STORTINGET

Datatilsynet
Postboks 458 Sentrum
0105 Oslo

Vår ref.:	Deres ref.:	Dato:
2020/3038-11	20/03500-8	14.02.2022

Svar på varsel om vedtak

1. Innledning

Det vises til brev fra Datatilsynet datert 13. januar 2022, mottatt her 17. januar 2022, med varsel om at tilsynet vurderer å fatte vedtak om overtredelsesgebyr grunnet overtredelse av personvernforordningen (GDPR) art. 32 nr. 1 bokstav b og d. Datatilsynet har satt frist for tilsvar til forhåndsvarselet til 14. februar 2022.

Stortingets administrasjon ønsker med dette å inngi tilsvar, slik at Datatilsynet får et mest mulig fyllestgjørende grunnlag for å treffe sitt endelige vedtak. Punkt 2 angir enkelte faktiske forhold av sentral betydning for vurderingen av ivaretakelsen av informasjonssikkerheten ved dataangrepet. I punkt 3 har vi knyttet noen kommentarer til de rettslige vurderingstemaene i saken.

Stortingets administrasjon er opptatt av at Datatilsynet får all nødvendig informasjon i saken før endelig vedtak treffes. Ut over redegjørelsen i brevet her viser vi særlig til de to avviksmeldingene som ble sendt Datatilsynet umiddelbart etter dataangrepet, henholdsvis 6. september og 9. oktober 2020, og den mer utførlige redegjørelsen datert 8. desember 2020.

Enkelte opplysninger om dataangrepet og hvilke tekniske sikkerhetstiltak Stortinget har implementert er av stor sikkerhetsmessig betydning for Stortinget å unnta offentlighet. Det er derfor enkelte forhold vi ikke har omtalt i detalj. Av samme grunn har vi heller ikke lagt noen dokumenter ved som vedlegg til brevet her. Alle opplysninger og dokumenter som det henvises til, kan selvsagt formidles til Datatilsynet om ønskelig. Vi står for øvrig til disposisjon dersom Datatilsynet skulle ha spørsmål til tilsvaret eller vil etterspørre ytterligere dokumentasjon. Om ønskelig kan vi gjerne sette opp møter med relevante personer for muntlig gjennomgang av temaer som ønskes utdypet.

2. Faktiske forhold av betydning for Datatilsynets vurdering

2.1 Innledning

Datatilsynet har i varselet om vedtak om overtredelsesgebyr knyttet til dataangrepet i 2020 tatt utgangspunkt i at Stortingets administrasjon ikke hadde «*gjennomført egnede tekniske og organisatoriske tiltak, herunder tofaktorautentisering, for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen for å oppnå vedvarende konfidensialitet, integritet og robusthet, jf. GDRP art. 32 nr. 1 bokstav b) og d), jf. art. 5 nr. 1 bokstav f)*», jf. forhåndsvarselet punkt 2.

Datatilsynet har i forhåndsvarselet lagt betydelig vekt på administrasjonens angivelige manglende oppfølgning av sårbarheter som ble identifisert i en risiko- og sårbarhetsanalyse gjennomført fra november 2019 til april 2020 (heretter ROS2020). Det heter i Datatilsynets oppsummering i forhåndsvarselet punkt 8:

«*Etter Datatilsynets vurdering, er saken prinsipielt viktig. Datatilsynet anser det som svært alvorlig at Stortingets administrasjon har vist manglende evne til å iverksette nødvendige sikkerhetstiltak som administrasjonen selv har identifisert behovet for i kartleggingen av risikoen ved behandling av personopplysninger. Vi presiserer at personvernforordningen stiller krav om at resultatet fra slike kartlegginger skal følges opp med egnede tiltak, og at det er nettopp dette som er formålet med å gjennomføre risikovurderinger, jf. personvernforordningen artikkel 32 nr. 1 bokstav b. Hendelsen som utløste meldingen til Datatilsynet og som danner grunnlag for dette varselet, kunne og burde ha vært unngått dersom Stortinget hadde iverksatt tiltak for å avhjelpe de sårbarhetene som ble gjort kjent gjennom risikovurderingen.*»

Også flere andre steder i forhåndsvarselet er det vist til og lagt vekt på forhold identifisert i ROS2020, og administrasjonens angivelige manglende oppfølgning av disse. Vi har derfor i dette tilsvaret fokusert på vår oppfølgning av denne risiko- og sårbarhetsanalysen.

I forhåndsvarselet er det særlig vist til at Stortinget ikke hadde innført tofaktorautentisering for brukere av deres e-postsystemer på tidspunktet for sikkerhetsbruddet i september 2020, noe som i ROS2020 var identifisert som «høy risiko» for tilgang for uautoriserte. Datatilsynet gir i forhåndsvarselet uttrykk for at implementering av dette tiltaket tok uforholdsmessig lang tid.

