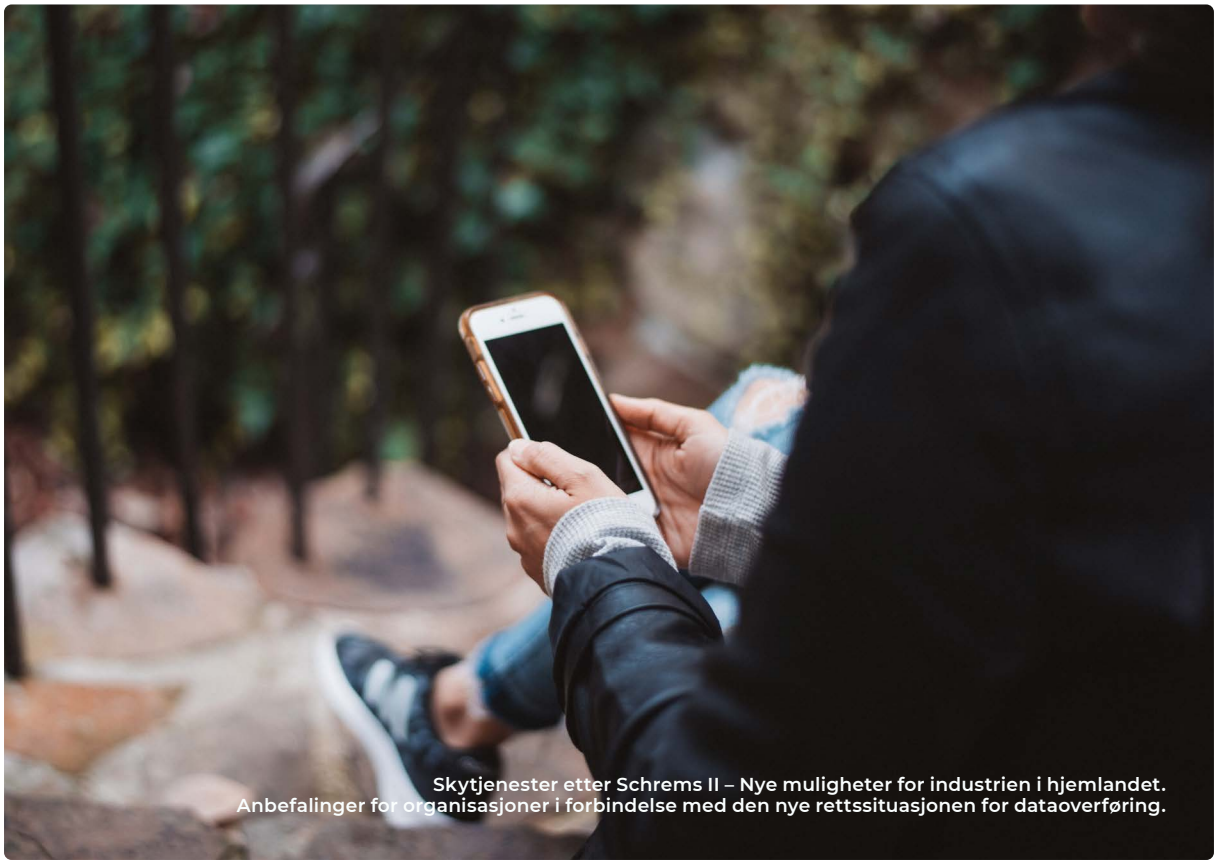
safespring

INFORMASJONSGUIDE:

# EU-domstolens ugyldiggjøring av Privacy Shield

Forutsetninger og anbefalinger for offentlig sektor og leverandører til offentlig sektor



