Datatilsynet

Narvik kommune
Rådhuset
8512 NARVIK

| Deres referanse | Vår referanse (bes oppgitt ved svar) | Dato |
|---|---|---|
| | 11/00593-18/RTH | 21. september 2012 |

## Saken avsluttes - Ny e-postløsning i Narvik Kommune - Google Apps

Det vises til Datatilsynets brev av 30. juni 2011, kommunens brev av 8. juli 2011, Datatilsynets brev av 1. august 2011, kommunens redegjørelse mottatt 2. september 2011, og til Datatilsynets varsel om vedtak av 16. januar 2012. Saken dreier seg om kommunens eksisterende, og planlagt utvidede, bruk av produktet "Google Apps".

Datatilsynet varslet vedtak om at kommunes bruk av løsningen måtte opphøre. Det varslede vedtaket var knyttet til kommunes redegjørelse rundt problemstillinger anført nedenfor.

I Datatilsynets brev av 30. juni 2011 ble det bedt om en redegjørelse fra kommunen om følgende punkter:

1. En redegjørelse for hvilke personopplysninger kommunen skal behandle i Google Apps.
2. Risikovurderingen som kommunen har foretatt i anledning behandling av personopplysninger i Google Apps, jf personopplysningsloven § 13 og personopplysningsforskriftens § 2-4.
3. Kopi av avtalen kommunen eventuelt har inngått med Google, samt oversikt over hvilke sikkerhetstiltak Google har i løsningen kommunen har valgt å benytte.
4. Kopi av eventuelt inngått databehandleravtale mellom kommunen og Google, samt en beskrivelse av informasjonssystemets utforming og fysiske plassering.
5. En beskrivelse av hvordan følgende problemstillinger er avklart med Google:
    - Sikkerhetskopiering
    - Hvem hos Google som har tilgang til kommunens personopplysninger
    - På hvilken måte kommunen skal gjennomføre sikkerhetsrevisjon hos Google, jf personopplysningsforskriften § 2-5.

**Vurdering av tilsvar fra Simonsen Advokatfirma DA**
Datatilsynet har i brev av 30.03.2012 mottatt tilsvar på tilsynets varsel om vedtak, fra Simonsen Advokatfirma DA (heretter: 'Simonsen') som representerer Narvik kommune i sakens anledning. I det følgende vil Datatilsynet kommentere tilsvaret. For oversiktens skyld

er overskriftene fra tilsvaret beholdt, og de ulike spørsmålene behandles i samme rekkefølge som i tilsvaret.

**Punkt 1**. **Vedrørende redegjørelse for hvilke personopplysninger kommunen skal behandle i Google Apps**

**Vedr. Kommunens kontroll over bruken av e-posttjenesten**
Det fremgår av Datatilsynets brev av 16. januar 2012 hvilke krav som personopplysningsloven stiller til den behandlingsansvarlige ved behandling av personopplysninger, jf. lovens § 13 og personopplysningsforskriften § 2-11 sikring av konfidensialitet:

> *"Personopplysningsloven § 13 stadfester at den behandlingsansvarlige gjennom planlagte og systematiske tiltak skal sørge for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet og tilgjenglighet ved behandling av personopplysninger.*
>
> *Personopplysningsforskriften § 2-11 tredje ledd stadfester at personopplysninger som overføres elektronisk ved hjelp av overføringsmedium utenfor den behandlingsansvarliges fysiske kontroll, skal krypteres eller sikres på annen måte når konfidensialitet er nødvendig."*

Datatilsynet merker seg at kommunen anfører at e-postløsningen i Google Apps ikke benyttes til saksbehandling men at bruken knyttes til kommunikasjon mellom de ansatte i kommunen og eksterne myndigheter og at det ikke skal forekomme forsendelse av e-postmeldinger med sensitive personopplysninger.

For å hindre eventuelt forsendelse av sensitive personopplysninger opplyser kommunen om at det er innført tiltak slik som interne rutiner og systematisk opplæring av ansatte for bruk av e-postløsningen i Google Apps. I kommunens kvalitetssystem for informasjonssikkerhet(KIS) er det blant annet beskrevet, "*Det er forbudt å sende personidentifiserbare sensitive data via elektronisk post".* Det fremkommer videre at kommunen har informert på kommunens nettside om at borgerne ikke skal benytte e-post til forsendelse av sensitive personopplysninger.[1]

Kommunen har gjennomført en risiko- og sårbarhetsanalyse av tjenesten Google Apps i henhold til personopplysningslovens regler.[2] Det fremkommer av dokumentets punkt 6: Vurdering av ulike risikofaktorer og 6.1 E-post med sensitivt innhold,

> *"at på bakgrunn av kontinuerlig interne kompetansehevende tiltak og informasjon til borgerne og ansatte i kommunen anser kommunen det som usannsynlig at det vil bli sendt sensitivt innhold på e-post.*

[1] Ytterligere tiltak anføres i tilsvar fra Simonsen punkt 3 og 3.2 Om sikkerhetstiltak i løsningen.
[2] Risiko- og sårbarhetsanalyse for innføring av nytt e-postsystem i Narvik kommune – Google Apps 2012.

