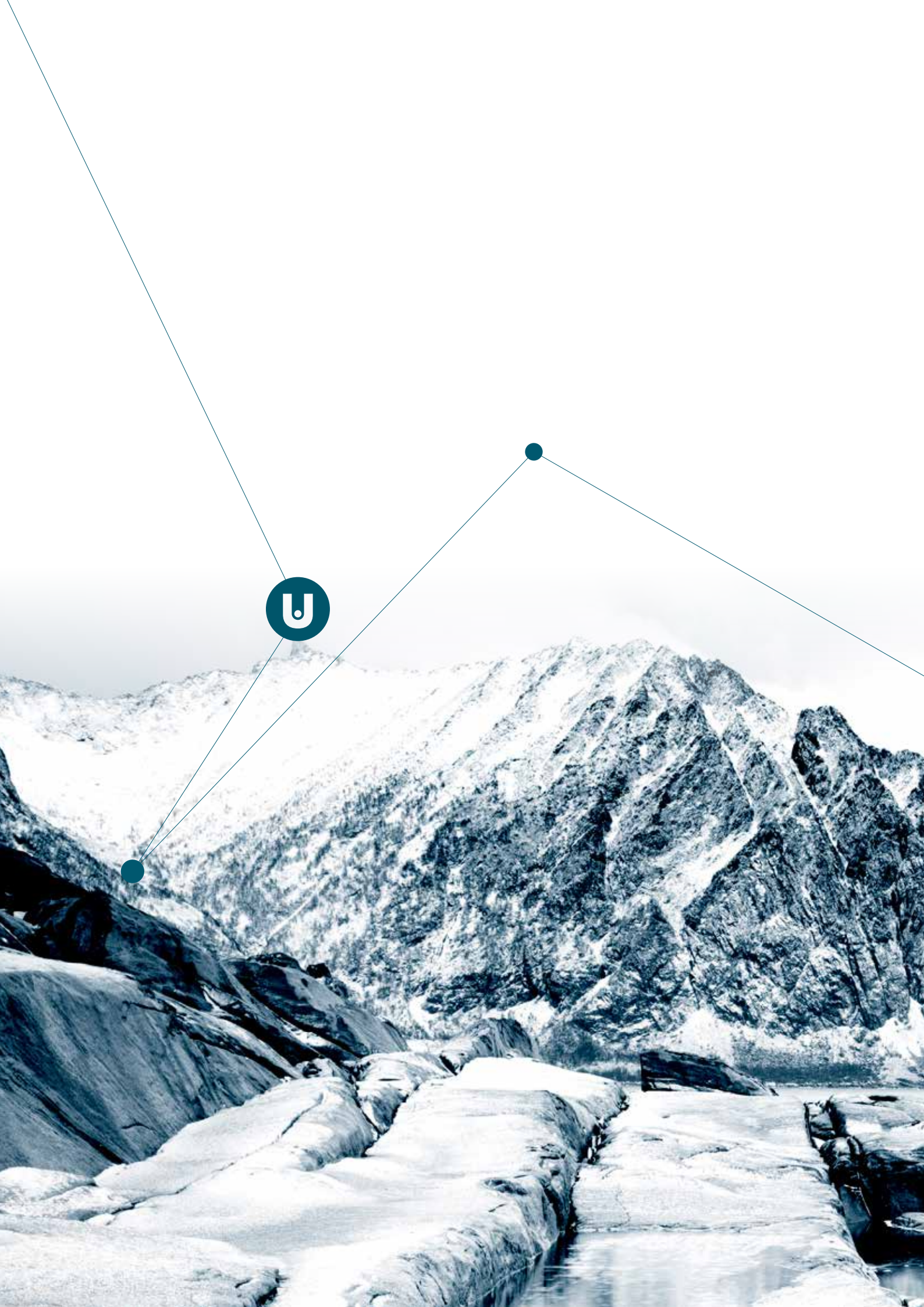
Temarapport 2020 – informasjonssikkerhet og personvern
i høyere utdanning og forskning

TJENESTEUTSETTING AV DIGITALE SYSTEMER OG TJENESTER



INNHOLD

SAMMENDRAG

I denne temarapporten presenteres utvalgte resultater fra Units kartlegginger av sektortilstanden på informasjonssikkerhets- og personvernområdet. Kartleggingene ble gjennomført i 2020. Resultatene har ikke tidligere blitt publisert.

Spørsmålene som drøftes i temarapporten er

1) Hvor stor andel av den samlede databehandlingen i sektoren var tjenesteutsatt, det vil si at den skjedde ved hjelp av eksterne tjenesteleverandører?

2) I hvilken grad hadde virksomhetene i UH-sektoren – 21 statlige universiteter og høgskoler, og åtte direktorater og selskaper – etablert rutiner for informasjonssikkerhet og personvern i forbindelse med tjenesteutsetting?

3) I hvilken utstrekning ble etablerte rutiner faktisk praktisert før tjenesteutsetting og underveis i tjenesteleveransene?

Hvilke krav som gjelder med hensyn til etablering og praktisering av rutiner for informasjonssikkerhet og personvern i forbindelse med tjenesteutsetting, spesifiseres i Kunnskapsdepartementets «Policy for informasjonssikkerhet og personvern i høyere utdanning og forskning».

Temarapporten gir følgende svar på spørsmålene ovenfor:

OMFANGET AV TJENESTEUTSETTING

Rapporten viser at tjenesteutsetting har blitt en viktig del av digitaliseringen i UH-sektoren. 18 av virksomhetene svarte at det trolig dreide seg om 50 prosent eller mer av all databehandling. 12 virksomheter svarte at det dreide seg om mer enn 75 prosent. To virksomheter oppga at all databehandling var tjenesteutsatt.

Samtlige virksomheter forventet at omfanget av tjeneste-utsetting ville øke de kommende årene.

RUTINER FOR INFORMASJONSSIKKERHET OG PERSONVERN

25 virksomheter oppga at de hadde rutiner for risiko-vurdering av informasjonssikkerheten ved tjenesteutsetting som innebar behandling av personopplysninger. 26 svarte at de hadde rutiner for inngåelse av databehandleravtaler med sine databehandlere.

Åtte virksomheter oppga at de i noen grad hadde rutiner for periodisk sjekk av at vilkår i databehandleravtaler faktisk ble overholdt av databehandlerne. Kun én virksomhet svarte at alle rutiner var på plass.

PRAKTISERING AV RUTINER

Virksomhetene som hadde rutiner for risikovurdering av informasjonssikkerheten og inngåelse av databehandler-avtaler oppga at rutinene stort sett ble praktisert, i alle fall når det gjaldt store og viktige tjenesteleveranser. Det var en viss usikkerhet om dette var tilfelle for mindre systemer eller tjenester med få brukere.