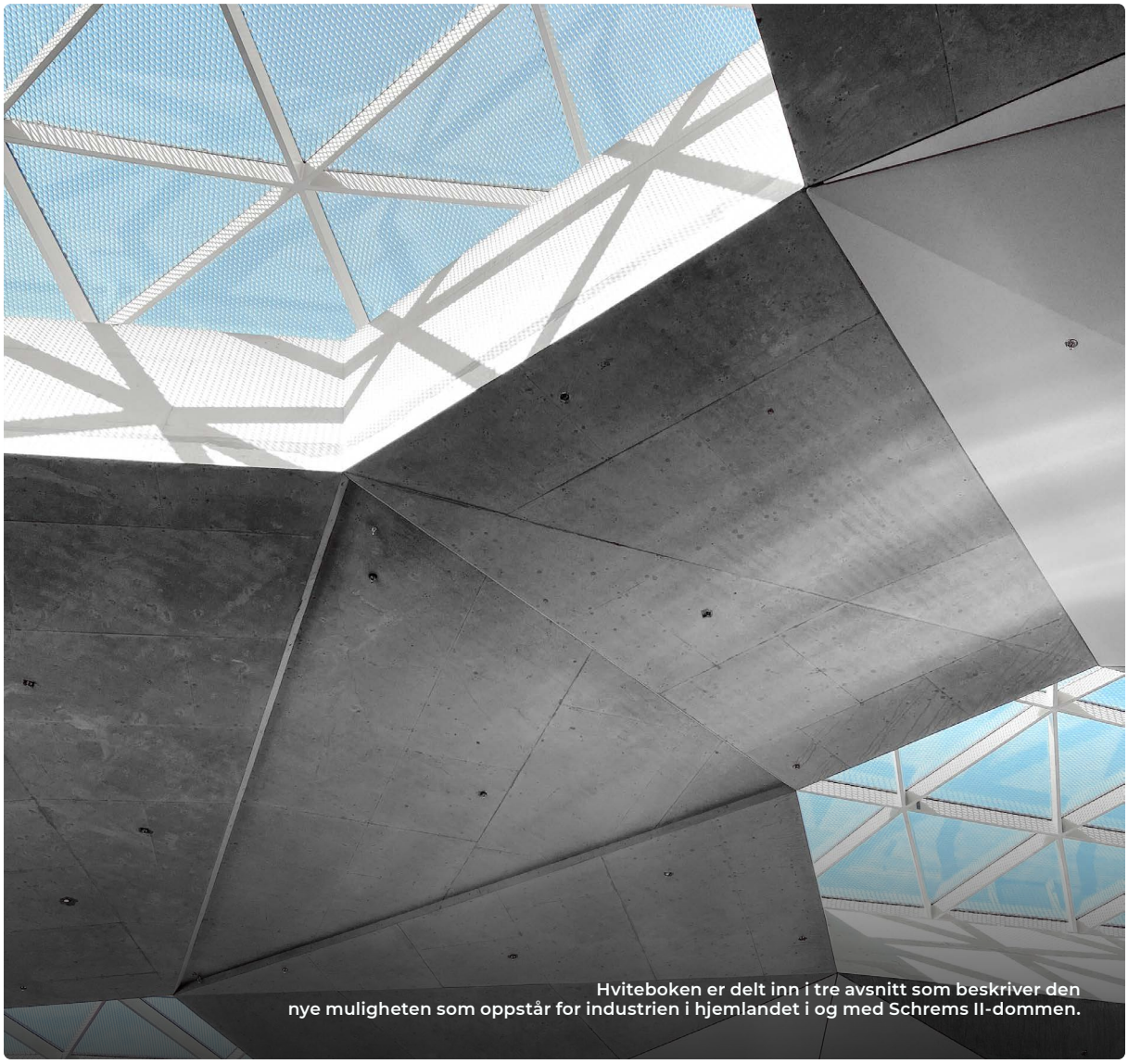

# Bakgrunn

## Våren 2018 publiserte Safespring en informasjonsguide om hvilke konsekvenser den europeiske personvernforordningen (GDPR)[1] og den amerikanske CLOUD Act har på skyanskaffelser i Sverige.

Safesprings informasjonsguide ble avsluttet med elleve anbefalinger til organisasjoner som jobber med skyinfrastruktur når det gjelder personvern, datasikkerhet og jurisdiksjonsspørsmål. Nå har EU-domstolen i en dom av 16. juli 2020, presisert ytterligere hvilke betingelser som gjelder for overføringen av europeiske privatpersoners opplysninger til amerikansk jurisdiksjon. Dermed kreves det en oppdatering av Safesprings tidligere anbefalinger. Dette dokumentet går gjennom Schrems II-avgjørelsen (del I), markedsstrukturen for skytjenester og samspillet mellom de tekniske kravene og jussen (del II), ulike norske aktørers rolle i videreutviklingen av markedsstrukturen og særlig behovet for koordinering av tiltak på statlig nivå (del III), samt en kort beskrivelse av veien framover (del IV). I del II og IV fordypes Safesprings tidligere anbefalinger for virksomheten til organisasjoner i forbindelse med den nye rettssituasjonen. Del III gir organisasjoner bedre forutsetninger for å stille de riktige kravene de til den statlige samordningen.

# Innehåll





Hviteboken er delt inn i tre avsnitt som beskriver den nye muligheten som oppstår for industrien i hjemlandet i og med Schrems II-dommen.

