Hvidbog om databeskyttelse i EU

November 2016

(Du kan finde den seneste udgave af denne hvidbog på http://aws.amazon.com/compliance/aws-whitepapers/ og den tyske udgave på http://aws.amazon.com/de/data-protection/).

Indledning

Dette dokument er udarbejdet som en hjælp til kunder, der vil benytte AWS til at lagre indhold, der omfatter personoplysninger. Dokumentet gennemgår navnlig, hvordan kunderne kan bruge AWS-tjenesterne i overensstemmelse med Europa-Parlamentet og Rådets direktiv 95/46/EF af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger ("direktivet"). Det har til formål at give kunderne kendskab til:

- Hvordan AWS-tjenesterne fungerer, herunder hvordan kunderne kan overholde EU-lovgivningen, opfylde deres sikkerhedsbehov samt kryptere og på anden måde beskytte deres indhold
- Kundernes fulde kontrol over, hvor deres indhold rent geografisk kan lagres og tilgås, og andre relevante spørgsmål om overholdelse af regler og standarder
- De roller, som henholdsvis kunden og AWS spiller i administrationen og sikringen af indhold, der er lagret på AWS-tjenesterne

Denne hvidbog giver svar på de spørgsmål, som AWS' kunder oftest stiller om direktivets konsekvenser for lagring af indhold, herunder personoplysninger, på AWS-tjenesterne. Kunderne bør også tage højde for andre relevante forhold, såsom hvorvidt de er pålagt at overholde bestemte branchespecifikke krav og love i andre jurisdiktioner, de opererer i. Oplysningerne i denne hvidbog er kun vejledende. De hverken udgør eller bør anvendes som juridisk rådgivning. Da behovene varierer fra kunde til kunde, opfordrer AWS sine kunder til at søge passende rådgivning om implementering af miljøer til beskyttelse af privatlivets fred og data og mere generelt om den lovgivning, som den enkelte kundes forretningsaktiviteter er omfattet af.

Overvejelser vedrørende kundens indhold

Alle organisationer er nødt til at søge svar på en række praktiske spørgsmål vedrørende lagring af indhold, såsom:

- Vil indholdet være tilstrækkeligt beskyttet?
- Hvor lagres indholdet?
- Hvem har adgang til indholdet?
- Hvilke love og regler er indholdet omfattet af, og hvad skal der til for at overholde dem?

Disse overvejelser er hverken nye eller specifikke for lagring i skyen. De er relevante for både internt drevne systemer og traditionelle eksterne tjenester, der drives af tredjepart. Kunder, der anvender AWS-tjenester, bevarer kontrollen over deres indhold og er ansvarlige for – og fuldt ud i stand til – at administrere og styre netop deres krav til indholdssikkerhed, herunder:

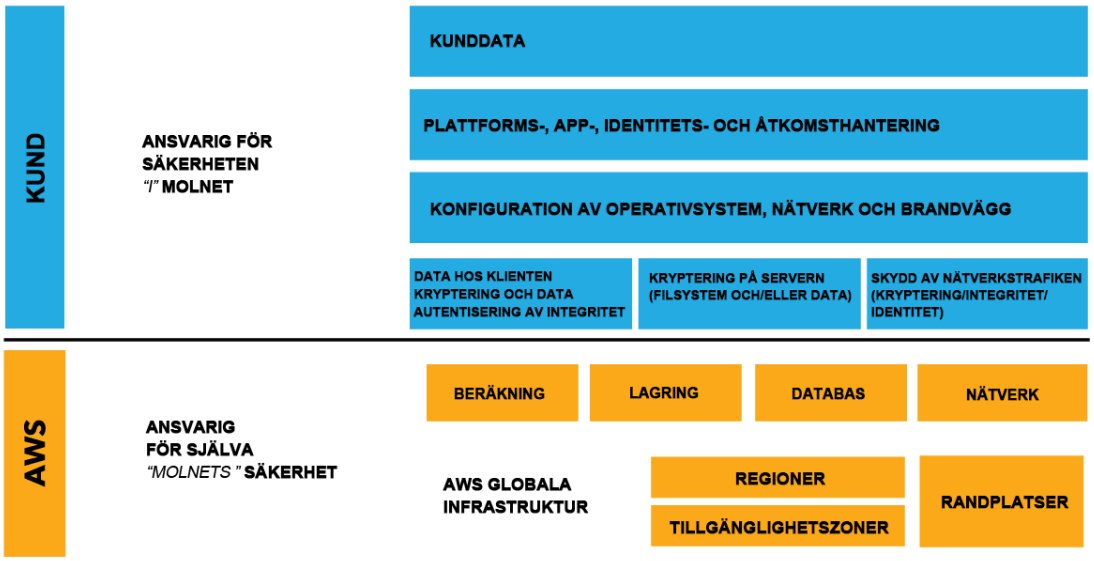
- Hvilket indhold de vælger at lagre på AWS
- Hvorvidt indholdet skal krypteres – når det lagres og overføres
- Hvilke AWS-tjenester der bruges med indholdet
- Hvor i verden det pågældende indhold lagres og behandles
- Indholdets format og struktur, og om det skal maskeres eller anonymiseres
- Hvem de giver adgang til indholdet, og hvordan adgangsrettighederne tildeles, administreres og tilbagekaldes

Både AWS og kunden skal implementere passende foranstaltninger til at beskytte indholdet. AWS har implementeret sikkerhedskontroller i det underliggende skybaserede miljø, men kunden har kontrollen over sit indhold og dets sikkerhed. For at afklare, hvilke databeskyttelseskrav der gælder for personoplysninger, som lagres på AWS, er det vigtigt at forstå henholdsvis kundens og AWS' rolle.