*Konsekvensen av at det kan forekomme sensitivt innhold i e-post vurderes som marginale.*
*E-post sendes over kryptert forbindelse, og sikkerheten i løsningen er generell meget god.[3] Risikoen for at det en skjeden gang kan forekomme e-post med sensitivt innhold er innenfor kommunes akseptkriterier for konfidensialitet og tilgjengelighet."*

Det fremkommer videre av tilsvaret fra Simonsen under punkt 1 og 2.1 Kommunens reviderte risikovurdering, at kommunen har foretatt en ny risikovurdering som etter "*kommunens syn gir en oversikt over alle relevante risikoer som er forbundet med løsningen."*

Det er i risikoanalysen foretatt nærmere vurderinger med hensyn til konfidensialitet, integritet og tilgjengelig. Her trekkes blant annet frem

*"at risikoen for uønskede hendelser med eksponering av personopplysninger ved bruk at e-post i sum er svært lav."*

Det følges opp med at

*"kommunen baserer denne vurderingen på de sikkerhetsmekanismer som ligger i teknisk løsning, fysisk sikring som databehandler dokumenterer, organisatorisk sikring hos databehandler gjennom interne rutiner og kompetente medarbeidere. Videre vises til kommunens interne rutiner og tiltak for informasjon om akseptabelt innhold for e-post som sendes til Narvik kommune og for e-post som sendes fra kommunen til borgerne og eventuelt samarbeidspartnere.*

*Informasjon om hva som er egnet eller ikke egnet innhold for elektroniske forsendelser (e-post og kontaktskjema) til Narvik kommune publiseres på kommunens portalsider og kan vurderes annonsert i kommunens fellesannonser i lokalpressen"*

På bakgrunn av de opplysninger som kommunen har presentert i ettertid, er tilsynet tilfreds med de tiltak som er gjennomført for blant annet å hindre eventuelt forsendelse av sensitive personopplysninger i e-postløsningen i Google Apps. Se også punkt 2 om risikovurdering.

**Punkt 2. Vedrørende redegjørelse med hensyn til risikovurderingen som kommunen har foretatt i anledning behandling av personopplysninger i Google Apps, jf personopplysningsloven § 13, jf personopplysningsforskriftens § 2-4.**

**Vedr. Risikovurderingen**
Som nevnt under punkt 1 viser kommunen til at det er gjennomført risiko og sårbarhetsanalyse av e-postløsningen, Google Apps i henhold til personopplysningslovens regler.

[3] Kommunen benytter teknologi, kryptering SSL(Secure Sockets Layer,(https:) som tilbys i Google Apps for alle sine brukere. Google Apps tilbyr også bruk av TLS(Transport Layer Security). Dokumentasjon på sikkerhetstiltak fremgår av Security Whitepaper: Google Apps Messaging and Collaboration Products, Security feature Customizations.

Datatilsynet merker seg at risikoanalysen er utført i flere omganger og at målet er å avdekke risiko- og trusselfaktorer som Narvik kommune har vurdert ut fra kommunens akseptkriterier og informasjonssikkerhet knyttet til bruk av e-postløsning i Google Apps.

Det er 16 risikofaktorer som er blitt vurdert ut fra en risikomatrise som bygger på angivelse av sannsynlighet og konsekvens med eksisterende og ny e-postløsning.[4] Rapporten oppsummerer blant annet med,

> *"En flytting av e-post løsning til Google Apps vil på enkelte aspekter gi likt risikobilde som for gammel, men på mange områder innebærer ny løsning redusert risiko. Lagring av e-post data utenfor kommunens datasenter vil gi en lavere risiko med hensyn til konfidensialitet, integritet og tilgjengelighet."*

Det fremkommer videre av tilsvaret fra Simonsen en gjengivelse av hovedelementene i risikoanalysen og de vurderingene som kommunen har foretat med hensyn til konfidensialitet, integritet og tilgjengelighet ved e-postløsningen, Google Apps og at

> *"Kommunen vil imidlertid gjøre en løpende vurdering av risikobildet, og foreta en ny risikovurdering dersom det skjer endringer som har betydning for informasjonssikkerheten, jf forskriften § 2-4."*

Datatilsynet anser risikovurderingen som tilfredsstillende men ønsker å påpeke viktigheten av at kommunen gjennomfører ny risikovurdering ved endringer som har betydning for informasjonssikkerheten. Se også punkt 1 om hvilke personopplysninger kommunen skal behandle i Google Apps.

**Vedr. Tredjepartsrevisjon**

Det fremkommer av tilsvaret fra Simonsen under punkt 2 og 2.2 Tredjepartsrevisjon at *Google har forpliktet seg ovenfor kommunen at det foretas revisjon av sikkerhetssystemer tilknyttet tjenesten, jf redegjørelse for databehandleravtalen i punkt 3.1.* Blant annet er det fremhevet:

> *"Slik revisjon samt utarbeidelse av rapport er basert på både rammeverket SSAE 16 og rammeverket ISAE 3402 og revisjonen gjennomføres av lisensierte og godkjente revisjonsfirma som er uavhengig tredjepart.*
>
> *I det følgende refereres til ISAE 3402 rapporten som er relevant for dette tilfelle. Revisjonsrapporten beskriver virksomhetens tiltak og kontroll på et bestemt tidspunkt og bygger på detaljert testing over en minimumsperiode på seks måneder. Dette er en effektiv måte for en virksomhet å dokumentere intern kontroll til alle sine brukere/kunder.*

[4] Risiko- og sårbarhetsanalyse for innføring av nytt e-postsystem i Narvik kommune – Google Apps 2012 side 3 og 4.