DEL I

# Innledning – Ytterligere presisering av dataoverføringsregler i EU/EØS

## Den 16. juli 2020 avsa EU-domstolen dom i sak C-311/18, ofte kalt Schrems II.

Den 16. juli 2020 avsa EU-domstolen sin dom i sak C-311/181, ofte også kalt «Schrems II», gjeldende spørsmålet om de europeiske konstitusjonelle prinsippene er forenelige med hva som fram til avgjørelsen falt, var politisk aksepterte normer for dataoverføringer til tredjelandet USA. I store trekk bekreftet dommen det som EU-domstolen allerede i flere avgjørelser etter at Lisboa-traktaten trådte i kraft i 2009, har understreket: Personvern er et konstitusjonelt prinsipp i EU/EØS-området (artikkel 8 i Den europeiske unionens pakt om grunnleggende rettigheter), og presiseringen av regler som skal opprettholde dette konstitusjonelle prinsippet i for eksempel personvernforordningen (GDPR), undergraver ikke det konstitusjonelle prinsippet.

Schrems II-dommen konkretiserer at disse konstitusjonelle normene medfører at visse deler av den amerikanske etterretnings- og sikkerhetslovgivningen forhindrer at selskapene som berøres av lovens forpliktelser, regnes som sikre mottakere av data i henhold til europeisk lovgivning. EU-domstolen minner også europeiske politikere om at de administrative beslutningene om tilstrekkelig beskyttelsesnivå som EU-kommisjonen kan fatte i henhold til GDPR artikkel 45, og overføringsavtalen i henhold til GDPR artikkel 46 og 49, ikke kan brukes for å tilsidesette de europeiske konstitusjonelle prinsippene om personvern.

Dommen har konsekvenser for selskaper og myndigheter som behandler europeiske borgeres personopplysninger, fordi muligheten for avtaler og samarbeid med aktører som kan berøres av forpliktelser i henhold til amerikansk lovgivning om datautlevering til myndigheter, nå er kraftig begrenset.

### Hva er en beslutning om tilstrekkelig beskyttelsesnivå?

En beslutning om tilstrekkelig beskyttelsesnivå betyr at EU-kommisjonen beslutter at et tredjeland har normer som beskytter europeiske statsborgeres rettigheter. En beslutning om tilstrekkelig beskyttelsesnivå er ikke en avtale i den forstand, men en unilateral kunngjøring fra EU-kommisjonens side. I praksis tar ikke EU-kommisjonen slike beslutninger alene, men får hjelp av en komité som består av representanter fra medlemslandene og ble dannet med grunnlag i artikkel 93 av personvernforordningen. EU-kommisjonens beslutninger kommer ofte etter forhandlinger med tredjelandet.

### Hva er en overføringsavtale?

Dataoverføringsavtaler kan være standardiserte personvernbestemmelser (GDPR artikkel 46.2), databehandleravtale (GDPR artikkel 46.3) eller avtaler mellom næringsvirksomhet og privatperson (GDPR artikkel 49).

Standardiserte personvernbestemmelser skal gi et i hovedsak likeverdig beskyttelsesnivå som den interne europeiske lovgivningen.

**EU-DOMSTOLEN HAR UTTRYKKELIG BESLUTTET**

- At sikkerhetslovgivningen i tredjelandet ikke påvirker hvordan europeiske statsborgeres rettigheter praktiseres, selv om den europeiske statsborgeren interagerer med næringsdrivende fra tredjelandet (C-311/18 paragraf 89)
- At kravet på en i hovedsak likeverdig beskyttelse av rettighetene til europeiske statsborgere ved dataoverføringer ikke påvirkes av den spesifikke mekanismen for overføringer som brukes (C-311/18 paragraf 92)
- At «beskyttelsesnivået» for personopplysninger skal være i hovedsak likeverdig med det som etableres i EU-retten, uten hensyn til særlige nasjonale bestemmelser i ulike EU-land (C-311/18 paragraf 101 og 103)
- At mulighetene for myndighetene i tredjeland til å skaffe seg tilgang til opplysninger påvirker beskyttelsesnivået (C-311/18 paragraf 103)
- At tilsynsmyndigheter plikter å agere når det ikke er mulig å etablere en i hovedsak likeverdig beskyttelse, særlig når en beslutning om tilstrekkelig beskyttelsesnivå mangler (C-311/18 paragraf 120-121)
- At en beslutning fra EU-kommisjonen om standardavtaleklausuler ikke påvirker forpliktelser som ansvarlige for personopplysninger og mottakere av personopplysninger har til å avbryte overføringer, hvis det viser seg at beskyttelsen som klausulene gjelder, ikke kan realiseres (C-311/18 paragraf 142).
- At EU-kommisjonens beslutning om tilstrekkelig beskyttelsesnivå, Privacy Shield, er ugyldig (C-311/18 paragraf 201)

EU-domstolen har i hovedsak bekreftet konklusjonene som allerede framgikk av Safesprings informasjonsguide fra 2018 om hvordan den usikre situasjonen pga CLOUD Act og GDPR bør håndteres («Hur du hanterar det osäkra läget i och med CLOUD Act och GDPR»). Mens det økonomiske stresset forårsaket av ytterligere spenninger mellom USA og EU i personvernspørsmål, ikke har avtatt verken på grunn av de politiske reaksjonene på Schrems I eller nå Schrems-II-dommen, er den juridiske situasjonen klarere nå.

