Datatilsynet

Melding om brudd på personopplysningssikkerheten

Dato sendt:	23.11.2026 / 05:40
Avsender:	833735462-WAYSCLOUD AS
Mottaker:	Datatilsynet
Referansenummer:	58dd4a567918

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?
Ny melding om brudd

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

1.5.2 Behandlingsansvarlig

1.5.2.1 Andre involverte parter

Vet ikke

Beskrivelse av bruddet

Tidslinje

2.1 Bruddet pågikk fra

Du har ikke lagt inn informasjon her

Vet ikke

2.2 Bruddet pågikk til

Du har ikke lagt inn informasjon her

Bruddet pågår fortsatt

2.3 Når oppdaget dere bruddet?

Dato oppdaget

22.11.2026

Tid oppdaget

18:08

2.4 Beskriv hvordan dere oppdaget bruddet

Sikkerhetssvakheten ble oppdaget 22. november 2026 gjennom en intern sikkerhets- og kodegjennomgang av WAYSClouds administrasjons-API, i forbindelse med forberedelser til en ny integrasjon mot skyplattformen.

Gjennomgangen avdekket at autorisasjonskontrollen for enkelte API-legitimasjoner ikke håndhevet tildelte handlings- og ressursrettigheter tilstrekkelig. Kontrollen verifiserte i visse tilfeller at en API-nøkkel hadde tilgang til den aktuelle tjenesten, men ikke nødvendigvis at nøkkelen hadde tillatelse til den konkrete operasjonen. Det ble også identifisert svakheter i håndteringen av enkelte autorisasjonsparametere.

Funnene ble undersøkt videre gjennom kildekodeanalyse, gjennomgang av historiske endringer og målrettede sikkerhetstester. Svakhetene ble deretter registrert og prioritert for utbedring.

Det er foreløpig ikke påvist at sårbarheten har blitt utnyttet til uautorisert tilgang til eller behandling av personopplysninger. Undersøkelsen har imidlertid avdekket begrensninger i historisk forespørselslogging, slik at eventuell utnyttelse ikke kan utelukkes med sikkerhet. Hendelsen undersøkes derfor videre som et mulig brudd på personopplysningssikkerheten.

2.5 Hvis aktuelt, angi når databehandleren varslet dere om bruddet

Dato varslet

Du har ikke lagt inn informasjon her

2.6 Merknader til datoene

Sikkerhetssvakheten ble identifisert internt 22. november 2026, og ikke som følge av varsel fra en ekstern databehandler. Dato i punkt 2.5 er derfor ikke relevant.

Historisk kildekodegjennomgang viser at svakheten var til stede fra 28. oktober 2025. Nøyaktig tidspunkt for første eksponering i produksjon er ikke fastslått. Det er heller ikke dokumentert når et eventuelt personopplysningsbrudd kan ha inntruffet.

Produksjonsutbedringen var ikke bekreftet fullført ved førstegangsmeldingen. Opplysningene vil bli oppdatert ved behov i en tilleggsmelding.

2.7 Unntak fra offentlig innsyn?
Nei

Beskrivelse av bruddet

Et meldepliktig brudd på personopplysningssikkerheten kan kategoriseres som brudd på konfidensialitet, integritet eller tilgjengelighet, eller en kombinasjon av disse. Velg én eller flere kategorier som beskriver bruddet.

2.8 Type brudd

Annet

2.8.1 Annet
Identifisert svakhet i autorisasjons- og tilgangskontrollen i virksomhetens administrasjons-API, med potensiell påvirkning på personopplysningers konfidensialitet og integritet.

Det er foreløpig ikke påvist faktisk uautorisert tilgang til, endring av eller tap av personopplysninger. Hendelsen undersøkes og følges opp som et mulig brudd på personopplysningssikkerheten.

2.9 Hva førte til bruddet?

Manglende/feil i tilgangsstyring

System- eller programmeringsfeil

2.10 Beskrivelse
Den 22. november 2026 identifiserte WAYSCloud AS gjennom en intern sikkerhets- og kodegjennomgang en svakhet i autorisasjonskontrollen i selskapets offentlige administrasjons-API for skyplattformen. Gjennomgangen ble gjennomført i forbindelse med videreutvikling av plattformens integrasjonsmuligheter.

Svakheten bestod i at autorisasjonskontrollen for enkelte typer API-legitimasjoner ikke i tilstrekkelig grad håndhevet de spesifikke handlings- og ressursrettighetene som var tildelt. Under bestemte forutsetninger kunne en autentisert API-nøkkel derfor få utført operasjoner innenfor en tjeneste som gikk utover nøkkelens uttrykkelig tildelte rettigheter. Det ble også identifisert svakheter i håndteringen av enkelte autorisasjonsparametere.

Den identifiserte svakheten gjaldt kontrollen av rettigheter etter autentisering. Det er ikke påvist et generelt autentiseringsbypass. Plattformen har dessuten separate mekanismer for kunde- og ressurseierskap, og undersøkelsene har så langt ikke påvist uautorisert tilgang på tvers av kundekontoer.