*Google gjør den konfidensielle revisjonsrapporten tilgjengelig for sine kunder i tråd med interne retningslinjer for konfidensialitet."*

Tilsvaret viser også til følgende:

*"Kommunen har tilgang til og har foretatt en grundig gjennomgang av den seneste ISAE 3402-revisjonsrapporten vedrørende Google Apps. Rapporten er svært nyansert og dekker alle de tekniske og organisatoriske tiltak som er på plass for å sikre informasjonssikkerhet og personvern i løsningen. Rapporten gir kommunen et godt grunnlag for å verifisere at personopplysninger behandles i henhold til personopplysningsregelverkets krav og de krav som følger av databehandleravtalen med Google."*

Det fremgår av Google Apps for Buisness (Online) Agreement punkt 2. Data processing og 2.8 Security Audit,[5] at det i avtaleperioden utarbeides en rapport ifølge SSAE nr. 16 type II (SSAE, Statement on Standards for Attestation Engagements) og ISAE nr. 3402 (ISAE, International Standards for Assurance Engagements) (eller en tilsvarende rapport) om Googles systemer med undersøkelse av logiske sikkerhetskontroller, fysiske sikkerhetskontroller og systemtilgjengelighet («revisjonsberetning») i forbindelse med tjenestene. Minst hver 18. måned ber Google en tredjepart utarbeide en oppdatert revisjonsberetning.

Artikkel 29 *Opinion 05/2012 on Cloud Computing*,[6] omtalt uavhengige tredjepartsrevisjoner slik:

*"Individual audits on data hosted in a multi-party, virtualized server environment may be impractical technically and can in some instances serve to increase the risks to those physical and logical network security controls in place. In such cases, a relevant third party audit chosen by the controller may be deemed to satisfy in lieu of an individual controller's right to audit.*
*[…]*

*In the context of cloud computing, potential customers should look to see whether cloud services providers can provide a copy of this third party audit certificate or indeed a copy of the audit report verifying the certification […]."*

Datatilsynet har vurdert kommunens kontroll med sikkerhetsrevisjon slik at den er i samsvar med personopplysningsforskriften § 2-5. Datatilsynet presiserer at kommunen jevnlig, for eksempel årlig, må sørge for at sikkerhetsrevisjon blir gjennomført. Revisjonen omfatter organisering, sikkerhetstiltak og bruk av kommunikasjonspartner og leverandører.

[5] http://www.google.com/apps/intl/en/terms/premier_terms_ie.html
[6] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf

Det legges videre til grunn at tredjepartsrevisjonen også omfatter at databehandleren generelt etterlever avtalen(e) med den behandlingsansvarlige, også for oppgaver utover informasjonssikkerhet. Herunder for eksempel at opplysninger ikke benyttes til andre formål enn hva som er avtalt. Det vises i denne sammenheng til omtale om databehandleravtale senere i dette dokumentet.

Det vil være opp til kommunen å følge opp slik at de mottar og gjennomgår de til enhver til gjeldene revisjonsrapporter, eksempel, ISAE 3402-revisjonsrapporten fra Google og hvilke deler av rapportene som er relevant for kommunens behandlinger av personopplysninger.

**Vedr. Exit-mulighet fra Google Apps**
Det fremkommer av kommunes risiko og sårbarhetsanalyse under punkt 6.10 Exit til annen leverandør, at Google legger til rette for exit og mulighet for å ta med seg sine egne data hvis Narvik kommune ønsker dette. Det henvises til at Google har opprettet et eget nettsted hvor all informasjon om flytting av data er dokumentert.[7]

Det fremgår videre av Google Apps for Business-avtale (nettbasert) den engelskspråklige versjonen av vilkårene under punkt *11 Oppsigelse og 11.5 Virkninger av oppsigelse* at [8]

> *"Hvis denne avtale (deriblant alle bestillingssider) sies opp,*
> *i)opphører rettighetene gitt av den ene part til den andre umiddelbart,*
>
> *ii) gir Google kunden tilgang til, og mulighet til å eksportere, kundeopplysningene i en kommersielt rimelig periode til Googles priser på det aktuelle tidspunktet for de relevante tjenestene,*
>
> *iii) sletter Google kundeopplysningene etter en kommersielt rimelig periode ved å fjerne pekere til dem på Googles aktive servere og replikasjonsservere og etter hvert overskrive dem og*
>
> *iv) gjør hver part etter forespørsel umiddelbart sitt ytterste for å returnere eller destruere alle andre fortrolige opplysninger om den andre parten.*

Etter kommunens oppfatning er risikoen for ikke å kunne hente ut data ved exit vurdert til å være innenfor kommunens akseptkriterier for tilgjengelighet.

Se også punkt 6 Vedr. Sletting av data.

**Punkt 3 og 4 – databehandleravtalen**

*Det rettslige utgangspunktet*
Datatilsynet har i brevet av 16. januar 2012 redegjort for de krav som personopplysningsloven stiller til en databehandleravtale, jf. lovens § 15. Lovbestemmelsen lyder:

[7] www.dataliberation.org
[8] http://www.google.com/apps/intl/en/terms/premier_terms_ie.html

*"En databehandler kan ikke behandle personopplysninger på annen måte enn det som er skriftlig avtalt med den behandlingsansvarlige. Opplysningene kan heller ikke uten slik avtale overlates til noen andre for lagring eller bearbeidelse.*

*I avtalen med den behandlingsansvarlige skal det også gå frem at databehandleren plikter å gjennomføre slike sikringstiltak som følger av § 13."*

Den 30. juni 2011 ba Datatilsynet kommunen om å redegjøre for flere forhold angående avtaleforholdet mellom Narvik kommune og Google. Samtidig ble det varslet at det ville kunne bli fattet vedtak, med mindre kommunens tilbakemeldinger avdekket at det ikke var grunnlag for det, se brevet av 16. januar 2012 på side 9.