### Hva er leverandørplassering?

Schrems II-dommen konstaterer at det er leverandørens geografiske plassering og ikke dataenes geografiske plassering som begrenser mulighetene for dataoverføringer til tredjeland, særlig amerikansk jurisdiksjon.

Domstolen mener at datavernet til europeiske privatpersoner vil bli undergravet hvis myndighetene i tredjelandet kan pålegge tjenesteleverandører i tredjelandet forpliktelser som gjør at personopplysningene til europeiske privatpersoner ikke får i hovedsak samme datavern som innenfor EUs, og i kraft av EØS-avtalen, hele EØS-områdets grenser. Disse konklusjonene er ikke nye i europeisk rett.

### Hva er et tredjeland?

Et tredjeland betyr i europeisk rett et land som ikke er medlem i Det europeiske økonomiske samarbeidsområde (EØS), som består av alle EU-landene og de tre EFTA-landene Norge, Island og Liechtenstein. Dataoverføringer til tredjeland reguleres i personvernforordningen (GDPR 5. kapittel).

Etter Schrems-II-dommen har det blitt tydeligere at det ikke først og fremst er et problem hvor selve dataene lagres, men hvilken geografisk plassering aktøren som lagrer dataene har. Rettighetene som kodifiseres i europeisk rett beskytter fysiske personer, og pliktene til å opprettholde rettighetene som kodifiseres i europeisk rett gjelder fysiske og juridiske personer. Hvis lovgivningen i tredjelandet er gyldig for en fysisk eller juridisk person på en slik måte at denne hindres fra å opprettholde plikter gjeldende grunnleggende rettigheter for en fysisk person, er dette altså et viktig hinder for interaksjon med denne fysiske eller juridiske personen.

Dommen setter nytt fokus på Safesprings anbefalinger til organisasjoner om skytjenester.[2] Men organisasjoner må ikke bare sørge for at de har en grundig juridisk analyse av datakataloger og juridisk grunnlag for personopplysningsbehandling og -overføringer, de må også sørge for at tjenester de benytter, bruker åpen spesifisert protokoll og er teknisk konstruert med formålet å muliggjøre eventuelle leverandørbytter i framtiden. Ved investeringer i eller bruk av skytjenester som i et markedsledd kan gjelde (europeiske) myndigheters behandling av personopplysninger, synes samhandel med amerikanske selskaper å være nesten utelukket med mindre USA ikke endrer sin nasjonale lovgivning til fordel for europeiske rettssubjekter.

Den siste forutsetningen vil være særlig interessant ved den prosessen som EU-kommisjonen har annonsert skal innlede samtaler om en ny beslutning om tilstrekkelig beskyttelsesnivå[3].

**Etter Schrems-II-dommen har det blitt tydeligere at det ikke fremfor alt er et problem hvor selve dataene lagres, men hvilken jurisdiksjon som gjelder for leverandøren.**

DEL II

# Skyen – lokal infrastruktur med lokal tilpasning

## Skytjenester har gitt organisasjoner store muligheter til å effektivisere og automatisere arbeidet.

Det er fremfor alt via stordriftsfordeler at skytjenester bidrar til alt fra miljømessige fordeler til bedre sikkerhetsarbeid. Men økte muligheter til raskt å få tilgang til enten datalagringskapasitet eller databehandlingskapasitet uten formelle tilbudsrunder har også bidratt til at den moderne formen for IT-drift har gjort framskritt både i privat og offentlig sektor.[4]

Fordelene ved en viss sentralisering viser seg også som økte tilpasningsmuligheter. Kostnader for utvikling og vedlikehold av grunnfunksjonaliteter kan fordeles på flere ulike parter. De siste 10 årene har det blitt etablert flere globale konsortier med formålet å vedlikeholde og utvikle nyttige grunnfunksjoner ved håndteringen av et stort antall servere.[5] Oppgaver som i et mindre IT-system kan ta mange manuelle timer, kan automatiseres i stordriftsmiljøer. Oppgaver som normalt er dyre og tidskrevende, for eksempel investeringer i sanntidsovervåking av IT-miljøets sikkerhet eller tiltak mot sikkerhetstrusler, er lettere å motivere. Med sikre og motiverte basisfunksjoner som utgangspunkt kan spesialiserte tjenester utvikles og tilpasses avhengig av virksomhetens spesifikke behov. Virksomheten kan stå på et stabilt og solid grunnlag uten at den må bygge opp en hel IT-arkitektur fra bunnen hver gang en nytt konsept skal prøves ut.

