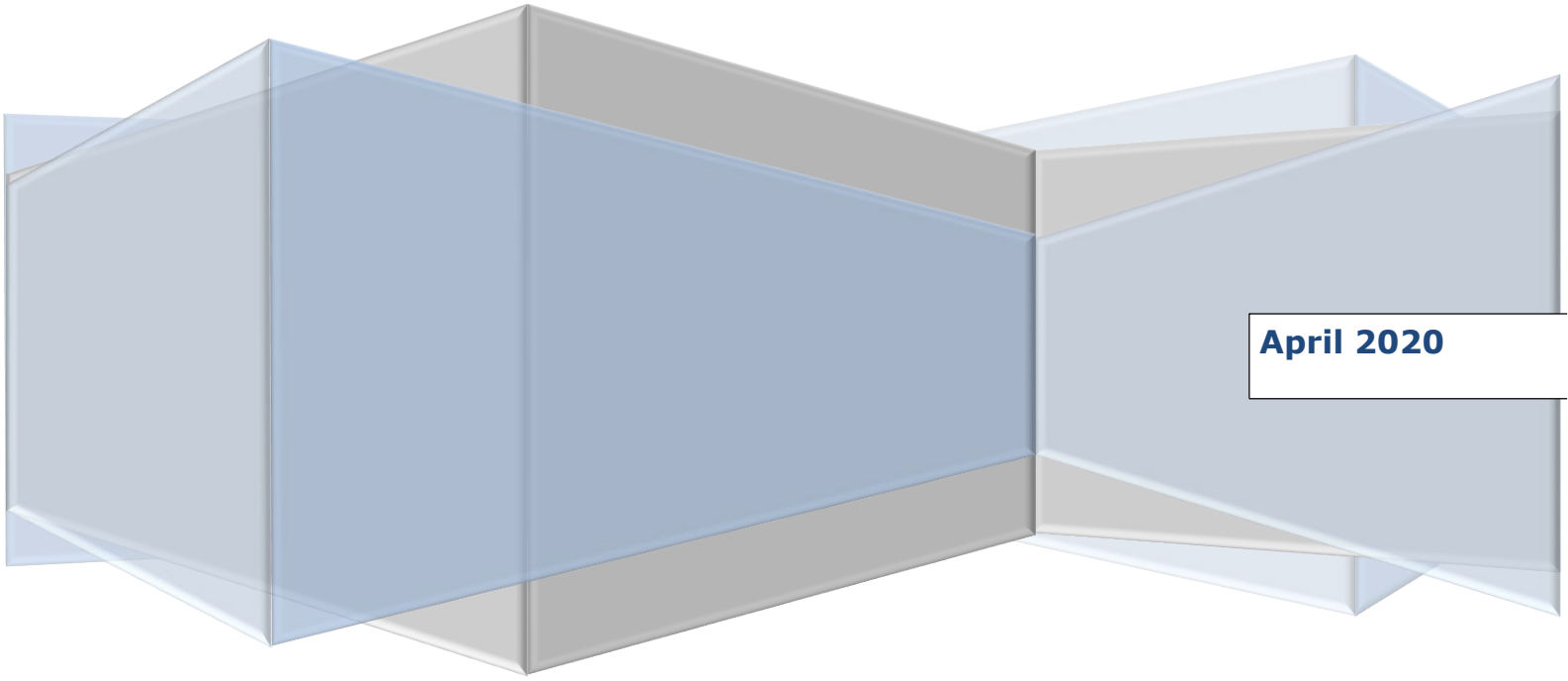
Veiledning



April 2020

Innhold

1 BAKGRUNN OG MANDAT

1.1 Opprinnelig bakgrunn og mandat

Advokatforeningen får jevnlig henvendelser fra medlemmer om advokaters bruk av Cloud computing, og om det er forsvarlig for advokater å ta slike tjenester i bruk i sin advokatvirksomhet.

Foreningens hovedstyre oppnevnt et utvalg for å lage en veiledning for advokaters bruk av Cloud-tjenester. Utvalget ble oppnevnt 21. februar 2014.

Utvalget ble gitt følgende mandat:

> Utarbeide veiledning for advokaters bruk av Cloud-tjenester.

Utvalgets arbeid ble ferdigstilt i løpet av første halvår 2014.

Utvalget har bestått av:

> Arve Føyen, Partner – Advokat M.N.A, FØYEN Advokatfirma DA (utvalgets leder)
>
> Tore Larsen Orderløkken, administrerende direktør for Norsk Senter for Informasjonssikring (NorSIS)
>
> Advokat Morten Foss, juridisk direktør i Telenor Digital AS.

Utvalgets arbeidsform har i det vesentlige vært basert på 14.- daglige telefonmøter, med elektronisk utveksling av utkast og kommentarer på utkast mellom møtene.

Utvalget har i noen grad benyttet seg av veiledninger og materiale fra Datatilsynets hjemmesider. Dette materialet er imidlertid bearbeidet og tilpasset av utvalget spesielt med hensyn til denne veiledningen.

I veiledningen gir vi først en summarisk oversikt over hva Cloud Computing er, og hvilke typer tjenester som omfattes (pkt 2). Dernest gir vi en nærmere oversikt over kategorier av personinformasjon og andre typer av fortrolig informasjon som typisk behandles ved advokatkontorer (pkt. 3), før vi (pkt 4) gjennomgår hvilke regler og formkrav som gjelder for advokaters behandling av de forskjellige informasjonstypene, og over kravene i GDPR til etablering og etterlevelse av et internkontrollsystem og sikkerhetsløsninger. Utvalget har videre funnet det hensiktsmessig å innta en sjekkliste for krav knyttet til bruk av Cloud-tjenester (pkt 5), og avslutningsvis (pkt 6) har utvalget gitt anvisning på hvorledes en konkret risikovurdering bør foretas og dokumenteres.