*Skriftlighetskravet*
Det følger av bestemmelsen at den behandlingsansvarlige og databehandleren er forpliktet til å inngå *skriftlig* avtale om den aktuelle behandlingen av personopplysninger.

Kommunen bekrefter at slik avtale nå foreligger.[9] Skriftlighetskravet i lovens § 15 er således oppfylt.

*Avtalens formålsavgrensning*
For det andre følger det av bestemmelsen at databehandleren ikke kan behandle personopplysningene på annen måte, eller til andre formål, enn det som er avtalt med den behandlingsansvarlige.

I dette ligger det at databehandleren ikke kan gå utover de instruksjoner som den behandlingsansvarlige gir om den aktuelle databehandlingen – databehandleren er bundet av de behandlingsformål og de behandlingsmåter som den behandlingsansvarlige kan gjøre gjeldende i medhold av personopplysningsloven.

Dersom leverandøren behandler personopplysningene på andre måter, eller til andre formål, enn det som er avtalt, vil databehandleravtalen være brutt. Leverandøren vil i tillegg bli å regne som behandlingsansvarlig. I så fall må leverandøren svare for oppfyllelsen av samtlige rettslige krav som stilles til behandlingen.[10]

Kommunen har redegjort for Googles rådighet over de persondata som behandles ved bruk av tjenesten. Kommunen viser til databehandleravtalen, hvor det fremgår at Google skal behandle data på vegne av Narvik Kommune "*i henhold til Reseller Agreement og underliggende SLA-er*":

"*[…] Google will provide the Service in accordance with this Agreement and the SLA. Google will provide Customer with Admin Account to use for administering the End User Accounts and other features of the Services. Customer shall: (a) administer End User Accounts using the Admin Console and Admin Tools; and (b) determine the Services to be provided to End Users*"

[9] "Narvik kommunes merknader til Datatilsynets varsel om vedtak datert 16. januar 2012" avsnitt 3.1.
[10] Under forutsetning av at vilkårene i personopplysningsloven § 4 er oppfylt.

I tillegg fremgår det av databehandleravtalen at norsk personvernlovgivning skal gjelde for den aktuelle behandlingen av personopplysninger. Avtalen fastslår videre at Google er å anse som databehandler, og følgelig forpliktet til å oppfylle de kravene som stilles til databehandlere i medhold av de norske reglene:

> *"For the purposes of this Agreement and in respect of Customer Personal Data, the parties agree that Customer shall be the controller and Google shall be a processor. Within the scope of this Agreement, Customer shall comply with its obligations as a controller and Google shall comply with its obligations as a processor under the Data Protection Legislation*"

Datatilsynet har funnet at kravene i lovens § 15 er oppfylt på dette punktet.

*Forbudet mot å overlate opplysningene til andre*
Det følger av § 15 at Google ikke kan utlevere data til andre uten etter godkjennelse fra kommunen.

Av avtalens avsnitt 7.1 fremgår det at databehandleren ("*the recipient*") kan "*disclose confidential information when required by law after giving reasonable notice to the discloser*" – den behandlingsansvarlige skal altså gis forhåndsvarsel om at personopplysninger i et konkret tilfelle vil utleveres på bakgrunn av et rettskrav.

Utlevering av opplysninger etter krav fra justismyndigheter i USA eller andre stater, vil kunne være i overensstemmelse med § 15, under forutsetning av at det enkelte kravet er rettslig bindende overfor tjenesteleverandøren, og en påfølgende utlevering ikke er i strid med øvrige bestemmelser i norsk lov.
Den behandlingsansvarlige bør imidlertid også forsikre seg om at databehandleren kan garantere at ingen personopplysninger vil bli utlevert til noe annet lands justismyndigheter, med mindre de ovennevnte kriteriene er oppfylt.[11]

I tillegg bør de registrerte informeres om denne utleveringsadgangen, jf. prinsippene i personopplysningsloven § 19 bokstav c og e.

*Informasjonssikkerhetstiltak, jf. personopplysningsloven § 13*
I tillegg er databehandleren forpliktet til å implementere og gjennomføre slike informasjonssikkerhetstiltak som følger av personopplysningsloven § 13. Dette omfatter også bestemmelsene i personopplysningsforskriften kapittel 2. Tiltakene skal være beskrevet i kontrakten.

Avtalen fastsetter at Google skal implementere og iverksette tilstrekkelige tekniske og organisatoriske sikringstiltak for å beskytte kundedata mot tilfeldig eller ulovlig ødeleggelse eller tap, endring, uautorisert avsløring eller tilgang.

[11] Jf. Artikkel 29-gruppens uttalelse 05/2012 om Cloud Computing, avsnitt 3.4.2 nr. 13, jf. også avsnitt 4.1 femte strekpunkt tredje kulepunkt.

