

Narvik kommune  
Postboks 64  
8501 NARVIK

Deres referanse  
1111/1210-6/PEJA

Vår referanse (bes oppgitt ved svar)  
11/00593-7/SEV

Dato  
16. januar 2012

## **Varsel om vedtak - 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, samt kommunens redegjørelse mottatt 2. september 2011. Saken dreier seg om kommunens eksisterende, og planlagte utvidet, bruk av produktet "Google Apps".

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 kommunens redegjørelse**

### **Punkt 1.**

*En redegjørelse for hvilke personopplysninger kommunen skal behandle i Google Apps.*

### **Regelverkets krav**

Personopplysningsloven § 13 stadfester at den behandlingsansvarlige gjennom planlagte og systematiske tiltak skal sørge for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet og tilgjengelighet 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.

### **Kommunens redegjørelse**

Kommunen stadfester at det er kun e-postløsning som nå er tatt i bruk. Det opplyses imidlertid at virksomheten også vurderer å ta i bruk andre tjenester som tilbys via Google Apps. Kommunen begrunner dette med behov for effektiv intern samhandling gjennom deling av dokumenter, presentasjoner, regneark, skjema eller tegning.

Kommunen oppstiller deretter eksempler på områder hvor det kan være aktuelt å benytte de øvrige verktøyene. Felles for eksemplene er at behandling av personopplysninger, hva gjelder de ansatte, vil avgrenses til navn, telefonnummer, e-postadresse og organisasjonstilhørighet. Kommunen stadfester videre at alle disse opplysningene allerede er publisert på kommunens websider.

### **Datatilsynets vurdering**

Datatilsynet begrenser sin vurdering til det oppgitte anvendelsesområdet: E-post til/fra- og mellom kommunens ansatte.

Kommunen beskriver klarhet i reglementet at ingen sensitive personopplysninger skal sendes med e-post. Mye av arbeidet i kommunen er knyttet til tjenesteyting overfor innbyggerne i kommunen, og det er derfor naturlig at mye av kommunikasjonen til/fra kommunen og mellom kommunens ansatte inneholder personopplysninger. Rent praktisk har kommunen, etter tilsynets vurdering, utfordringer med å forhindre at sensitive personopplysninger blir sendt via e-post, verken til/fra- eller mellom kommunens ansatte. Kommunen kan imidlertid begrense risikoen ved systematisk opplæring og gjentatt kommunikasjon av gjeldende rutiner.

Datatilsynet mener at faren for uautorisert sending av sensitive eller konfidensielle personopplysninger vil gjelde så vel mellom ansatte som forsendelse til og fra publikum. Tilsynet ser imidlertid at dette ikke er en problemstilling som avgrenses til Google Apps. Årsaken til at det likevel trekkes frem er at slike opplysninger med foreskrevet løsning vil behandles i systemer som ikke er under behandlingsansvarliges direkte kontroll. Uautoriserte forsendelser (for eksempel e-post som inneholder sensitive personopplysninger) vil ligge på databehandlerens servere i lang tid, etter hva tilsynet erfarer også en tid etter at brukeren aktivt har slettet meldinger. Dette skyldes blant annet replikering av innhold.

Kommunen trekker frem en analogi til postens distribusjonssystem når det gjelder publikum sin mulighet til å vurdere sikkerhetsnivået i kommunikasjonen mellom kommunen og publikum uavhengig om dette er e-post eller post. Datatilsynet slutter seg ikke til et slikt resonnement. Sikkerhetsnivå og organisering av postens distribusjonssystem er underlagt streng regulering gjennom postloven med tilhørende forskrift. Brev med beskyttelsesverdig innhold blir formidlet i lukkede konvolutter, i nødvendige tilfeller også som rekommandert sending. Sikkerhetsnivået for ukryptert e-post er derimot basert på en standardisert protokoll kalt "Simple Mail Transfer Protocol (SMTP)". Denne protokollen tilfører i praksis ingen beskyttelse av innholdet i forsendelsen.