Enkelte steder i veiledningen vil vi komme inn på noen særegne problemstillinger knyttet til avtaler om Cloud-leveranser sett i forhold til kravene i personvernlovgivningen og enkelte andre lover. Vi understreker imidlertid at denne veiledningen ikke tar sikte på å være noen anskaffelsesveiledning eller noen uttømmende veiledning i inngåelse av avtaler om Cloud-leveranser. Forfatterne fraskriver seg ethvert ansvar for eventuelle mangler i denne veiledningen og presiserer at det er opp til det enkelte advokatkontor å søke profesjonell bistand i den grad det er nødvendig.

Vi vil videre understreke at veiledningen ikke er uttømmende når det gjelder hvilke plikter advokatvirksomheter har i forhold til etablering av internkontroll og forsvarlige rutiner for behandling av personopplysninger. Vi har kun tatt sikte på å fremheve noen sentrale problemstillinger og veilede om i hvilken grad bruk av Cloud-tjenesteleveranser skaper særlige utfordringer i forhold til bruk av databehandlere som benytter denne tjenesteleveransemodellen – og særlig når slike databehandlere er lokalisert utenfor EØS-området.

1.2 Revisjon pr mai 2020

Etter oppfordring fra Advokatforeningen har veiledningen blitt revidert av Advokat Arve Føyen i april 2020, for å ajourføre den i henhold til GDPR, og til videre utvikling i markedet for Cloud Computing.

2 CLOUD COMPUTING – HVA DET ER OG HVILKE TJENESTER SOM OMFATTES

Virksomheter som tar i bruk Cloud-tjenester er juridisk ansvarlig for bruk av tjenestene, og må sørge for at personopplysninger og annen informasjon og dokumenter mv som skal behandles konfidensielt, håndteres i henhold til personvernregelverket, og annet relevant regelverk som gir anvisning på taushetsplikt, og fortrolig behandling av relevante opplysninger.

Levering av databehandlingstjenester fra eksterne tjenesteleverandører er ikke noe nytt. Det har eksistert siden 1950-tallet i forskjellige former og under forskjellige navn. De tekniske og juridiske problemstillingene som oppstår ved bruk av tradisjonelle eksterne driftstjenester, er langt på vei de samme også ved bruk av Cloud computing som leveransemodell. Noen problemstillinger blir imidlertid mer fremtredende ved bruk av Cloud-leveransemodeller.

Cloud Computing, er en samlebetegnelse på alt fra dataprosessering og datalagring til programvare på servere som er tilgjengelig fra eksterne serverparker tilknyttet internett.

Det er vanlig å skille mellom Software som tjeneste (Software as a Service), Plattform som tjeneste (Platform as a Service) og Infrastruktur som tjeneste (Infrastructure as a Service). Disse typene tjenester kan leveres i form av offentlig tilgjengelig Cloud (Public Cloud), privat tilgjengelig Cloud (Private Cloud – benyttes innenfor en bedrift eller et konsern), eller en hybrid Cloud (Hybrid Cloud – som er en kombinasjon av de to andre leveranseformene).

Vi går ikke nærmere inn på de forskjellige tjenesteformene eller leveranseformene her. En oversikt over disse kan man få blant annet ved å lese informasjonsmaterialet for Cloud computing som er publisert på Datatilsynets websider. De juridiske og informasjonssikkerhetsmessige problemstillingene vil imidlertid langt på vei være de samme, uavhengig av tjeneste- eller leveranseform, selv om de konkrete vurderingene som må gjøres og tiltakene som må iverksettes kan være forskjellige.

Det mest sentrale og relevante for mindre og mellomstore advokatkontor, vil være det vi kaller Software as a Service. Dette er den mest komplekse tjenesten, og den vil gjerne omfatte de to andre hovedtypene av tjenester (Platform as a Service og Infrastructure as a Service).

Som eksempel på noen viktige forskjeller mellom tradisjonelle leveransemodeller og Cloud-leveransemodeller, kan nevnes at ved tradisjonelt kjøp av servere (eller serverkapasitet og lagring) kjøper eller leaser man et antall severe med betydelig mer kapasitet enn man til enhver tid benytter. Videre kjøper man gjerne lisenser for programvare til et nærmere angitt antall brukere (må ofte kjøpes i «blokker» à 10, 50 eller andre bestemt angitte antall av lisenser, og man betaler som oftest for mye mer enn det som rent faktisk til enhver tid benyttes aktivt). Cloud-leveransemodeller er derimot kjennetegnet ved at de databehandlingsressursene som benyttes (Platform, Infrastructure og Software) er laget for dynamisk skalering. Svært ofte kan tjenester tas i bruk eller skaleres opp og ned ved bruk av selvbetjeningsløsninger over internett. Det betyr at datakraft kan tilpasses kapasitetsbehov, og kunden betaler bare for de ressursene som til enhver tid rent faktisk benyttes. Avregning av forbrukte tjenester foretas automatisk og faktureres automatisk

etterskuddsvis.

Leverandørene av Cloud-tjenester kan være norske virksomheter eller virksomheter etablert hvor som helst i verden, med internett som underliggende bæretjeneste for levering av tjenestene. Databehandlingsressursene som benyttes er i mange tilfelle lokalisert fysisk utenfor Norge og utenfor EU.

En stor utfordring for advokatkontor som bruker slike tjenester er å sørge for at avtalen med Cloud-tjeneste-leverandøren er i samsvar med norsk lovgivning, slik at gjeldende krav i norsk lovgivning til behandling av opplysninger og sikkerhet til enhver tid kan oppfylles.