Googles sikkerhetstiltak for tjenesten er dokumentert i detalj i Googles «Security Whitepaper». Googles sikkerhetstiltak oppfyller, slik kommunen har vurdert det, kommunens krav til akseptabel risiko. Dette fremgår av den ovennevnte risikoanalysen, ifølge kommunen.

Datatilsynet har funnet at kravene i lovens § 15 er oppfylt på dette punktet.

**Punkt 4 – overføring av personopplysninger til utlandet**

*Lagring og behandling i Googles datasentre*
Det følger av personopplysningsloven § 29 at personopplysninger bare kan overføres til stater som sikrer en forsvarlig behandling av opplysningene. I praksis vil dette si at overføring av persondata til andre land enn medlemsstatene i EU og EØS-landene, som hovedregel er utelukket.

Det finnes imidlertid unntak. For eksempel kan dataeksportøren gi individuelle garantier, eller EU-kommisjonen kan ha besluttet at visse enkeltstater er trygge mottakerstater.[12]

Kommunen opplyser at "*databehandleravtalen […] fastslår at data skal lagres og behandles i Googles datasentre innenfor EU/EØS og innenfor USA. Det vises til at Google er sertifisert under Safe Harbor-regimet*".

Det følger av artikkel 1 i EU-kommisjonens beslutning 2000/520/EF av 26. juli 2000 at Safe Harbor-prinsippene sikrer et tilstrekkelig beskyttelsesnivå, i den forstand som omtalt i artikkel direktiv 95/46/EF artikkel 25 (1) og (2). Det følger videre av den samme bestemmelsen at personopplysninger kan eksporteres fra EU-/EØS-land til foretak som er etablert i USA, under de nærmere forutsetninger som er angitt i artikkelen. Kommisjonsbeslutningen er bindende for Norge, jf. personopplysningsforskriften § 6-1.

Det fremgår av offentlig tilgjengelig informasjon at Google Inc. er sertifisert under Safe Harbor-programmet.[13]

Under forutsetning av at samtlige aktuelle "*Googles datasentre*", jf. sitatet over, utgjør en del av det Safe Harbor-sertifiserte foretaket Google Inc., vil overføring av personopplysninger fra Norge til disse datasentrene være i samsvar med personopplysningsloven § 29.

*Caching/mellomlagring i nettet*
Kommunen har vist til at "*det vil skje bufring av data underveis i transportnettet* " i forbindelse med overføring av data via Internett. Kommunen uttaler at det ikke kan utelukkes at "*data under overføring mellomlagres (caches) midlertidig i Googles datasentre utenfor EU/EØS eller USA eller av andre ISP-er avhengig av hvordan trafikken rutes i nettet.*"

Kommunen ser ut til å forutsette at den omtalte "*cachingen*" er synonym med forbigående lagring eller mellomlagring.[14]

[12] Jf. Artikkel 29-gruppens uttalelse 05/2012 om Cloud Computing, avsnitt 3.4.2 nr. 13, jf. også avsnitt 4.1 femte strekpunkt tredje kulepunkt.

Overføringsbegrepet er omtalt i forarbeidene til personopplysningsloven:

> *"Bestemmelsen gjelder overføring til en adressat i utlandet. Det forhold at opplysninger som sendes elektronisk til en adressat i Norge rent faktisk transporteres via et annet land, medfører ikke at det må anses som en overføring til en annen stat i henhold til denne bestemmelsen. Det samme gjelder dersom opplysningene mellomlagres i utlandet uten at den behandlingsansvarlige på forhånd kjenner til dette."*

På bakgrunn av kommunens beskrivelse av de faktiske forhold og uttalelsene i forarbeidene, har vi lagt til grunn at den omtalte "*caching*" utgjør slik mellomlagring som nevnt, og at det således ikke dreier seg om noen overføring, i den forstand som omtalt i personopplysningsloven § 29.

<u>*Indeksering*</u>
Kommunen har oppgitt at *dataindekser* i en viss ustrekning vil lagres "*i de landene der Google opererer*". I den grad dette omfatter andre stater enn de som er nevnt over, blir spørsmålet om de omtalte dataindeksene omfatter eller inneholder personopplysninger. I så fall vil det kunne dreie seg om overføring av personopplysninger til tredjeland.

Begrunnelsen er ifølge kommunen at indekseringen er "*nødvendig for å understøtte søkefunksjonalitet for brukerne av tjenesten. Indekseringen gjør at brukernes egne søk i underliggende meldinger (brukerens egen e-post) kan gjøres mer effektivt og raskt.*"

I avtalen mellom kommunen og Google er det videre uttalt at

> "*[i]ndeksene inneholder bare fragmenter av data fra de underliggende meldinger og er logisk sammenstillet på en måte som bare er gjenkjennelig for maskinell lesning"*

Kommunen viser for øvrig til at indekseringen ikke innebærer noen behandling av IP-adresser, i hvert fall ikke for det formål å gi tilpassede søkeresultater i Googles søkemotorer. I forlengelsen av dette, uttaler kommunen at indekseringen utelukkende er relatert til funksjoner i Google Apps. Kommunen viser igjen til søkefunksjoner i e-posttjenesten.

At en bestemt informasjonsmengde er "*gjenkjennelig for maskinell lesning*" utelukker ikke at det dreier seg om en behandling av personopplysninger i personopplysningslovens forstand. Således kan det vanskelig utledes av kommunens beskrivelse at det ikke behandles personopplysninger i forbindelse med denne indekseringen.