Det er i varselet videre vist til at manglende sikkerhetskultur i ROS2020 ble identifisert som «høy risiko» for uautorisert tilgang til Stortingets systemer. Risikoen er bl.a. forklart med at det er utfordrende at ulike brukergrupper ikke er underlagt instruksjonsmyndighet fra Stortingets administrasjon.

ROS2020 avdekket etter Datatilsynets syn også sårbarheter som kunne ha vært kompensert med andre organisatoriske tiltak. Eksempel på slike tiltak er kartlegging av de ansattes kunnskap om informasjonssikkerhet og personvern, og målrettet opplæring. Som organisatoriske tiltak vil retningslinjer og rutiner for bruk av virksomhetens e-postkonto kunne være effektive og nødvendige for å redusere risikoen de menneskelige faktorene utgjør.

Samlet sett finner Datatilsynet det klart at dersom nødvendige tekniske og organisatoriske sikkerhetstiltak hadde blitt gjennomført på et tidligere tidspunkt, så ville Stortingets infrastruktur vært mer robust. Dataangrepet kunne dermed ha vært unngått.

Stortingets administrasjon ser med stort alvor på hendelsen med dataangrepet i 2020. Arbeid med sikkerhet er og har vært et prioritert område for administrasjonen. Samtidig erkjenner vi at IT-sikkerheten kunne vært bedre da angrepet inntraff.

I det følgende vil vi først redegjøre for hvilket handlingsrom administrasjonen hadde fra avlevering av ROS2020 til dataangrepet fant sted, se punkt 2.2. Detter vil vi i punkt 2.3 vise hvordan sårbarhetene som ble avdekket i ROS2020 rent faktisk ble fulgt opp, før vi i punkt 2.4 gjennomgår forhold særskilt knyttet til tofaktorautentisering. Endelig vil vi i punkt 2.5 si noe om hvilke andre tekniske og organisatoriske sikkerhetstiltak administrasjonen hadde implementert før dataangrepet.

2.2 Stortingets administrasjons handlingsrom fra avlevering av ROS2020 til dataangrepet fant sted

Datatilsynet har i varselet lagt til grunn at ROS2020 ble avlevert til Stortinget i mars 2020, og at sikkerhetsbruddet skjedde i september 2020. Datatilsynet fremhever at raskere oppfølging av sårbarheter avdekket i ROS2020, herunder manglende tofaktorautentisering, kunne ha forebygget dataangrepet.

Stortingets administrasjon slutter seg til Datatilsynets utgangspunkt om at ROS2020 er av sentral betydning når Stortingets arbeid med informasjonssikkerhet i 2020 skal vurderes. Vi er i utgangspunktet også enig i at en etablert løsning med tofaktorautentisering for e-postsystemet kunne ha bidratt til å forebygge det dataangrepet som fant sted. Det er imidlertid enkelte mangler i Datatilsynets gjengivelse av faktum knyttet til ROS2020, hvilke tiltak som ble anbefalt der og administrasjonens oppfølgning av disse. Vi vil også presisere at administrasjonen hadde implementert og var i ferd med å iverksette flere andre tekniske og organisatoriske tiltak med sikte på økt informasjonssikkerhet.

Vi vil også gjøre oppmerksom på at oppfølgingen av ROS2020 må ses i lys av at Stortingets administrasjon våren 2020 var sterkt preget av pandemien og nedstengningen som traff landet i begynnelsen av mars 2020. Den ekstraordinære situasjonen som oppstod medførte at både IT-avdelingen og andre deler av administrasjonen måtte bruke store ressurser på å sikre at nasjonalforsamlingen fortsatt kunne fungere og fylle sine samfunnskritiske funksjoner.

Som en overordnet illustrasjon av situasjonen våren 2020 og oppfølgningen av ROS2020 har vi nedenfor oppstilt en tidslinje med oversikt over relevante begivenheter og tiltak. Flere av punktene i tidslinjen er utdypet i det etterfølgende.

- ***November 2019:*** Oppstart av ROS2020, ledet av ekstern aktør med spesialkompetanse (Sopra Steria).

- ***12. mars 2020:*** Pandemien medfører full nedstengning av Norge, inkludert Stortinget og Stortingets administrasjon. Det oppstår et ekstraordinært behov for tilpassede IT-tjenester for å understøtte den parlamentariske kjernevirksomheten.