3 KATEGORIER AV PERSONINFORMASJON OG ANDRE TYPER AV FORTROLIG INFORMASJON SOM TYPISK BEHANDLES VED ADVOKATKONTORER

3.1 GENERELT

I dette avsnittet vil vi kort gjennomgå noen viktige kategorier av informasjon som typisk behandles av et advokatfirma. Felles for disse er at det ofte er informasjon som er underlagt taushetsplikt og med strenge krav til tilgangskontroll og sikkerhet.

Et hovedskille går mellom opplysninger av bedriftsintern karakter i advokatvirksomheten på den ene siden (Personopplysninger om ansatte og partnere i virksomheten, informasjon om strategier, og andre bedrifts- og forretningshemmeligheter knyttet til selve advokatforretningens virksomhet mv.), og på den annen side personopplysninger eller bedrifts- og forretningshemmeligheter knyttet til utøvelse av advokatvirksomheten (Personopplysninger knyttet til klientforhold, informasjon i saksdokumenter og annen informasjon som omfattes av advokaters taushetsplikt, og som for øvrig kan være underlagt avtalebaserte taushetsforpliktelser og konfidensialitetsavtaler mv.).

Årsakene til at informasjon skal beskyttes kan være forskjellige. Tiltakene for å beskytte informasjonen er imidlertid langt på vei de samme – uavhengig av årsakene. Det er mer et spørsmål om viktighetsgraden – hva er risikoen for at informasjon kommer på avveie, og hvor store er konsekvensene av at den kommer på avveie.

3.2 OPPLYSNINGER OM ANSATTE

Etter den tidligere Personopplysningsloven av år 2001, og forskriftene var det fastsatt egne bestemmelser om behandling av opplysninger om arbeidsgiveres behandling av opplysninger om ansatte. Etter innføringen av GDPR er behandling av personopplysninger om ansatte i advokatvirksomheter underlagt de alminnelige reglene i GDPR. Et unntak er forskriften om innsyn i ansattes e-post, som nå er overført til en egen forskrift gitt med hjemmel i arbeidsmiljøloven § 9-5.

Dette innebærer at advokatvirksomheten må lage policies og rutiner som dokumenterer hvorledes opplysninger om de ansatte behandles i henhold til kravene i GDPR. Se i denne sammenheng til Advokatforeningens veileder om Advokatvirksomheters etterlevelse av GDPR, kapittel 2.

3.3 PERSONOPPLYSNINGER OG ANDRE OPPLYSNINGER I KLIENTFORHOLD

Den sentrale bestemmelsen om advokaters taushetsplikt fremgår av Straffeloven § 211, som lyder:

«Med bot eller fengsel inntil 1 år straffes prester i Den norske kirke, prester eller forstandere i registrerte trossamfunn, advokater, forsvarere i straffesaker, meklingsmenn i ekteskapssaker, og disses hjelpere, som uberettiget røper hemmeligheter som er betrodd dem eller deres foresatte i anledning av stillingen eller oppdraget.»

Det som beskyttes ved denne bestemmelsen er *«….hemmeligheter som er betrodd dem eller deres foresatte i anledning av stillingen eller oppdraget.».* Bestemmelsen gjelder i utgangspunktet enhver hemmelighet advokaten har mottatt i kraft av sin rolle som advokat. Vi går ikke her nærmere inn på rekkevidden av advokaters taushetsplikt, men konstaterer at taushetsplikten og plikten til beskyttelse av informasjon («hemmeligheter») som advokater har mottatt i et klientforhold er klar og sterk. Den gjelder ikke bare personopplysninger, men *enhver* opplysning som er betrodd advokaten i klientforholdet.

Dette medfører en plikt for advokaten til å treffe relevante og tilstrekkelige tiltak for å beskytte informasjonen, slik at den ikke blir røpet for uvedkommende. Denne plikten omfatter alle former for tilgjengeliggjøring av informasjonen for uvedkommende – enten dette skjer muntlig, på papir, elektronisk, eller ved tap av minnepinner eller mobiltelefoner eller andre elektroniske enheter. For å avgjøre hvilke tiltak som skal iverksettes for å beskytte informasjon mottatt fra klienter, må advokaten foreta en risikovurdering, og iverksette tiltak for å begrense risikoen. Denne risikovurderingen og de tiltakene som iverksettes, vil være helt lik de vurderingene som gjøres i henhold til kravene til Behandlingsansvarlige som angitt i Kapittel IV i GDPR, og særlig til tekniske og organisatoriske tiltak som angitt i GDPR Artikkel 24. Se nærmere om dette nedenfor under pkt. 6.

Taushetsplikt kan i tillegg til taushetspliktbestemmelsen i straffeloven § 211 være avtalehjemlet i forholdet mellom advokaten og klienten, eller i forhold til øvrige parter i en sak. Dette gjøres gjerne gjennom forskjellige former for konfidensialitetsavtaler eller NDAer («Non Disclosure Agreements»). Slike avtaler inneholder ofte en konkretisering av krav til beskyttelse og ikke-spredning av konfidensiell informasjon, og mulige sanksjoner knyttet til mislighold av avtalen. Advokaten må i hvert enkelt tilfelle foreta en konkret risikovurdering for å avgjøre om de generelle tiltak for å beskytte den relevante informasjonen er tilstrekkelig, eller om det er nødvendig å iverksette ytterligere tiltak.

Etter den tidligere Personopplysningsloven av år 2001, og forskriftene var det fastsatt egne bestemmelser om behandling av personopplysninger i klientforhold i personopplysningsforskriften § 7- 23. Etter innføringen av GDPR er behandling av personopplysninger om klienter underlagt de alminnelige reglene i GDPR. Se i denne sammenheng til Advokatvirksomheters etterlevelse av GDPR.