Sikkerheden af kundens indhold:

Kunden og AWS har hver deres vigtige ansvarsområder med hensyn til driften og administrationen af sikkerhed, når it-infrastruktur flyttes til AWS. AWS driver, administrerer og styrer komponenterne fra værtsoperativsystemet og virtualiseringslaget til sikkerheden af de fysiske faciliteter, der driver AWS-tjenesterne. Kunden er ansvarlig for at administrere gæsteoperativsystemet (herunder installere opdateringer og sikkerhedsrettelser på systemet) og tilhørende software samt konfigurere sikkerhedsgruppefirewallen og de øvrige sikkerhedsfunktioner, der leveres af AWS. Kunden opretter som regel forbindelse til AWS-miljøet via tredjepartstjenester (f.eks. internetudbydere). AWS leverer ikke disse forbindelser, og kunden bør vurdere forbindelsessikkerheden og sådanne tredjeparters ansvar i forhold til systemsikkerheden. Det svarer i det store hele til situationen, hvor en netværksudbyder leverer forbindelse til lokale datacentre.

Denne model er vist nedenfor i figur 1:



Figur 1 – sikkerhedsmodel

Hvilken betydning har denne model for sikkerheden af kundens indhold?

Ved sikkerhedsvurderingen af en skybaseret løsning er det vigtigt, at kunden forstår og skelner mellem:

- De sikkerhedsforanstaltninger, som udbyderen af skytjenesten (AWS) implementerer og driver – dvs. "sikkerheden ***af*** skyen", og
- De sikkerhedsforanstaltninger, som kunden implementerer og driver for at sikre sit indhold og sine applikationer, der benytter AWS-tjenester – dvs. "sikkerheden ***i*** skyen"

Hvor AWS varetager sikkerheden ***af*** skyen, er sikkerheden ***i*** skyen kundens ansvar. Det skyldes, at kunderne selv vælger, hvilke sikkerhedsforanstaltninger de vil anvende til at beskytte deres indhold, platform, applikationer, systemer og netværk – ligesom hvis de benyttede et lokalt datacenter. AWS tilbyder sine kunder en række forskellige sikkerhedsforanstaltninger, og kunderne kan også benytte sikkerhedsløsninger fra tredjeparter. AWS' kunder kan frit udforme deres sikkerhedsarkitektur, så den opfylder netop deres behov. Dette er en afgørende forskel i forhold til traditionelle hostingløsninger, hvor arkitekturen er fastlagt af udbyderen. AWS giver kunden mulighed for selv at afgøre, hvilke sikkerhedsforanstaltninger – hvis nogen overhovedet – der skal implementeres i skyen, og om de er passende for kundens aktiviteter. Hvis der f.eks. er behov for en arkitektur med højere tilgængelighed for at beskytte data, kan kunden tilføje redundante systemer, sikkerhedskopiering, placeringer, netværksuplink mv. for at gøre arkitekturen mere robust. Hvis det er nødvendigt at begrænse adgangen til data, kan kunden via indstillingerne i AWS implementere modeller for styring af adgangsrettigheder både på systemniveau og via kryptering på dataniveau. AWS giver dermed kunden direkte kontrol over en lang række elementer, der udgør tekniske og organisatoriske datasikkerhedsforanstaltninger.

Forstå sikkerheden af skyen

AWS er ansvarlig for at administrere sikkerheden af det underliggende skybaserede miljø. Skyens infrastruktur gør AWS til et af de mest fleksible og sikre cloudcomputingmiljøer med både optimal tilgængelighed og fuld adskillelse af kunder. AWS er en ekstremt skalerbar og pålidelig platform, hvor kunderne hurtigt og sikkert kan installere applikationer og indhold i stor og global skala, når det er nødvendigt. AWS-tjenesterne gør ikke forskel på indholdstyper. Alle kunder får gavn af samme høje sikkerhedsniveau, uanset hvilken type indhold der er tale om, og hvilken geografisk region det lagres i. Da AWS ikke ved, hvilke data kunderne lagrer i AWS-tjenesterne, kan AWS ikke skelne personoplysninger fra andre typer af data, der udgør en kundes indhold.

Det meget høje sikkerhedsniveau i AWS' datacentre opnås ved hjælp af topmoderne elektronisk overvågning og avancerede adgangskontrolsystemer. Uddannede sikkerhedsvagter bevogter datacentrene døgnet rundt, og kun personer med et bestemt minimum af rettigheder har adgang til dem – og kun for at udføre systemadministration. Du kan finde en detaljeret liste over alle de sikkerhedsforanstaltninger, der er indbygget i AWS' skyinfrastruktur, platforme og tjenester, i hvidbogen Overview of Security Processes.

Vi tager sikkerheden i vores underliggende skybaserede miljø meget alvorligt og har derfor indført avancerede tekniske og organisatoriske foranstaltninger for at forhindre uautoriseret adgang. Kunderne kan få bekræftet sikkerhedsforanstaltningerne i AWS-miljøet via diverse AWS-certificeringer og -rapporter, herunder rapporterne AWS Service Organization Control (SOC) 1 og 2 og rapporterne om ISO 27001-certificering og PCI-DSS-overholdelse. Disse rapporter og certificeringer er udarbejdet af uafhængige tredjeparter og bekræfter designet og effektiviteten af AWS' sikkerhedskontroller. De gældende AWS-certificeringer og -rapporter kan rekvireres på https://aws.amazon.com/compliance/contact. Du kan få flere oplysninger om AWS' overholdelsescertificeringer, rapporter og overensstemmelse med bedste praksis og standarder på AWS' websted for overholdelse af regler og standarder.

AWS tilbyder et databehandlingstillæg for at hjælpe kunderne med at overholde deres databeskyttelsesforpligtelser. AWS kan også føje standardkontraktbestemmelserne 2010/87/EU (omtales ofte som "modelklausuler") til en kundes databehandlingstillæg, hvis det er nødvendigt i forbindelse med overførsel af personoplysninger fra EU til et land uden for Det Europæiske Økonomiske Samarbejdsområde.

