. Dette er typisk en del af en organisations eksisterende styringsrisiko- og kontrolproces. Hovedfokus er at igangsætte en solid tilgang til kategorisering og prioritering af krav og start af vurderingen af cloud-løsningen. Igen er der flere gode rammer, der kan hjælpe med at vurdere sikkerheds- og privatlivsrisikoen, såsom NIST CSF og NIST RMF, ISO 27005 og ISO27001 og COSO-rammerne.

Det er vigtigt at sikre, at alle relevante discipliner er involveret for at sikre grundige vurderinger fra forskellige vinkler. Igen kan due diligence-tjeklisten give en vis baggrund, men generelt skal i det mindste følgende discipliner involveres (selvom disse discipliner kan organiseres forskelligt inden for organisationer):

- Erhverv: business case; 'hvorfor'
- Arkitektur: bringer viden om løsning; 'hvordan'
- Funktion til sikkerhedsrisiko for oplysninger: 'Fortrolighed, integritet, tilgængelighed'
- Compliance- og privatlivsfunktion: "Mod hvilken lovgivning"
- Juridisk funktion: »På hvilke betingelser og kontrakter«
- Revisionsfunktion: 'Revisionsevne'

En del af GRC's risikostyringsaktiviteter er at reducere, mindske og kontrollere risikoen ved at udvælge og gennemføre kontroller. Med offentlig cloud computing kan flere kontroller dog ikke implementeres eller drives af cloud-forbrugerorganisationen selv. Med hensyn til cloud-servicemodellen er kontroller, der opererer på lag, der administreres af cloud-tjenesteudbydere, CSP'ens ansvar. For eksempel er sikkerhedsforanstaltninger, der adresserer datadestruktion, når fysiske infrastrukturkomponenter bortskaffes, som disk makulering, under CSP'ens kontrol alene, selv med IaaS. I det væsentlige betyder det, at cloud-forbrugeren skal spørge cloud-tjenesteudbyderen, hvordan flere risici mindskes, eller hvilke kontroller der implementeres.

3. Anmod om kreditorgarantier

Under GRC-vurderingen skal cloud-forbrugerorganisationen anmode om oplysninger fra CSP'en vedrørende de kontroller, der implementeres. Selv om CSP kan være en betroet part i god stand, er det vigtigt, at oplysningerne rent faktisk giver sikkerhed og garantier. Det er klart, at når cloud-forbrugeren er ansvarlig, skal den sikre, at den modtager solide beviser fra CSP'en for, at den gennemfører og driver de kontroller, som den er ansvarlig for.

Der findes flere typer oplysninger og forsikringer, som en CSP kan tilbyde sine kunder:

- Kontraktlige forpligtelser: kontrakter, databehandleraftaler, SLA'er, vilkår og betingelser.
- Tredjeparts validerede attester: typisk revisionsrapporter, certificeringer, penetrationstest og andre attester fra betroede tredjeparter, der vurderede kontrollerne fra CSP.. Disse dokumenter og attester, der også omtales som TPM (tredjepartsmemorandum), bør give indsigt i, om kontrollerne som standard er en del af det iboende design, om kontrollerne findes, og om de rent faktisk er operationelle og fungerer.
- Beskrivende oplysninger: Selv om de beskrivende oplysninger ikke er faktiske, kan de give de nødvendige oplysninger om mange områder af CSP's tjenester. Det giver typisk arkitekturer, tekniske detaljer, beskrivelser af driftsprocesser, referencer til implementerede basislinjer og standarder. Disse dokumenter giver, selv om de stammer fra selve landeudbyderen, yderligere dybde og forståelse. ofte vurderes mange af disse dokumenter også af tredjeparter i deres revision, hvilket giver indirekte sikkerhed.
- Interaktiv information: Mange organisationer vil gerne overvåge eller få mere realtidsindsigt i CSP's tjenester. Programmet til udvikling af datakørsel kan derfor tilbyde direkte adgang til aktivitetslogfiler, hændelseslogfiler og diagnosticering. Nogle CSP'er tilbyder endda konfigurationsrådgivere eller trusselsintelligens og sikkerhedsanbefalinger baseret på avanceret AI og maskinlæring.