### **Datatilsynets konklusjon**

Kommunen kan ikke utelukke at det vil bli behandlet sensitive personopplysninger i løsningen, og må derfor ta høyde for at det i systemet vil bli behandlet både sensitive personopplysninger og personopplysninger generelt. Datatilsynet kan ikke se at kommunen har gjennomført tilstrekkelige tiltak, jf personopplysningsforskriftens § 2-11, med hensyn til at det i løsningen vil bli behandlet konfidensielle opplysninger.

Dette må kommunen ta hensyn til ved en vurdering av informasjonssikkerheten, jf drøftelsen i punktene nedenfor.

### **Punkt 2.**

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

### **Regelverkets krav**

Personopplysningsloven § 13 stadfester at den behandlingsansvarlige gjennom planlagte og systematiske tiltak skal sørge for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet og tilgjengelighet ved behandling av personopplysninger. Personopplysningsforskriften § 2-4 annet ledd stadfester at den behandlingsansvarlige skal gjennomføre risikovurdering for å klarlegge sannsynligheten for og konsekvenser av sikkerhetsbrudd.

### **Kommunens redegjørelse**

Kommunen redegjør for at det er gjennomført en helhetlig risikoanalyse når det gjelder innføring av nytt IKT-system. Analysen var vedlagt kommunens brev. Ifølge analysen vil bruken av Google Apps i de fleste tilfeller gi et tilsvarende risikobilde som kommunens gamle løsning – med noen unntak.

Kommunen skisserer at eksisterende utfordring med plassmangel og tilgang til teknologiresurser utgjorde en viktig faktor i valg av løsning. Kommunen peker videre på at risikoen for at eksisterende organisasjon ikke klarer å skaffe og vedlikeholde spesialkompetanse til drift av nok et spesialisert IT-system. Kommunen redegjør for at det av hensyn til plassmangel ikke er ønskelig å belaste kommunens datasentral ytterligere.

Kommunen redegjør videre for at man skal legge til et nytt IT-system. Enkelte av systemene kommunen bruker i dag er funnet formålstjenelig å bytte ut med en løsning som krever mindre driftsressurser. Slik Datatilsynet forstår det skal kommunen fullstendig avvikle bruken av gammel løsning for så å gå over til ny. I en slik migrering vil det være naturlig at det blir frigjort maskinpark og fysisk plass.

Kommunen redegjør for at man legger til grunn at Google Apps sin løsning er tilstrekkelig med tanke på tilgjengelighet, integritet og sikkerhet. Likevel erkjenner kommunen at *”det er verdt å merke seg at det i flere tilfeller ikke kan beskrives noen sannsynlighet/hyppighet da det ikke forefinnes noe anvendbart referansemateriale for denne type hendelser.”*

Kommunen redegjør også for hvordan den skal kunne revidere sin databehandler. Dette skal skje ved at et 3. parts firma, som databehandleren engasjerer, reviderer basert på standarden ISAE3402 og tilgjengliggjør sine funn i en revisjonsrapport. Kommunen skal få tilgang til denne og vil kunne ta opp tema i kommunens informasjonssikkerhetsutvalg.

### **Datatilsynets vurdering**

Kommunen velger på tross av manglende underlag å sette verdier for å definere sannsynligheten i sin risikovurdering. Tilsynet merker seg at det i analysen stadfestes at det er svært liten sannsynlighet for datainnbrudd, svikt i kontinuitet og manglende monitorering i Google Apps sin løsning – som nevnt uten å ha anvendbare referansemateriale. Datatilsynet mener at usikkerheten knyttet til sannsynligheten burde komme vesentlig mer til uttrykk i analysen.

Når det gjelder svikt i kontinuitet kan kommunen ikke utelukkende vurdere oppetid hos databehandler, men må også forholde seg til oppetid i infrastrukturen fra kommunens nett til databehandleren.