AWS' databehandlingstillæg, inklusive modelklausulerne, blev den 6. marts 215 godkendt af de EU-databeskyttelsesmyndigheder, der samlet kaldes Artikel 29-gruppen. Det betyder, at alle AWS-kunder, som har AWS' databehandlingstillæg med modelklausulerne indføjet, opfylder kravene til internationale datastrømme i overensstemmelse med direktivet. Du kan få flere oplysninger om Artikel 29-gruppens godkendelse på webstedet for Luxembourgs databeskyttelsesmyndighed:
http://www.cnpd.public.lu/en/actualites/international/2015/03/AWS/index.html

Ud over databehandlingstillægget og modelklausulerne kan kunder, som har behov for at overføre personoplysninger fra AWS' EU-regioner til AWS' amerikanske regioner, drage fordel af AWS' deltagelse i EU-U.S. Privacy Shield Framework (ordningen for EU's og USA's værn om privatlivets fred). Amazon.com, Inc., og visse af dets amerikanske datterselskaber, herunder AWS, blev certificeret i henhold til EU-U.S. Privacy Shield Framework den 21. oktober 2016. EU-U.S. Privacy Shield Framework påvirker ikke kundernes brug af AWS, men udgør en ekstra, EU-godkendt mekanisme til overførsel af personoplysninger fra EU til USA. Du kan få flere oplysninger om amerikanske udbyderes forpligtelser i henhold til EU-U.S. Privacy Shield Framework på Europa-Kommissionens websted: http://ec.europa.eu/justice/data-protection/international-transfers/eu-us-privacy-shield/index_en.htm og på webstedet for EU-U.S. Privacy Shield Framework: https://www.privacyshield.gov/welcome.

Forstå sikkerheden i skyen

Kunden bevarer kontrollen over sit indhold ved brug af AWS-tjenesterne. Det er kunderne – og ikke AWS – der bestemmer, hvilket indhold de lagrer i AWS, hvordan de konfigurerer deres miljø og sikrer deres indhold, om de vil kryptere indholdet ved lagring og overførelse, hvem der skal have adgang til indholdet og med hvilke legitimationsoplysninger (herunder brug af multifaktorgodkendelse), samt hvilke yderligere sikkerhedsfunktioner og -værktøjer de bruger og hvordan.

Da kunderne bevarer kontrollen over sikkerheden, har de også ansvaret for sikkerheden af alt det, de lægger op på AWS, eller som de forbinder til AWS-infrastrukturen, såsom gæsteoperativsystemet, applikationer på beregningsinstanserne samt indholdet, der lagres og behandles på AWS' lager-, platforms- og databasetjenester.

Kunderne kan indstille AWS-tjenesterne til at beskytte indholdet med forskellige valgfri sikkerhedsfunktioner, -værktøjer og -kontroller, herunder avanceret identitets- og adgangsstyring, tilgængelighedskonfigurationer, sikkerhedskopiering, sikkerhedsfunktioner, kryptering og netværkssikkerhed. AWS tilbyder en bred vifte af sikkerhedsfunktioner, så kunderne kan udforme, implementere og drive deres eget sikre AWS-miljø. Kunderne kan også benytte egne eller en tredjeparts sikkerhedsværktøjer og -kontroller. Kunderne kan bl.a. sikre deres indhold ved:

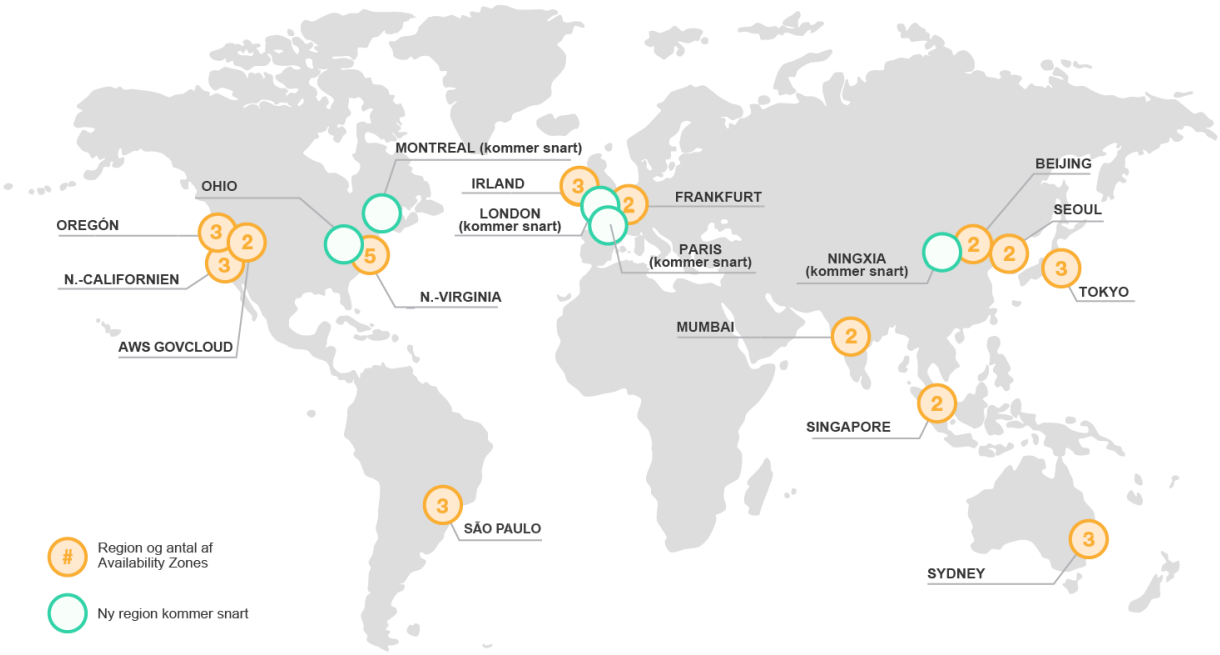
- at indføre politikker om stærke adgangskoder, tildele relevante tilladelser til brugerne og sikre behørig beskyttelse af deres adgangsnøgler
- at anvende firewalls og netværkssegmentering, herunder Virtual Private Cloud, kryptere indhold, bruge SSL og passende systemarkitektur for at mindske risikoen for datatab og uautoriseret adgang
- at indføre relevante redundansmodeller og strategier til sikkerhedskopiering for at mindske risikoen for tab eller manglende tilgængelighed af data

Det er alt sammen noget, kunderne har kontrol over, og ikke AWS. AWS kan hverken se det indhold, kunderne lægger op på AWS, eller ændre deres konfigurationsindstillinger – det kan kun kunden gøre. Derfor er det også alene kunden, der kan afgøre, hvilket sikkerhedsniveau der er passende for kundens indhold i AWS-skyen.