Den store interessen for skytjenester har ført til en rask utvikling av markedet, som nå omfatter en rekke forskjellige tjenester som har ulike fordeler for interesserte kunder. Ulike grader av automatisering og stordrift er mulig avhengig av hvilke spesifikke krav som gjelder for den enkelte organisasjonen som ønsker tjenesten.

Dermed omfatter betegnelsen «skytjeneste» delvis sentralisert håndtering av infrastruktur – virtualiserte servere med et operativsystem som kunden selv kan disponere etter eget ønske, og ved selv å legge til og vedlikeholde spesifikke tjenester for spesifikke formål (for eksempel databaser, internettservere eller administrative systemer). Og delvis omfatter betegnelsen spesifikke systemer der leverandøren av skytjenesten selv leverer databaseverktøy og andre grunnleggende komponenter for mer spesialisert funksjonalitet. Den mest synlige delen av skymarkedet for en typisk sluttforbruker består av tjenester der skytjenesteleverandøren allerede i stor grad har tilført verdi: Sentraliserte systemer for alt fra tekstredigering til planlegging og videokonferanser.

Skymarkedet har også utviklet seg slik at ulike typer skytjenester fungerer sammen i B2B-forhold. En skytjeneste med tilført verdi i form av et personalregistersystem kan også fungere sammen med en mer infrastrukturell skytjeneste som tilbyr virtuelle servere. Dermed må sluttkunden bare håndtere selve registreringen og verifiseringen av aktuelle opplysninger, og ikke vedlikeholde og administrere kodebaser og underliggende operativsystemer. Det er også vanlig at både infrastrukturelle tjenester og verditilførte tjenester leveres av samme markedsaktør. På samme måte som telekommarkedet på 1980-tallet var preget av vertikal integrasjon, domineres også skymarkedet i dag av aktører med en stor grad av vertikal integrasjon. Det betyr at selskapene leverer både infrastruktur, plattformer og programvare.


### Software as a service

SaaS er en programvare som tilbys som en tjeneste via internett. Kunden sørger vanligvis for dataregistreringen der kundens data behandles og lagres på server- og lagringskapasitet som leverandøren av tjenesten velger.

### Platform as a service

PaaS er en kombinasjon av serverkapasitet og programvare som utgjør en plattform for å utvikle og/eller kjøre applikasjoner. PaaS omfatter operativsystem og nødvendig kjøretid (f.eks. beholder) til å kjøre applikasjoner.

### Infrastructure as a service

IaaS er en nettbasert skytjeneste som tilbyr virtuell serverkapasitet og lagring via et programbasert grensesnitt, såkalt API. Muligheten for å programmere gjør at kunder kan skalere forbruket sitt opp og ned ved behov.

Sluttbrukere som anskaffer skytjenester bør nøye vurdere fordelene og ulempene ved vertikal integrasjon. I et vertikalt separert marked der mange ulike selskaper kan bidra med nye funksjonaliteter på alle nivåer i verdikjeden, finnes det større mulighet for et variert og tilpasset tjenestetilbud. Dessuten får store sluttbrukere bedre kunnskapsposisjon i forhold til leverandørene. Akkurat som vertikal separasjon og konkurranse på telekommarkedet åpnet for utvikling av innovative tjenester på 1990-tallet, kan separasjon og konkurranse på skymarkedet gi plass for innovative tjenester på 2020-tallet.

En viktig forskjell er at skymarkedet allerede i stor grad utspringer fra grenseoverskridende og felles åpne kodebaser. Opprinnelsen til markedet er global, ikke nasjonal, og et høyere nivå av vertikal separasjon medfører ikke nødvendigvis en høyere grad av nasjonalisering. Det gjør at både applikasjoner, beregningskraft og data som legges inn i applikasjonene er geografisk og organisatorisk bevegelige. Dataoverføringer har blitt vanlige både i grenseoverskridende betydning og i den forstand at data overføres mellom organisasjoner som hver enkelt spiller en egen rolle ved leveringen av den faktiske

tjenesten. Et tysk prosjekt som prøver å sammenføre erfaringer fra telekomindustrien med fordelene fra skyindustrien er GAIA-X[6]. Det er et rammeverk for kostnadsdeling mellom aktører med geografisk tilknytning og som tilbyr interoperable tjenester. I Frankrike har man i nesten ti år fremhevet at anskaffelsesinstrument kan være særlig egnet for å styrke europeiske småbedrifters rolle i digitale økosystemer, med særlig vekt på nettopp løsninger for åpne data og skytjenester.[7]

## Fleksibilitet krever økt ansvar

Skytjenester betyr i praksis at data som en anskaffende organisasjon har ansvaret for, og applikasjoner som bruker slike data som input, vil befinne seg på infrastruktur som ikke administreres av organisasjonen selv. Uansett hvilket verdiøkningsnivå organisasjoner velger til skytjenestene sine, er mange av stordriftsfordelene avhengige av at administratoren for infrastrukturen til skytjenesten har tilgang til nok informasjon om dataene som behandles for at det skal være mulig å gjøre ressursene tilgjengelige og tilby det sikkerhetsnivået som kunden krever. Det er i dette tekniske kravet som anskaffende organisasjoners plikter i henhold til Schrems II-dommen til EU-domstolen oppstår.