- ***22. april 2020:*** ROS2020 ferdigstilles og avleveres Stortingets administrasjon. Rapporten omfatter 59 risikoscenarier og identifiserer 146 tiltak innen fire hovedområder: Mobile enheter, nettverk, PKU og Fellesperson. Den gir en klar anbefaling om at administrasjonen først må analysere, strukturere og prioritere tiltakene før iverksettelse og gjennomføring. Dette planleggingsarbeidet påbegynnes umiddelbart. Dette krever interaksjon mellom flere deler av administrasjonen, og tar samlet sett omtrent to måneder å ferdigstille.

- ***Mai-juni 2020:*** Prioriteringene i Stortingets administrasjon er fortsatt preget av å sikre den parlamentariske kjernevirksomheten under pandemien. Avslutningen av vårsesjonen, med en betydelig mengde pandemi-relaterte saker, er svært krevende å håndtere. Arbeidet med ROS2020 fortsetter likevel, herunder iverksettelsen av enkelte tiltak som for eksempel beskyttelse mot DDoS-angrep (tjenestenektangrep).

- ***24. juni 2020:*** Ledergruppen i administrasjonens IT-avdeling får fremlagt status og rapport om tiltak og risiko fra ROS2020, samt kategorisering og prioriteringer av arbeid for å iverksette ytterligere tiltak. Ledergruppen støtter prioriteringene som legges frem, herunder fortsettelse av arbeidet med å innføre multifaktorautentisering på alle tjenester der det er mulig.

- ***Juli til medio august 2020:*** Ferieavvikling i perioden Stortinget ikke er samlet. Begrenset aktivitet i prosjekter og tiltak som krever koordinering på tvers av enheter i administrasjonen.

- ***21. august 2020:*** Dataangrepet mot Stortinget starter.

- ***24. august 2020*****:** Dataangrepet stanses.

- ***2. september 2020:*** Administrasjonen får bekreftet at personopplysninger kan ha kommet på avveie. Stortingets sikkerhetssjef varsler samme dag Datatilsynet telefonisk om angrepet. Skriftlig varsel oversendes fire dager senere.

- ***3. september 2020:*** Intervjuer med rammede enkeltpersoner påbegynnes, med sikte på skadevurdering og deres mulighet for ivaretakelse av egne interesser.

- ***3. september 2020:*** Prosjekt for implementering av tofaktorautentisering for e-postsystemet iverksettes. Det jobbes også med å implementere andre tiltak fra ROS2020.

Fra administrasjonen fikk avlevert ROS2020 til angrepet fant sted, gikk det altså fire måneder. Vi gjør oppmerksom på at avleveringen av ROS2020 skjedde 22. april 2020, og ikke i mars 2020, slik Datatilsynet har lagt til grunn i sitt varsel. Arbeidet med oppfølgning av rapporten ble påbegynt straks, og ved inngangen til sommerferien var det gjort et betydelig arbeid med vurdering og prioritering av anbefalte tiltak. Arbeidet med prioriterte tiltak skulle gjenopptas etter ferieavviklingen i august. Kort tid etter dette skjedde dataangrepet.

Som nevnt sto Stortingets administrasjon i denne perioden også overfor ekstraordinære utfordringer knyttet til håndtering av koronapandemien. Da ROS2020 ble avlevert 22. april 2020, var administrasjonen, herunder IT-avdelingen og sikkerhetsstaben, svært opptatt med å gjennomføre ulike tiltak for å sikre at Stortinget kunne utføre sine samfunnskritiske oppgaver under nye og stadig skiftende omstendigheter. Den 6. mars 2020 ble det iverksatt arbeid med kontinuitetsplaner, med formål å sikre den parlamentariske virksomheten. På kort varsel ble en rekke digitale løsninger implementert, slik at Stortinget og komiteene kunne fungere på tross av smittesituasjonen og nedstengningen av samfunnet. Dette var helt kritisk for at Stortinget kunne fortsette sitt arbeid blant annet med nødvendig lovgivning og økonomiske støtteordninger knyttet til pandemien. Andre oppgaver, som oppfølging av ROS2020, kunne derfor ikke prioriteres tilsvarende.

For å illustrere betydningen av det arbeidet som ble gjort våren 2020, vil vi vise til Koronakommisjonens rapport (NOU 2021:6), der kommisjonen skriver i punkt 20.2:

> «I en slik krisesituasjon som Norge har opplevd med koronapandemien, er det utvilsomt at behovet for hurtig behandling av lovendringer er mer framtredende enn i en normalsituasjon. (…) For å imøtekomme de behovene som håndteringen av covid-19 krevde, var det nødvendig å finne løsninger for det konstitusjonelle samarbeidet som både ivaretok behovet for hurtig saksbehandling og samtidig sikret at grunnleggende demokratiske og rettssikkerhetsmessige prinsipper ble respektert».