4 KRAVENE I GDPR TIL ETABLERING OG ETTERLEVELSE AV ET INTERNKONTROLLSYSTEM OG SIKKERHETSLØSNINGER

4.1 HVEM HAR ANSVAR FOR FORTROLIG INFORMASJON

Det overordnede ansvaret for å iverksette nødvendige og tilstrekkelige tiltak for å sikre og beskytte fortrolig informasjon i bedrifter – også i advokatvirksomheter – ligger hos den øverste ledelse i virksomheten.

En del av dette ansvaret omfatter det å etablere et system for informasjonssikkerhet i henhold til GDPR Artikkel 32. Det må settes mål for informasjonssikkerheten, hvilket sikkerhetsnivå man skal ha og hvordan bedriften skal arbeide med risikohåndtering. Videre må det etableres styringsmidler. Det er også ledelsens ansvar å sørge for nødvendige dokumenter, som informasjons-sikkerhetsstrategi, og at instrukser lages og revideres.

Hvis advokatvirksomheten skal ta i bruk Cloud-leveranse av tjenester, må systemet for informasjonssikkerhet omfatte vurderinger og tiltak som også omfatter Cloud-tjenesteleverandøren med eventuelle underleverandører – slik at hele kjeden av leverandører og underleverandører er dekket.

Behandling av personopplysninger ved hjelp av Cloud-tjenester følger de samme regler som bruk av databehandlingsressurser for øvrig. Det vises i denne sammenheng til Advokatforeningens veileder om advokatvirksomheters etterlevelse av GDPR, kapittel 8.

Advokatvirksomheten er den behandlingsansvarlige i henhold til definisjonen i GDPR Artikkel 4, nr. 7 og Cloud-tjenesteleverandøren (med eventuelle underleverandører) er databehandler(e) som definert i GDPR Artikkel 4 nr. 8.

Ansvaret for behandling av personopplysninger i advokatvirksomheten ligger som nevnt hos virksomhetens ledelse, og etablering av nødvendig og tilstrekkelig sikkerhet for behandlingen av opplysninger hos Cloud-tjenesteleverandøren må sikres gjennom databehandleravtale eller slike øvrige mekanismer som er nærmere angitt i GDPR Artikkel 28. Det er den behandlingsansvarlige (advokatvirksomheten) som – enten direkte eller gjennom en databehandler - velger å ta i bruk Cloud-tjenesten. Hvis Cloud-tjenesten behandler personopplysninger (f. eks epost, tekstbehandling, kontakt og adresseopplysninger, regnskaps- og faktureringstjenester, kalenderoppføringer osv.) på vegne av den behandlingsansvarlige, er Cloud-leverandøren (med eventuelle underleverandører) en *databehandler* – eller eventuelt underdatabehandler - i GDPRs forstand. Datatilsynet anser derfor en leverandør av Cloud-tjenester som en databehandler (eller eventuelt en underdatabehandler), uavhengig av hvilken tjeneste som leveres.

En databehandler kan ikke behandle personopplysninger på annen måte enn det som er avtalt med den behandlingsansvarlige, jf. GDPR Artikkel 28 nr. 3. Databehandleren plikter i tillegg å gjennomføre sikringstiltak som følger av GDPR Artikkel 28 nr. 3 c), jfr Artikkel 32.

En databehandleravtale fritar ikke behandlingsansvarlige for lovfestet juridisk ansvar. Derimot er det slik at den behandlingsansvarlige gjennom databehandleravtalen må pålegge databehandleren å gjennomføre de nødvendige sikringstiltak som den behandlingsansvarlige har analysert seg frem til gjennom sitt system for informasjonssikkerhet og IKT-sikkerhet.

Datatilsynet har laget en veileder om og eksempel på avtaleskisser for en slik databehandleravtale.

I avtaleskissen og veilederen finnes oversikt over minimumskravene som Datatilsynet forventer at en slik avtale inneholder. Det kan være andre punkter som tilkommer selve avtalen, men det er avhengig av internkontrollen til den behandlingsansvarlige som kjøper tjenesten. Noen slike punkter kan være sikkerhetskopiering, sletting, tilgangsstyring og segmentering av databaser. Med segmentering forstås i denne sammenheng at den behandlingsansvarliges personopplysninger ikke skal sammenblandes med personopplysninger fra en annen behandlingsansvarlig. Hva som nærmere ligger i forbudet mot sammenblanding beror på en konkret vurdering som det vil føre for langt å gå inn på her.

4.2 RISIKOVURDERING OG INFORMASJONSSIKKERHET

En sentral plikt etter personopplysningsloven av år 2001 var at den behandlingsansvarlige skulle etablere og holde vedlike et internkontrollsystem, som var nokså omfattende og detaljert beskrevet. Dette har blitt mer fleksibelt med innføringen av GDPR. Se nærmere om dette i Advokatforeningens veileder om advokatvirksomheters etterlevelse av GDPR., Kapittel 2.

Den behandlingsansvarlige skal gjennomføre en risikovurdering for sin behandling av personopplysninger. Risikovurderingen må ses i sammenheng med etablerte akseptkriterier for *risiko*, og den behandlingsansvarlige skal iverksette nødvendige tiltak for å oppnå en tilfredsstillende *informasjonssikkerhet*. En mal for risikovurdering er inntatt i punkt 6 i denne veilederen.

Det følger av GDPR Artikkel 24 nr. 1 at virksomheten selv må fastlegge kriterier for akseptabel risiko forbundet med behandlingen av personopplysninger. Hva som defineres som akseptabel risiko kan variere fra virksomhet til virksomhet. En konsekvens av dette

er at en Cloud-tjeneste som anses å ha en tilfredsstillende sikkerhet for én behandlingsansvarlig ikke nødvendigvis har det for en annen. Dette altså til tross for at sikkerheten i tjenesten kan være nøyaktig den samme.