EU-domstolens vurdering av grunnleggende rettigheter i EU/EØS-området legger et krav på organisasjoner med ansvar for personopplysninger om å skaffe seg et overblikk over hele verdikjeden, også når man anskaffer en spesifikk og avgrenset programvareapplikasjon som kun skal gi begrenset nytte i egdn virksomhet. Sluttbrukeren bør ikke bare vurdere fordelene ved tjenesten man anskaffer, men også se på hvordan tjenesteleverandøren interagerer med underleverandører.

IT-infrastrukturen har det særtrekket at den er usynlig når det finnes hensiktsmessige standarder. Først når standarder ikke finnes, blir det tydelig at de mangler og gir problemer. IT-standarder er også i stor utstrekning usynlige i avgjørelser som de ansvarlige i virksomheten tar. Virksomhetsavgjørelser, for eksempel anskaffelse av e-tjenester, medfører ofte også avgjørelser om valg av standarder, men det virker ikke som disse beslutningene tas separat og uttrykkelig, i hvert fall ikke på ledelsesnivå, men blir en ikke-uttalt konsekvens av ulike andre virksomhetsbeslutninger. En konsekvens av både GDPR og Schrems II-dommen bør være at de ikke-uttalte konsekvensene må spesifiseres og uttales.

Databehandleren skal sørge for at eventuelle andre databehandlere denne benytter som underleverandører, er underlagt de samme avtalerettslige forpliktelsene overfor den behandlingsansvarlige, som databehandleren selv (GDPR artikkel 28).

Men det er den behandlingsansvarlige som er ansvarlig for at både databehandlerne og databehandlernes underleverandører har mulighet til å oppfylle de nødvendige avtalerettslige garantiene. Når enten en databehandler eller databehandlerens underleverandør er gjenstand for rettslige forpliktelser i et tredjeland, mener EU-domstolen at den behandlingsansvarlige har et omfattende ansvar for å sikre at de rettslige forpliktelsene ikke gir europeiske borgere dårligere personvern. EU-domstolen mener dessuten at den behandlingsansvarliges plikter ikke minsker når det ikke er mulig å konstatere en faktisk realisering av slike rettslige forpliktelser forspesifikke opplysninger, men at det er tilstrekkelig at en slik rettslig forpliktelse kan oppstå (jfr C-311/18 paragraf 142).

Safesprings informasjonsguide fra 2018 tar opp spørsmålene som alle organisasjoner bør drøfte ved valget av infrastruktur.[8] I lys av Schrems II-dommen må det konstateresat det vil være vanskelig for skytjenesteleverandører som er underlagt lovgivningen i tredjeland, å oppfylle kravene i EU-retten. Særlig for tredjelandet USA gjelder at den amerikanske lovgivningen må forandres for at selskaper som er basert i landet skal være mottakere av personopplysninger