Cloud computing tilbyder meget standardiserede (men stadig mere konfigurerbare) tjenester, især når man overvejer udbydere af hyperskaleringsskytjenester. Standardiseringsniveauet giver mange fordele med hensyn til omfang, stabilitet og omkostninger, men det betyder også standardiserede kontrakter og forsikringer. Det behøver ikke nødvendigvis at være en udfordring, da disse CSP'er leverer kontroller og forsikringer, der valideres med mange kunder, foreninger og tilsynsførende og konstant revurderes og forbedres eller tilpasses, hvor det er muligt, relevant eller mandat. For eksempel kræver GDPR-overholdelse yderligere kontraktlige forpligtelser fra deres processorer, og nogle af de hyperskala cloud-tjenesteudbydere, som Microsoft, var blandt de første til at levere disse vilkår og betingelser integreret i deres standardkontraktsæt. [34]

Der kan dog være nogle valgfrie yderligere forsikringer til rådighed. Nogle gange kræver disse, at der indgås kontrakter om yderligere cloudtjenestekomponenter eller professionelle tjenester som omfattende proaktive supporttjenester. Der kan også være domænespecifikke overholdelsesprogrammer for kunder i specifikke regulerede sektorer eller brancher som finans eller regering.

34 Hyperskala refererer til et distribueret computermiljø, hvor mængden af data og efterspørgslen efter visse typer arbejdsbelastninger kan stige eksponentielt (for at F.eks. millioner af servere), men stadig indkvarteres hurtigt på en omkostningseffektiv måde. Der er kun få virksomheder i verden, der leverer cloud-tjenester i hyperskala.

4. Vurder erstatningskrav og vurder (rest) risiko
De krav og forsikringer, som CSP'en har givet, skal derefter inddrages i GRC-processen og vurderes. Dette kræver igen en tværfaglig tilgang til at analysere sikringerne fra CSP'en og integrere eller korrelere dem med kravene og kontrollerne fra cloud-forbrugerorganisationen.

Der er mange forskellige tilgange, lige fra blot at acceptere sikkerhedsrapporter eller certificeringer fra CSP som tilstrækkelige, til en kontrol-by-control analyse og kortlægning til interne risiko- og kontrolrammer, der allerede er på plads i organisationen.

Når du evaluerer tredjepartsgarantier fra leverandører, er det vigtigt at vurdere, om de cloudtjenester, der evalueres, er omfattet af rapporterne, og i forhold til, hvilken kontrol cloudtjenesterne revideres. I ISO27001 definerer soa-erklæringen f.eks., hvilke kontroller fra ISO27002 der vurderes, så et ISO 27001-certifikat uden SOA har ikke meget værdi. På samme måde bør en ISAE3000 SOC2-type II-rapport give kontekst med hensyn til, hvilke kontrolelementer eller kontrolelementer kategorier er ved at blive evalueret, typisk en markering fra "TSP Afsnit 100, Trust Services Kriterier" fra AICPA.

5. Adresser risici ved at vælge yderligere kontroller
Risikovurderingen og overensstemmelsesevalueringen bør resultere i en klar forståelse og kvalificering af de forsikringer, som CSP'en giver, og som bidrager til at håndtere de risici og krav, som cloudforbrugerorganisationen har identificeret. Organisationen skal dog supplere disse CSP-leverandørgarantier med deres egne implementeringsvalg, yderligere teknologikontrol og administrative processer. Dette kommer ned på princippet om fælles ansvar: For at håndtere sikkerheds-, privatlivs- og overholdelseskrav fra ende til anden skal både CSP'en og cloud-forbrugeren implementere, vedligeholde og drive passende kontroller.