En etterfølgende historisk kildekodegjennomgang viser at den grunnleggende svakheten var til stede allerede i den opprinnelige implementasjonen fra 28. oktober 2025. Tilgjengelig produksjonsdokumentasjon bekrefter at administrasjons-API-et var etablert i produksjonsmiljøet senest i november 2025. Det eksakte tidspunktet da den berørte funksjonaliteten først ble eksternt tilgjengelig, har ikke kunnet fastslås.

Vi har gjennomført en kartlegging av API-legitimasjoner som potensielt kunne være berørt av den mangelfulle rettighetshåndhevingen. Kartleggingen identifiserte 41 begrensede legitimasjoner fordelt på åtte kundekontekster, hvorav en betydelig andel tilhører virksomhetens egne kontoer, ansatte og testmiljøer. Dette representerer en teknisk risikopopulasjon, ikke dokumentert uautorisert bruk eller et tilsvarende

antall berørte personer.

Vi har også undersøkt tilgjengelige aktivitets- og revisjonslogger. Undersøkelsen omfatter omtrent 3,5 millioner aktivitetsregistreringer, men avdekket at historiske opplysninger ikke gir tilstrekkelig detaljert kobling mellom den enkelte API-legitimasjonen og alle utførte operasjoner. Dette begrenser muligheten til å etterprøve om enkelte historiske operasjoner lå utenfor legitimasjonenes tildelte rettigheter.

Det er på rapporteringstidspunktet ikke dokumentert at svakheten faktisk er blitt utnyttet til uautorisert tilgang til, endring av eller tap av personopplysninger. Den mangelfulle historiske sporbarheten innebærer imidlertid at vi ikke med sikkerhet kan utelukke slik aktivitet.

Umiddelbart etter oppdagelsen ble forholdet prioritert som en kritisk sikkerhetssak. Det er utviklet korrigeringer som innfører eksplisitt håndheving av handlings- og ressursrettigheter, strengere skille mellom legitimasjonstyper og sikrere håndtering av rettigheter ved nøkkelrotasjon. Korrigeringene har gjennomgått omfattende automatiserte tester, herunder sikkerhetstester, regresjonstester og uavhengige kodekvalitetskontroller. Endelig produksjonsutrulling og etterfølgende verifikasjon er ikke bekreftet fullført på tidspunktet for denne førstegangsmeldingen.

Det er videre iverksatt arbeid med å forbedre revisjonssporbarheten, slik at fremtidige API-operasjoner i større grad kan knyttes til den konkrete legitimasjonen som har utført dem.

WAYSCloud AS har valgt å sende denne innledende meldingen som et føre-var-tiltak, selv om det foreløpig ikke er fastslått at sikkerhetssvakheten har medført et faktisk brudd på personopplysningssikkerheten.

Undersøkelsen og utbedringsarbeidet pågår. Vi vil supplere meldingen med dokumentert produksjonsutbedring, oppdatert risikovurdering og eventuelle nye opplysninger om påvirkning på personopplysninger eller registrerte, uten ugrunnet opphold.

Personopplysninger som er berørt av bruddet

3.1 Personopplysninger
Det er på rapporteringstidspunktet ikke dokumentert at konkrete personopplysninger har vært gjenstand for uautorisert tilgang, utlevering, endring eller tap.

Den identifiserte autorisasjonssvakheten gjelder administrasjons-API-et for WAYSClouds skyplattform. Opplysninger som potensielt kan være berørt, omfatter kunde- og brukeridentifikatorer, navn og kontaktopplysninger knyttet til kundekontoer, IP-adresser, DNS-relaterte opplysninger samt tekniske metadata om kundenes tjenester og ressurser.

Disse kategoriene beskriver mulig eksponering og ikke bekreftet kompromitterte opplysninger.

Det er foreløpig ikke påvist at innhold lagret i kundenes virtuelle servere, databaser eller objektlagring er blitt tilgjengelig for uvedkommende som følge av svakheten.

Den tekniske kartleggingen har identifisert åtte kundekontekster med til sammen 41 API-legitimasjoner som potensielt kunne omfattes av autorisasjonssvakheten.

Ettersom skjemaet krever et numerisk anslag, er tallet 8 foreløpig benyttet med utgangspunkt i antallet identifiserte kundekontekster. Dette er ikke et bekreftet antall berørte fysiske personer. Antallet registrerte som faktisk eller potensielt kan være berørt, er foreløpig ukjent og kan være både lavere og høyere.

Det er ikke dokumentert at personopplysninger faktisk har blitt uautorisert utlevert, endret eller gjort utilgjengelige. Anslaget vil bli korrigert i en tilleggsmelding dersom videre undersøkelser gir et mer presist grunnlag.

3.2 Særlige kategorier av personopplysninger

Foreløpig ukjent

Om de registrerte som er berørt

3.3 Beskrivelse av de berørte

De potensielt berørte registrerte er i første rekke fysiske personer tilknyttet WAYSClouds kundekontoer, herunder kontoeiere, administratorer, kontaktpersoner og brukere av skyplattformens administrasjonstjenester.