For Datatilsynet er det uklart hvordan kommunen gjennom ovennevnte revisjonsrapporter skal kunne endre på hvordan databehandleren behandler deres data. For tilsynet fremstår det som om kommunen kun kan endre på hvordan de selv bruker løsningen, og i mindre grad utformingen av løsningen i seg selv. Det siste synspunktet er basert på observasjoner tilsynet har generelt med avtaler mellom virksomheter.

En revisjonsrapport, basert på standarden ISAE3402, er forøvrig normalt en bekreftelse eller avkreftelse om at virksomheten etterlever en gitt standard, egne regler, eget sikkerhetsregime og eventuelle sertifiseringer løsningen skal ha. Slike rapporter vil dermed i mindre grad gi svar på om kommunens standard hva gjelder sikkerhetstiltak er oppfylt.

Kommunen kan selvsagt velge en annen leverandør hvis resultatene i revisjonsrapporten ikke er tilfredsstillende, men det må altså antas at det vil være utfordrende å få til direkte endringer hos eksisterende leverandør. Datatilsynet er kjent med at et skifte av leverandør kan by på store utfordringer med tanke på innlåsingseffekt. Dette kan for eksempel være kontraktstid og merarbeid i migreringsprosess. I beste fall må kommunen verifisere at dette rent praktisk lar seg gjøre om en tvist skulle oppstå.

### **Datatilsynets konklusjon**

Datatilsynet kan ikke se at risikovurderingen gir et fullstendig bilde av hvilke risikoer som er forbundet med løsningen kommunen har valgt. En slik risikovurdering som kommunen har foretatt i dette tilfellet, er ikke tilstrekkelig i henhold til personopplysningsforskriftens § 2-4.

### **Punkt 3 og 4.**

*Kopi av databehandleavtalen kommunen eventuelt har inngått med Google, herunder:*

- *Oversikt over hvilke sikkerhetstiltak Google har i løsningen kommunen har valgt å benytte.*
- *En beskrivelse av informasjonssystemets utforming og fysiske plassering.*

### **Regelverkets krav**

#### Databehandleravtale

Personopplysningsloven § 15 stadfester at en databehandler ikke kan behandle personopplysninger på annen måte enn det som er skriftlig avtalt med den behandlingsansvarlige. Opplysningene kan heller ikke uten en 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.

#### Informasjonssystemets utforming og sikkerhetstiltak

Personopplysningsloven § 13 første ledd stadfester at den behandlingsansvarlige gjennom planlagte og systematiske tiltak skal sørge for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet og tilgjengelighet ved behandling av personopplysninger.

Personopplysningsloven § 13 tredje ledd stadfester at en behandlingsansvarlig som lar andre få tilgang til personopplysninger, for eksempel en databehandler eller andre som utfører oppdrag i tilknytning til informasjonssystemet, skal påse at disse oppfyller kravene i første og annet ledd.

#### Fysiske plassering

Personopplysningsloven § 29 stadfester at personopplysninger bare kan overføres til stater som sikrer en forsvarlig behandling av opplysningene. Stater som har gjennomført direktivet 95/46/EF om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger, oppfyller kravet til forsvarlig behandling.

### **Kommunens redegjørelse**

Kommunen har ikke inngått gjensidig avtale med Google om leveranse av løsning for e-post, men har gjennom systemintegrator Avalon Information Systems AB blitt referert til Googles dokument for beskrivelse av tjenestenivå og kundestøtte. Kommunen beskriver at siden løsningen er basert på Cloud-computing fordrer dette ikke ekstra avtale om support fra leverandør, ut over de tjenestenivåene som er listet i standardavtalen fra Google.

Kommunen redegjør for hvilke sikkerhetstiltak Google har beskrevet i ”Security Whitepaper: Google Apps Messaging and Collaboration Products”. Datatilsynet har i andre sammenhenger

erfart at slike dokumenter ofte er gjenstand for justering fra leverandørens side uten forhandling. Kommunen vil i så fall enten måtte forhold seg til endringer eller velge bort leverandøren.