De virksomhetene som helt eller delvis hadde rutiner for oppfølging av databehandlere underveis i tjeneste-leveransen, opplyse om at rutinene ble praktisert overfor utvalgte databehandlere. Virksomhetene hadde ikke kapasitet til å følge opp samtlige databehandlere.

ANBEFALINGER

Unit mener at resultatene i denne temarapporten viser at sektoren i hovedsak jobber godt med personvern og informasjonssikkerhet i forbindelse med tjenesteutsetting. Sektoren har imidlertid et forbedringspotensial når det gjelder avtaleoppfølging.

Videre mener Unit at den forventede veksten i omfang av tjenesteutsettingen, sammen med at tjenesteporteføljen trolig blir mer sammensatt og kompleks, vil stille sektoren overfor enkelte nye utfordringer. Dette gjelder særlig behovet for å rekruttere eller utvikle kompetanse om hvordan tjenesteutsatte systemer og tjenester kan settes opp og driftes på trygge og sikre måter.

Det kan også være behov for å styrke sektorens kompetanse om juridiske, spesielt personvernrettslige, problemstillinger som kan oppstå i forbindelse med tjenesteutsetting.

OM UNITS TEMARAPPORTER

Units temarapporter retter søkelyset mot viktige områder i arbeidet med informasjonssikkerhet og personvern, og vil vanligvis bli publisert i forbindelse med nasjonal sikkerhetsmåned.

Rapportene retter seg mot alle i sektoren som jobber med, har lederansvar for eller er interessert i spørsmål om informasjonssikkerhet og personvern.

I tillegg til å gi informasjon om utvalgte temaområder, kan virksomhetene benytte rapportene til å vurdere eget ståsted opp mot den generelle tilstanden i sektoren.

INNLEDNING

I Kunnskapsdepartementets «Policy for informasjonssikkerhet og personvern i høyere utdanning og forskning»[1] forventes det at alle tjenesteleverandører som behandler personopplysninger og annen type informasjon på vegne av virksomheter i UH-sektoren, for eksempel økonomi- og regnskapsdata,[2] er skikket for oppgaven. Det forventes også at virksomhetene stiller krav til og følger opp informasjonssikkerheten og personvernet i tjenesteutsatte leveranser.

I 2020 kartla Unit hvordan virksomheter i UH-sektoren som omfattes av departementets policy for informasjonssikkerhet og personvern ivaretok sitt ansvar ved tjenesteutsetting av digitale systemer og tjenester. Fokuset var særlig rettet mot tjenesteutsetting hvor leverandører håndterte personopplysninger som virksomhetene er behandlingsansvarlige for (bruk av databehandlere).

Unit kartla også omfanget av tjenesteutsetting på digitaliseringsområdet i UH-sektoren.

I denne temarapporten presenteres resultatene fra kartleggingen.

POLICY FOR INFORMASJONSSIKKERHET OG PERSONVERN

Kunnskapsdepartementet har fastsatt krav til arbeidet med informasjonssikkerhet og personvern i «Policy for informasjonssikkerhet og personvern i høyere utdanning og forskning». Det er Unit som forvalter policyen. Policyen gjelder for 31 virksomheter – statlige universiteter og høgskoler, direktorater og selskaper – underlagt departementet.

I punkt 5 i policyen oppsummeres de viktigste rettslige kravene som stilles til virksomheter som benytter seg av eksterne leverandører av digitale systemer eller tjenester. Det forventes blant annet at

i. virksomheten forsikrer seg om at eksterne leverandører ivaretar sikkerheten til informasjon og personopplysninger på en tilfredsstillende måte (gjennomfører risikovurderinger),
ii. virksomheten og leverandøren avtaler hvilke sikkerhetskrav og krav til behandling av personopplysninger som skal gjelde (databehandleravtaler),
iii. virksomheten forsikrer seg jevnlig om at avtalte krav til informasjonssikkerheten og personvern overholdes av leverandøren (revisjoner),
iv. virksomheten forsikrer seg om at leverandørens overføring av personopplysninger til land utenfor EU/EØS skjer på lovlig måte.

For virksomheter i UH-sektoren som leverer digitale systemer eller tjenester til øvrige virksomheter i eller utenfor sektoren, krever policyen at disse virksomhetene er i stand til å overholde sine rettslige og avtalefestede forpliktelser.

1 Policy for informasjonssikkerhet og personvern i høyere utdanning og forskning (https://www.unit.no/media/1981/download)

2 Se «Bestemmelser om økonomistyring i staten», kapittel 2.6 (https://www.regjeringen.no/globalassets/upload/fin/vedlegg/okstyring/reglement_for_okonomistyring_i_staten.pdf#page=23).

BAKGRUNN

Tjenesteutsetting har i løpet av de siste årene blitt en viktig del av digitaliseringsarbeidet i mange sektorer og bransjer. «Mørketallsundersøkelsen 2020» viser for eksempel at 54 prosent av virksomhetene som deltok i undersøkelsen helt eller delvis hadde tjenesteutsatt driften av digitale systemer eller tjenester.[3] 41 prosent av virksomhetene svarte at all drift fortsatt skjer internt.

Tjenesteutsetting og ekstern drift av digitale løsninger er et viktig trekk ved digitaliseringen også i UH-sektoren (se nedenfor). Tjenesteutsettingen i UH-sektoren er i noen grad sektor-intern. Unit, Uninett og Universitetet i Oslo er eksempler på sektor-interne aktører som leverer viktige tjenester til øvrige virksomheter i UH-sektoren, blant annet «Felles studentsystem» og «Tjenester for sensitive data».

I tillegg leverer andre offentlige virksomheter digitale løsninger til UH-sektoren, for eksempel lønns- og økonomisystemer fra Direktoratet for forvaltning og økonomistyring (DFØ).

Ut over dette leveres mange digitale systemer og tjenester av kommersielle aktører, både norske og utenlandske. Dette inkluderer blant annet Inspera (digital eksamen), Instructure (Canvas), Zoom Video Communications (videokonferanse) og Microsoft (Office 365 og Azure).

ANSVAR, UNDERLEVERANDØRER OG DATALOKASJON

Når slike og andre eksterne tjenesteleveranser tas i bruk i UH-sektoren, er det virksomheten (behandlingsansvarlig) som formelt sett har det største ansvaret for at informasjonssikkerheten og personvernet i leveransene er tilfredsstillende. Ansvaret inkluderer alle underleverandører som hovedleverandøren (databehandleren) eventuelt benytter seg av, for eksempel tilbydere av datasentre, vedlikeholdstjenester eller brukerstøtte.