Disse kan omfatte både personer tilknyttet WAYSClouds egen virksomhet og representanter for eksterne kunder.

Den tekniske kartleggingen har identifisert et begrenset antall API-legitimasjoner med mulig utvidet operasjonell tilgang. En betydelig andel av disse tilhører WAYSClouds egne kontoer, ansatte og testmiljøer.

Det er foreløpig ikke identifisert bestemte enkeltpersoner som faktisk har fått sine personopplysninger kompromittert.

Vi undersøker også om forholdet kan ha hatt konsekvenser for personopplysninger som WAYSCloud behandler på vegne av sine kunder.

Antallet eventuelt berørte registrerte er derfor foreløpig ukjent.

3.4 Antall berørte

8

Konsekvenser

4.4 Potensielle konsekvenser

Tap av kontroll over egne personopplysninger

Andre konsekvenser

4.4.1 Beskriv andre konsekvenser

Den identifiserte autorisasjonssvakheten kunne under bestemte forutsetninger muliggjøre uautoriserte endringer i kunders skyressurser og tjenestekonfigurasjoner. Dette kunne indirekte påvirke personopplysningers integritet eller tilgjengelighet, eksempelvis gjennom endret tilgang til tjenester eller driftsforstyrrelser.

Det er ikke dokumentert at slike konsekvenser faktisk har inntruffet, eller at registrerte har lidt konkret skade. Plattformens separate kontroller for kunde- og ressurseierskap har begrenset den identifiserte eksponeringen.

Vurderingen er foreløpig og vil bli oppdatert dersom videre undersøkelser avdekker faktisk påvirkning på personopplysninger.

4.5 Alvorlighetsgrad

3 - Betydelig

Oppfølging av hendelsen

5.1 Har hver enkelt av de berørte personene blitt informert om bruddet?

Ikke avklart på nåværende tidspunkt

5.5 Beskriv hvilke tiltak som er gjort og planlagt for å håndtere bruddet
WAYSCloud AS iverksatte umiddelbart etter oppdagelsen 22. november 2026 en prioritert intern sikkerhetshåndtering av den identifiserte autorisasjonssvakheten i skyplattformens administrasjons-API.

Det er gjennomført en teknisk analyse av årsaken, berørte funksjoner og eksisterende tilgangskontroller. Undersøkelsen har også omfattet historisk kildekode, produksjonshistorikk, relevante API-legitimasjoner og tilgjengelige aktivitetslogger.

På bakgrunn av funnene er det utviklet omfattende korrigeringer som styrker håndhevingen av handlings- og ressursrettigheter, sikrer tydeligere skille mellom legitimasjonstyper og ivaretar eksisterende tilgangsbegrensninger ved fornyelse av legitimasjoner.

Korrigeringene har gjennomgått automatiserte sikkerhets-, integrasjons- og regresjonstester, samt uavhengige kvalitetskontroller. Testene omfatter blant annet kontroll av tilgangsrettigheter, kundeisolasjon og avvisning av uautoriserte operasjoner.

Den endelige produksjonsutrullingen og etterfølgende verifikasjonen er ennå ikke bekreftet fullført på tidspunktet for denne førstegangsmeldingen. Utbedringen gjennomføres i henhold til virksomhetens etablerte prosedyrer for endringskontroll og sikkerhetsverifikasjon.

Det er videre identifisert forbedringsbehov knyttet til historisk sporbarhet av API-operasjoner. Tiltak er registrert for å styrke revisjonslogging, hendelsesoppfølging og muligheten til å etterprøve autorisasjonsbeslutninger.

Etter produksjonsutrullingen vil WAYSCloud gjennomføre målrettede sikkerhetskontroller og overvåke relevante drifts- og tilgangshendelser for å verifisere at svakheten er utbedret, uten utilsiktede konsekvenser for legitime brukere.

Det er foreløpig ikke dokumentert at svakheten har medført uautorisert tilgang til, endring av eller tap av personopplysninger. Undersøkelsen pågår fortsatt, og behovet for direkte varsling av kunder eller registrerte vurderes fortløpende.

WAYSCloud AS vil supplere meldingen til Datatilsynet uten ugrunnet opphold når produksjonsutbedringen er verifisert og ytterligere opplysninger om hendelsens omfang og eventuelle konsekvenser foreligger.

Grenseoverskridende behandling

6.1 Har dere etableringer innenfor EU/EØS?
Kun i ett land i EU/EØS

6.1.1 I hvilket EU-/EØS-land har dere etablering?
Norge

6.2 I hvilke(t) land befinner personene seg som dere behandler personopplysninger om?
I flere land i EU/EØS

6.3 I hvilke av deres etableringer tas beslutningene om aktiviteten, systemet eller rutinen som bruddet gjelder?
En etablering i Norge

Vedlegg

Last opp vedlegg som er relevante for bruddet.

WAYSCLOUD-TR-2026-0034-forelopig-aktivitetsoversikt.pdf