Webinar i regi av Normen

Sky og tjenesteutsetting

Norsk helsenett

19.05.2021

Agenda

Kort om skytjenester

Normens veileder

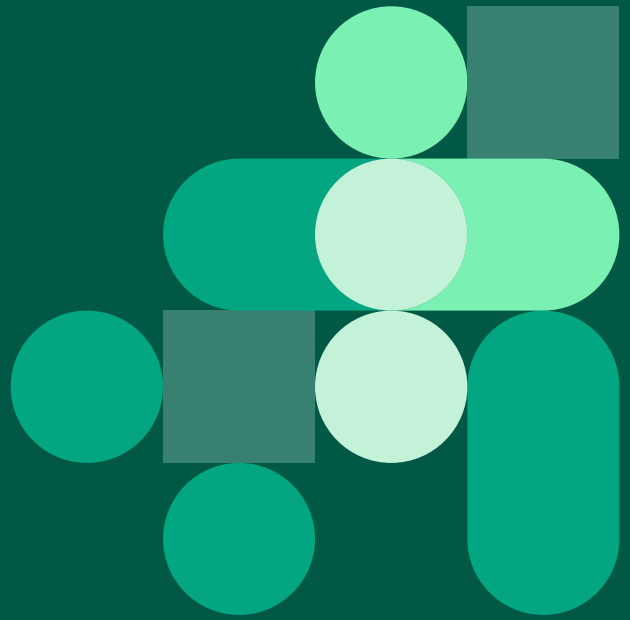
Schrems II

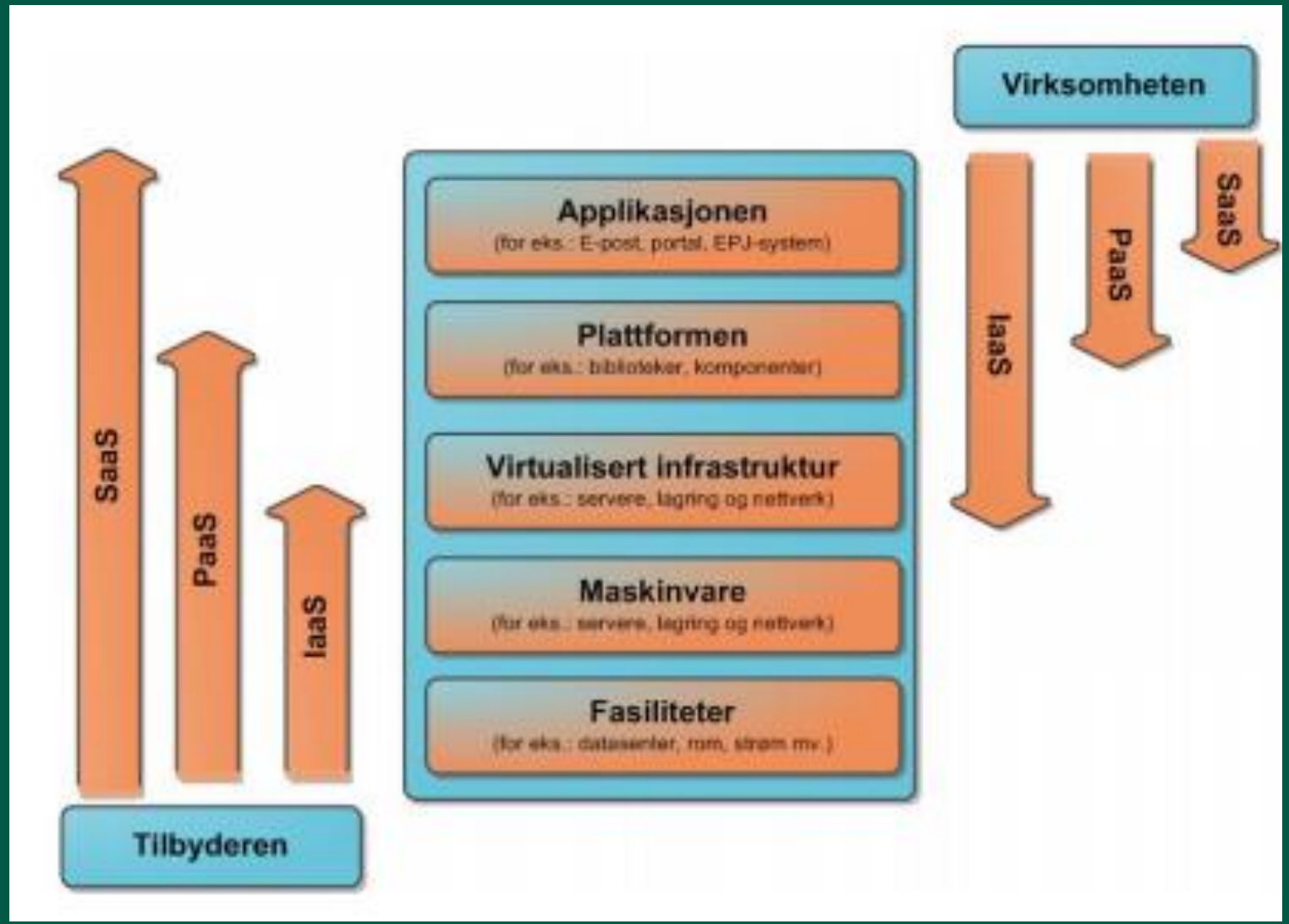
Kort om skytjenester

Norsk helsenett

Kort om skytjenester

Skytjenester har etablert seg i markedet som en mulighet for å leie programmer og infrastruktur, som en tjeneste, i stedet for at virksomheten selv eier programmer og infrastruktur.




Virksomheten
SaaS
PaaS
IaaS
Applikasjonen
(for eks.: E-post, portal, EPJ-system)
Plattformen
(for eks.: biblioteker, komponenter)
Virtualisert infrastruktur
(for eks.: servere, lagring og nettverk)
Maskinvare
(for eks.: servere, lagring og nettverk)
Fasiliteter
(for eks.: datasenter, rom, strøm mv.)
SaaS
PaaS
IaaS
Tilbyderen

Fordeler med sky


Hvor er data lagret?
Hvordan kan vi utføre kontroll med leverandør?
Kan vi etablere god nok avtale med leverandør?
Har leverandør innsyn i våre data?
Hvordan skal vi trygt nå tjenestene for drift?
Hvilke underleverandører benytter skyleverandøren?
Kan vi slette data på leverandørens delte infrastruktur?
Har vi kontroll når leverandør patcher?
Hvordan sikrer vi admintilgang?
Kan vi hindre ondsinnet kode i løsningen?
Hvordan sikrer vi tilgang til loggene?
Er sikkerheten i valgte tjenester/komponenter ivaretatt?
Har vi kontroll på tilgangene som gis?
Er sertifikater og tokens godt nok sikret?
Beskyttes tjenesten mot eksterne angrep?
Sletter vi data som ikke lengre er relevante?

Normens veileder

Norsk helsenett

Veilederen gir praktisk hjelp innenfor områdene:

- Fastsette ansvar, inngå avtaler, ivareta kontroll og vurdere risiko
- Belyse fordeler ved teknologien
- Synliggjøre trusler og behov for kontroll
- Ivaretakelse av pasientens rettigheter til samtykke, innsyn, retting sletting mv.
- Eksempler på risikoområder som det er naturlig å belyse
- Etabler databehandleravtale
- Behandling av helse- og personopplysninger under Normens virkeområde