AWS udgiver en række hvidbøger om sikkerhed, styring, risiko og overholdelse af regler og standarder samt en række tjeklister og bedste praksis for at hjælpe kunderne med at integrere AWS' sikkerhedskontroller i eksisterende kontrolrammer samt udarbejde og gennemføre sikkerhedsvurderinger af organisationens brug af AWS' tjenester. Kunderne kan også frit udforme og gennemføre tilpassede sikkerhedsvurderinger og anmode om tilladelse til at gennemføre scanninger af deres skyinfrastruktur (forudsat at scanningerne kun omfatter kundens beregningsinstanser og ikke overtræder AWS' politik om acceptabel brug).

AWS-regioner

AWS' datacentre er bygget i klynger og placeret i forskellige lande i verden. Vi kalder hver af vores datacenterklynger i et givet land for en "region". Kunderne har adgang til fjorten AWS-regioner rundt om i verden, herunder to regioner i EU – Irland (Dublin) og Tyskland (Frankfurt). Kunderne kan vælge at bruge én region, alle regioner eller en kombination af regioner. Figur 2 viser placeringen af AWS-regionerne:



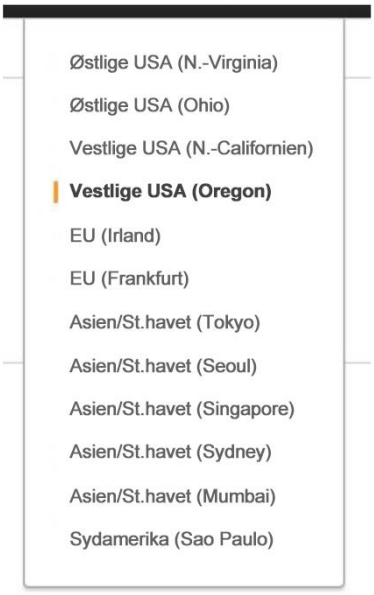
Figur 2 – globale AWS-regioner

AWS' kunder vælger den eller de AWS-regioner, hvor deres indhold skal lagres. Det giver kunder med særlige geografiske krav mulighed for at vælge det eller de steder, de vil etablere miljøer. Eksempelvis kan en kunde i Europa vælge udelukkende at implementere sine AWS-tjenester i EU-regionen (Tyskland). I så fald lagres kundens indhold i Tyskland, medmindre kunden vælger en anden AWS-region.

Kunderne kan replikere og sikkerhedskopiere indhold i flere regioner, men AWS flytter ikke kundens indhold uden for kundens valgte region(er).

Hvordan vælger kunderne deres region(er)?

Når kunden bruger AWS Management Console eller afgiver en anmodning via en af AWS' API'er (programmeringsgrænseflader), vælger kunden den eller de regioner, hvor AWS-tjenesterne skal bruges. Figur 3: Valg af globale AWS-regioner er et eksempel på proceduren for upload af indhold til en AWS-lagringstjeneste eller klargøring af beregningsressourcer i AWS Management Console.



Figur 3 – valg af globale AWS-regioner i AWS Management Console

Kunderne kan desuden vælge, hvilken AWS-region der skal bruges til deres beregningsressourcer, ved at benytte Amazon Virtual Private Cloud (VPC). Med Amazon VPC kan kunden klargøre en sektion i AWS-skyen til kørsel af AWS-ressourcer i et virtuelt netværk, som kunden definerer. Med Amazon VPC kan kunderne definere en virtuel netværkstopologi, der i høj grad minder om det traditionelle netværk, som kunden kunne have kørende i sit eget datacenter.

Alle beregningsressourcer og øvrige ressourcer, som kunden kører i VPC, vil være placeret i den region, kunden har valgt.

Kundekontroller og adgang til kundens indhold

Kundens kontrol over indholdet

AWS' kunder bevarer kontrollen over deres indhold i AWS-miljøet. De kan:

- vælge, hvor det skal placeres, f.eks. typen af lagringsmiljø og lagerets geografiske placering
- bestemme formatet af indholdet, såsom almindelig tekst, maskeret, anonymiseret eller krypteret, enten ved hjælp af AWS' egen kryptering eller en krypteringsmekanisme fra en tredjepart, som kunden selv vælger
- administrere andre adgangskontroller, adgangsstyring efter identitet samt sikkerhedslegitimationsoplysninger
- styre, om der skal bruges SSL, Virtual Private Cloud og andre former for netværkssikkerhed for at forhindre uautoriseret adgang

Dette bevirker, at AWS' kunder kan styre hele livscyklussen for deres indhold på AWS og administrere indholdet i overensstemmelse med egne specifikke behov, herunder indholdsklassificering, adgangskontrol, opbevaring og sletning.

Adgang til kundens indhold

AWS tilgår aldrig kundens indhold, medmindre det er nødvendigt for at levere de AWS-tjenester, som kunden har valgt. AWS tilgår kun kundernes indhold med dette ene formål.

AWS kan ikke se, hvilket indhold kunderne vælger at lagre på AWS, og derfor heller ikke skelne mellem personoplysninger og andet indhold. Det betyder, at AWS behandler alt kundeindhold på samme måde. Det betyder samtidigt, at alt indhold er omfattet af de samme robuste AWS-sikkerhedsforanstaltninger, uanset om det indeholder personoplysninger eller ej. AWS yder blot kunden de aftalte beregnings-, opbevarings-, database- og netværkstjenester koblet med de meget avancerede sikkerhedsforanstaltninger, der beskytter AWS' skyinfrastruktur. Kunden kan derefter frit tilpasse sikkerheden i infrastrukturen til sine egne specifikke behov.

Myndigheders ret til adgang

Mange er interesseret i at vide, i hvilket omfang indenlandske og udenlandske myndigheder har ret til at få adgang til indhold i skytjenester. Kunderne er ofte bekymrede over forhold omkring datasuverænitet, herunder om og under hvilke omstændigheder myndigheder kan få adgang til deres indhold. For nogle kunder er det vigtigt at tage højde for lovgivningen i den jurisdiktion, hvor indholdet er placeret. Kunderne bør dog også tage højde for, om de er omfattet af lovgivningen i andre jurisdiktioner, alt efter hvor de – eller deres kunder – opererer. Kunderne bør rådføre sig for at få afklaret, hvordan relevante love finder anvendelse på deres forretning og aktiviteter.