Virksomheten har i tillegg ansvaret for at informasjonssikkerheten og personvernet ivaretas dersom hovedleverandøren eller eventuelle underleverandører overfører virksomhetens personopplysninger til datalokasjoner utenfor EU/EØS-området.

Leverandøren (databehandleren) har også et selvstendig ansvar for informasjonssikkerhet og personvern i sine tjenesteleveranser.

3 «Mørketallsundersøkelsen 2020» ble gjennomført av Opinion på oppdrag av Næringslivets sikkerhetsråd. Undersøkelsen kartla arbeidet med informasjonssikkerhet og personvern hos 1600 norske virksomheter fordelt på 11 bransjer. Årets og tidligere års mørketallsundersøkelser er tilgjengelige her: https://www.nsr-org.no/produkter-og-tjenester/publikasjoner/morketallsundersokelsen.

OVERFØRING AV PERSONOPPLYSNINGER TIL LAND UTENFOR EU/EØS

Bruk av eksterne tjenesteleverandører kan innebære at personopplysninger overføres til land utenfor EU/EØS (tredjeland), for eksempel til USA. Prinsippet ved slik overføring er at beskyttelsen som personopplysningene har under europeisk personvernlovgivning (GDPR) skal følge opplysningene uansett hvor i verden de tar veien. Dette blir en utfordring når beskyttelsesnivået som tilbys i ulike tredjeland er svært variabelt.

For å løse dette problemet er det etablert en rekke overføringsmekanismer (eller -grunnlag) som er ment å sørge for at beskyttelsesnivået følger opplysningene når de overføres til tredjeland, inkludert USA (se GDPR kapittel V). For overføringer til USA ble det i tillegg etablert en egen ordning som var ment å forenkle overføringer til private amerikanske selskaper; den såkalte «Privacy Shield»-ordningen.

I juli 2020 avsa EU-domstolen en dom som underkjente «Privacy Shield». Begrunnelsen var at ordningen, sett i lys av amerikansk overvåkingslovgivning, ikke sikret at beskyttelsesnivået i EU/EØS fulgte med opplysningene på reisen til og under oppholdet i USA. «Privacy Shield» er derfor ikke lenger et gyldig grunnlag for overføringer til USA. EU-domstolen problematiserte også bruken av andre overføringsgrunnlag, blant annet EUs standard overføringsavtaler, som ofte benyttes ved overføringer til USA og øvrige tredjeland som ikke har det samme beskyttelsesnivået som i EU/EØS.

Hva som blir resultatet at EU-domstolens dom – hva virksomheter som overfører personopplysninger til USA og andre tredjeland nå må gjøre – er i skrivende stund noe uklart.[4] Dette er spørsmål som EU-kommisjonen, i samarbeid med amerikanske myndigheter, og Det europeiske personvernrådet (EDPB) jobber med å avklare.

Virksomheter i UH-sektoren bør i mellomtiden kartlegge hvilke eksterne tjenesteleveranser som innebærer overføringer til tredjeland, hvilke tredjeland det handler om og hva overføringsgrunnlaget er. Unit og Uninett vil gjøre det samme for fellestjenester som de leverer til sektoren. Dette inkluderer leverandører som det er inngått rammeavtaler med.

4 Se Datatilsynets informasjon om dommen og virkningene av den (https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2020/sos-om-nye-regler-for-overforing/).

ARBEIDSDELING

I mange tjenesteleveranser, spesielt når det gjelder skytjenester, er det praktiske arbeidet med informasjonssikkerhet og personvern delt mellom virksomheten og leverandøren: noen oppgaver blir ivaretatt av leverandøren, mens andre oppgaver må virksomheten selv ta seg av («Shared Responsibility Model»).

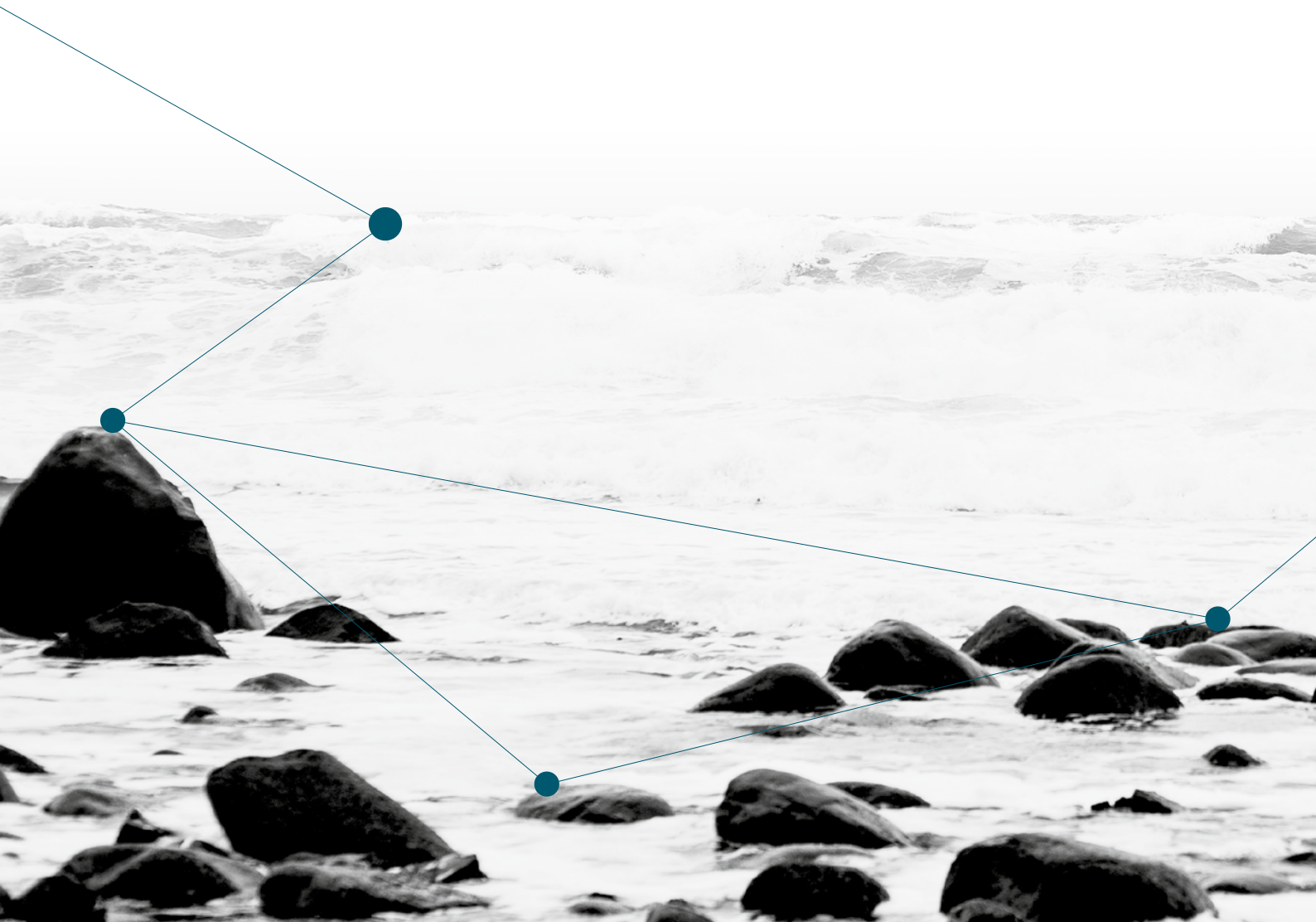
Hvordan oppgavefordelingen ser ut kan variere en del avhengig av hvilke typer tjenesteleveranser det er snakk om.[5] Det forutsettes imidlertid at virksomheten setter seg godt inn i hvordan oppgavefordelingen er for den enkelte tjeneste. Virksomheten må også være i stand til å utføre de oppgaver den er ment å gjennomføre på egen hånd.[6] Avhengig av type tjeneste, kan dette for eksempel omfatte oppgaver som tilgangsstyring, sikkerhetskopiering, kryptering, logging og sikkerhetsovervåking, osv.