Kommunen viser til sikkerhetsmekanismer som Google beskriver i sitt Whitepaper. I dette omtales en rekke sikkerhetsmessige tilpasninger og muligheter den behandlingsansvarlige kan iverksette gjennom løsningen. Kommunen har ikke beskrevet om de har valgt noen av disse tilpasningene og mulighetene.

Kommunen mener at leverandørens "Whitepaper", Googles tilslutning til Safe Harbor avtalen, samt at kommunen har tilgang til revisjonsrapportene, burde være tilstrekkelig for å tilfredsstille myndighetenes krav om databehandleravtale. Kommunen beskriver at Google ikke ønsker av sikkerhetsmessige årsaker å frigi detaljer rundt leverandørens datasentre. Google ønsker heller ikke å offentliggjøre tekniske detaljer som kan være kompromitterende for sikkerheten.

### **Datatilsynets vurdering**

Datatilsynet har på sine internettsider laget et forslag til databehandleravtale som inneholder de punktene tilsynet mener som et minimum bør inngå i en databehandleravtale. Disse punktene er: Avtalens hensikt, formål, databehandlers plikter, bruk av underleverandør, sikkerhet, sikkerhetsrevisjoner, avtalens varighet, ved opphør, meddelelser, samt lovvalg og verneting.

Når databehandleren ikke ønsker å frigi opplysninger om i hvilke land deres datasentre er plassert, skaper dette utfordringer med hensyn til kravene til en databehandleravtale, jf personopplysningslovens §§ 15 og 29. Kommunen vil ikke i avtalen kunne klargjøre sikkerhetsnivået i løsningen på en tilstrekkelig måte, uten å kunne vite at stater opplysninger overføres til har et tilstrekkelig vern for personopplysninger.

Stater som har gjennomført direktivet 95/46/EF "Om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger", oppfylder kravet til forsvarlig behandling. Google er et amerikansk selskap og det er derfor mulig at opplysninger som behandles i kommunens e-postløsning vil blant annet lagres i USA. Enn så lenge står ikke USA på listen over land som kommisjonen har anerkjent at sørger for tilstrekkelig personopplysningsvern.

For å bøte på dette ble Safe Harbor ordningen etablert i år 2000. Ordningen innebærer at amerikanske selskaper vil kunne anses å tilby tilstrekkelig vern for personopplysninger som de mottar fra EU/EØS, ved at de frivillig implementerer et sett regler for behandling av opplysningene. Etter at Safe Harbor ble etablert har USA innført loven "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act", forkortet USA Patriot Act, som en følge av terrorangrepet 11. september 2001. Loven er svært komplisert og omfattende. Denne loven gir amerikanske myndigheter mulighet til å overvåke terrormistenkte uten siktelse eller rettergang.

Tilsynet ønsker i denne sammenhengen å påpeke at USA Patriot Act må anses å være en utfordring med hensyn til ivaretagelse av personvernet, også innenfor Safe Harbor-ordningen.

### **Datatilsynets konklusjon**

Datatilsynet kan på bakgrunn av det ovennevnte ikke se at standardavtalen til Google er tilstrekkelig i forhold til hva som forventes av en databehandleravtale, jf personopplysningsloven § 15. Etter tilsynets vurdering vil manglende databehandleravtale være et avvik i forhold til kravene i personopplysningsloven § 15.

Datatilsynet kan ikke se at kommunen har anledning til å benytte en databehandler som bl.a. ikke oppgir hvilket land opplysningene vil bli behandlet i og som en konsekvens av det ikke tilstrekkelig redegjørelse for sikkerhetstiltak, jf personopplysningsloven § 29.