Når der opstår bekymring eller spørgsmål om lokale eller udenlandske myndigheders ret til at få adgang til indhold i skyen, er det vigtigt at forstå, at de pågældende myndigheder kan have beføjelse til at udstede en anmodning om adgang til sådant indhold i henhold til love, som kunden allerede er omfattet af. F.eks. kan en virksomhed med forretningsaktiviteter i land X være pålagt at opfylde en retlig anmodning om oplysninger, selv om indholdet er lagret i land Y. Som regel vil en statslig myndighed, der anmoder om adgang til en juridisk persons data, rette anmodningen direkte til den pågældende juridiske person i stedet for udbyderen.

Lovgivningen i EU's medlemsstater giver generelt de nationale retshåndhævende myndigheder og sikkerhedsorganer beføjelse til at søge adgang til oplysninger. Også udenlandske retshåndhævende myndigheder kan få adgang til oplysninger i EU via lokale og nationale retshåndhævende myndigheder. Faktisk har de fleste lande procedurer (herunder aftaler om gensidig retshjælp) for overførsel af oplysninger til andre lande, hvis de modtager en retsgyldig anmodning om oplysninger (f.eks. om kriminelle handlinger). Det er dog vigtigt at huske på, at anmodningen kun kan godkendes, når en række kriterier i henhold til den relevante lovgivning er opfyldt. Eksempelvis skal den myndighed, der anmoder om adgang, have en gyldig grund til at pålægge en part at give adgang til indhold og muligvis også indhente en retskendelse eller ransagningskendelse.

De fleste landes lovgivning om dataadgang foregiver at gælde uden for landets egne grænser. Et eksempel er USA's Patriot Act, der ofte kommer på tale i forbindelse med skytjenester. Patriot Act adskiller sig ikke væsentligt fra den lovgivning i de fleste andre udviklede lande, der giver myndighederne mulighed for at indhente oplysninger i forbindelse med efterforskning af international terrorisme og andre udenlandske efterretningsopgaver. En anmodning om udlevering af dokumenter i henhold til Patriot Act kræver en retskendelse, der godtgør, at anmodningen er i overensstemmelse med loven, og at den f.eks. vedrører en legitim undersøgelse.

AWS' politik

AWS prioriterer altid beskyttelsen af kundernes indhold højt, uanset hvor en anmodning om kundeindhold kommer fra, eller hvem kunden er. AWS udleverer aldrig indhold, medmindre vi modtager en retsgyldig og bindende afgørelse, såsom en stævning eller retskendelse. Statslige myndigheder eller organer uden for USA skal typisk følge internationale procedurer, såsom aftaler med den amerikanske regering om gensidig retshjælp, for at indhente retsgyldige og bindende afgørelser. Vi sikrer os altid, at den enkelte anmodning er retsgyldig og udstedt i overensstemmelse med gældende lovgivning. Vi forkaster en anmodning, hvis den er alt for generel, falder uden for den anmodende myndigheds beføjelser eller ikke er i fuld overensstemmelse med gældende lov. Hvis vi tvinges til at udlevere en kundes indhold, underretter vi kunden forud, så kunden kan beskytte sig mod udleveringen, medmindre dette ville udgøre en lovovertrædelse.

Databeskyttelse i EU: direktivet

Nedenfor behandler vi forpligtelserne i direktivet[1]. Direktivet opstiller overordnet set en række databeskyttelseskrav, der gælder for behandling af personoplysninger. I denne sammenhæng defineres "behandling" som enhver operation eller række af operationer, som personoplysninger gøres til genstand for. I direktivet defineres "personoplysninger" som oplysninger, ud fra hvilke en levende person (benævnt "den registrerede") kan identificeres eller er identificerbar. Derudover skelner direktivet mellem a) den "registeransvarlige" – den part, der afgør, til hvilket formål og med hvilke hjælpemidler der må foretages behandling af personoplysninger, og b) en "registerfører" – en part, der behandler personoplysninger på den registeransvarliges vegne.

Det er pålagt den registeransvarlige at sikre, at behandlingen af personoplysninger overholder kravene til databeskyttelse. Den registeransvarlige skal f.eks. sikre, at personoplysninger behandles rimeligt og lovligt og er sikret mod uautoriseret eller ulovlig behandling.

AWS er klar over, at AWS-tjenesterne anvendes som led i en række forskellige forretningsaktiviteter, og at en given forsyningskæde kan omfatte flere parter. Hvis det indhold, en kunde lagrer ved hjælp af AWS-tjenesterne, omfatter personoplysninger, vil det som hovedregel forholde sig sådan, at:

[1] Vi bør huske på, at direktivet ikke finder direkte anvendelse på organisationer, der er etableret i EU's medlemsstater. Medlemsstaterne er til gengæld forpligtet til at gennemføre direktivet i deres nationale lovgivning. Derfor kan kravene variere fra medlemsstat til medlemsstat, og kunderne bør rådføre sig om, hvilke nationale love der gælder for dem.

- kunden vil være den registeransvarlige for de pågældende personoplysninger, hvis det er denne, der afgør, til hvilket formål oplysningerne skal behandles og hvordan
- kunden vil være en registerfører i forhold til de pågældende personoplysninger, hvis kunden blot behandler personoplysningerne på AWS-netværket på vegne af og efter anvisning fra en tredjepart (der kan være den registeransvarlige, en anden tredjepart i forsyningskæden eller en person, der alene opererer nationalt).

AWS udbyder selvbetjeningsinfrastruktur, som kunderne har fuld kontrol over – også med hensyn til hvordan og hvorvidt dataene "behandles" – og leverer kun infrastrukturtjenesterne til kunder, der vil uploade og behandle indhold på AWS-netværket. AWS kan ikke se og har ikke kendskab til, hvad kunderne uploader til AWS-netværket, og hvorvidt dette indhold omfatter personoplysninger. AWS' kunder har også mulighed for at bruge kryptering til at gøre indholdet ulæseligt for AWS. AWS behandler ikke kundernes indhold, medmindre det er nødvendigt for at levere tjenesterne (eller for at efterleve loven eller en retsgyldig og bindende afgørelse).