VEILEDNING OG RÅDGIVING OM TJENESTEUTSETTING

Virksomheter som har behov for praktisk veiledning og rådgiving om hvordan krav til informasjonssikkerhet og personvern kan ivaretas ved tjenesteutsetting av digitale systemer og tjenester, kan ta kontakt med rådgivingstjenesten hos Uninetts «Cybersikkerhetssenter for forskning og utdanning».[7]

Rådgivingstjenesten hos Uninett vil blant annet kunne bistå ved risikovurderinger av eksterne tjenesteleveranser og ved utarbeidelse eller gjennomgang av databehandleravtaler.

Virksomhetene vil også kunne få bistand til gjennomføring av periodiske revisjoner av arbeidet med informasjonssikkerhet og personvern hos sine tjenesteleverandører.



KORT OM DATAGRUNNLAGET

Resultatene som presenteres i denne temarapporten er basert på data innhentet i forbindelse med Units årlige kartlegginger av sektortilstanden på informasjons-sikkerhets- og personvernområdet. Kartleggingene omfattet 29 virksomheter (universiteter og høgskoler, direktorater og selskaper) som omfattes av Kunnskapsdepartementets policy for informasjonssikkerhet og personvern.

Kartleggingene ble gjennomført i januar-mars og mai-juni 2020.

REDEGJØRELSE FOR DATAINNSAMLINGEN

Nærmere beskrivelser av hvordan Units kartlegginger blir gjennomført finnes i vedlegget til rapporten «Informasjonssikkerhet og personvern i høyere utdanning og forskning. Risiko- og tilstandsvurdering 2020» (se side 52-53).

5 For eksempel applikasjonstjenester ("Software-as-a-Service"), plattformtjenester ("Platform-as-a-Service") eller infrastrukturtjenester ("Infrastructure-as-a-Service"). Utgangspunktet her er at når man går fra applikasjonstjenester via plattformtjenester til infrastrukturtjenester, så øker også omfanget av de sikkerhets- og personvernrelaterte oppgaver som virksomheten må løse på egen hånd.

6 Se for eksempel "Demystifying the Cloud Shared Responsibility Security Model. Oracle and KPMG Cloud Threat Report 2020 Series. Volume 2" (https://www.oracle.com/a/ocom/docs/cloud/oracle-ctr-2020-shared-responsibility.pdf).