Kommisjonen skriver videre i sin oppsummering i punkt 20.3:

> «Det er kommisjonens vurdering at Stortinget organiserte seg på en god måte under håndteringen av koronapandemien våren 2020. Tiltakene som ble iverksatt fremstår som adekvate og effektive, og gjorde at Stortinget ivaretok og opprettholdt sin konstitusjonelle oppgave som lovgivende makt på en god måte.»

2.3 Oppfølgningen av sårbarhetene som ble avdekket i ROS2020

Som nevnt i punkt 2.1 ovenfor, uttaler Datatilsynet i sin oppsummering i punkt 8 i forhåndsvarselet at dataangrepet «… *kunne og burde ha vært unngått dersom Stortinget hadde iverksatt tiltak for å avhjelpe de sårbarhetene som ble gjort kjent gjennom risikovurderingen*».

Etter administrasjonens oppfatning ble de sårbarhetene som ble avdekket i ROS2020 i stor utstrekning fulgt opp på de premisser som ROS2020 selv anga. Avleveringen av ROS2020 den 22. april 2020 innebar ikke at foreslåtte tiltak med enkelhet kunne settes i verk umiddelbart. Tvert imot ble det i ROS2020 påpekt at mange av de foreslåtte tiltakene krevde *ytterligere analyse* før de kunne gjennomføres. Dette fordi ROS2020 bygde på en forutsetning om at alle tiltak måtte vurderes og analyseres, blant annet opp mot hvor raskt og effektivt tiltaket kunne iverksettes, kostnader, eksisterende infrastruktur og mulige tilgjengelige løsninger.

Som nevnt ble det i ROS2020 identifisert til sammen 59 ulike risikoscenarioer, presentert i 146 ulike forslag til tiltak. 39 av disse gjaldt mobile enheter. For 9 av 59 risikoscenarioer ble risikoen ansett som «svært høy», og for 34 som «høy». Analysen inneholdt fem hovedanbefalinger, som gikk på tvers av de fire områdene som ble vurdert (mobile enheter, nettverk, parti-, komité- og utredningsportalen (PKU), og systemet Fellesperson).

I perioden fra 22. april 2020 og frem mot sommeren gjennomførte derfor Stortingets administrasjon et grundig arbeid med videre analyse og prioritering av de 146 forslagene til tiltak. Med rådgivning fra leverandøren av ROS2020, Sopra Steria, ble tiltakene strukturert og prioritert. Dette ledet frem til en anbefaling om 25 tiltak som ivaretok de fem hovedanbefalingene. Resultatet fra prioriteringsarbeidet ble presentert for ledelsen i administrasjonens IT-avdeling i et møte 24. juni 2020. Tofaktorautentisering var da ett av flere tiltak som ble besluttet prioritert. Andre og enkle tiltak var allerede blitt iverksatt. Tofaktorautentisering på mobile enheter var imidlertid et mer komplekst og krevende tiltak, som det ikke var mulig å gjennomføre raskt og med enkle grep. Dette kommer vi tilbake til nedenfor.

I Datatilsynets varsel heter det videre at «*Vi har også notert oss at manglende sikkerhetskultur ble identifisert som 'høy risiko' for uautorisert tilgang til Stortingets systemer i ROS analysen*», jf. varselet punkt 5. Den høye risikoen som det ble vist til i ROS2020, var imidlertid ikke knyttet til manglende sikkerhetskultur generelt. Det som ble påpekt i ROS2020 var en konkret og avgrenset risiko knyttet til forvaltningen av «Fellesperson», som er Stortingets system for å håndtere brukere og kontaktinformasjon. Arbeidet med tiltak etter ROS2020 har for øvrig adressert denne

sårbarheten, bl.a. gjennom bedre opplæring av administrasjonen og informasjon til de registrerte.

Administrasjonen tilføyer at de fleste anbefalte tiltak fra ROS2020 var iverksatt i juni 2021. I forbindelse med oppfølgingen av den siste risiko- og sårbarhetsanalysen, som ble ferdigstilt 30. november 2021 (ROS2021), skal det – ved siden av andre og nye tiltak – gjennomføres en større evaluering av tiltakene fra ROS2020.

2.4 Særlig om tofaktorautentisering

2.4.1 Innledning

I varselet fra Datatilsynet er det som nevnt fremholdt at Stortinget ikke hadde «*innført tofaktorautentisering for brukere av deres e-post systemer på tidspunktet for sikkerhetsbruddet*». Det fremgår videre at Datatilsynet mener at Stortinget på bakgrunn av ROS2020 burde ha implementert tofaktorautentisering for e-postsystemer før angrepet i august 2020, og at det ble brukt «*uforholdsmessig lang tid*» på implementeringen.