Det kan være en udfordring at opnå en klar sondring mellem det, der betragtes som tjenesteudbyderkontroller i forhold til kundekontrol. Især hvor selve programmet til forbedring af kundeforsendelser også kan levere (valgfrit) konfigurerbare kundekontroller som en del af tjenesten eller som separate tilføjelsesprogrammer. Som en del af Office 365 tilbyder Microsoft f.eks. Men fordi det er op til kunden at konfigurere og bruge disse teknologier, betragtes de som valgfrie kundekontroller (eller 'kundesikkerhedsovervejelser'). Dette er helt adskilt fra for eksempel at anvende sikkerhedsopdateringer til den Office 365-software, der bruges af selve tjenesten, som er et CSP-kontrolelement.

For at vurdere, hvilke yderligere kontroller der kræves, bør cloud-forbrugeren derfor have en grundig forståelse af:

- Den iboende kontrol af den tjeneste, der forvaltes og drives af CSP (»service integrated controls«)
- De valgfrie konfigurerbare kontrolelementer, der administreres og administreres, men ikke administreres af programmet til brug af kundeservice som en del af tjenesten ('overvejelser i forbindelse med kundekontrol – service')
- De valgfrie konfigurerbare kontrolelementer, der kan føjes til tjenesten. Disse kontroller kan være separate teknologier eller processer, der leveres af CSP'en, af andre leverandører eller tjenesteudbydere eller administreres og drives af cloud-forbrugerne selv ('kundekontroloverveljelser – tilføjelse')

Nogle udbydere tilbyder vejledning, der viser kontroller (ofte baseret på kontrolrammer som NIST 800-53 eller ISO27002) i kombination med en ansvars- og løsningsmatrix. For hver kontrol beskrives det, hvem der er ansvarlig for implementeringen og driften (CSP, cloud-forbruger eller delt), og hvordan kontrollen kan implementeres (eller implementeres, hvis CSP'en har et ansvar). Se næste afsnit for at få flere oplysninger.

6. Påvise overholdelse / revurdere

Efter at have dokumenteret kravene, risikovurderingen, kombinerede kontroller og den overordnede vurdering bør organisationen have en grundig forståelse af, hvordan løsningen kan implementeres og vedtages på en kontrolleret måde. Dette bør give tillid til, hvordan organisationen kan opnå værdi fra de teknologier, der er blevet vurderet, mens sikkerhed, kontinuitet, privatlivets fred og juridiske bekymringer kan løses tilstrækkeligt. Vurderingen danner også grundlag for at påvise overholdelse gennem en intern og muligvis ekstern revision.

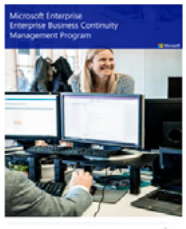
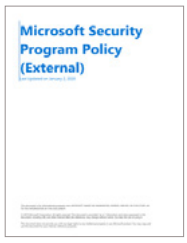
Et af kendetegnene ved organisationer, der innoverer deres processer gennem digital transformation, er den øgede smidighed og indførelseshastighed for teknologi. Derfor bliver det afgørende, at en cloud-sikringsproces afspejler denne fleksibilitet og samtidig sikrer kvalitet. Desuden ændrer omfanget af det, der skal vurderes, sig også oftere. Cloudplatforme udvikler sig, nye servicekomponenter introduceres over tid, og cloud-forbrugeren kan skabe nye løsninger ved hjælp af forskellige servicekomponenter – sidstnævnte er ekstremt almindeligt med brugen af PaaS- og IaaS-platforme. Endelig kan kravene også ændre sig. nye former for lovgivning kan vedtages, nye sikkerhedstrusler kan opstå eller ændre forretningsmæssige antagelser, principper, krav og kontekst kan udvikle sig. Det betyder, at en cloud-sikkerhedsproces også skal være repeterbar og fleksibel og ikke bør ses som en engangsproces.