7 Cybersikkerhetssenter for forskning og utdanning (https://www.uninett.no/educsc)

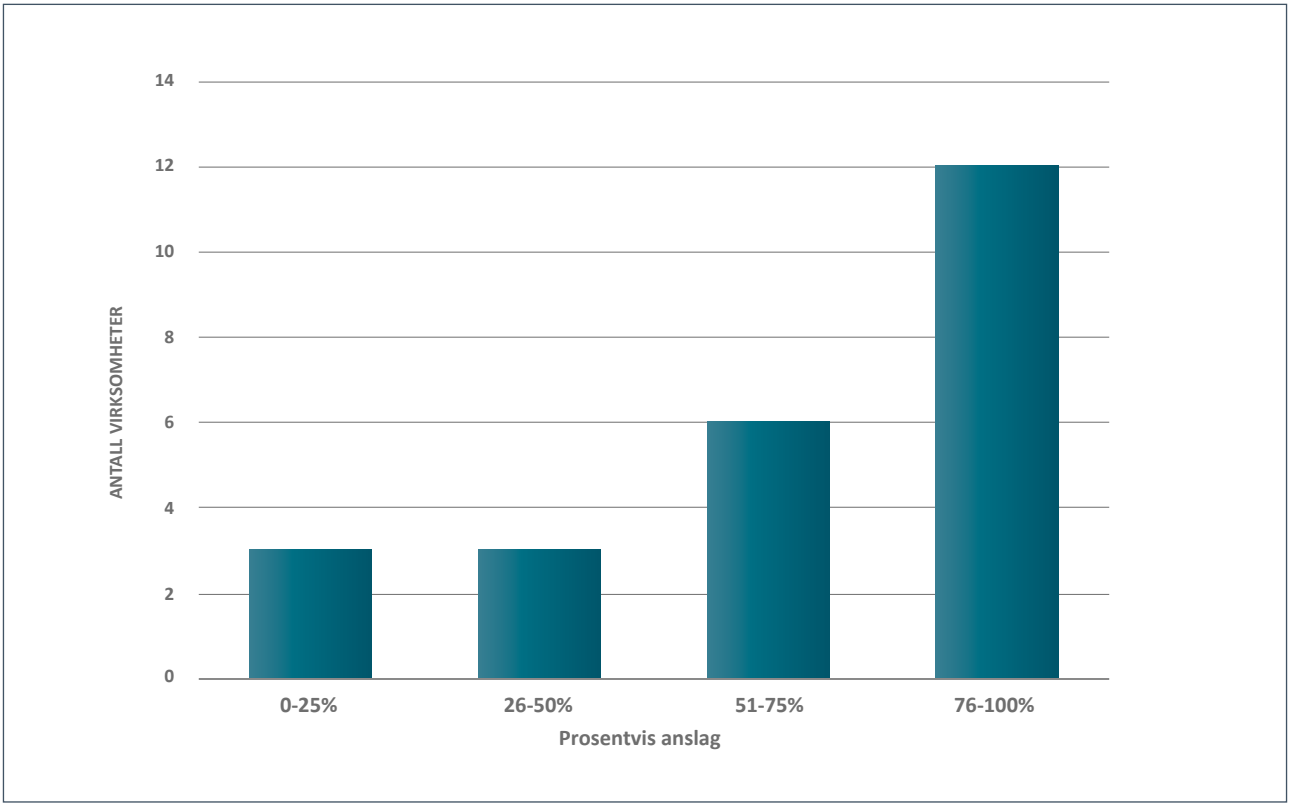
OMFANGET AV TJENESTEUTSETTINGEN

I Units kartlegging i 2020, ble virksomhetene spurt om de kunne gi et prosentvis anslag over hvor stor andel av den samlede databehandlingen i forskning, undervisning, administrasjon og formidling som var satt ut til eksterne leverandører.

24 av 29 virksomheter mente de kunne gi et slikt anslag, mens fem virksomheter mente det ble for vanskelig. De ønsket derfor ikke å oppgi et spesifikt anslag.

Også flere av de 24 virksomhetene som ga et prosentanslag understreket at anslaget var heftet med en viss usikkert, blant annet på grunn av at enkelte virksomheter savnet en fullstendig oversikt over den samlede system- og tjeneste-porteføljen.

Oversikten i figur 1 nedenfor må derfor ikke leses som en nøyaktig måling av tjenesteutsettingens omfang. Den gir likevel en pekepinn på hvor mye av databehandlingen i sektoren som skjer ved hjelp av eksterne tjeneste-leverandører.



Figur 1: Anslått omfang av tjenesteutsetting, 2020

Figur 1 viser at hos 3/4 av de 24 virksomhetene som oppga et prosentanslag, foregikk majoriteten av den totale databehandlingen ved hjelp av eksterne tjenesteleverandører (51 prosent eller mer). Figuren viser også at halvparten av disse virksomhetene svarte at tjenesteutsetting var et dominerende trekk ved digitaliseringen, det vil si at 76 prosent eller mer av databehandlingen foregikk ved hjelp av eksterne tjenesteleverandører.

To virksomheter oppga at all databehandling var tjenesteutsatt.

Ingen av virksomhetene, inkludert de som ikke ønsket å oppgi et prosentanslag, svarte at all databehandling foregikk internt.

FORVENTET ØKNING

Flere av virksomhetene som opplyste om at 76 prosent eller mindre av databehandlingen skjedde ved hjelp av eksterne tjenesteleverandører, forventet at omfanget av tjenesteutsettingen ville øke i tiden fremover. Én virksomhet svarte for eksempel at omkring fem prosent av den totale databehandlingen foregikk ved hjelp av eksterne tjenesteleverandører på kartleggingstidspunktet, men antok at dette ville endre seg til over 90 prosent i løpet av det kommende året.

Videre er det verdt å merke seg at også de fem virksomhetene som ikke oppga et spesifikt prosentanslag opplyste om at tjenesteutsetting representerte «en økende andel» av den totale databehandlingen, eller at det var «økende bruk av skytjenester». Andre svarte at de observerte «en trend i retning av mer ekstern drift». Flere av disse virksomhetene vurderte å sette ut driften av konkrete tjenester, for eksempel e-postløsninger eller systemer for økonomi og lønn.

HYPPIG BRUKTE TJENESTELEVERANDØRER

Mange av de vanligste brukte tjenesteleverandørene er nevnt ovenfor, for eksempel Unit, Uninett og leverandører som Unit og Uninett har inngått rammeavtaler med. Andre hyppig nevnte tjenesteleverandører inkluderte Microsoft, spesielt Office 365, Universitetet i Oslo («Tjenester for sensitive data») og NSD (forskningsadministrative tjenester). I tillegg opplyste flere virksomheter om at de brukte systemer for økonomi og lønn levert av Direktoratet for forvaltning og økonomistyring.

Ut over dette ble det opplyst om et mangfold av andre eksterne tjenesteleveranser innenfor alle virksomhetsområder (forskning, undervisning, administrasjon og formidling).

SOURCINGSTRATEGI

Virksomhetene ble ikke spurt om tjenesteutsettingen hadde skjedd som en del av sourcingstrategier, eventuelt skystrategier.[8] Flere virksomheter ga likevel uttrykk for at de hadde en slik strategi. Enkelte andre virksomheter opplyste om at de var i ferd med å utarbeide en sourcing- eller skystrategi.

Det var også noen virksomheter som hadde overordnede føringer i sine digitaliseringsstrategier for valg mellom intern drift og tjenesteutsetting.

RESULTATENE I KONTEKST

Sammenliknet vi resultatene ovenfor med tilsvarende resultater fra «Mørketallsundersøkelsen 2020» (se ovenfor), indikerer våre tall at tjenesteutsetting er en mer vanlig digitaliseringsstrategi innen høyere utdanning og forskning enn i mange andre sektorer og bransjer.

41 prosent av respondentene i «Mørketallsundersøkelsen 2020» svarte for eksempel at tjenesteutsetting ikke ble benyttet. Hos de virksomhetene som omfattes av Kunnskapsdepartementets styringsmodell for informasjonssikkerhet og personvern var det ingen virksomheter som opplyste om det samme.

RISIKOVURDERING VED TJENESTEUTSETTING

Mange tjenesteutsatte systemer og tjenester innebærer at eksterne leverandører behandler personopplysninger på oppdrag fra virksomhetene. Som nevnt ovenfor, betyr dette at virksomhetene er ansvarlige for at informasjonssikkerheten til personopplysningene blir tilfredsstillende ivaretatt av tjenesteleverandøren (databehandleren).

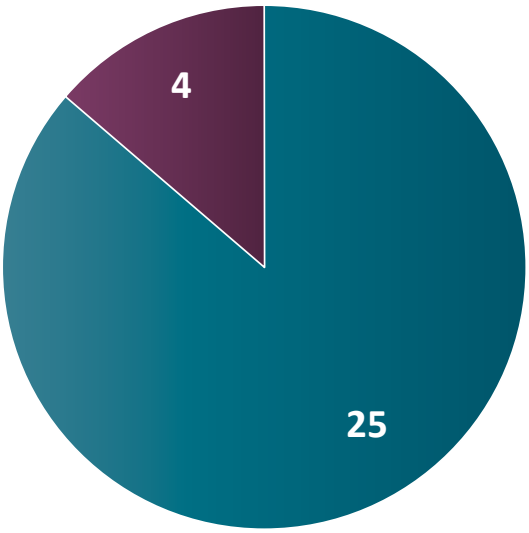
For å forsikre seg om dette er virksomhetene pålagt å gjennomføre risikovurderinger av informasjonssikkerheten i systemer og tjenester som tilbys av databehandlere.[9] En realistisk vurdering av risiko forutsetter blant annet at virksomhetene er kjent med hvordan sikkerheten til opplysningene ivaretas i hele leverandørkjeden, og har kunnskap om arbeidsdelingsmodellen for den aktuelle tjenesten («Shared Responsibility Model», se ovenfor).