For å oppnå tilfredsstillende informasjonssikkerhet må den behandlingsansvarlige kunne forvisse seg om at Cloud-tjenesten møter de kravene som er fastlagt under arbeidet med akseptkriteriene og risikovurderingen. Virksomheten må tillegge vurderingen større vekt når den går fra egen drift til Cloud-baserte løsninger, ettersom personopplysningene vil ligge utenfor den behandlingsansvarliges direkte kontroll.

Spørsmålet blir da hvordan den behandlingsansvarlige skal kunne forvisse seg om at informasjonssikkerheten faktisk er tilfredsstillende.

Databehandleravtalen skal inneholde en del som omhandler informasjonssikkerhet, og det er viktig at den behandlingsansvarlige går grundig gjennom denne. Avtalen i seg selv er ingen forsikring for at leverandøren har en tilfredsstillende informasjonssikkerhet.

GDPR Artikkel 28 nr. 3 h stiller krav om at databehandler gjennom databehandleravtale skal forplikte seg til å gjøre tilgjengelig for den behandlingsansvarlige all informasjon som er nødvendig for å påvise at forpliktelsene fastsatt i artikkel 28 er oppfylt, samt muliggjør og bidrar til revisjoner, herunder inspeksjoner, som gjennomføres av den behandlingsansvarlige eller en annen revisor på fullmakt fra den behandlingsansvarlige.

Databehandleren må kunne legge frem dokumentasjon for informasjonssystemets utforming og sikkerhetsløsninger. Dette for at den behandlingsansvarlige kan forvisse seg om at løsningen har tilfredsstillende informasjonssikkerhet sett opp mot risikovurdering og akseptkriterier. ISO 27001 og tilsvarende standarder gir i seg selv ikke tilstrekkelig informasjon om valgt sikkerhetsnivå. Slike standarder gir først og fremst informasjon om måten Cloud-leverandøren jobber med sikkerhet på (plan-do-check-act-rutiner), men altså ikke om valgt sikkerhetsnivå. For å få vite noe om de valgte sikkerhetsnivåene må man få innsyn i annen type sikkerhetsdokumentasjon. Advokatkontoret må stille krav til Cloud-leverandøren om slik konkret dokumentasjon. Det kan være et godt alternativ å få tilgang til revisjonsrapporter utarbeidet av eksterne revisjonsselskap som beskriver it-sikkerheten. Normalt gis kunden tilgang til disse mot at de forplikter seg til å signere konfidensialitetsavtale.

Databehandleren (Cloud-leverandøren) skal ikke kunne endre informasjons-sikkerhetstiltak uten at den behandlingsansvarlige er blitt informert skriftlig og har godkjent endringen.

Den behandlingsansvarlige må sørge for å gjøre en fornyet vurdering av informasjonssikkerhetstiltakene når det skjer endringer i faktiske forhold. Dette kan f. eks være ny kunnskap om myndigheters praksis for tilsyn og tilgang til informasjon hos Cloud-leverandøren el. Den behandlingsansvarlige bør også følge opp avtalene og revidere de på gitte tidspunkter, ut fra at leverandøren kan endre leveranser, eller ta i bruk nye løsninger, som gjør at tiltakene må vurderes på nytt.

4.3 INFORMASJONSPLIKT

Den behandlingsansvarlige har informasjonsplikt og øvrige plikter overfor den enkelte registrerte som følger av GDPR Kapittel III, med visse unntak som er fastsatt i personopplysningsloven kapittel 4.

Bestemmelsene går ut på at den registrerte har en rekke rettigheter som kan gjøres gjeldende mot databehandleren. Se nærmere om de registrertes rettigheter i Advokatforeningens veileder om advokatvirksomheters etterlevelse av GDPR, Kapittel 7.

Når den behandlingsansvarlige benytter Databehandler (Cloud-tjenesteleverandør), skal

krav om informasjon og innsyn rettes til den behandlingsansvarlige, men i henhold til GDPR Artikkel 28 nr. 3 e) og f) skal det inngås en databehandleravtale som bl.A. angir at databehandler (Cloud-leverandøren) skal bistå den behandlingsansvarlige, slik at denne kan oppfylle sine forpliktelser etter GDPR kapittel III, og Artikkel 32 – 36.

Et slikt krav vil i mange tilfelle by på spesielle utfordringer ved bruk av Cloud-tjenesteleverandører som databehandlere. Databehandleravtalen mellom advokatvirksomheten som den behandlingsansvarlige og Cloud-tjenesteleverandøren må regulere forholdet slik at det legges til rette for ivaretakelse av informasjonsplikten.

Advokatvirksomheten må sikre at de har rutiner etc. for å oppfylle dette kravet i loven og dette må reflekteres i internkontrollsystemet til advokatvirksomheten.

4.4 SPESIELLE PROBLEMSTILLINGER

Leverandører av Cloud-tjenester har i utgangspunktet noen fordeler i forhold til tradisjonelle leverandører av servertjenester. For eksempel kan Cloud-tjenestene gi mer fleksible og integrerte løsninger.

Men slike fordeler fører også med seg noen spesielle problemstillinger som den behandlingsansvarlige må ta stilling til:

Sikkerhetskopiering/Speiling
- Hvordan fungerer dette?
- Overføres personopplysningene til et annet land for redundans, eksempelvis fra Irland til USA eller fra Tyskland til India?
- Er en slik redundans i henhold til de avtaler som er inngått?
- Hvordan behandles personopplysningene etter at de er overført?

Segmentering
Datatilsynet har uttalt at den behandlingsansvarliges personopplysninger ikke skal sammenblandes med personopplysninger fra en annen behandlingsansvarlig. Hvordan håndterer leverandøren dette?