Den ramme, vi præsenterede, giver en tilgang på højt niveau til at evaluere en organisations ikke-funktionelle krav i forhold til cloud-tjenesteudbyderens forsikringer. Strukturen kan også hjælpe med at strukturere de oplysninger, Microsoft tilbyder sine (potentielle) kunder, både i sin rolle som cloud-tjenesteudbyder og som leverandør af teknologier, der kan hjælpe kunderne med at håndtere kundekontrolkrav. Det næste afsnit vil præsentere flere detaljer om de oplysninger, Microsoft deler, og hvordan du får adgang til disse oplysninger. Det vil også evaluere nogle af de mest almindelige bekymringer og spørgsmål i forbindelse med cloud computing, som ofte evalueres under den cloud assurance-proces, vi diskuterede.

G. Andre whitepapers, der henvises til i dette dokument

Papir	Emner	Link	Seneste opdatering
	**Azure til sikker cloudimplering i hele verden** Beskæftiger sig med 'data residency', 'data suverænitet' og andre sikkerhedsmæssige opmærksomhed punkter, der er relevante for Offentlig Sektor kunder. Emnerne omfatter: - data i hvile og data i transit - Datakryptering, herunder Azure Key Vault, Dedicated HSM, SQL DB og andre. - Fortrolig databehandling - Customer Lockbox, - Regulatoriske undersøgelser, herunder CLOUD-loven. - Håndtering af sikkerhedshændelser. - etc.	https://docs.microsoft.com/en-us/azure/azure-government/documentation-government-overview-wwps	Marts 2021
	**Aktivering af dataopbevaring og databeskyttelse i Microsoft Azure-regioner** Dækker de oplysninger og værktøjer, der er nødvendige for at optimere dataplaceringen og dataadgangen Emnerne omfatter: – Forstå Azure regional infrastruktur - Hvordan man træffer optimale arkitekturbeslutninger. - Garantier for datalokation - Hvordan kunder kan administrere dataplacering, - Adgang til telemetridata, herunder øget adgang til støttedata, og - Hvordan kunder kan administrere dataadgang.	https://aka.ms/AzureDataResidencyWP	April 2021

Papir	Emner	Link	Seneste opdatering
	**Dynamics 365 og Power Platform** Indeholder omfattende oplysninger om produkttilgængelighed og kundedataplacering for kundeengagement, virksomhedsressourceplanlægning og Power Platform-programfamilien. I denne rapport findes følgende oplysninger: - Produkttilgængelighed - Dataplacering - Sprog - Lokalisering	https://aka.ms/dynamics_365_international_availability_deck	EO 2020
	**Tillidsvækkende databeskyttelse** Forsøger at omgå de nødvendige oplysninger om Microsofts behandling af data i Hyper Scale Data Center: Emnerne omfatter: - Kunden ejer egne data, - Microsoft og underleverandører har IKKE stående adgang - Databehandlingen sker udelukkende efter kundens anvisning - Opbevaring af data - Dataplacering - Dataoverførsler - Behandling af anmodninger fra myndigheder om tilvejebringelse af oplysninger og - Hvordan kunderne kan overholde GDPR (osv.)	https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4FhZn	Oktober 2020
	**Planlægning af brugen af Microsoft Cloud Services** Dette dokument vil hjælpe vores kunder i den finansielle sektor med at opfylde lovmæssige krav omkring service-erstatbarhed. Dokumentet fremhæver nogle af de gældende regler, en skabelontilgang til levering af en exitplan og et par overflytningsscenarier på højt niveau for Microsoft Cloud Services.	https://servicetrust.microsoft.com/ViewPage/TrustDocumentsV3?command=Download&downloadType=Document&downloadId=4aa0c653-312f-4098-b78a-0d499e07825e&tab=7f51cb60-3d6c-11e9-b2af-7bb9f5d2d913&docTab=7f51cb60-3d6c-11e9-b2af-7bb9f5d2d913_FAQ_and_White_Papers	August 2020