Dersom risikovurderingen viser at informasjonssikkerheten til personopplysningene ikke er tilfredsstillende, vil det ikke være lovlig å benytte den aktuelle tjenesten. For at bruken skal være lovlig må det i slike tilfeller iverksettes sikringstiltak som styrker sikkerheten i selve tjenesten eller i den lokale bruken av den, eventuelt begge deler.

I Units kartlegging i 2020 ble virksomhetene spurt om de hadde etablert rutiner for risikovurdering av informasjonssikkerheten ved tjenesteutsetting til databehandlere. De ble også spurt om rutinene faktisk ble praktisert.

8 Se «Digitaliseringsrundskrivet 2020» punkt 1.10 og 1.11 (https://www.regjeringen.no/no/dokumenter/digitaliseringsrundskrivet/id2683652/).

9 Risikovurderinger av informasjonssikkerheten skal også gjennomføres dersom det skjer vesentlige endringer i tjenestenes oppbygning eller funksjonalitet. Slike vurderinger bør også gjøres ved større endringer i den lokale bruken av eksterne tjenesteleveranser, for eksempel dersom tjenestene benyttes til behandling av andre typer personopplysninger enn det som opprinnelig var planlagt.



Figur 2:
Rutiner for risikovurdering av tjenester levert av databehandlere

Har rutiner

Har ikke rutiner

Figuren viser at 25 virksomheter hadde etablert formelle og dokumenterte rutiner for risikovurdering av informasjonssikkerheten i tjenester levert av databehandlere. Fire virksomheter svarte at de ikke hadde etablert formelle og dokumenterte rutiner for dette.

PRAKTISERING AV RUTINER

Av de 25 virksomhetene som hadde etablert formelle og dokumenterte rutiner for risikovurderinger, opplyste alle at rutinene ble praktisert. Graden av praktisering kunne imidlertid variere. Noen mente at rutinene i stor grad ble fulgt, mens andre mente at det trolig ble tatt i bruk systemer og tjenester uten at informasjonssikkerheten ble skikkelig vurdert (eller ikke ble vurdert i det hele tatt). Dette dreide seg likevel om mindre systemer eller tjenester. De største og viktigste ble vanligvis risikovurdert.

Det var også enkelte virksomheter som mente at de ikke hadde full oversikt over graden av praktisering. Disse virksomhetene opplyste om at det var vanskelig å vite hvordan lokale enheter, for eksempel fakulteter og institutter, forholdt seg til rutinene. Praktiseringen kunne derfor variere noe mellom ulike lokale enheter.

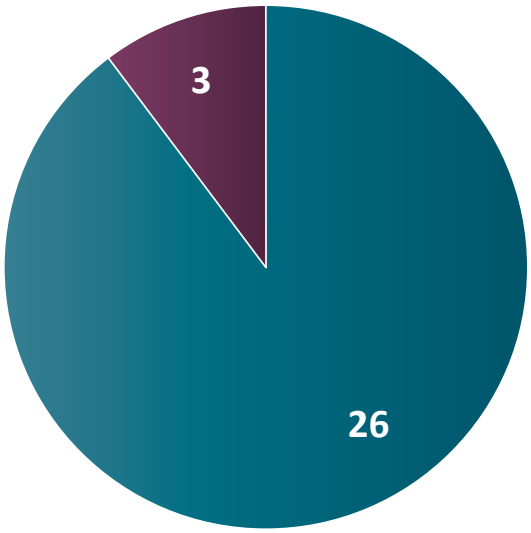
IKKE-FORMALISERT PRAKSIS

I enkelte av de fire virksomhetene som svarte at de ikke hadde etablert formelle og dokumenterte rutiner for risikovurdering av informasjonssikkerheten, ble det opplyst om at det likevel ikke var uvanlig at slike vurderinger ble gjennomført. I disse virksomhetene virket det derfor som at manglende formalisering av praksis var den største utfordringen.

INNGÅELSE AV DATABEHANDLERAVTALER

Når tjenesteutsetting av systemer og tjenester innebærer at eksterne leverandører (databehandlere) behandler personopplysninger på oppdrag fra virksomheten, skal det inngås en databehandleravtale mellom virksomheten og leverandøren. I avtalen skal virksomheten stille krav til leverandørens behandling av personopplysninger, inkludert bruk av underleverandører, overføringer til land utenfor EU/EØS og hvordan opplysningene skal sikres i hele leverandørkjeden. Hvilke minimumskrav som databehandleravtalen skal inneholde, er regulert i GDPR artikkel 28.

I Units kartlegging ble virksomhetene spurt om de hadde rutiner for inngåelse av databehandleravtaler med leverandører som behandler personopplysninger på deres vegne. De ble også spurt om rutinene faktisk ble praktisert.



Figur 3:
Rutiner for inngåelse av databehandleravtaler

Har rutiner

Har ikke rutiner

Figuren viser at 26 virksomheter hadde etablert formelle og dokumenterte rutiner for inngåelse av databehandler-avtaler med leverandører (databehandlere) som behandler personopplysninger på oppdrag fra virksomhetene. Tre virksomheter svarte at de ikke hadde etablert formelle og dokumenterte rutiner for dette.

PRAKTISERING AV RUTINER

Som når det gjaldt rutiner for risikovurdering, svarte alle de 26 virksomhetene som hadde rutiner for inngåelse av databehandleravtaler at rutinene ble praktisert, men at det kunne være utfordrende å ha full oversikt over graden av praktisering. Enkelte virksomheter mente for eksempel at der hvor det ble tatt i bruk systemer eller tjenester uten at de ble skikkelig risikovurdert, var det også en viss fare for at databehandleravtaler ikke ble inngått. Som nevnt ovenfor, dreide dette seg vanligvis om mindre systemer og tjenester som ble tatt i bruk av lokale enheter (fakulteter, institutter, sentre, osv.).

Når det gjaldt de største og viktigste eksterne data-leveransene ble det opplyst om at det alltid ble inngått databehandleravtaler.