AWS har også indført systemer, procedurer og politikker, som forhindrer AWS' medarbejdere i at få adgang til kundernes indhold. AWS tilbyder desuden kunder med behov for at behandle personoplysninger et databehandlingstillæg som en hjælp til at overholde forpligtelserne vedrørende databeskyttelse. AWS kan også føje modelklausulerne til en kundes databehandlingstillæg, hvis det er nødvendigt i forbindelse med overførsel af personoplysninger fra EU til et land uden for Det Europæiske Økonomiske Samarbejdsområde.

AWS' databehandlingstillæg, inklusive modelklausulerne, blev den 6. marts 215 godkendt af de EU-databeskyttelsesmyndigheder, der samlet kaldes Artikel 29-gruppen. Det betyder, at alle AWS-kunder, som har AWS' databehandlingstillæg med modelklausulerne indføjet, opfylder kravene til internationale datastrømme i overensstemmelse med direktivet. Du kan få flere oplysninger om Artikel 29-gruppens godkendelse på webstedet for Luxembourgs databeskyttelsesmyndighed:
http://www.cnpd.public.lu/en/actualites/international/2015/03/AWS/index.html

Det er pålagt den registeransvarlige at indføre passende tekniske og organisatoriske foranstaltninger til at beskytte personoplysningerne mod hændelig eller ulovlig tilintetgørelse, mod hændeligt tab, forringelse og ubeføjet udbredelse eller ikke-autoriseret adgang. Hvis behandlingen foretages af en registerfører på den registeransvarliges vegne, er den registeransvarlige også pålagt at vælge en registerfører, der har truffet de omtalte tekniske og organisatoriske foranstaltninger.

I oversigten nedenfor har vi sammenfattet nogle af de centrale databeskyttelsesprincipper, som kunderne normalt tager i betragtning i denne sammenhæng. Vi ser også på de aspekter af AWS-tjenesterne, der er relevante for disse principper. I oversigten har vi antaget, at AWS-kunden er den registeransvarlige. Vi er dog som nævnt ovenfor klar over, at AWS-kunden i mange tilfælde er registerføreren. I disse situationer vil AWS-kunden dog stadig kunne bruge nedenstående oplysninger i forhold til sin relation til den registeransvarlige.

Databeskyttelsesprincip	**Sammenfatning af databeskyttelsesforpligtelsen**	**Overvejelser**
Rimelighed	Den registrerede bør gives nøjagtige og fyldestgørende oplysninger om den registeransvarliges identitet, formålet med behandlingen samt andre nødvendige oplysninger for at garantere en rimelig behandling.	**Kunde:** Det er kunden (eller dennes kunde), der beslutter, hvilke oplysninger der indsamles, og hvilke formål de bruges til. I mange tilfælde vil kunden have en direkte relation til de registrerede og derfor være bedst i stand til at kommunikere direkte med dem. Desuden bør kunden kende omfanget af eventuelle meddelelser, der tidligere er givet til de registrerede. **AWS:** AWS har ingen kontrol over, hvilke typer af indhold kunden vælger at lagre i AWS og til hvilke formål. AWS har heller ikke indblik i dette indhold (og ved derfor ikke, om det indeholder personoplysninger). AWS har ikke mulighed for at identificere eller kontakte de registrerede, hvis personoplysninger kunden har valgt at gemme i AWS-infrastrukturen, og kan derfor ikke forsyne de relevante registrerede med nogen form for oplysninger.
Hjemmel	Den registeransvarlige skal have hjemmel til behandlingen, der skal opfylde mindst ét af kriterierne i direktivet.	**Kunde:** Når kunden beslutter, om og til hvilket formål personoplysningerne skal behandles, skal kunden vurdere, om et af kriterierne i direktivet er opfyldt. Kriteriet kan f.eks. være, at den registrerede har givet sit samtykke, eller at behandlingen er nødvendig for opfyldelsen af en aftale, som den registrerede har indgået. **AWS:** Som nævnt ovenfor har AWS ingen kontrol over, hvilke typer af indhold kunden vælger at lagre i AWS (og ved derfor heller ikke, om det indeholder personoplysninger). AWS bestemmer ikke, hvilken arkitektur kunden vælger at opbygge ved at kombinere forskellige AWS-tjenester, eller hvorvidt den egner sig til kundens specifikke behov. AWS spiller ingen rolle i beslutningen om, hvorvidt og til hvilke formål disse oplysninger behandles. Derfor kan AWS heller ikke vurdere, om der er hjemmel til at udføre behandlingen.

Formålsbeg-rænsning	Personoplysninger må kun indsamles til udtrykkeligt angivne og legitime formål, og de må ikke senere gøres til genstand for behandling, der er uforenelig med disse formål.	**Kunde:** Det er kunden, der bestemmer, hvilke personoplysninger der indsamles og til hvilke formål. Kunden skal sikre, at der foreligger et udtrykkeligt angivet og legitimt formål. Kunden bestemmer, om oplysningerne efterfølgende skal behandles til andre formål, og kan foretage en vurdering af, om disse er forenelige med det oprindelige formål. **AWS:** AWS har ingen kontrol over, til hvilke formål kunden bruger sit indhold og gemmer det i AWS-skyen. Hvis kundens indhold omfatter personoplysninger, behandler AWS kun disse med henblik på at levere de valgte AWS-tjenester til kunden (bortset fra de begrænsede tilfælde, hvor det er påkrævet for at overholde loven eller efterleve en retsgyldig og bindende afgørelse).
Registreredes rettigheder	De registrerede skal kunne få adgang til deres personoplysninger og få berigtiget, slettet eller blokeret personoplysninger, som behandles på anden måde end i overensstemmelse med direktivet.	**Kunde:** Kunden bevarer kontrollen over det indhold, der er lagret på AWS, og bestemmer derfor, hvordan de registrerede kan få adgang til deres personoplysninger, der indgår i dette indhold. Det er ligeledes også kunden, der er bedst i stand til at besvare en anmodning eller en klage fra en registreret vedrørende lovligheden af kundens databehandlingsaktiviteter. **AWS**: Som nævnt ovenfor har AWS ingen kontrol over, hvilke typer af indhold kunden vælger at lagre i AWS og til hvilke formål. AWS har heller ikke indblik i dette indhold (og ved derfor ikke, om det indeholder personoplysninger). AWS kan ikke identificere og har ingen kontakt med de registrerede, hvis personoplysninger kunden har valgt at lagre i AWS-infrastrukturen (ud over de tilfælde, hvor det vedrører kunden selv), og kan derfor ikke forsyne de relevante registrerede med nogen form for oplysninger. AWS har ingen mulighed for at knytte oplysninger, der er lagret på AWS, til en bestemt person. De oplysninger har alene kunderne kontrol over.
Rigtighed	De registeransvarlige skal sikre, at personoplysninger er korrekte og om nødvendigt ajourførte.	**Kunde:** Kunden har kontrol over de personoplysninger, som denne vælger at lagre på AWS. Det er derfor kundens ansvar at bekræfte og løbende ajourføre de lagrede oplysninger. Desuden administrerer kunden sikkerheden "i" skyen og har derfor både ansvaret og muligheden for at indføre passende foranstaltninger mod beskadigelse af data.