Tilgangsstyring

Hvem hos leverandøren har tilgang til personopplysningene som behandles? Merk at om driftspersonell etc. som befinner seg i «tredjeland» (land utenfor EØS og som ikke er godkjent av EU for å ha etablert et «tilfredsstillende nivå av personvern») kan aksessere personopplysninger vil dette normalt også innebære at personopplysninger blir overført til landene hvor det aktuelle driftspersonellet etc. befinner seg.

Er det tilgangsstyring (hvem har tilgang til hvilken informasjon – innmelding av nye brukere og utmelding av brukere som ikke lenger skal ha tilgang mv) og administrasjon av brukernavn, passord og tilganger i samsvar med lovpålagte krav og egen *internkontroll* (se avsnitt 4.2 over om risikovurdering og informasjonssikkerhet)?

Autorisert og uautorisert bruk
Gir Cloud-tjenesten mulighet for registrering av autorisert og uautorisert bruk (loggføring)

Dokumentasjon
Er løsningen tilstrekkelig dokumentert med hensyn til kontroll fra offentlige myndigheter (jfr. GDPR Artikkel 30 om etablering av protokoller over behandlingsaktiviteter og Artikkel 32 om Sikkerhet ved behandlingen)? Se nærmere om intern dokumentasjon og Internkontroll i Advokatforeningens veileder om advokatvirksomheters etterlevelse av GDPR, Kapittel 2.

Overføring til tredjeland

Personopplysninger kan ikke uten videre overføres til utlandet. GDPR Kapittel V fastsetter nærmere regler for når slik overføring kan skje og hvilke vilkår som gjelder for overføringen. Datatilsynet stiller videre kav om at man skal vite i hvilke land en databehandler og/eller dens underleverandører prosesserer personopplysninger. Det er derfor sentralt å stille dette spørsmålet til Cloud-leverandøren og få dokumentert skriftlig i hvilke land personopplysninger behandles. Enkelte Cloud-leverandører tilbyr kunden å kunne velge mellom land/regioner hvor dataen lagres innenfor.

Utgangspunktet er at opplysninger kan overføres innenfor EØS-området og til en del andre stater som *«..sikrer en forsvarlig behandling av opplysningene»* jfr. GDPR Artikkel 45. En liste over slike stater finnes på EU kommisjonens hjemmesider på følgende adresse: http://ec.europa.eu/justice/data- protection/document/international-transfers/adequacy/index_en.htm)

For øvrig kan opplysninger overføres til andre land enn de som der er angitt, hvis betingelsene i Artikkel 46 er oppfylt, f. eks hvis mottaker av opplysningene er en databehandler, og grunnlaget for overføringen er EUs standardkontrakt inntatt i kommisjonsbeslutning 2010/87/EU datert 5. februar 2010.

5 RETNINGSLINJER FOR ANSKAFFELSE AV CLOUDBASERTE IT-LØSNINGER

5.1 FORBEREDENDE ØVELSER

1. Skaff oversikt over hvordan flyten av personopplysninger vil være (hvor blir dataene overført, direkte og indirekte).
2. Skaff oversikt over hvordan IT-sikkerheten er ivaretatt i systemet som vurderes. Mye av dette kan typisk være beskrevet i whitepapers etc. som leverandøren publiserer på nettet, men innholdet der er ofte ikke tilstrekkelig. For å få nok informasjon til å kunne vurdere sikkerheten kan det være nødvendig med tilgang til annen dokumentasjon, slik som revisjonsrapporter fra uavhengige tredjeparter etc. Leverandøren vil normalt gå med på å dele slik informasjon med kunden, forutsatt at denne signerer en konfidensialitetsavtale med leverandøren.
3. Forsikre deg om at IT-sikkerheten tilfredsstiller GDPR's krav (evt. andre relevante rettsregler avhengig av hva slags type informasjon som prosesseres).
4. Forsikre deg om at det også ut fra et forretningsmessig ståsted og ut fra ditt eget foretaks risikoprofil vil være ok å ta i bruk tjenesten.
5. Forsikre deg om at du som kunde fullt ut eier dataen som lagres og at leverandøren ikke kan utnytte den for andre formål enn det som spesifikt er avtalt med deg.
6. Forsikre deg om at dataen blir slettet når du gir beskjed om dette og/eller når avtalen med leverandøren avsluttes.
7. Gjennomfør en risikovurdering i samsvar med GDPR's krav og sørg for at denne dokumenteres.
8. Vurder om det er behov for forhåndsdrøfting med Datatilsynet i henhold til GDPR Artikkel 36.

5.2 INNGÅELSE AV AVTALE

1. Vær forberedt på at det er lite rom for forhandlinger, spesielt når avtalen inngås med store USA-baserte cloud computing-leverandører. Men stå samtidig fast på de krav som følger av norsk rett. De fleste leverandører vil ha et incitament til å levere tjenester som det er lovlig å bruke, ettersom det motsatte vil kunne påvirke leverandørens muligheter for å selge tjenesten.
2. Forsøk å få en rett til å terminere avtalen om det skulle bli avdekket at leverandøren ikke opererer på en måte som tilfredsstiller kravene i norsk lovgivning, evt. slik disse kravene kommer til uttrykk i avtalen.
3. Vær på vakt etter bestemmelser som gir leverandøren en ensidig adgang til å endre (deler av) kontraktens innhold, typisk underliggende dokumentasjon.

4. Sørg for at forhold som er viktige å regulere for å sørge for ivaretakelse av sikkerhet er på plass i avtalen. Eksempler på dette er krav til sikkerhet, sanksjoner ved brudd på slike, back-up/failover-løsninger etc.