### **Punkt 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.*

### **Regelverkets krav**

Personopplysningsforskriften § 2-12 fjerde ledd stadfester at personopplysninger og annen informasjon som er nødvendig for gjenoppretting av normal bruk, skal sikkerhetskopieres. Personopplysningsforskriften § 2-8 stadfester at medarbeidere hos den behandlingsansvarlige bare skal bruke informasjonssystemet til å utføre pålagte oppgaver, og selv være autorisert for slik bruk. Medarbeiderne skal ha nødvendig kunnskap for å bruke informasjonssystemet i samsvar med de rutiner som er fastlagt. Personopplysningsforskriften § 2-5 stadfester at sikkerhetsrevisjon av bruk av informasjonssystemet skal gjennomføres jevnlig. Sikkerhetsrevisjonen skal omfatte vurdering av organisering, sikkerhetstiltak og bruk av kommunikasjonspartner og leverandører. Dersom sikkerhetsrevisjonen avdekker bruk av informasjonssystemet som ikke er forutsatt, skal dette behandles som avvik, jf § 2-6.

### **Kommunens redegjørelse**

Kommunen viser til Googles Whitepaper, der det står at dataene blir lagret på flere systemer på samme datasenter og replikeres samtidig til et sekundært datasenter. Det er ingen beskrivelse av hvordan Google har konstruert deres sikkerhetskopieringssystem, bortsett fra at det forutsettes at det aldri skal mistes noen data. Når det gjelder avhending beskriver Whitepaper hvordan filen vil bli avindeksert og etter hvert skrevet over av andre data.

Google beskriver heller ikke hvem som har tilgang til kommunens opplysninger, men at disse er underlagt Googles system for autorisasjon og tilgangskontroll. Det beskrives ikke hvor mange personer dette utgjør eller avgrenses konkret til stillingstype eller behov for tilgang. Sikkerhetsrevisjon er besvart under spørsmål 2.

### **Datatilsynets vurdering og konklusjon**

Kommunen har lagt til grunn Googles beskrivelse av løsningen. Datatilsynet kan ikke se at kommunen har noen påvirkningsmulighet på hvordan denne er satt i sammen. På bakgrunn av dette kan ikke Datatilsynet se at kommunen har godtgjort at vilkårene i personopplysningsforskriftens kapittel 2 er oppfylt.

### **Andre forhold**

I vedlegget "Risiko- og sårbarhetsanalyse for innføring av nytt e-postsystem i Narvik kommune – Google Apps" (analysedokument) side 11, 13 og 15 står det at Google nylig har innført en tilleggsfunksjon som kan aktiveres av kommunen for å avslå forsendelse av e-post som inneholder ord eller uttrykk som kan tyde på sensitivt eller uakseptabelt innhold i henhold til gjeldende retningslinjer. Datatilsynet kan ikke se at innføringen av en slik tilleggsfunksjon alene vil løse ovennevnte utfordringer. Det er mulig at en slik løsning, avhengig av hvordan den praktiseres, kan være problematisk sett i sammenheng med personopplysningsforskriften kapittel 9.

På side 13 i analysedokumentet står det at det kan legges på et ytterligere lag med sikkerhet ved at den enkelte ansatte som sender e-post må bekrefte at e-posten ikke inneholder sensitive personopplysninger ved å skrive teksten "Inneholder ikke sensitive personopplysninger" i meldingen. Datatilsynet mener at det ikke nødvendigvis er slik at denne rutinen i realiteten tilfører et ekstra lag med sikkerhet. Vi ser at dette kan bli automatisert av brukerne for å få sendt e-poster. Dermed er dette et tiltak som lett lar seg gjøre å omgå, og som kun i liten grad er egnet til å forhindre uønsket adferd.

### **Segmentering av ulike behandlingsansvarlige**

En databehandler kan ikke behandle personopplysninger på vegne av en behandlingsansvarlig uten at det er inngått en databehandleravtale, jf personopplysningslovens § 15. Det betyr i praksis, at dersom man behandler personopplysninger på vegne av flere behandlingsansvarlige, må databehandler behandle personopplysningene for hver enkelt behandlingsansvarlig tilstrekkelig separat.