		AWS: AWS har ingen kontrol over, hvilke typer af indhold kunden vælger at lagre i AWS, og heller ikke indblik i indholdet. AWS hverken angiver eller ændrer data på kundens vegne. Derfor kan AWS hverken bekræfte rigtigheden af eller opdatere dataene. Rapporten SOC 1 Type 2 indeholder oplysninger om de kontroller, som AWS gennemfører for at sikre integriteten af dataene på det underliggende skybaserede miljøs niveau.
Datasikkerhed	De registeransvarlige skal indføre passende tekniske og organisatoriske foranstaltninger til at beskytte personoplysninger ne mod hændelig eller ulovlig tilintetgørelse, mod hændeligt tab, forringelse og ubeføjet udbredelse eller ikke-autoriseret adgang.	**Kunde:** Det er alene kunden, der kan afgøre, hvorvidt en bestemt sikkerhedsarkitektur, som kunden udformer eller implementerer, egner sig til en specifik type indhold, der måtte indeholde personoplysninger. Kunderne er ansvarlige for sikkerheden ***i*** skyen, herunder for at beskytte indholdet (og eventuelle personoplysninger deri) og implementere en egnet arkitektur ved hjælp af de enkelte komponenter i AWS. Kunderne er navnlig ansvarlige for på korrekt vis at a) konfigurere AWS-tjenesterne, b) benytte kontrollerne, der er tilgængelige i tilknytning til tjenesterne, og c) indføre de foranstaltninger, som de finder nødvendige for at sikre løbende sikkerhedskontrol og sikkerhedsko-piering af deres personoplysninger (f.eks. ved at beskytte personoplysninger mod uautoriseret adgang ved hjælp af kryptering og udføre rutinemæssig arkivering). **AWS:** AWS er ansvarlig for at administrere sikkerheden ***af*** det underliggende skybaserede miljø. Du kan finde en liste over alle de sikkerhedsforanstaltninger, der er indbygget i AWS' skyinfrastruktur, platforme og tjenester, i hvidbogen Overview of Security Processes[3]. AWS benytter eksterne undersøgere til at kontrollere effektiviteten af AWS' sikkerhedsforanstaltninger, herunder beskyttelsen af de fysiske datacentre, der leverer AWS-tjenesterne. Efter skriftlig anmodning fra kunden og ved undertegnelse af en fortrolighedsaftale kan kunden få et resumé af undersøgelsesrapporten og derved verificere AWS' sikkerhedsforanstaltninger. AWS stiller også resuméet til rådighed for databeskyttelsesmyndigheder efter anmodning.

Dataopbe-varing	Personoplysninger bør ikke opbevares (i identificerbar form) i et længere tidsrum end det, der er nødvendigt af hensyn til de formål, hvortil de indsamles, eller i forbindelse med hvilke de behandles på et senere tidspunkt.	**Kunde:** Det er kunden, der bestemmer, hvilke formål personoplysninger i AWS-skyen skal anvendes til, og dermed også hvor længe det er nødvendigt at opbevare dem. Kunden kan slette eller anonymisere personoplysningerne, når der ikke længere er behov for dem. **AWS:** AWS har ikke indblik i, om de lagrede data omfatter personoplysninger, eller kundens formål med at behandle bestemte data, der er lagret i skyen. AWS kan derfor ikke afgøre, hvor længe det er nødvendigt at bevare dataene for at opfylde dette formål. Når en kunde sletter sit indhold fra AWS-tjenesterne, bliver indholdet deaktiveret eller gjort ulæseligt, og de underliggende lagerområder på AWS-netværket, hvor indholdet var lagret, slettes fuldstændigt, inden de bliver frigjort og overskrevet i overensstemmelse med AWS' standardpolitikker og tidsplaner for sletning. AWS' procedurer omfatter desuden sikker nedlukning af lagringsmedier, der har været anvendt til at levere AWS-tjenesterne, inden de bortskaffes. Under denne proces bliver lagringsmedierne afmagnetiseret eller slettet og fysisk destrueret eller deaktiveret i overensstemmelse med almindelig standardpraksis.
Overførsel	Personoplysninger må ikke overføres til et land eller område uden for Det Europæiske Økonomiske Samarbejdsområde, medmindre det pågældende land eller område i tilstrækkeligt omfang beskytter de registreredes rettigheder og frihedsrettigheder i forhold til behandlingen af personoplysninger.	**Kunde:** Kunderne kan vælge den eller de AWS-regioner, hvor deres indhold og de relevante servere skal være placeret. Kunden kan vælge udelukkende at implementere sine AWS-tjenester i AWS' EU-regioner i Tyskland eller Irland. **AWS:** AWS flytter ikke en kundes indhold til noget sted uden for den eller de valgte regioner, medmindre det er nødvendigt for at overholde loven eller opfylde en retsgyldig og bindende afgørelse. AWS tilbyder et databehandlingstillæg for at hjælpe kunderne med at overholde deres databeskyttelsesforpligtelser. AWS kan også føje modelklausulerne til en kundes databehandlingstillæg, hvis det er nødvendigt i forbindelse med overførsel af personoplysninger fra EU til et land uden for Det Europæiske Økonomiske Samarbejdsområde. AWS' databehandlingstillæg, inklusive modelklausulerne, blev den 6. marts 215 godkendt af de EU-databeskyttelsesmyndigheder, der samlet kaldes Artikel 29-gruppen. Det betyder, at alle