NORMEN

CCM™ Cloud Controls Matrix

Nr	Krav (formulert som spørsmål)	Kap. i Normen	Kap. i ISO 27001 og Annex A	CSA CCM Control ID	Systemkrav i behandlings-rettet helse-register	Kravet gjelder ikke helt eller delvis for virksomheten (Må begrunnes)	Er kravet ivaretatt?	Hjemmel til kravet i lov eller forskrift	Kravet blir ivaretatt av data-behandler
1.	Er valg av egnede tekniske og organisatoriske tiltak vurdert i forhold til virksomhetens størrelse, art og omfang for behandling av helse- og personopplysninger, pasientsikkerhet, risikobildet mv?	1.5	6.1.1 8.1	(GRM-09)			☐Ja ☐Nei	PVF artikkel 32 PJL § 22 HRL § 21 FLK § 6	
2.	Er valgte tiltak basert på risikovurderinger?	1.5	6.1.3 8.3	GRM-08 STA-04			☐Ja ☐Nei	PVF artikkel 32 PVF artikkel 35 (1) PJL § 22 HRL § 21	☐Ja ☐Nei
3.	Er valgte tiltak forholdsmessige ift virksomhetens størrelse og omfanget av behandling av personopplysninger?	1.5	6.1* 8.1.*	(GRM-09)			☐Ja ☐Nei	PVF artikkel 32 PVF artikkel 35 (1) PJL § 22 HRL § 21	
4.	Sørger virksomhetens øverste leder for virksomheten at gjeldende krav til informasjonssikkerhet og personvern følges?	2	5.1 5.2 5.3	(GRM-03)			☐Ja ☐Nei	PJL § 22 HRL § 21 HTL § 5-10 første punktum PVF artikkel 24 FLK § 7	
5.	Har virksomhetens øverste leder bestemt nivå for akseptabel risiko?	2 3.2	6.1.2	GRM-11			☐Ja ☐Nei	PJL § 22 HRL § 21 PVF artikkel 32 FLK § 5 og 6	☐Ja ☐Nei
6.	Har virksomhetens øverste leder bestemt regler for håndtering av risiko?	2	6.1.3	GRM-04			☐Ja ☐Nei	PJL § 23 HRL § 22 PLF § 6	☐Ja ☐Nei
7.	Har virksomhetens øverste leder sørget for velfungerende styring og kontroll?	2	6.2	GRM-04 GRM-05			☐Ja ☐Nei	PVF artikkel 24 første ledd FLK §§ 3 og 4 PLF § 7	☐Ja ☐Nei
8.	Er alle tiltak dokumentert	2	6.1.3	GRM-04			☐Ja ☐Nei	PVF artikkel 5 nr. 2 og 32 PJL §§ 22 og 23	☐Ja ☐Nei

Schrems II

Norsk helsenett

Schrems

2012 – Schrems krever at Facebook utleverer all informasjon om seg selv – mottok et dokument på 1222 sider.

2015 – Schrems vinner frem med en klage mot Facebook, og Safe harbor-avtalen oppheves.

2020 – Schrems II dommen faller, og forsterker kravene knyttet til overføring av personopplysninger til tredjeland. Privacy Shield opphører som godkjent overføringsgrunnlag.

