Datatilsynet

Melding om brudd på personopplysningssikkerheten

Dato sendt:	23.11.2026 / 18:39
Avsender:	833735462-WAYSCLOUD AS
Mottaker:	Datatilsynet
Referansenummer:	2a3ec7cb24b0

Dette skjemaet er for virksomheter som har eller har hatt et avvik. Et avvik er i denne sammenhengen et brudd på personopplysningssikkerheten som er meldepliktig etter personvernforordningen artikkel 33.
Vi ber deg om å unngå å fylle ut personopplysninger om de personene som er berørt av bruddet. Dersom du legger ved filer, ber vi deg om å sladde eller slette eventuelle personopplysninger i vedleggene før de lastes opp.
Mer informasjon om avvikshåndtering finner du på Datatilsynets nettsider https://www.datatilsynet.no/avvik

1.1 Informasjon om virksomheten

1.1.1 Organisasjonsnummer
833735462

1.1.2 Navn
WAYSCLOUD AS

1.1.3 Adresse
Universitetsgata 2

1.1.4 Postnr.
0164

1.1.5 Poststed
OSLO

1.1.6 Deres interne referanse (referansenr. eller lignende)
WAYSCLOUD-TR-2026-0034

1.2 Hva slags type melding er dette?
Tilleggsmelding

1.2.1 Tidligere innsendte meldinger
Dato sendt inn: 23.11.2026 05:41 | Altinn Referanse: 58dd4a567918 | Intern Referanse: WAYSCLOUD-TR-2026-0034

1.3 Kontaktinformasjon

1.3.1 Fornavn
Knut Michael Knutsen

1.3.2 Etternavn
Haugland

1.3.3 Stillingstittel
Daglig leder

1.3.4 E-post
knut@wayscloud.eu

1.3.5 Landskode
Norge (+47)

Telefon
[redacted]

Alternativ kontaktinformasjon

1.3.6 Vil du legge til informasjon om en alternativ kontakt?
Du har ikke lagt inn informasjon her

1.5 Om innmelderen
Behandlingsansvarlig

Tilleggsinformasjon

Her kan du legge inn tilleggsinformasjon til den opprinnelige avviksmeldingen. Eventuell dokumentasjon kan også lastes opp her.

2.1 Tilleggsinformasjon
Vi viser til vår tidligere melding om en identifisert svakhet i autorisasjonskontrollen for tjenestespesifikke API-nøkler i WAYSClouds administrasjons-API.

Etter den opprinnelige meldingen har vi gjennomført en teknisk utbedring, en utvidet historisk undersøkelse, en konkret vurdering av mulig eksponering av personopplysninger og individuell orientering av de relevante eksterne kundene.

Undersøkelsen har gitt et vesentlig mer presist bilde av hendelsens omfang og mulige konsekvenser enn det som forelå ved den innledende varslingen. Vi ønsker derfor å supplere og presisere opplysningene som tidligere er oversendt.

Identifisert svakhet og teknisk utbedring:

Svakheten ble identifisert 22. november 2026, med første dokumenterte registrering omkring kl. 18:08 CET.

Den tekniske undersøkelsen avdekket at autorisasjonskontrollen i enkelte tilfeller verifiserte eksistensen av en tjenestetillatelse uten konsekvent å håndheve hvilken konkret handling og ressurs tillatelsen omfattet. Enkelte autorisasjonsparametere kunne dessuten påvirkes gjennom klientens forespørsel.

Dette kunne i prinsippet medføre at en autentisert, begrenset API-nøkkel fikk tilgang til flere administrasjonsoperasjoner enn den var tildelt, innenfor tilhørende kundekontekst.

Den historiske svakheten ble reprodusert og verifisert i et isolert testmiljø. Undersøkelsen har ikke identifisert noen tilsvarende omgåelse av kontrollene som skiller ulike kundekontoer.