Vi vil presisere at det var implementert tofaktorautentisering for deler av Stortingets informasjonssystemer, inkludert deler av e-postsystemet (se oversikten nedenfor). Tofaktorautentisering hadde også tidligere vært vurdert for e-post på mobile klienter, men blant annet på grunn av ustabilitet i valgt løsning og utfordringer for viktige brukergrupper ble dette ikke prioritert – foran andre tiltak som ble gjennomført – før ROS2020 identifiserte multifaktorautentisering som anbefalt tiltak for mobile enheter. Denne anbefalingen ble fulgt i det videre arbeidet med oppfølgningen av ROS2020.

Vi vil nedenfor forsøke å belyse hvor krevende det var å implementere tofaktorautentisering for Stortingets e-postsystemer. Vi mener dette er av betydning for vurdering av tidsaspektet.

En generell utfordring for Stortingets administrasjon ved innføring av sikkerhetstiltak som kan ha negative praktiske konsekvenser for brukerne, er at et betydelig antall brukere – herunder stortingsrepresentantene og de ansatte i partigruppene – ikke er underlagt instruksjonsmyndighet fra Stortingets direktør. Dette innebærer ofte at nye tiltak må avklares og forankres i flere miljøer, og kan gjøre innføring av nye sikkerhetstiltak mer tidkrevende enn i mer enhetlig organiserte virksomheter. Dette ble også påpekt som en utfordring i ROS2020.

For ordens skyld vil vi påpeke at ROS2020 ikke omtaler autentiseringsløsninger for e-post spesifikt, men anbefaler innføring av multifaktorautentisering, ut fra en risikobasert tilnærming, som ett av flere tiltak for å styrke sikkerheten knyttet til Stortingets mobile enheter. For mobile enheter handlet dessuten kun ett av femten risikoscenarier om autentisering.

2.4.2 Tofaktorautentisering var allerede innført på viktige deler av Stortingets plattform

Stortingets administrasjon har i lengre tid benyttet tofaktorautentisering som sikkerhetstiltak på en rekke deler av IT-infrastrukturen. Dette gjaldt blant annet:

- Løsning for nettbrett basert på Citrix: Tofaktorautentisering fra 2011. (Løsningen er senere faset ut.)
- E-post via Internett (webmail): Tofaktorautentisering fra 2016.
- System for fjernadministrasjon: Tofaktorautentisering fra 2017.
- Parti-, komite- og utredningsportalen (PKU): Tofaktorautentisering fra 2019.

- Microsoft Teams: Tofaktorautentisering fra februar 2020.
- Reiseportalen. Tofaktorautentisering fra februar 2020.
- E-læringsportalen. Tofaktorautentisering fra februar 2020.
- Intranettet: Tofaktorautentisering fra februar 2020.
- Pålogging Direktoratet for forvaltning og økonomistyring: Tofaktorautentisering fra februar 2020.

For Stortingets e-postsystem, som Datatilsynet har viet særlig oppmerksomhet i sitt varsel, ble altså tofaktorautentisering implementert allerede i 2016 for pålogging fra Internett (webmail).

2.4.3 Innføring av tofaktorautentisering var komplekst og teknisk krevende

I varselet har Datatilsynet som nevnt lagt vekt på at administrasjonen skal ha brukt uforholdsmessig lang tid på å implementere tofaktorautentisering. Vi ønsker i det følgende å redegjøre for hvor komplekst dette arbeidet viste seg å være. Ettersom tofaktorautentisering på mobile enheter kan fremstå som et tiltak som kan gjennomføres med enkle grep, ser vi det som hensiktsmessig med en relativt detaljert beskrivelse av administrasjonens arbeid med dette tiltaket.

Som nevnt ble ROS2020 fulgt opp med en analyse og kartlegging av aktuelle og prioriterte tiltak våren 2020. Dette gjaldt også et tiltak som innebar innføring av tofaktorautentisering på mobile enheter. Dette viste seg imidlertid å være svært komplekst med den IT-infrastrukturen som foreslå. Det var derfor behov for ekstern kompetanse og ekstra kapasitet, og arbeidet ble besluttet gjennomført i samarbeid med spesialkompetanse fra Crayon/Rewired, Sopra Steria og Microsoft. Selv i disse miljøene med kompetanse på Microsoft-løsninger, var det imidlertid mangel på erfaring med den type endring som var påkrevd for Stortingets e-postsystem. Kompetanse knyttet til tofaktorautentisering på enkelttjenester og skytjenester basert på standardkomponenter var ikke tilstrekkelig.