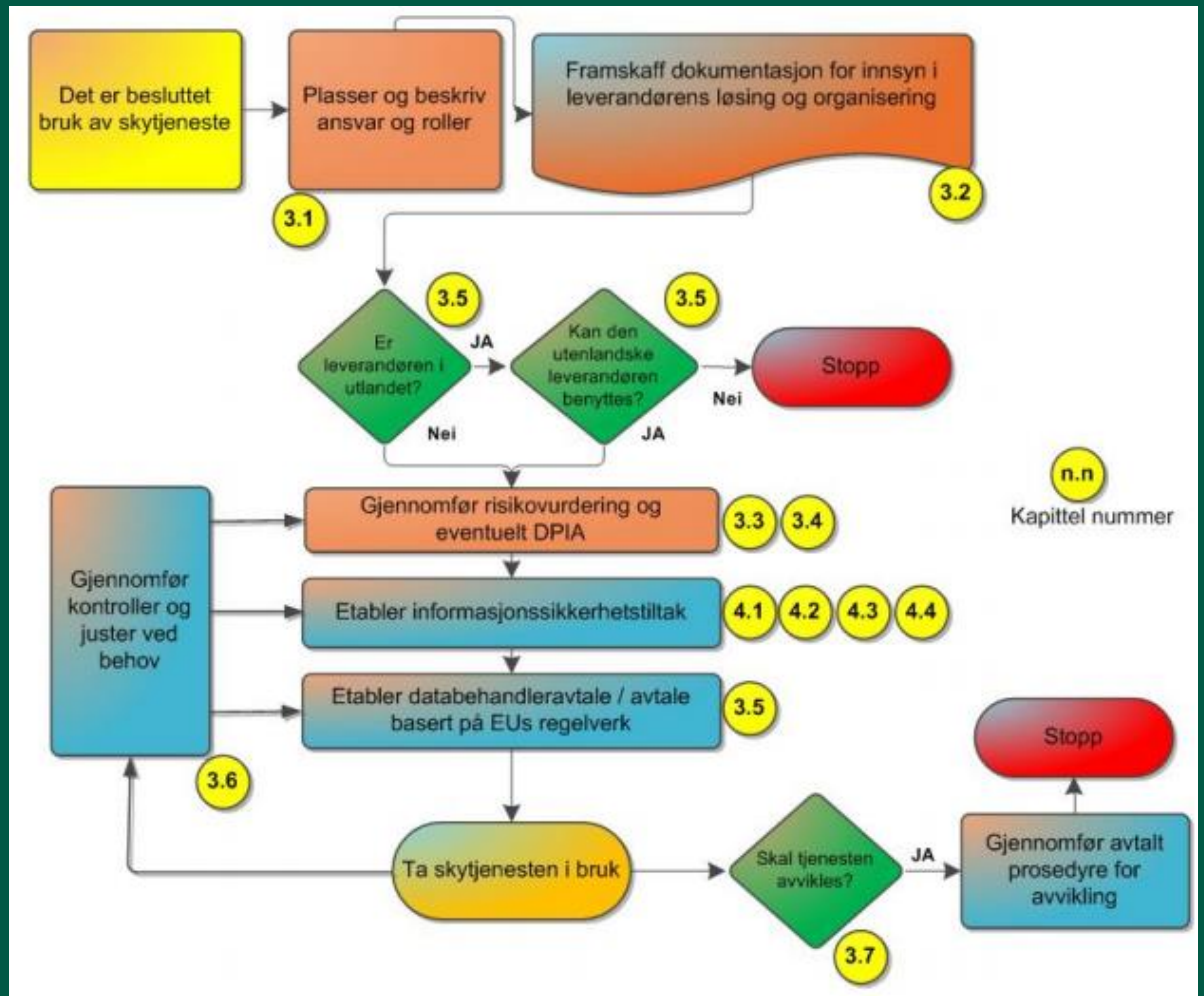

Utvikling
Lovkrav

1. Finn et passende overføringsgrunnlag i personvernforordningen artikkel 46.
   Les mer om de mest brukte overføringsgrunnlagene, EU-kommisjonens standardbestemmelser og bindende konsernregler (BCR)

2. Du må sørge for at beskyttelsesnivået som vil oppnås i praksis, faktisk er tilsvarende som i EØS, alle forhold tatt i betraktning. Undersøk derfor nøye om det finnes omstendigheter som gjør at beskyttelsesnivået som overføringsgrunnlaget er ment å sikre, ikke vil realiseres i praksis. Her er det viktig å undersøke om dataimportøren, dataimportørens infrastruktur eller eventuelle underleverandører er underlagt lover, regler eller systemer som er i strid med importørens forpliktelser etter overføringsgrunnlaget eller som på annet vis senker beskyttelsesnivået.

3. Dersom du kommer frem til at det foreligger forhold som gjør at beskyttelsesnivået ikke vil være tilsvarende som i EØS, må du iverksette ytterligere tiltak som veier opp for dette og som sikrer et tilsvarende beskyttelsesnivå i praksis. Dersom det ikke finnes slike ytterligere tiltak eller du ikke er i stand til å iverksette slik tiltak, kan du ikke overføre personopplysningene.

4. Dersom du er sikker på at beskyttelsesnivået som vil oppnås i praksis, faktisk er tilsvarende som i EØS, kan du begynne å overføre personopplysningene.



SPESIELLE FORHOLD KNYTTET TIL USA

Amerikanske overvåkingsregler

! For å kunne benytte tjenester fra amerikanske virksomheter må dataansvarlig gjøre en vurdering på hvordan personopplysninger kan sikres med øvrige tiltak.

ØVRIGE TILTAK, HVA KAN DET VÆRE?

Organisatoriske

Juridiske

Tekniske

Norsk helsenett