De første korrigerende kodeendringene ble registrert allerede om kvelden 22. november. Arbeidet fortsatte gjennom natten med teknisk kartlegging, feilretting, sikkerhetstesting, gjennomgang av rettighetskontroller og forberedelse av produksjonssetting.

- Den opprinnelige avviksmeldingen ble sendt til Datatilsynet 23. november 2026 kl. 05:41 CET, med referansenummer 58dd4a567918.

- Den tekniske rettelsen ble satt i produksjon 23. november 2026 kl. 09:06 CET, under 15 timer etter den første dokumenterte oppdagelsen.

Produksjonssettingen er dokumentert gjennom tidsstemplede release-artefakter, sikkerhetskopier, tjenesteomstart og funksjonelle etterkontroller.

Rettelsen innebærer at autorisasjonskravene nå fastsettes på serversiden og håndheves mot den konkrete tjenesten, handlingen og ressursen. Klientens forespørselsparametere kan ikke lenger overstyre autorisasjonskravene på den tidligere identifiserte måten.

Etter produksjonssettingen ble det bekreftet at den oppdaterte autorisasjonskontrollen var aktiv. Forespørsler uten nødvendig handlingsrettighet ble avvist med HTTP 403.

Utvidet undersøkelse av historisk aktivitet:

Ved den første varslingen ble begrensninger i historisk sporbarhet fremhevet som en usikkerhetsfaktor.

Vi har etter dette gjennomført en vesentlig mer omfattende undersøkelse ved å sammenstille autentiseringsmetadata, nøkkelrettigheter, historiske bruksregistreringer, kilde-IP-adresser, aktivitetslogger, plattformhendelser, tjenestespesifikke revisjonsspor og ressurshistorikk.

Denne korrelasjonen har gjort det mulig å rekonstruere konkrete bruksmønstre, undersøke hvilke ressurser som faktisk eksisterte, og avgrense det relevante eksterne omfanget betydelig.

Den videre undersøkelsen har dermed vesentlig redusert usikkerheten som ble beskrevet i den opprinnelige meldingen

Vi presiserer at WAYSCloud ikke har manglet historiske aktivitetsdata generelt. Flere strukturerte registre har bevart informasjon over lengre tidsperioder og har muliggjort den etterfølgende analysen.

Det gjenstår enkelte begrensninger på enkeltforespørselsnivå. Ikke alle historiske administrasjonsforespørsler kan knyttes entydig til en bestemt API-nøkkel, og enkelte ordinære HTTP-logger har kortere oppbevaringstid enn de strukturerte aktivitetsregistrene.

Disse begrensningene er hensyntatt i den samlede risikovurderingen.

Gjennomgang av relevante eksterne legitimasjoner:

Den utvidede kartleggingen har avgrenset den relevante eksterne legitimasjonskohorten til to kundekontoer med til sammen fire begrensede API-nøkler

For den første kundekontoen ble tre legitimasjoner undersøkt.

Én legitimasjon var tildelt tilgang til LLM-inferens. Det ble identifisert 87 ordinære inferensforespørsler mellom 2. og 16. desember 2025, fordelt på to allerede kjente kilde-IP-adresser knyttet til kundens ordinære tjenestebruk.

Det ble ikke identifisert administrativ API-aktivitet fra de aktuelle adressene eller operasjoner som indikerer utnyttelse av autorisasjonssvakheten.

Den historiske svakheten kunne prinsipielt ha muliggjort andre operasjoner med legitimasjonen. Ingen slik bruk er imidlertid identifisert i den tilgjengelige dokumentasjonen.

De to øvrige legitimasjonene var opprettet i forbindelse med GPU- og Redis-relatert testing. Begge hadde én tidlig registrert validering i desember 2025, uten ordinære forbruksregistreringer eller senere dokumentert bruk.

Samtidige GPU- og Redis-operasjoner er undersøkt nærmere og knyttet til interne tester under utvikling og innføring av tjenestene. Det er ikke dokumentert at de aktuelle kundetestnøklene utførte disse operasjonene.