AVTALEVURDERING OG UNDERTEGNING

Hvem som vurderte og hadde myndighet til å undertegne databehandleravtaler på vegne av virksomhetene kunne variere noe. Hos enkelte virksomheter var det direktøren som undertegnet avtalene etter at de først hadde blitt vurdert av lokale sikkerhets- og personvernekspertер, vanligvis sikkerhetsleder (CISO) eller personvernombudet, eller begge.

I andre virksomheter var det leder for IT-avdelingen/seksjonen eller de aktuelle system- eller tjenesteeierne som var delegert myndigheten til å undertegne avtalene på vegne av virksomheten. Også her var det vanlig at sikkerhetsleder (CISO) og/eller personvernombudet deltok i vurderingen av avtalene før de ble undertegnet.

HVEM SIN AVTALE?

For de store internasjonale tjenesteleverandørene, og for leverandører som sektoren hadde inngått rammeavtaler med, var det enten leverandørenes egne databehandler-avtaler eller avtaler som inngikk i rammeavtalen, som ble benyttet. I andre tilfeller var det virksomhetens egen standardavtale som ble anvendt.

I forbindelse med enkelte tjenesteleveranser kunne det oppstå diskusjoner om det var leverandørens eller virksomhetens avtale som skulle legges til grunn.

Flere virksomheter opplyste også om at mindre leverandører kunne mangle kompetanse om databehandleravtaler. Virksomhetene måtte derfor hjelpe disse leverandørene med å få på plass slike avtaler – de utførte i realiteten en form for konsulentbistand overfor disse leverandørene.

OPPFØLGING AV AVTALEVILKÅR

Etter at det er gjennomført risikovurderinger og inngått databehandleravtaler, har virksomhetene et oppfølgingsansvar overfor sine tjenesteleverandører (databehandlere). Det innebærer at virksomhetene skal sjekke at databehandlerne gjør det de har lovet i databehandleravtalene.

Oppfølgingsansvaret kan ivaretas på litt ulike måter. Det kan skje ved at virksomhetene ber om tilgang til og gjennomgår dokumentasjon på at avtalte oppgaver blir utført slik som forutsatt, for eksempel dokumentasjon fra sikkerhetsrevisjoner hos databehandleren.[10] Det kan også tenkes at det gjøres endringer i tjenesten som virksomhetene først må godkjenne, for eksempel dersom databehandleren tar i bruk nye underleverandører etablert i land utenfor EU/EØS.

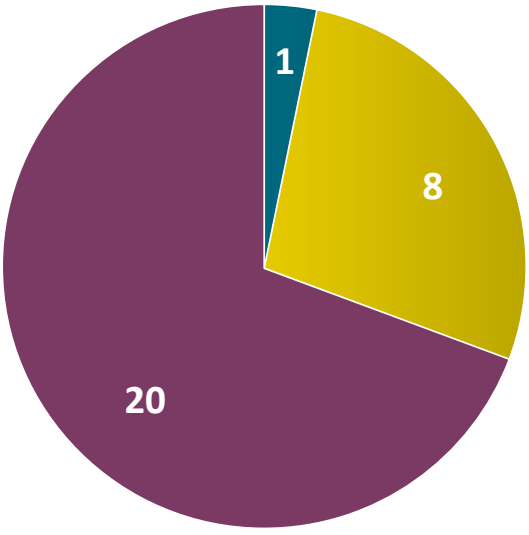
Databehandleren har i tillegg plikt til å varsle virksomhetene om brudd på informasjonssikkerheten til personopplysninger som behandles på oppdrag fra virksomheten.

I Units kartlegging ble virksomhetene spurt om de hadde rutiner for oppfølging av vilkår i databehandleravtaler underveis i tjenesteleveransen.

Figuren viser at én av 29 virksomheter svarte at det var etablert rutiner for oppfølging av vilkår i databehandleravtaler, og at dette faktisk ble gjort.

8 virksomheter svarte at de i noen grad hadde rutiner for avtaleoppfølging – dette var et arbeid som var påbegynt, men ikke sluttført – og at oppfølging ble gjort overfor utvalgte databehandlere. Hos noen av disse virksomhetene skjedde oppfølging kun i forbindelse med konkrete hendelser, for eksempel varsler fra databehandlere om brudd på informasjonssikkerheten.

20 virksomheter opplyste om at de ikke hadde rutiner for avtaleoppfølging. Det var heller ikke slik at oppfølging likevel ble gjort til tross for manglende rutiner.



Figur 4:
Oppfølging av vilkår i databehandleravtaler

10 Tjenesteleverandørene har pliktig til å dokumentere at de ivaretar sitt ansvar som databehandlere, se GDPR artikkel 28 nr. 3, bokstav h.

KAPASITETSUTFORDRINGER

Kapasitetsutfordringer ble oppgitt å være hovedårsaken til at 20 virksomheter verken hadde rutiner for eller fulgte opp sine databehandlere. Flere av disse virksomhetene uttrykte samtidig usikkerhet om hvilken oppfølging det var meningen at de skulle gjøre, og hvordan oppfølgingen i praksis kunne foregå.

I tillegg var enkelte virksomheter skeptiske til at de skulle følge opp store leverandører, med langt mer kompetanse og ressurser på informasjonssikkerhets- og personvernområdet enn det de selv rådde over. Det ble stilt spørsmål ved om dette ville ha noen særlig praktisk nytte og verdi, eller om det i realiteten ville bli en ren formell øvelse i regeletterlevelse.

VARSLER FRA DATABEHANDLERE

Som allerede nevnt, oppga enkelte virksomheter at de fulgte opp sine databehandlere når de fikk varsler fra dem om uønskede hendelser. Det var imidlertid få virksomheter som hadde mottatt slike varsler i løpet av det siste året (2019).

Det var også svært få virksomheter som opplyste om at de hadde mottatt andre typer varsler fra sine databehandlere, for eksempel om vesentlige endringer i tjenestenes oppbygning eller funksjonalitet. Majoriteten av virksomhetene mente derfor at så langt de visste, så hadde det ikke skjedd endringer i tjenestene som gjorde det nødvendig for dem å oppdatere sine risikovurderinger eller som krevde deres godkjenning.

OPPSUMMERING

Denne temarapporten viser at tjenesteutsetting utgjør en viktig og økende del av digitaliseringen i UH-sektoren. 18 virksomheter svarte for eksempel at mer enn 50 prosent av den totale databehandlingen foregikk ved hjelp av eksterne tjenesteleverandører. 12 av disse oppga at mer enn 75 prosent av den totale databehandlingen var tjenesteutsatt. Tjenesteutsetting var vanlig innenfor alle virksomhetsområder (forskning, utdanning, administrasjon og formidling).