På bakgrunn av de opplysninger som foreligger i saken, legger vi likevel til grunn at indekseringen ikke innebærer behandling av personopplysninger. Følgelig gjør begrensningene i lovens § 29 seg ikke gjeldende på dette punktet. Det er imidlertid kommunens ansvar å forsikre seg om at dette er tilfellet.

---

[14] Ot.prp. nr. 92 (1998-1999), kapittel 16, merknadene til § 29.

**Punkt 5. Vedrørende beskrivelse av hvordan følgende problemstillinger er avklart med Google**

- **Sikkerhetskopiering**
- **Hvem hos Google som har tilgang til kommunens personopplysninger**
- **På hvilken måte kommunen skal gjennomføre sikkerhetsrevisjon hos Google, jf personopplysningsforksriften § 2-5.**

**Vedr. Sikkerhetskopiering**
Det fremkommer av tilsvaret fra Simonsen under punkt 4 og 4.1 Sikkerhetsrevisjon at

> *"Google Apps benytter Google File System (GFS) som er et distribuert filsystem som er designet til å lagre store mengder data på tvers av tusenvis av dataservere. Data er replikert over mange systemer slik at ikke noe enkeltsystem utgjør "single point of failure". Hver enkelt brukers data er replikert til minst to data sentre, der begge senterne kan betjene brukeren."*

Videre anføres det at

> *"Systemets sikkerhetskopieringsprosess og påliteligheten av systemet er gjennomgått i detalj i revisjonsrapporten ISAE 3402 som kommunen har mottatt fra Google. Det fremgår av rapporten at systemet er kontrollert for tilgjengelighet og det dokumenteres at systemet gir tilstrekkelig redundans og mulighet for gjenoppretting av kundedata.*
>
> *Som nevnt ellers i kommunens svar er det ingen saksbehandling som vil foregå ved bruk av dette systemet. Således vil alle kommunale tjenester være i drift uavhengig om e-post data skulle risikere å gå tapt. Sannsynligheten for dette er vurdert å være svært liten og risikoen tilknyttet backup-systemet hos leverandøren ansees av samme grunn til å være akseptabel for Narvik kommune."*

Videre er Google File System(GFS) architecture og sikkerhetskopiering for tjenesten dokumentert i Googles «Security Whitepaper» under Disaster Recovery and Business Continuity slik:[15]

> *"Google Apps uses a distributed file system designed to store large amounts of data across large numbers of computers. Structured data is then stored in a large distributed database built on top of the file system. Data is chunked and replicated over multiple systems such that no one system is a single point of failure. Data chunks are given random file names and are not stored in clear text so they are not humanly readable. For more information please download the abstract at http://labs.google.com/papers/gfs.html*

[15] http://static.googleusercontent.com/external_content/untrusted_dlcp/www.google.com/en/us/a/help/intl/en-GB/admins/pdf/ds_gsa_apps_whitepaper_0207.pdf, side 12

*Data replication and backup: To help ensure availability in the event of a disaster, Google Apps data is replicated to multiple systems within a data center, and also replicated to a secondary data center.*

*Google operates a geographically distributed set of data centers that is designed to maintain service continuity in the event of a disaster or other incident in a single region. High-speed connections between the data centers help ensure swift failover. Management of the data centers is also distributed to provide location-independent, around-the-clock coverage, and system administration."*

Datatilsynet vil bemerke at det vil være opp til kommunen å følge opp at rutiner for sikkerhetskopiering gjennomføres gjennom sikkerhetsrevisjon og i henhold til mottatt revisjonsrapport, ISAE 3402 fra Google.

**Vedr. Hvem hos Google som har tilgang til kommunens personopplysninger**
Ved krav om Googles tilgang til kommunens sine personopplysninger, jf. beskrivelse i vårt brev av 30. juni 2011,[16] legger vi til grunn kommunens risikovurdering, revisjonsrapport ISAE 3402 fra Google og Googles sikkerhetstiltak for tjenesten som er dokumentert i detalj i Googles «Security Whitepaper» som vi tidligere har referert til:

*"Access Control*
*Authentication Controls*
*Google requires the use of a unique User ID for each employee. This account is used to identify each person's activity on Google's network, including any access to employee or customer data. This unique account is used for every system at Google. Upon hire, an employee is assigned the User ID by Human Resources and is granted a default set of privileges described below. At the end of a person's employment, policy requires that the account's access to Google's network be disabled from within the HR system.*

*Where passwords or passphrases are employed for authentication (e.g., login to workstations), systems enforce Google's strong password policies, including password expiration, restrictions on password reuse, and sufficient password strength.*

*Google makes widespread use of two-factor authentication mechanisms, such as certificates and one-time password generators.*

*Authorization Controls*
*Access rights and levels are based on an employee's job function and role, using the concepts of least privilege and need-to-know to match access privileges to defined responsibilities.*

[16] 5. En beskrivelse av hvordan følgende problemstillinger er avklart med Google: Hvem hos Google som har tilgang til kommunens personopplysninger

*Google employees are only granted a limited set of default permissions to access company resources, such as email, Google's internal portal, and HR information. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google's security policies. Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorization settings and the approval process to ensure consistent application of the approval policies.*

*An employee's authorization settings are used to control access to all resources, including data and systems for Google Apps products."*

Datatilsynet observerer positivt at det er funksjonalitet i Googles tjenesten for å ivareta administrative funksjoner for tilgangssyring og informasjonssikkerhet for ansatte hos Google og underleverandører.