Google har i sine dokumenter ikke redegjort for hvordan dette er tilstrekkelig håndtert i løsningen. Det er dog beskrevet at totalsystemet skal sikre at den behandlingsansvarliges data ikke skal være mulig å kunne ta ut fra en lokasjon. Dette kan innebære en sammenblanding av informasjon tilhørende forskjellige behandlingsansvarlige. Nivået for informasjonssikkerhet er felles for alle behandlingsansvarlige, basert på retningslinjer fastsatt av databehandleren. En slik praksis kan komme i konflikt med rollen til Google som databehandler for ulike aktører, som kan ha ulike krav til sikkerhet. Problemet med slik sekvensiell lagring aktualiseres videre ved behov for å slette informasjon fra løsningen. Dette må gjøres etter de retningslinjer som forskjellige behandlingsansvarlige fastsetter.

Videre aktualiseres problemstillingen ved spørsmål om sletting i sikkerhetskopier, jf personopplysningslovens § 28 om sletting. Ved en sekvensiell database vil man måtte gå igjennom hver eneste post i databasen for å vurdere om den skal slettes, i motsetning til en segmentert database for hver enkelt databehandlers data hvor man kan gå inn og slette elementer som ikke lenger er relevante. Dette kan gjøres i form av segmentering av databasen.

En slik løsning innebærer at data fra ulike behandlingsansvarlige ikke "blandes sammen" i en stor base, men holdes tilstrekkelig atskilt. En segmentering vil være nødvendig for all aktivitet som kan tilskrives en behandlingsansvarlig. Dette omfatter også kopi av kommunisert innhold, logger og liknende.

### **Datatilsynets konklusjon**

Kommunen må i henhold til regelverket implementere en tilfredsstillende logisk eller fysisk segmentering av informasjonssystemet slik at krav til tilfredsstillende informasjonssikkerhet og ulike behov mht. sletting mellom ulike behandlingsansvarlige, kan ivaretas, jf personopplysningslovens §§ 13 og 15.

### **Oppsummering**

Ut fra det ovennevnte kan ikke Datatilsynet se at kommunen i tilstrekkelig grad har forsikret seg om at bruken av Google Apps er i tråd med personopplysningsloven. Dette gjelder særlig inngåelse av en gyldig databehandleravtale i henhold til personopplysningslovens § 15, krav med hensyn til overføring av personopplysninger til utlandet, jf lovens § 29 og ivaretagelse av kravene til informasjonssikkerhet i henhold til personopplysningslovens § 13.

Med bakgrunn i tilsynets konklusjon varsles det vedtak mot kommunen. Det vises til påfølgende avsnitt.

### **Varsel om vedtak**

Dette er et varsel om at Datatilsynet, med hjemmel i personopplysningslovens § 46, vil fatte vedtak om følgende pålegg:

1. *Narvik Kommunes bruk av Google Apps må bringes til opphør, med mindre behandlingen av personopplysninger i løsningen kan bringes i tråd med personopplysningslovens krav, jf personopplysningslovens §§ 13, 15 og 29.*

### **Frist for tilsvar**

Eventuelle merknader til foreliggende varsel bes sendt Datatilsynet snarest, og senest **innen 1.mars 2012**. Det anbefales at virksomheten oversender Datatilsynet et forslag til fremdriftsplan for lukking av de avvik som er beskrevet i kontrollrapporten. Datatilsynet vil se hen til denne fremdriftsplanen når det skal beslutte en frist for virksomhetens gjennomføring av vedtaket.

Datatilsynet vil likevel ikke fatte vedtak som her nevnt dersom virksomheten innen samme frist dokumenterer at de avvikene som er beskrevet i kontrollrapporten er lukket.

Med hilsen

Bjørn Erik Thon  
direktør

Stein Erik Vetland  
overingeniør