		AWS-kunder, som har AWS' databehandlingstillæg med modelklausulerne indføjet, opfylder kravene til internationale datastrømme i overensstemmelse med direktivet. Du kan få flere oplysninger om Artikel 29-gruppens godkendelse på webstedet for Luxembourgs databeskyttelsesmyndighed: http://www.cnpd.public.lu/en/actualites/international/2015/03/AWS/index.html Ud over databehandlingstillægget og modelklausulerne kan kunder, som har behov for at overføre personoplysninger fra AWS' EU-regioner til AWS' amerikanske regioner, drage fordel af AWS' deltagelse i EU-U.S. Privacy Shield Framework (ordningen for EU's og USA's værn om privatlivets fred). EU-U.S. Privacy Shield Framework påvirker ikke kundernes brug af AWS, men udgør en ekstra, EU-godkendt mekanisme til overførsel af personoplysninger fra EU til USA. Du kan få flere oplysninger om amerikanske udbyderes forpligtelser i henhold til EU-U.S. Privacy Shield Framework på Europa-Kommissionens websted: http://ec.europa.eu/justice/data-protection/international-transfers/eu-us-privacy-shield/index_en.htm og på webstedet for EU-U.S. Privacy Shield Framework: https://www.privacyshield.gov/welcome.

Databrud

Da kunderne administrerer og har kontrollen over de personoplysninger, de har lagret på AWS, har de også ansvaret for at overvåge deres eget miljø for databrud og for at underrette myndigheder og berørte personer i henhold til gældende lovgivning. Det er alene kunden, der kan varetage dette ansvar.

Kunderne har kontrollen over deres egne adgangsnøgler og vælger selv, hvem der skal kunne få adgang til deres AWS-konto. AWS har ikke overblik over adgangsnøgler eller over, hvem der har og ikke har tilladelse til at logge ind på en konto. Det er derfor kundens ansvar at overvåge al brug, misbrug, fordeling eller tab af adgangsnøgler.

Når loven kræver det, underretter AWS straks kunden, hvis AWS har konkret kendskab til et bekræftet brud på AWS' sikkerhedsstandarder vedrørende AWS-netværket.

Underleverandører

AWS benytter en række underleverandører til at levere sine tjenester. Disse underleverandører har dog ikke adgang til kundernes indhold. Desuden bruger AWS kun underleverandører, som vi har tillid til, ligesom vi bruger relevante kontraktlige sikkerhedsforanstaltninger, som vi overvåger, for at sikre, at de krævede standarder opretholdes.

Kundens tredjepartsudbydere

Som nævnt tidligere i dette dokument er AWS-miljøet også forbundet til andre tjenester, som leveres direkte af tredjeparter (f.eks. internetudbydere). Disse tredjeparter har ansvaret for deres egne systemer, herunder systemernes sikkerhed, og AWS er ikke ansvarlig for disse tredjeparters aktiviteter.

Andre overvejelser

Denne hvidbog behandler ud over direktivet ikke anden lovgivning om privatlivsspørgsmål, der kan være relevant for kunderne, herunder eventuelle branchespecifikke krav. Hvilke love og regler om beskyttelse af privatlivets fred og data der gælder for den enkelte kunde, afhænger af flere faktorer, herunder hvor kunden udøver virksomhed og i hvilken branche, hvilken type indhold kunden vil lagre, hvorfra eller fra hvem indholdet stammer, og hvor det lagres.

Kunder, der er i tvivl om deres forpligtelser vedrørende databeskyttelse, bør først identificere og forstå de krav, der gælder for dem, og søge passende rådgivning.

Afsluttende kommentarer

Sikkerhed er altid AWS' højeste prioritet. Vi leverer tjenester til hundredtusindvis af kunder, herunder virksomheder, uddannelsesinstitutioner og offentlige styrelser i over 190 lande. Vores kunder tæller finanshuse og sundhedsudbydere, som betror os nogle af deres mest følsomme oplysninger, herunder helbredsoplysninger og regnskaber.

AWS-tjenesterne er udformet sådan, at kunderne frit kan konfigurere og implementere deres løsninger og have fuld kontrol over deres indhold, herunder hvor og hvordan det lagres, samt hvem der har adgang til det. AWS' kunder kan opbygge deres egne sikre applikationer og lagre indhold sikkert på AWS.

Yderligere ressourcer

Vi opfordrer vores kunder til at læse hvidbøgerne om risici, overholdelse af regler og standarder samt sikkerhed og de øvrige oplysninger om bedste praksis, tjeklister og vejledning på AWS' websted. Det giver kunderne en dybere forståelse af, hvordan de opfylder specifikke krav til beskyttelse af privatlivets fred og data. Dette materiale kan findes på http:/aws.amazon.com/compliance og http://aws.amazon.com/security.

AWS tilbyder også sine kunder kurser i at udforme, udvikle og drive effektive og sikre applikationer i AWS-skyen og udnytte mulighederne i AWS' tjenester og løsninger. Vi tilbyder gratis instruktionsvideoer, laboratorier, der kan gennemføres i eget tempo, og instruktørledede lektioner. Du kan få flere oplysninger om AWS' kurser på http://aws.amazon.com/training/.

AWS-certificeringerne attesterer de tekniske færdigheder og den tekniske viden, der er forbundet med bedste praksis for opbygning af sikre og pålidelige skybaserede applikationer ved hjælp af AWS-teknologi. Du kan få flere oplysninger om AWS-certificeringerne på http://aws.amazon.com/certification/.

Hvis du har behov for yderligere oplysninger, kan du kontakte AWS på: https://aws.amazon.com/contact-us/eller tage kontakt til din lokale kundeansvarlige hos AWS.