For den andre kundekontoen ble én DNS-relatert legitimasjon undersøkt.

Denne har ingen registrert vellykket validering, ingen registrerte bruksforespørsler og ingen dokumenterte administrasjonsoperasjoner. Kundekontoen hadde heller ingen DNS-soner eller DNS-poster som kunne ha blitt lest eller endret.

Samlet er det ikke identifisert uautoriserte operasjoner som følge av den aktuelle svakheten for de fire undersøkte eksterne legitimasjonene.

Vurdering av mulig eksponering av personopplysninger:

Den identifiserte svakheten representerte en reell risiko for at en autentisert, begrenset API-nøkkel kunne benyttes til operasjoner utover sine tiltenkte rettigheter.

Undersøkelsen har derfor omfattet både teoretiske tilgangsmuligheter, faktisk registrert aktivitet, eksisterende ressurser og mulige konsekvenser for personopplysninger.

For WAYSClouds ordinære LLM-inferensflyt behandles forespørselsinnhold i forbindelse med den enkelte inferensoperasjonen. WAYSCloud lagrer ikke kundenes promptinnhold som del av denne ordinære behandlingen. De historiske bruksregistreringene som er undersøkt, omfatter tekniske opplysninger om forespørslene, ikke selve promptinnholdet.

Tekniske logger og driftsregistreringer er underlagt ulike oppbevarings- og rotasjonsrutiner. Selv om enkelte eldre HTTP-detaljer ikke lenger er tilgjengelige, har strukturerte bruks- og aktivitetsregistreringer muliggjort en omfattende historisk analyse.

Undersøkelsen har ikke identifisert uautorisert innsyn i kunders lagrede opplysninger, urettmessig utlevering av personopplysninger, uautoriserte endringer eller sletting av kundeopplysninger som følge av svakheten, eller uautorisert tilgang til andre kundekontoers ressurser.

Det er heller ikke identifisert konkrete fysiske personer hvis personopplysninger er dokumentert kompromittert.

Det foreligger dermed ingen påvist eksponering eller kompromittering av personopplysninger som følge av den undersøkte autorisasjonssvakheten.

Denne vurderingen bygger på den samlede tilgjengelige dokumentasjonen og innebærer ikke at enhver historisk forespørsel kan utelukkes med absolutt sikkerhet.

Presisering av opprinnelig anslag over berørte registrerte:

I den opprinnelige meldingen ble tallet åtte oppgitt som et foreløpig anslag over mulige berørte registrerte.

Dette var et beregningsteknisk anslag basert på kundekontekster identifisert under den innledende tekniske kartleggingen, og representerte ikke åtte identifiserte fysiske personer.

Den etterfølgende undersøkelsen har avgrenset den relevante eksterne legitimasjonskohorten til to kundekontoer med fire begrensede API-nøkler.

Antall kundekontoer eller legitimasjoner kan ikke likestilles med antall berørte fysiske personer. Ingen konkrete registrerte med dokumentert kompromitterte personopplysninger er identifisert, og et eksakt antall eventuelt berørte personer kan ikke fastslås.

Vi ønsker med dette å korrigere og presisere grunnlaget for det opprinnelige anslaget.

Gjennomførte og forebyggende tiltak:

WAYSCloud har gjennomført en kodebasert rettelse som håndhever autorisasjonskrav mot den konkrete tjenesten, handlingen og ressursen som den enkelte API-operasjonen gjelder.

Autorisasjonskravene er nå bundet til operasjonen på serversiden, slik at klienten ikke kan påvirke hvilke rettigheter endepunktet krever gjennom forespørselsparametere på den tidligere identifiserte måten.

Rettelsen er verifisert gjennom automatiserte regresjonstester, negative autorisasjonstester, kodegjennomgang og produksjonskontroller.

Produksjonsutrullingen ble gjennomført med kontrollert release- og tilbakeføringsmekanisme. Tjenestens helsetilstand og oppdaterte rettighetshåndhevelse ble etterkontrollert.