5.3 FORHOLD Å VÆRE SPESIELT OPPMERKSOM PÅ VEDR. PERSONVERN

1. Sørg for at du har oversikt over hvor personopplysningene behandles.
2. Skaff deg oversikt over hvor leverandørens representanter med potensiell tilgang til personopplysningene befinner seg. Om dette er i andre land enn det som er nevnt under punkt 1 i dette underkapittelet, må oversikten over land utvides tilsvarende.
3. Det er et krav etter norsk rett at det er mulighet for å gjennomføre sikkerhetsrevisjoner hos leverandøren. Undertiden kan det å få tilgang til leverandørens eksterne revisors rapporter vedr. sikkerhetsevalueringer være tilstrekkelig, men dette kan ikke tas som en generell regel og må derfor vurderes konkret. Avgjørende er om man gjennom revisjonsrapporten får tilgang på informasjon som gjør det mulig å fastslå om lovens og avtalens krav overholdes eller ikke.
4. Overføring av personopplysninger til utlandet må skje i samsvar med bestemmelsene i GDPR kapittel 5.
5. Påse at personopplysninger ikke overføres til land som ikke er forhåndsgodkjent av EU, med mindre overføringen skjer i henhold til EUs Standard modellavtaler for overføring, BCR (Binding Corporate Rules), Privacy Shield eller tilsvarende gyldig overføringsgrunnlag. Det er viktig å være oppmerksom på at ved overføring av sensitive opplysninger i henhold til modellavtalene, skal hver enkelt person hvis sensitive data overføres, varsles om overføringen.
6. Merk at ikke alle amerikanske selskap vil være underlagt Privacy Shield. Du må få bekreftet at leverandøren du forhandler med er tilsluttet Privacy Shield og at leverandørens tilslutning til instituttet også omfatter de kategorier av data som det er aktuelt at denne behandler for deg.
7. Påse at leverandøren har en plikt til å informere deg som kunde om brudd på sikkerheten som innebærer at personopplysninger har kommet eller kan komme på avveie. I gitte situasjoner vil du kunne ha en selvstendig plikt til å informere Datatilsynet (og de personene den kompromitterte dataen relaterer seg til) om dette.
8. Sørg for å ha en databehandleravtale på plass som ivaretar ovennevnte.

5.4 ØVRIGE FORHOLD

1. Sett deg inn i hva avtalen sier om responstider ved feilmelding, oppetidsgarantier etc. og vurder om dette er tilfredsstillende for din virksomhet.
2. Sett deg inn i hvor enkelt/komplisert det vil være å migrere kundedataen til løsninger som tilbys av andre leverandører. Enkelte cloud-baserte IT-tjenester er kjent for å kunne (bevisst eller ubevisst) skape en såkalt lock-in-effekt som innebærer at terskelen for å ta i bruk alternative tjenester blir høy.
3. Sjekk hvordan tap av data reguleres i kontrakten. Ofte tar ikke leverandøren ansvar for dette overhodet. Det må vurderes om dette er akseptabelt for din virksomhet. Verdt å merke seg for advokatvirksomhet er at for dårlig sikring mot eventuelt tap av data vil kunne komme i konflikt med plikten til å oppbevare visse kategorier av data i en gitt periode.
4. Sjekk om avtalen gir leverandøren mulighet til leveransenekt ved manglende betaling (selv om betalingsmisligholdet ikke er vesentlig). Mange leverandører opererer med slike krav, noe som kan skape utfordringer om avtalen ikke endres på dette punkt.

MERK: Ovennevnte retningslinjer er en ikke-uttømmende liste utarbeidet i tilknytning til denne veiledningen for Cloud Computing. Retningslinjene er ikke ment å bli benyttet som det eneste verktøy ved anskaffelser av cloud-baserte IT-løsninger. Det forutsettes at det

enkelte foretak søker juridisk assistanse før avtale om cloud-baserte IT-løsninger inngås, i den grad kunden ikke har tilstrekkelig kunnskap om dette selv.

6 MATRISE FOR RISIKOVURDERING

6.1 VERDIVURDERING

Informasjon er en stor del av virksomheters verdi. Ved bruk av Cloud-tjenester er det derfor viktig å forstå verdien av virksomhetens informasjon slik at riktige beskyttelsestiltak kan iverksettes. Det kan være mange forhold å vurdere i forhold til hvilken beskyttelse informasjonen må ha. Er beskyttelsen av informasjonen underlagt lovverk, virksomhetens retningslinjer eller andre former for beskyttelseskrav? Har kundene satt egne krav til beskyttelse? Alle disse momenter må vurderes i fastsettelsen av sikringstiltak.

Vårt behov for å beskytte informasjon springer ut av det forholdet at den har en verdi som kan gå tapt for oss eller føre til et tap av verdier dersom den blir misbrukt, ødelagt eller endret. Vi kan finne eksempler på slik type informasjon på alle nivåer i samfunnet.

Klassifiserer man informasjonen vil det også bli lettere å iverksette riktige sikringstiltak. Som et ledd i en god informasjonshåndtering er verdivurdering en fremgangsmåte for å gi virksomheten et bilde på verdien av informasjon. På alle nivåer finnes det informasjon som det er et behov for å beskytte i ulik grad. Det er ikke sikkert at de som ”eier” informasjon er like bevisste på hvilken verdi informasjonen kan ha, også med tanke på misbruk. Informasjon kan ha krav til beskyttelse av både konfidensialitet, integritet og tilgjengelighet. Verdivurdering av informasjon dreier seg om å analysere informasjon med tanke på hvilke konsekvenser det kan få dersom denne informasjonen går tapt, endres eller kan bli misbrukt.