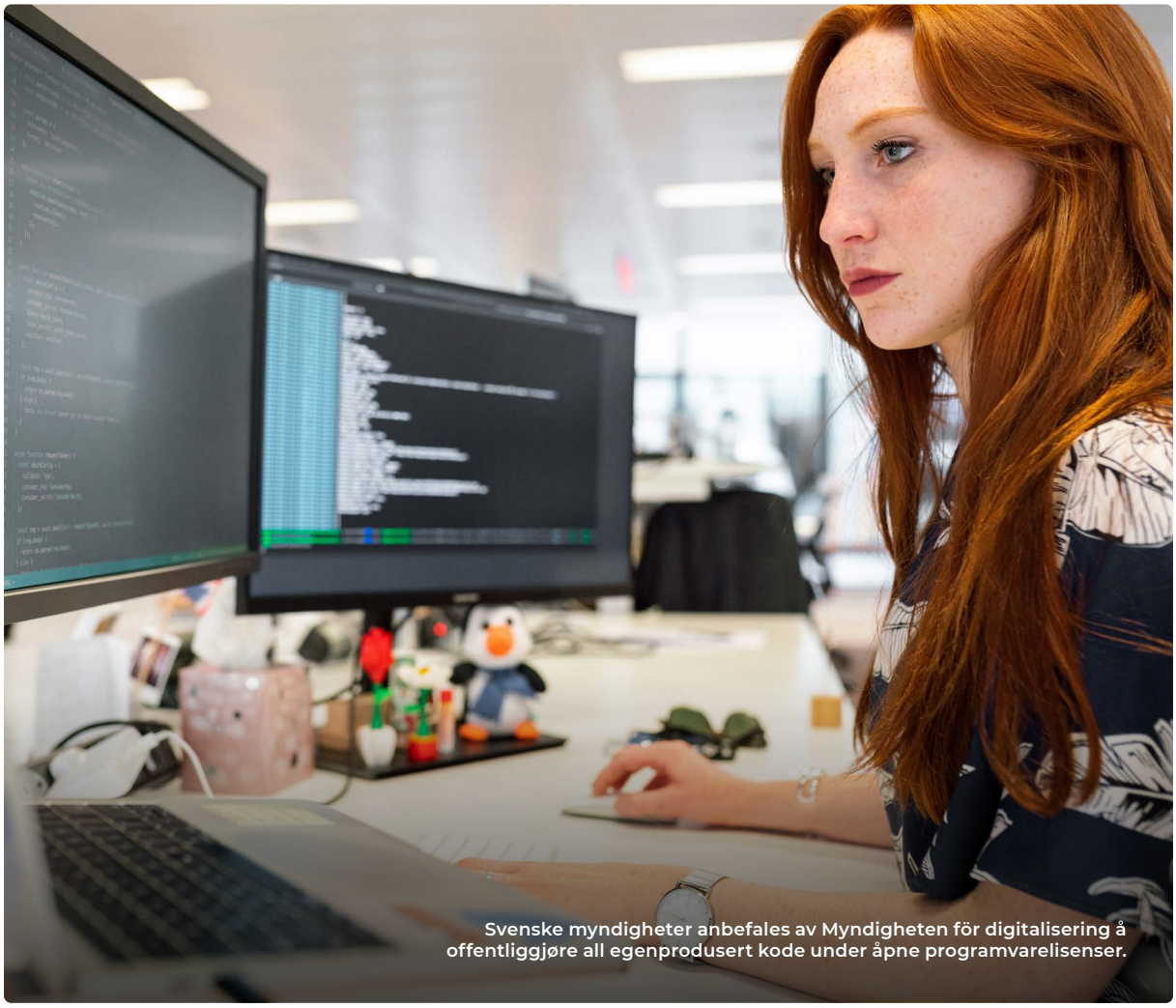
Gjør en grundig kontroll av tjenesteleverandøren og dennes underleverandører.

som kan godkjennes ut fra personvernrettslige hensyn. Det er ikke lenger nok kun å holde rede på hvilke (sensitive) personopplysninger som kan havne hos en utenlandsk myndighet. Faren for at slike opplysninger kreves utlevert må nå forebygges aktivt.

Det betyr i praksis at anskaffende organisasjoner bør begrense sine valg av tjenesteleverandører og underleverandører til slike leverandører som har sin juridiske base i EØS-området. Det kan også være behov for å sikre at administrasjon og vedlikehold av IT-systemer ikke utføres av personer som er virksomme utenfor EØS-området. Det at europeiske politikere og EU-kommisjonen to ganger har mislyktes med å formulere beslutninger om tilstrekkelig beskyttelsesnivå med tilstrekkelig gode personverngarantier, bør også føre til at anskaffende organisasjoner ikke ukritisk stoler på framtidige beslutninger om tilstrekkelig beskyttelsesnivå.[9]

**KOMPLETTERENDE ANBEFALINGER** [11]

- Kontroller om tjenesteleverandører i rett nedadgående linje bruker underleverandører i form av PaaS- eller SaaS-tilbydere.
- Kontroller om tjenesteleverandører ved utformingen av tjenesten har brukt åpent spesifiserte programvarefunksjonaliteter (som API-er eller dataformat).
- Kontroller at det finnes avtaler mellom tjenesteleverandøren og underleverandøren, og at avtalen avtalene overholder personvernkravene.
- Kontroller at underleverandøren tilbyr dokumentasjon for de åpne standardene og spesifikasjonene som underleverandøren har brukt til infrastrukturløsningene sine. Kontroller også at tjenesteleverandøren har forsikret seg om at de har mulighet til å migrere til en annen underleverandør ved behov.
- Kontroller om enten selve tjenesteleverandøren eller underleverandøren til tjenesteleverandøren har sin juridiske base i et tredjeland. Vurder om dette kan medføre at myndighetene i tredjelandet kan pålegge enten underleverandøren eller tjenesteleverandøren å overlevere opplysninger til myndighetene i tredjelandet.



Svenske myndigheter anbefales av Myndigheten för digitalisering å offentliggjøre all egenprodusert kode under åpne programvarelisenser.

## Åpenhet er en beskyttelse mot politisk instabilitet

På europeisk[11] nivå har man understreket at mer fokus på åpen tilgjengelig programkode og åpne standarder gir både innsyn og oversiktlige forhold, slik som det nå ser ut til at de europeiske personvernreglene vil kreve.