For å få til sikring av mobile enheter (telefoner/nettbrett) med tofaktorautentisering ble det våren 2020 klart at selve påloggingsmetoden måtte moderniseres. Den valgte nye metoden («Hybrid modern authentication») ble deretter gjort til eneste gyldige påloggingsmetode. Konsekvensen av en slik endring var at mange av tjenestene måtte omkonfigureres. For noen av endringene medførte dette en risiko for avbrudd i andre tjenester under omkonfigureringen. Denne risikoen resulterte i at endringene måtte legges til tidspunkter hvor konsekvensene ved eventuelle avbrudd i tjenestene var så små som mulig.

I tillegg til at omleggingen til tofaktorautentisering på mobile enheter viste seg å være teknisk komplisert, så innebar pandemien lite fysisk tilstedeværelse av ansatte og representanter. Ettersom endringene måtte implementeres på hver enkelt mobile enhet, tok arbeidet derfor adskillig lengre tid enn forutsatt. Høsten 2020 var det nasjonale føringer for hjemmekontor, og eneste alternativ ble da at stortingsrepresentanter og ansatte selv måtte gjennomføre endringene på sine mobile enheter. Det ble utarbeidet en veiledning for dette. Da veiledningen ble testet ut, viste det seg imidlertid at implementeringen ble for komplisert. Innføringen og veiledningen måtte derfor omarbeides, noe som forsinket de nødvendige endringene på mobiletelefoner og nettbrett ytterligere.

Endringer på den enkeltes mobile enhet kom i tillegg til de endringene som måtte gjøres sentralt av administrasjonens IT-avdeling. Avdelingen hadde i november 2020 ferdigstilt ny påloggingsmetode for tjenester både i skyen og «on prem». Endringene som måtte gjøres

sentralt på disse tjenestene innebar en reell fare for avbrudd i andre tjenester. Det var dermed en risiko for følgefeil som kunne medføre at stortingsrepresentanter og ansatte ble utestengt fra verktøy de hadde behov for i utførelsen av sitt arbeid. Som følge av at man var tett på innspurten av Stortingets arbeid med statsbudsjettet, ble det besluttet å legge de siste gjenstående systemendringene, som innebar høy risiko for driftsstans, til etter siste stortingsmøte i desember 2020. De siste store systemendringene ble utført tidlig i januar 2021, og nye versjoner av veiledninger for gjennomføring av endringer på representanter og ansattes mobile enheter, forelå også på dette tidspunktet.

Første pilotgruppe gikk over på ny påloggingsmetode 14. januar 2021. Pilotgruppen oppdaget imidlertid et alvorlig problem med pålogging, og endringen måtte rulles tilbake og videre utrulling stoppes. Etter feilsøking med mange eksterne involvert ble det identifisert en konflikt mellom Stortingets VPN oppkoblingsløsning og «Hybrid modern authentication». Saken ble eskalert så langt som mulig hos leverandøren Microsoft, men det ble konstatert at dette var en kompatibilitetsfeil som ikke lot seg rette. Prosjektet fant likevel en måte å omgå problemet på, og endringene ble implementert overfor pilotgruppen den 5. februar 2021.

Stortinget gjennomførte etter dette puljevis utrulling av løsningen med noen dagers mellomrom mellom hver pulje. Puljevis utrulling ble valgt fordi det ved en samtidig innføring for alle brukergrupper ville være en risiko for at mange representanter og ansatte kunne miste sine tilganger samtidig. Dette ville i så fall resultere i en kaotisk situasjon, der man ikke ville hatt kapasitet til å yte nødvendig bistand til alle samtidig. For å redusere utrullingstiden ble størrelsen på hver pulje økt etter hvert som man fikk mer rutine med håndtering av brukerhenvendelsene. Denne tilnærmingen var for øvrig i samsvar med et av de høyt prioriterte tiltakene fra ROS2020, om at «Store endringer bør settes i produksjon i flere puljer over tid og ikke hele miljøet samtidig». Arbeidet med implementering av tofaktorautentisering på mobile enheter ble sluttført 11. mars 2021.

Kompleksiteten av endringene, mangel på nøkkelferdige løsninger, de særlige forhold som gjorde seg gjeldende på Stortinget under pandemien i hele 2020, samt det faktum at det var lite tilgjengelig informasjon om hvordan løsningen skulle gjennomføres i praksis, innebærer etter Stortingets administrasjons oppfatning at det nødvendigvis måtte gå noe tid før arbeidet med implementering av en løsning for tofaktorautentisering var gjennomført. Uansett hvor snart etter avleveringen av ROS2020 man hadde startet arbeidet med dette, er det vanskelig å se for seg at man hadde rukket å få implementert en sikker løsning før dataangrepet fant sted.