Vi har ikke noen videre merknader utover å påpeke viktigheten av at kommunen er i dialog med Google vedrørende eventuelt avvik[17] og at kommunen sikrer mottak av relevant informasjon dersom avvik oppstår.

**Vedr. på hvilken måte kommunen skal gjennomføre sikkerhetsrevisjon hos Google, jf personopplysningsforksriften § 2-5.**
Dette punktet er behandlet under punkt 2 og Vedr. Tredjepartsrevisjoner

**Punkt 6 Vedrørende segmentering av ulike behandlingsansvarlige**

**Vedr. Behandlingsansvarliges data holdes adskilt i Google Apps**
*Regelverkets krav*
Skytjenester som Google Apps håndterer personopplysninger fra mange forskjellige virksomheter, og baserer seg i stor grad på virtualiseringsteknologi og logiske sikkerhetsbarrierer. Personopplysningsregelverket stiller krav til at personopplysninger som knyttes til forskjellige juridiske enheter skal holdes forsvarlig atskilt fra hverandre.

Det fremkommer av tilsvaret fra Simonsen under punkt 6 og 6.1 at data holdes adskilt i Google Apps:

*"Ved hjelp av en felles infrastruktur fordeles alle Google Apps kundedata (dvs. data som behandles i Google Apps på vegne forbrukere, virksomheter, og også Google selv) på en rekke servere på tvers av Googles datasentre. Infrastrukturen sørger for at data fordeles på flere systemer og sikrer at intet ledd er et potensielt "single point of failure". Kommunen vurderer at en slik løsning, der data for hver behandlingsansvarlig er fordelt på flere servere, innebærer en større grad av*

[17] De henviser her til avviksmelding etter personopplysningsforskriftens § 2-6 skal skje ved at databehandler melder avvik til behandlingsansvarlig.

*sikkerhet enn en løsning hvor den enkelte kundes data er samlet på en enkelt eller flere servere.*

*Filsystemet Google File System (GFS) som anvendes for løsningen er designet for å distribuere og lagre store mengder data over mange datamaskiner. Systemet fungerer slik at innkomne data stykkes opp i mindre biter som distribueres over flere systemer. Data-bitene gis tilfeldige filnavn og blir ikke lagret i klartekst, de er derfor ikke menneskelig lesbare. Ved hjelp av avansert filstruktur sikres logisk sammenheng av data som tilhører ulike behandlingsansvarlige.*

*Samtidig sørger filstrukturen for logisk adskillelse mellom ulike behandlingsansvarliges data, noe som hindrer en sammenblanding av ulike behandlingsansvarliges data. Dette sikres bl.a. ved at det skjer autentisering av alle tilgangsforespørsler fra brukere og ved utveksling av opplysninger mellom dataservere. Et av de grunnleggende designkriteriene for systemet er nettopp at ulike kunders data skal holdes adskilt slik at det ikke skjer brudd på konfidensialitet, integritet eller tilgjengelighet.*

*Revisjonsrapporten ISAE 3402 bekrefter at kundedata holdes adskilt, og en sammenblanding av kundedata ville naturligvis være ødeleggende for Googles omdømme og mulighet til å tilby denne type tjenester."*

Datatilsynet anser at logiske mekanismer for atskillelse av data, som regel i samspill med andre sikkerhetstiltak, kan oppfylle kravene i personopplysningsloven og forskriften. Det er imidlertid kommunens ansvar å påse gjennom risikovurdering og sikkerhetsrevisjon at databehandlerens sikkerhetstiltak er tilfredsstillende for de aktuelle behandlingene som foretas.

Datatilsynet vil bemerke at det vil være opp til kommunen å følge opp rutinene for segmentering av kundedata ved sikkerhetsrevisjon og i henhold til mottatt revisjonsrapport, ISAE 3402 fra Google.

**Vedr. Sletting av data**

*Regelverkets krav*

I henhold til personopplysningsloven § 11 første ledd bokstav e, jf. § 28, skal personopplysninger slettes når det ikke lenger er nødvendig å lagre dem for å gjennomføre formålet med behandlingen. Virksomheten skal etter personopplysningsloven § 14 ha rutiner for å sikre at sletting foretas i samsvar med bestemmelsene i loven.

Artikkel 29 *Opinion 05/2012 on Cloud Computing* beskriver sletting av data slik:[18]

*"According to Article 6(e) of Directive 95/46/EC, personal data must be kept in a form which permits the identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further*

[18] 3.4.1.3 Erasure of Data side 11.