Det finnes noen enkle spørsmål som kan gi grunnlag for en nærmere vurdering av informasjonens verdi:

- Hvordan kan informasjonen misbrukes?
- Hvem kan misbruke informasjonen?
- Hva blir konsekvensen dersom informasjonen blir tilgjengelig for uvedkommende?
- Kan informasjonen påføre skade for andre?
- I hvilket tidsrom har informasjonen verdi?

Hvilken informasjon som til enhver tid vil ha et beskyttelsesbehov, vil aldri være helt statisk over tid. Det vil alltid være et tilsig av ny informasjon som bør beskyttes, samtidig som behovet for beskyttelse av tidligere ansette verdier kan falle fra eller bli redusert. Det finnes informasjon som bare trenger beskyttelse ”over natten”, mens annen informasjon kanskje må beskyttes i mange tiår. Når informasjonen skal ut i en Cloud- tjeneste er det derfor svært viktig å ha gått igjennom og satt en klassifisering på informasjonen.

Det finnes flere forskjellige former for klassifisering, ett eksempel ved bruk av 4 klasser kan være:

- Åpen
- Intern
- Sensitiv
- Kritisk

Her vil det være behov for ulike sikkerhetstiltak avhengig av hvilken klasse informasjonen settes i.

6.2 RISIKOVURDERING

For å kunne vite noe om risikoen ved bruk av Cloud-tjenester sett opp mot verdien av informasjonen, er det krav om å gjennomføre risikovurderinger. En risikovurdering vil si noe om trusler, sannsynligheten for at en sikkerhetshendelse vil inntreffe og konsekvensen om hendelsen inntreffer. Virksomheten setter akseptansekriterier for hva som kan aksepteres av risiko. Tiltak iverksettes for de truslene som ikke aksepteres. I en risikomatrise får man et risikobilde, som på en enkel måte illustrerer hvilke trusler man ikke aksepterer.

I bruken av Cloud-tjenester er det mange forskjellige trusler man må vurdere. I denne veiledningen gis det ikke noen uttømmende liste men en kort innføring i hvordan man på en enkel måte kan sette opp en risikomatrise.

Eksempler på trusler advokatvirksomheten kan se for seg er:

- Konkurrenter eller andre uautoriserte parter får tilgang til strategier, anbudsinformasjon og forretningshemmeligheter.
- Personopplysninger kommer på avveier
- Flere PC-er blir angrepet av virus, og flere ansatte blir dermed hindret i arbeidet
- En Cloud-tjeneste som brukes har ikke tilstrekkelig sikkerhet og media skriver om saken

Det må etableres skalaer for konsekvens, sannsynlighet og risiko:

Sannsynlighet kan deles inn i hvor ofte man tror hendelsen vil inntreffe:

- Sjelden
- Kan skje
- Svært vanlig.

Evt. hvis man tallfester: 4 ganger pr år, 2 ganger pr mnd, 2 ganger pr uke.

Konsekvens kan deles inn i:

- Liten
- Middels
- Stor.

Evt. hvis man tallfester: Tap på mer enn 50.000,- tap på mer enn 500.000.- Tap på mer enn 1.000.000-.

Skalaer må settes opp av de som kjenner virksomheten.

I en tabell kan man etter en vurdering sette følgende risiko inn:

- Med stor risiko menes hendelser som skjer mer en to ganger i uken, gir tap på over 1.000.000 kr eller betydelig tap av renommé. Rød farge er brukt, og er ikke akseptabelt.
- Med moderat risiko menes hendelser som skjer mer enn to ganger i måneden, gir tap på over 500.000 kr eller tap av renommé. Oransje/gul farge brukes, og må ha oppmerksomhet.
- Med lav risiko menes hendelser som ikke skjer mer enn to ganger i halvåret, medfører tap på over 50.000 kroner eller ubetydelig tap av renommé. Grønn farge benyttes, og risikoen aksepteres.

Risikotabell

		Sansynlighet		
		Sjelden	Kan skje	Svært vanlig
Konsekvens	Liten	*Lav*	*Lav*	*Moderat*
	Middels	*Lav*	*Moderat*	*Stor*
	Stor	*Moderat*	*Stor*	*Stor*

Konsekvenser
Dersom uvedkommende får tilgang til sensitiv informasjon kan det få store konsekvenser, alt etter hvilken informasjon som blir kjent og hvem som blir kjent med denne.

Risikovurdering
Eksempel på vurdering av risiko for virksomheten og tabellen nedenfor viser aktuelle risikoer og hvilke tiltak som kan iverksettes. Gjennomgangen er ikke ferdigstilt og er ikke kun rettet mot trusler ifm. bruk av Cloud-tjenester.

Trussel: *Konkurrenter får tilgang til informasjon*

#	Årsaker	Risikovurdering			Mulige tiltak
		Konsekvens	Sannsynlighet	Risikonivå	
1	Egne ansatte kan ønske å spre sensitive opplysninger for egen vinnings skyld.	Stor	Sjelden	Moderat	Opplæring av ansatte
2	Uvedkommende kan få tilgang til informasjon som er lagret i en Cloud-tjeneste.	Stor	Kan skje	Stor	Opplæring av ansatte. Gode avtaler med Cloud-tjenesteleverandør. Test av Cloud-tjenesteleverandør.
3	Vi kan bli offer for generelle angrep (virus/ormer/trojanere, phishingangrep	Stor	Kan skje	Stor	Opplæring av ansatte. Innstalleringer av sikkerhetsoppdatering er skal bli fast rutine. Beskyttelsen av selve nettverket skal bli bedre og mer helhetlig
4	Utenforstående kan stjele utstyr der sensitiv informasjon er lagret.	Stor	Kan skje	Stor	Opplæring av ansatte. Bedre fysisk sikring. Bedre rutiner for avhending av utstyr og makulering. Kryptering av lagringsmedier