Som videre forebyggende oppfølging gjennomgår vi sporbarheten for individuelle API-legitimasjoner, oppbevaringsrutiner for sikkerhetslogger og samsvaret mellom utstedte rettigheter og rettighetene som håndheves ved konkrete tjenesteoperasjoner.

Vi viderefører samtidig negative sikkerhetstester som kontrollerer at begrensede legitimasjoner ikke kan utføre operasjoner utover tildelte rettigheter.

Formålet er både å redusere sannsynligheten for tilsvarende svakheter og å styrke etterprøvbarheten ved fremtidige sikkerhetshendelser.

Det skilles i den interne oppfølgingen mellom tiltak som allerede er gjennomført, og ytterligere forbedringer som er identifisert for videre implementering.

Kundevarsling og dokumentasjon:

Som ledd i oppfølgingen har WAYSCloud valgt å orientere de to identifiserte eksterne kundene individuelt, selv om undersøkelsen ikke har påvist uautorisert tilgang til eller kompromittering av personopplysninger.

Begge kundene ble varslet 23. november 2026, henholdsvis kl. 18:26 og 18:27 CET.

Varslingen ble gjennomført via WAYSClouds elektroniske kommunikasjonsløsning. Hver kunde mottok en individuelt tilpasset, elektronisk signert redegjørelse med informasjon om den identifiserte svakheten, gjennomført teknisk utbedring, resultatene av undersøkelsen for eget kundeforhold og kontaktinformasjon for videre oppfølging signert via Posten signering for etterprøvbarhet.

Kundene ble også orientert om at hendelsen er meldt til Datatilsynet, og at en samlet redegjørelse vil bli publisert i WAYSClouds Trust Center.

Anonymiserte kopier av kundeorienteringene vedlegges som dokumentasjon. De opprinnelige, elektronisk signerte dokumentene og tilhørende utsendelsesregistreringer er bevart internt for etterprøvbarhet.

Samlet vurdering

WAYSCloud identifiserte en reell teknisk svakhet i autorisasjonskontrollen for tjenestespesifikke API-nøkler.

Svakheten ble undersøkt, dokumentert og utbedret omgående etter oppdagelsen. De første korrigerende endringene ble gjennomført samme kveld, arbeidet fortsatte gjennom natten, og den korrigerte implementasjonen ble satt i produksjon mindre enn 15 timer etter første dokumenterte registrering.

Den oppdaterte rettighetshåndhevelsen ble funksjonelt verifisert.

Etter den første varslingen har WAYSCloud gjennomført en betydelig mer omfattende historisk undersøkelse, basert på korrelasjon av autentiseringsdata, IP-adresser, bruksregistreringer, aktivitetslogger og ressurshistorikk.

Dette har gjort det mulig å avgrense det relevante eksterne omfanget betydelig og undersøke de konkrete legitimasjonene og deres registrerte bruk.

Den samlede undersøkelsen har ikke avdekket uautorisert utnyttelse av den identifiserte svakheten eller dokumentert kompromittering av personopplysninger.

Det gjenstår enkelte begrensninger i den historiske sporbarheten på enkeltforespørselsnivå. Disse er vurdert og dokumentert, og vi gjør derfor ikke gjeldende at enhver tenkelig historisk forespørsel kan utelukkes.

De relevante eksterne kundene er individuelt orientert, den tekniske svakheten er rettet, produksjonskontroller er gjennomført, og ytterligere forebyggende forbedringer følges opp gjennom virksomhetens ordinære sikkerhets- og endringsstyring.

Disse opplysningene oversendes for å supplere den opprinnelige meldingen med den oppdaterte vurderingen av mulig eksponering, resultatene av den historiske undersøkelsen, gjennomført utbedring og dokumentert kundevarsling.

2.2 Vedlegg

WAYSCLOUD-TR-2026-0034-anonymiserte-kundeorienteringer.pdf

WAYSCLOUD-TR-2026-0034-sluttattest-hendelsesforlop.pdf