2.5 Andre tekniske og organisatoriske tiltak

Det er i varselet fra Datatilsynet også lagt vekt på at Stortinget kunne iverksatt andre organisatorisk tiltak for å redusere risikoen for dataangrep.

Stortingets administrasjon vil gjøre oppmerksom på at det gjennom lang tid har vært iverksatt en rekke tiltak for å styrke sikkerheten ved Stortingets informasjonssystemer. Vi vil i det følgende peke på noen slike tiltak.

Risiko- og sårbarhetsanalyser benyttes av Stortingets administrasjon som grunnlag for tiltak for å ivareta sikkerheten ved Stortingets systemer, basert på analysenes anbefalinger. Dette er analyser som til nå har vært gjennomført annethvert år med innleid spesialkompetanse fra blant annet mnemonic og Sopra Steria. Ut fra analysene identifiseres sårbarheter, og tiltaksplaner etableres i henhold til god praksis på området. Stortinget har brukt disse analysene som

grunnlag for det vedvarende og regelmessige arbeidet med å ivareta sikkerhet og understøttelse av personvern.

Stortingets administrasjon har innført en del tekniske sikringstiltak for både PCer og andre mobile enheter, herunder sentral administrering, begrensninger på installasjon av programvare og beskyttelse mot skadevare. En god del slike tiltak ble implementert i perioden mellom oktober 2019 og november 2020. Detaljer om disse tiltakene er unntatt offentlighet av sikkerhetsmessige grunner. Om ønskelig kan mer detaljert informasjon om hvilke tekniske tiltak som ble gjennomført, formidles til Datatilsynet på annen måte.

Utover tekniske tiltak har Stortingets administrasjon gjennomført opplæring innen IT-sikkerhet for både representantene og ansatte. En rekke sentrale temaer har blitt tatt opp: Skadevare, datalekkasje, sabotasje, spionasje, spam, phishing og sosial manipulering. Årlige IT-sikkerhetskampanjer har blitt gjennomført både på nett og ved fysiske arrangementer siden 2014. Representanter og ansatte har i tillegg fått innføring i flere viktige rutiner, bl.a. sikkerhet på reise generelt og sikkerhet ved reise til risikoområder.

Videre vil vi peke på at det i etterkant av dataangrepet ble gjort raske organisatoriske tiltak. Innføring av krav om 16-tegns passord ble implementert 3. september 2020. I tillegg ble omfanget av sikkerhetslogging og geosperring utvidet. Geosperring innebærer at trafikk fra spesifikke land og geografiske soner sperres fra å nå Stortingets systemer. Det ble i tillegg gjennomført organisatoriske tiltak knyttet til oppdaterte retningslinjer for mobile enheter, samt iverksatt ytterligere slike opplæringstiltak som redegjort for i vår avviksmelding til Datatilsynet.

Stortingets administrasjon har jobbet systematisk med styrking av IT-sikkerhet også uavhengig av dataangrepet. Arbeid med tiltak fra ROS2020 er videreført og tiltak implementert. I tillegg innfører vi fortløpende tiltak som identifiseres gjennom andre behov som strategiske satsninger i administrasjonen, brukerbehov og den til enhver tid gjeldende trusselsituasjon og situasjonsbilde.

3. Kommentarer til sakens rettslige sider

3.1 Forholdet til GDPR art. 32 nr. 1

Vi oppfatter det rettslige vurderingstemaet etter GDPR art. 32 nr. 1 i denne saken som todelt:

- Hadde administrasjonen gjennomført egnede tekniske og organisatoriske tiltak for å oppnå et risikobasert og egnet sikkerhetsnivå knyttet til e-postsystemet?
- Hadde administrasjonen gjennomført implementeringen av tofaktorautentisering på e-postsystemet tilstrekkelig raskt?

Når det gjelder det første spørsmålet, ønsker vi å peke på at tofaktorautentisering kun er ett av flere tekniske tiltak som kan oppfylle kravet om egnet sikkerhetsnivå for å forhindre enkelte typer dataangrep, slik som det som fant sted høsten 2020. Etter administrasjonens syn stiller GDPR art. 32 nr. 1 ikke noe spesifikt krav til tofaktorautentisering, men fordrer at det gjennomføres regelmessige risikovurderinger av informasjonssikkerheten knyttet til behandlingssystemer og -tjenester, slik som e-postsystemet. Det stilles krav om at dette gjennomføres regelmessig. For Stortingets administrasjon innebærer dette blant annet at vi kontinuerlig forsøker å møte endringer i trusselsituasjon gjennom en rekke konkrete

informasjonssikkerhetstiltak. Videre er kravet til informasjonssikkerhet søkt oppfylt gjennom regelmessig innleie av spesialkompetanse for å gjennomføre risiko- og sårbarhetsanalyser, og ved mer omfattende ROS-analyser annethvert år. Dermed har vi også fått uavhengige tredjepartsvurderinger av vår informasjonssikkerhet.