Papir	Emner	Link	Seneste opdatering
	**Microsoft Cloud-tjekliste for finansielle institutioner i Europa** Denne tjekliste henvender sig til finansielle institutioner i EU, der ønsker at bruge Microsoft Online Services. Udtrykket "finansielle institutioner" anvendes bredt til at omfatte enhver enhed, der reguleres og overvåges af en EU-tilsynsmyndighed. Disse enheder omfatter banker, betalingsinstitutter, forsikrings- og investeringsselskaber. Denne tjekliste fokuserer på EU-dækkende retningslinjer, navnlig: - 1.1 EBA's retningslinjer for outsourcingordninger (dateret 25. februar 2019) - 1.2 EIOPA's retningslinjer for cloud outsourcing (offentliggjort 31. januar 2020) - 1.3 ESMA's udkast til retningslinjer for outsourcing til cloudtjenesteudbydere (offentliggjort 3. juni 2020) - og ikke alle landespecifikke regler.	https://servicetrust.microsoft.com/ViewPage/TrustDocuments?command=Download&downloadType=Document&downloadId=86271bef-0c15-4e1d-b429-e9a21a0a4f7f&docTab=6d000410-c9e9-11e7-9a91-892aae8839ad_Compliance_Guides	November 2020
	**Microsoft business communityunity management-program**[35] Dette dokument opsummerer de foranstaltninger, Microsoft har truffet for at reagere på større eller væsentlige forretningsforstyrrelser med et effektivt og omfattende program for forretningskontinuitet og genoprettelse efter nedbrud	https://servicetrust.microsoft.com/ViewPage/TrustDocumentsV3?command=Download&downloadType=Document&downloadId=64f922a6-d624-40dd-a8ae-6f996b5186f3&tab=7f51cb60-3d6c-11e9-b2af-7bb9f5d2d913&docTab=7f51cb60-3d6c-11e9-b2af-7bb9f5d2d913_FAQ_and_White_Papers	Marts 2020
	**Microsofts sikkerhedspolitik** I dette dokument om sikkerhedsprogram-politik beskrives sikkerhedsmålene for alle oplysninger og processer, der bruges i forbindelse med Microsofts HSCC forretning.	https://servicetrust.microsoft.com/ViewPage/TrustDocumentsV3?command=Download&downloadType=Document&downloadId=b0034832-973d-4b24-878a-fff15fe6a060&tab=7f51cb60-3d6c-11e9-b2af-7bb9f5d2d913&docTab=7f51cb60-3d6c-11e9-b2af-7bb9f5d2d913_FAQ_and_White_Papers	Januar 2020

35 Dette whitepaper ledsages også af hyppige valideringsrapporter – senest er fra december 2020.

Papir	Emner	Link	Seneste opdatering
	Vejledning i hvordan Microsoft Cloud hjælper FSI-kunder med at adressere EBA's retningslinjer for cloud computing.	https://servicetrust.microsoft.com/ViewPage/TrustDocumentsV3?command=Download&downloadType=Document&downloadId=dff9e22e-8865-4c20-9ca5-80823709cdf4&tab=7f51cb60-3d6c-11e9-b2af-7bb9f5d2d913&docTab=7f51cb60-3d6c-11e9-b2af-7bb9f5d2d913_FAQ_and_White_Papers	Februar 2018
	**Microsoft Azure Compliance Offerings** Indeholder en oversigt over Microsoft Azure compliance portefølje, der har til formål at hjælpe kunderne med at opfylde deres egne compliance forpligtelser på tværs af regulerede brancher og markeder over hele verden. Azure har den største portefølje af compliance certificeringer i branchen, både med hensyn til bredde (samlet antal tilbud) og dybde (antal kundevendte tjenester i scope for certificeringerne). Azure Compliance Offerings er grupperet i fire segmenter: globalt gældende, føderal amerikansk, branchespecifikke og område-/landespecifik. Hver beskrivelse indeholder en opdateret erklæring og links til nyttige ressourcer til download.	https://aka.ms/AzureCompliance	November 2020
	**En guide til datastyring** - Hvad er data governance - Krav til styring af data i en moderne virksomhed - Komponenter, der er nødvendige for data governance - Teknologi, der er nødvendig for end-to-end data governance - Mastering af stamdata - Model for modenhed for data governance	https://aka.ms/MSDataGovernance	Oktober 2020