Åpne standarder og åpne kodebaser er ikke anbefalinger som stammer fra den europeiske personvernforordningen. Derimot tilbyr de sluttbrukere større bevegelsesfrihet mellom ulike leverandører. Hvis infrastrukturen er åpen og interoperabel, har sluttbrukeren større frihet til å tilpasse seg etter for eksempel domsavgjørelser.

Selv om personvernforordningen ikke i seg pålegger at organisasjoner skal sikre muligheten å bytte leverandør, ser det ut til at utviklingen av praksis på det personvernrettslige området er slik at organisasjoner muligens kan være interessert i å investere i slik fleksibilitet selv.

I forbindelse med dataoverføringer har for eksempel det politiske lederskapet i Europa ikke bare en, men to ganger feilkalibrert politiske beslutninger slik at EU-domstolen måtte annullere dem. For organisasjoner som må følge gjeldende lover og bestemmelser, innebærer det høye kostnader og stor usikkerhet og sløsing med tid. Bevisste satsninger på åpne standarder og kode minsker friksjonen hvis det oppstår behov for endringer.

Organisasjoner bør lage en plan for å migrere fra skytjenester som sorterer under amerikansk lovgivning.

DEL III

# Veier framover

## Organisasjoner i Norge kan per i dag være forhindret fra å velge skytjenester som er underlagt amerikansk lovgivning, for eksempel i anbudsprosesser.

Årsaken til dette er den amerikanske etterretningslovgivningen, men også CLOUD Act som Safespring har omtalt i tidligere informasjonsguider. På denne bakgrunnen bør organisasjoner, i tillegg til å følge Safesprings gjeldende anbefalinger og utdypninger vi har nevnt over, gjøre følgende:

- **UTARBEIDE EN PLAN** for å migrere fra skytjenester som er underlagt amerikansk lovgivning.[12]
- **UNDERSØKE** hvordan egen organisasjon allerede jobber med eksisterende retningslinjer fra Statens innkjøpssenter, eSam og ISA2 (for eksempel ved å evaluere pågående prosjekter med utgangspunkt i eksisterende anbefalinger).
- **AKTIVT ENGASJERE** regjeringen i utviklingen av en norsk plan for skytjenester som er forenelig med europeisk rett.

# Kildehenvisning

## Informasjonsguiden er skrevet av Amelia Andersdotter. Safespring tilbyr norskproduserte skytjenester.


1. ECLI:EU:C:2020:559
2. Safespring, informasjonsguide: ”Hur du hanterar det osäkra läget i och med CLOUD Act och GDPR”, fra 2018.
3. EU-kommisjonen, 10. august 2020, Joint Press Statement from European Commissioner for Justice Didier Reynders and U.S. Secretary of Commerce Wilbur Ross. https://ec.europa.eu/info/news/joint-press-statement-european-commissioner-justice-didier-reynders-and-us-secretary-commerce-wilbur-ross-7-august-2020-2020-aug-07_en
4. Jfr. Meld. St. 22 (2018–2019): ”Smartere innkjøp – effektive og profesjonelle offentlige anskaffelser”, Kommunal- og moderniseringsdepartementet (2016): ”Nasjonal strategi for bruk av skytenester” (H-2365) og Difi (2018): ”Innkjøpsordning/markedsplass for skytjenester. Forprosjektrapport.” (2018:6).
5. Jfr OpenStack Foundation (OSF) og Cloud Native Computing Foundation (CNCF).
6. GAIA-X: a federated data infrastructure for Europe. https://www.data-infrastructure.eu/GAIAX/Navigation/EN/Home/home.html
7. Rapport d’Information No 443, Union européenne -- colonie du monde numérique ?, 20. mars 2013, s. 115-116.
8. Jfr. fotnote 2 over.
9. Både Safe Harbor-vedtaket fra 2001 og Privacy Shield-vedtaket fra 2016 har EU-domstolen kjent ugyldige.
10. Se ”Rekommendationer för organisation” i fotnote 2 over.
11. C(2018) 7118, European Commission Digital Strategy - A digitally transformed, user-focused and data-driven Commission, 2018.
12. Spørsmål 5 i del II må egentlig alltid besvares med «ja» ved bruken av amerikanske skytjenester, så lenge USA ikke endrer sin lovgivning.

# Safespring er din sikre kilde for infrastrukturtjenester

Besøk gjerne nettstedet vårt for å lære mer om skytjenester og hvordan Safespring kan løse behovene dine for Compute og Storage.

**www.safespring.com/no**

safespring

+46 (0)8-55 10 73 70 | info@safespring.com
Smidesvägen 12, 171 41 Solna, Sweden

www.safespring.com