ROS-analysene gir anbefalinger om tiltak basert på en risikovurdering, som gir grunnlag for å vurdere og prioritere risikoreduserende tiltak med mål om å oppnå vedvarende konfidensialitet, integritet og robusthet. I ROS2020 ble det identifisert sårbarheter og anbefalinger som ga grunnlag for videre analyser og prioritering av mange ulike tiltak. Tiltak som raskt kunne implementeres ble nettopp det. For eksempel ble beskyttelse mot tjenestenektangrep prioritert og innført allerede våren 2020. Andre og mer kompliserte tiltak, som tofaktorautentisering, krevde altså et mer omfattende prosjekt med flere ressurser, både internt og eksternt, og teknisk utvikling, før det kunne iverksettes og fullføres.

Når det gjelder spørsmålet om administrasjonens tidsbruk knyttet til implementeringen av tofaktorautentisering for mobile enheter, må det etter vår oppfatning vektlegges at ROS2020 bygde på en forutsetning om videre analyser for å kategorisere og prioritere sårbarheter og relevante tiltak. Dette arbeidet ble som omtalt ovenfor igangsatt umiddelbart etter at ROS2020 ble avlevert 22. april 2020, pågikk frem til sommeren 2020, og var i ferd med å gjenopptas etter ferieavvikling da dataangrepet fant sted. Det må videre vektlegges at pandemien og nedstengningen av samfunnet stilte ekstraordinære krav til administrasjonen. Prioriteringen og gjennomføringen av tiltakene kunne derfor vanskelig ha skjedd særlig raskere. Det videre arbeidet med implementeringen av tofaktorautentisering utover høsten og vinteren 2020 – som var høyt prioritert – viser at dette arbeidet uansett ville ha tatt tid.

I lys av de nevnte forhold anmoder vi Datatilsynet om å foreta en fornyet vurdering av om det foreligger en klar sannsynlighetsovervekt for avvik etter personvernforordningens art. 32 nr. 1, herunder om det er faktisk og rettslig grunnlag for å karakterisere administrasjonens opptreden som grovt uaktsom.

3.2 Forholdet til art. 83 nr. 2

Datatilsynet har etter en samlet vurdering kommet til at Stortinget bør ilegges et overtredelsesgebyr på to millioner kroner, jf. GDPR art. 83 nr. 2. Bestemmelsen gir anvisning på at ileggelse av overtredelsesgebyr beror på en skjønnsmessig helhetsvurdering, men legger føringer på skjønnsutøvelsen ved å trekke frem momenter som skal tillegges særlig vekt.

Stortingets administrasjonen ønsker kort å fremheve enkelte forhold som vi mener bør få betydning for den skjønnsmessige vurderingen etter GDPR art. 83 nr. 2.

Vi er i utgangspunktet enig med Datatilsynet i at det er alvorlig at folkevalgte var blant de berørte av dataangrepet. Det var likevel svært få personer som ble rammet, både i antall og særlig i forhold til det store antall e-postkontoer som ble utsatt for angrep.

Når det gjelder omfanget av personopplysninger som ble kompromittert, var også dette meget begrenset. Av de få personene som ble rammet av angrepet var det kun et meget lite antall som fikk personopplysninger hentet ut.

Mer spesifikk informasjon om konsekvensene av dataangrepet er unntatt offentlighet av sikkerhetsmessige grunner. Om ønskelig kan mer detaljert informasjon om dette formidles til Datatilsynet på annen måte.

Videre er det korrekt som vist til i forhåndsvarselet, at enkelte helseopplysninger ble eksponert, men dette var knyttet til informasjon om deltagelse på møter/konferanser hvor det var etterspurt informasjon om matpreferanser eller matallergier. Selv om også dette er å anse som sensitive personopplysninger, anser vi dem generelt sett som mindre sensitive enn andre typer helseopplysninger.

Endelig mener vi at det under reaksjonsvurderingen også må vektlegges at Stortingets administrasjon i 2020 som omtalt ovenfor befant seg i en ekstraordinær situasjon med pandemi og nasjonal nedstengning. Hensynet til å sikre kontinuitet i Stortingets parlamentariske virksomhet gikk foran alt. Alle andre oppgaver, som oppfølging av ROS2020, kunne på dette tidspunktet ikke prioriteres tilsvarende.

Med hilsen

Marianne Andreassen
direktør

Kjersti Wilson
personvernombud