Papir	Emner	Link	Seneste opdatering
	**Model for delt ansvar** Denne hvidbog hjælper med at forklare forholdet mellem cloud-udbydere og deres kunder og noterer sig deres roller og ansvar. Standarder som National Institute of Standards and Technology (NIST) (Særpublikation 500-292) og PCI Standards Council (Information Supplement: PCI DSS Cloud Computing Guidelines) giver overvejelser om fælles ansvar. Dette dokument undersøger også forholdet mellem CSP'er og deres kunder mere detaljeret. Derudover hjælper det med at forklare de delte roller og ansvarsområder, som en organisation skal overveje, når den vælger en skymodel, såsom IaaS, PaaS og SaaS. Papiret undersøger også de compliancekrav, der skal tages i betragtning baseret på den valgte servicemodel.	https://aka.ms/SharedResponsibility	Juni 2020
	**Data Governance og beskyttelse af personlige oplysninger for Microsoft 365 Apps.** Indeholder oplysninger om brugen af diagnosticeringsdata og forbundne oplevelser(Connected Experiences) i Microsoft 365 Apps (tidligere kaldet Office 365 ProPlus), f.eks. Disse installeres og køres lokalt på din enhed og opretter forbindelse til Microsoft cloud for at sikre en højtydende oplevelse, for at levere specifikke forbedrede Office-relaterede oplevelser og -funktioner (beskrevet som forbundne oplevelser i produktdokumentationen) og for at oprette forbindelse til skybaserede tjenester som SharePoint Online, OneDrive og Exchange Online. For at hjælpe med at holde Microsoft 365 Apps sikre, opdaterede og fungere som forventet og levere de funktioner og den oplevelse, som brugerne forventer, behandler Microsoft både diagnosticeringsdata og data, der kræves til brug af forbundne oplevelser.	Offentligt Link endnu ikke tilgængeligt – ræk ud til Microsoft Account Executive for adgang til whitepaper: https://aka.ms/privacy/m365apps	April 2021
	Formålet med dette dokument er at skitsere de almindelige spørgsmål om sikkerhed, beskyttelse af personlige oplysninger og overholdelse af angivne standarder, som kunderne har i forbindelse med, hvordan Microsoft håndterer data, som kunden deler og gemmer i Microsoft Cloud, og som er specifikke for brugen af tredjeparter.	https://aka.ms/MSCloudDataHandling	EO 2020

H. Tidligere versioner af dette dokument

Dette dokument blev først udgivet på dansk (version 1.0) i november 2019.

Den nuværende version 4.0 - den du læser nu – indeholder primært opdateringer om de juridiske elementer, yderligere detaljer om og nyheder ift dokumentation for databehandlingen (tekniske, organisatoriske og processuelle foranstaltninger), inspiration til arbejdet med risikovurderinger, vurderinger af tredjelands-overførsler efter CJEU Schrems II afgørelsen og inkluderer specifikke nationale forhold i en række EU lande udover Danmark og endelig en samling af øvrige relevante whitepapers som refereres i dette dokument. Der findes også en engelsk version som kan findes her: https://aka.ms/MSCloudGovernanceEN

Dette whitepaper vil noget omfang blive opdateret i fald der skulle fremkomme væsentlige nye elementer for emnet – senest version kan altid findes her https://aka.ms/MSCloudGovernance.

Bemærk at i Maj 2021 annoncerede Microsoft et nyt initiativ kaldet 'EU Data Boundary', som i løbet af perioden frem imod 1. januar, 2023 vil ændre en række forhold ifm. Microsoft HSCC – for flere detaljer henvises til spørgsmål #2 i den første 'Q&A' sektion.

I. Liste over spørgsmål

Gode spørgsmål – til cloud-udbyderen

Gode spørgsmål – til egen organisation