*processed. Personal data that are not necessary any more must be erased or truly anonymised. If this data cannot be erased due to legal retention rules (e.g., tax regulations), access to this personal data should be blocked.*

*It is the cloud client's responsibility to ensure that personal data are erased as soon as they are not necessary in the aforementioned sense any more. The principle of erasure of data applies to personal data regardless of whether they are stored on hard drives or on other storage media (e.g., backup tapes). Since personal data may be kept redundantly on different servers at different locations, it must be ensured that each instance of them is erased irretrievably (i.e., previous versions, temporary files and even file fragments are to be deleted as well).*

*Cloud clients must be aware of the fact that log data facilitating auditability of, e.g., storage, modifications or erasure of data may also qualify as personal data relating to the person who initiated the respective processing operation.*

*Secure erasure of personal data requires that either the storage media to be destroyed or demagnetised or the stored personal data is deleted effectively through overwriting. For the overwriting of personal data, special software tools that overwrite data multiple times in accordance with a recognised specification should be used.*

*The cloud client should make sure that the cloud provider ensures secure erasure in the abovementioned sense and that the contract between the provider and the client contains clear provision for the erasure of personal data. The same holds true for contracts between cloud providers and subcontractors."*

Videre er sletterutiner for tjenesten dokumentert i Googles «Security Whitepaper» slik:

*"After a Google Apps user or Google Apps administrator deletes a message, account, user, or domain, and confirms deletion of that item (e.g., empties the Trash), the data in question is removed and no longer accessible from that user's Google Apps interface.*

*The data is then deleted from Google's active servers and replication servers. Pointers to the data on Google's active and replication servers are removed. The referenced data will be overwritten with other customer data over time."*

Googles sikkerhetstiltak oppfyller, slik kommunen har vurdert det, kommunens krav til sletting.

Datatilsynet legger til grunn kommunens vurdering om at sletting er tilfredsstillende for de opplysninger som i dette tilfellet benyttes i løsningen, og må ses som tilsvarende med hva som ville vært tilfellet for sletting om opplysningene ble behandlet lokalt i kommunen. Det bemerkes imidlertid at den beskrevne praksisen fremstår som svak sammenlignet med hva Art. 29 gruppen har lagt til grunn for sletting. Kommunen bør derfor følge opp at

leverandøren garanterer en maksimal tid før overskriving finner sted, samt forsikre seg om leverandøren har forsvarlige rutiner for avhending av brukte lagringsmedia.

Se også punkt 2 Vedr. Exit-mulighet fra Google Apps

**Kontroll med at leverandøren etterlever avtalene**
Det følger av personopplysningslovens § 14 om internkontroll at den behandlingsansvarlige skal etablere planlagte og systematiske tiltak for å sikre at lovens krav følges. Plikten tilligger den behandlingsansvarlige, og ikke databehandleren. Hvordan personopplysningene skal behandles, hvilke rutiner som skal følges, og hvordan etterlevelse kontrolleres, må derfor reguleres i avtalene mellom den behandlingsansvarlige og databehandleren. Kravet om internkontroll omfatter også andre plikter enn informasjonssikkerhet, som for eksempel at opplysningene ikke behandles til andre formål enn avtalt, plikten til å slette personopplysninger og pliktene knyttet til overføring av personopplysninger til tredjeland.

Som for informasjonssikkerhet fremstår det som naturlig at dette følges opp gjennom bruk av tredjepartsrevisjoner. Etter Datatilsynets syn fremstår det også som nødvendig at databehandlerens etterlevelse av avtalen bekreftes gjennom tredjepartsrevisjoner (med mindre behandlingsansvarlig selv gjennomfører revisjon). Dette for at behandlingsansvarlig skal ivareta kravet om systematiske tiltak for å sikre etterlevelse av loven.

Det vises til foregående beskrivelse av ISAE-revisjoner. Datatilsynet legger denne redegjørelsen til grunn, og følgelig at tredjepartsrevisjoner ikke er begrenset til informasjonssikkerhet, men generelt omfatter databehandlerens etterlevelse av det avtalte.

**Tillegg om Googles Privacy Policy**
Googles nye Privacy Policy (GPP) trådte i kraft 1. mars 2012, og er senere oppdatert 27. juli 2012. Vi understreker at innholdet i GPP ikke er vurdert i denne saken.[19] Etter det vi forstår, vil imidlertid GPP – i alle fall som et utgangspunkt – også gjelde for Google Apps.[20]

Dersom det foreligger motstrid mellom GPP og de individuelle avtalene som ligger til grunn for våre vurderinger i denne saken, forutsetter vi at sistnevnte avtaler går foran. Vi legger til grunn at kommunen forsikrer seg om at dette er tilfellet.

**Konklusjon**
På denne bakgrunn, kan Datatilsynet ikke se at det er grunnlag for å opprettholde det varslede vedtaket. Enkelte forutsetninger er imidlertid lagt til grunn for Datatilsynets vurderinger. Disse er det redegjort for under de enkelte punkter.

Datatilsynet avslutter dermed saken.

---

[19] Den franske Commission Nationale de l'Information et des Libertés (CNIL) er i gang med en analyse av vilkårene i GPP i lys av det felleseuropeiske regelverket (direkitv 95/46/EF), og vil ventelig publisere denne i løpet av høsten 2012.

[20] På www.google.com/policies/privacy refereres det til "*tjenestene våre*" – Google angir med andre ord ingen positiv avgrensning av tjenestene som er omtalt i GPP, og følgelig må det legges til grunn at Google Apps er underlagt GPP.

**Klageadgang**
Ovenstående beslutninger kan påklages i henhold til forvaltningslovens bestemmelser. En eventuell klage må fremsettes overfor Datatilsynet **innen tre uker** etter at vedtaket ble mottatt. Datatilsynet gjør i den forbindelse oppmerksom på retten til innsyn i sakens dokumenter, jf. forvaltningsloven § 18.

Med vennlig hilsen

Helge Veum
avdelingsdirektør

Renate Thoreid
senioringeniør