Alle de 29 virksomhetene i kartleggingen regnet med at omfanget av ekstern databehandling ville øke i årene fremover.

Temarapporten viser også at tjenesteutsetting av digitale systemer og tjenester er et av områdene hvor sektoren har styrket sitt arbeid med informasjonssikkerhet og personvern. Dette kommer til uttrykk på flere måter. Mange virksomheter hadde etablert rutiner for risikovurdering av informasjonssikkerheten ved utsetting av tjenester som innebærer behandling av personopplysninger. Risikovurderinger ble også gjennomført hos de få virksomheter som svarte at de ikke hadde formelle rutiner for dette. En vanlig oppfatning var likevel at mindre system- eller tjenesteleveranser ikke ble risikovurdert i samme grad som de store.

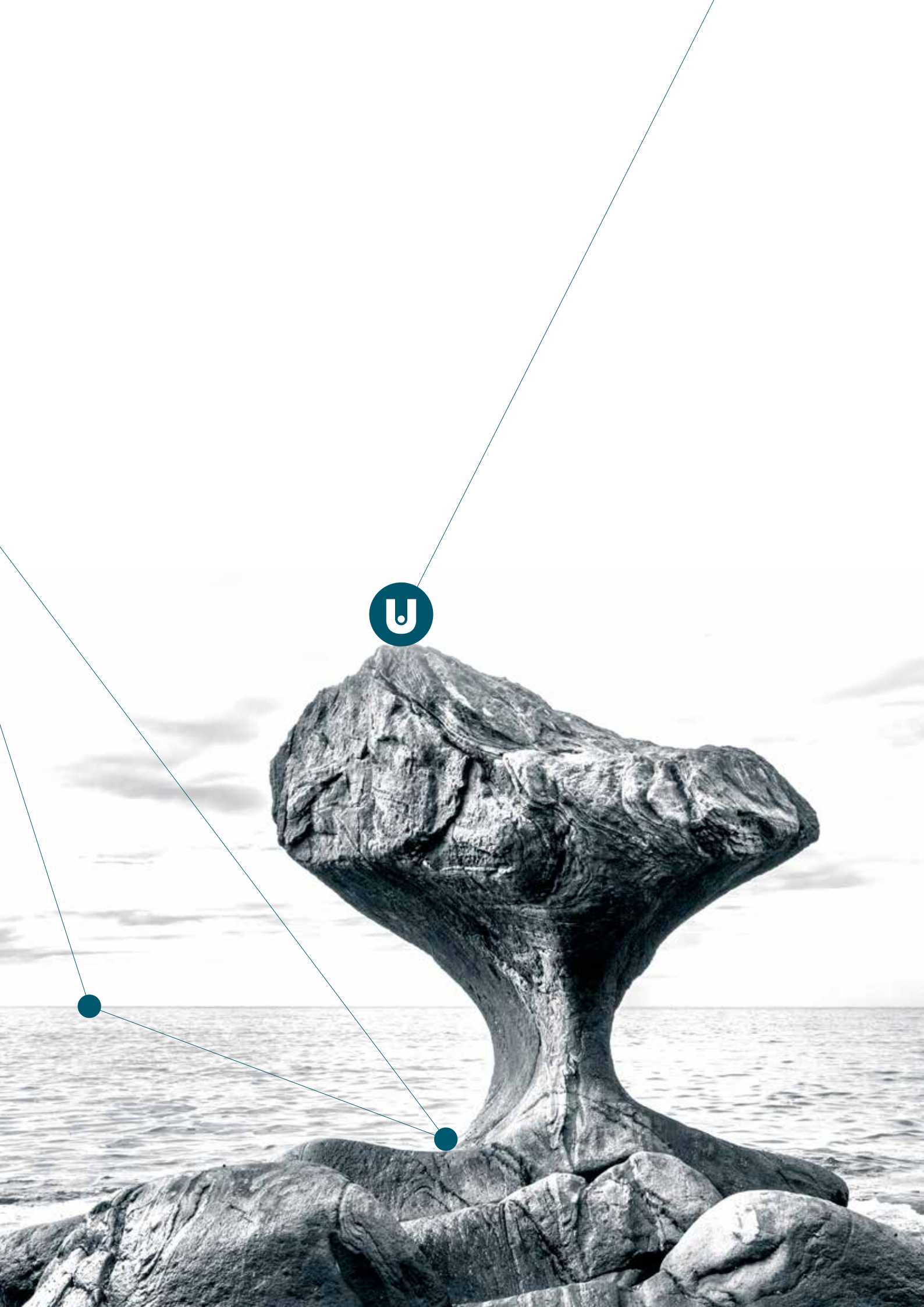
Mange virksomheter hadde i tillegg etablert rutiner for vurdering og inngåelse av databehandleravtaler ved tjenesteutsetting som omfattet behandling av personopplysninger. Databehandleravtaler ble inngått med leverandører av større og viktige digitale systemer og tjenester. For de mindre, gjerne tatt i bruk på privat initiativ, kunne det likevel tenkes at databehandleravtaler ikke ble inngått.

Det svakeste punktet som temarapporten avdekker, er oppfølgingen av databehandlere underveis i tjenesteleveransen. Her svarte knapt 1/3 av de 29 virksomhetene at de hadde ordninger for periodisk sjekk av at vilkår i inngåtte databehandleravtaler ble overholdt av databehandlerne. Kapasitetsutfordringer – manglende tid og ressurser til å følge opp databehandlere – ble oppgitt som den viktigste årsaken til at dette manglet hos de øvrige virksomhetene.

UNITS ANBEFALINGER

På bakgrunn av resultatene presentert i denne temarapporten, mener Unit at sektoren bør fortsette å styrke arbeidet med informasjonssikkerhet og personvern i forbindelse med tjenesteutsetting. Dagens arbeid fremstår i hovedsak som tilfredsstillende, men den forventede fremtidige veksten i omfang, sammen med at tjenesteporteføljen trolig blir mer sammensatt og kompleks, vil kreve mer av sektoren enn i dag. Dette gjelder særlig behovet for å rekruttere eller utvikle spisskompetanse om hvordan tjenesteutsatte løsninger kan settes opp og driftes på trygge og sikre måter.

Det kan også være behov for å styrke kompetansen om juridiske, spesielt personvernrettslige, spørsmål som kan oppstå i tilknytning til tjenesteutsetting.



Engasjert Byrå. Foto Shutterstock

UNIT

DIREKTORATET FOR IKT OG FELLESTJENESTER
I HØYERE UTDANNING OG FORSKNING