WORKFORCE, OPS & HMS

Trust & Compliance Brief

Versjon 1.0 · 29. november 2026

Til IT-, sikkerhets- og personverngjennomgangen av HR Cluster. Hvert utsagn er hentet fra HR Clusters publiserte sider for sikkerhet, personvern, underleverandører, databehandleravtale og informasjonskapsler. Side og punkt står under hver del.

Dette dokumentet gjengir HR Clusters publiserte juridiske sider per denne datoen. Sidene slik de til enhver tid er publisert på nett (hrcluster.app/security, /privacy, /subprocessors, /dpa, /cookies) har forrang.

Hva HR Cluster behandler, og i hvilken rolle

- HR Cluster håndterer data om arbeidsstyrken: personalia, vaktplaner, fremmøteregistreringer, hendelsesrapporter, kompetansebevis og kvalifikasjoner.
- For data om arbeidsstyrken som kunden legger inn i eller genererer i plattformen, er kundeorganisasjonen behandlingsansvarlig og HR Cluster AS databehandler. HR Cluster AS er behandlingsansvarlig for sin egen behandling, som fakturering, kontoadministrasjon, sikkerhetslogging av tilgang til plattformen og, med samtykke, bruksanalyse.

Kilder: hrcluster.app/security, punkt 1; hrcluster.app/privacy, punkt 2; hrcluster.app/dpa, punkt 2

Drift og datalokasjon

- HR Cluster driftes på Hetzner Cloud-servere i EU. Applikasjonsservere, produksjonsdatabaser og opplastede filer ligger i EU, primært i Helsinki, Finland, med en standby-replika av databasen i Nürnberg, Tyskland.
- Databasetjenesten kan ikke nås fra internett. Den tar bare imot tilkoblinger over vårt private nettverk og krypterte replikeringstunneler.

Kilder: hrcluster.app/security, punkt 2; hrcluster.app/subprocessors, punkt 2

Kryptering

- Under overføring: TLS (HTTPS) på hver forespørsel, terminert på vår administrerte lastbalanserer med automatisk fornyet sertifikat.
- Ved lagring: sensitive identifikatorer som nasjonale ID-numre og bankopplysninger krypteres med AES-256-GCM før de når databasen, ved hjelp av en nøkkel som lagres utenfor databasen. Dette gjelder disse feltene; det er ikke et utsagn om alle lagrede data.
- Passord og PIN-koder: passord hashes med bcrypt; PIN-koder for stempling hashes separat. HR Cluster lagrer aldri noen av dem i klartekst og skriver dem aldri til loggene sine. En ny PIN-kode som sendes på e-post, står i den e-posten, som e-postleverandøren oppbevarer i den oppbevaringsperioden som gjelder hos leverandøren.

Kilder: hrcluster.app/security, punkt 3

Dataisolasjon mellom kunder

- HR Cluster er multitenant. Spørringer mot kundeeide data er avgrenset til kundens konto, enten direkte med account_id eller gjennom en overordnet post der kontoen er kontrollert. Offentlige lenker, som signerings- og leverandørlenker, slås opp med sitt eget hemmelige token og gjelder deretter bare innenfor kontoen til den aktuelle posten. Plattformadministrasjon og planlagte vedlikeholdsjobber er konstruert for å operere på tvers av kontoer.
- Filopplastinger lagres utenfor webroten, organisert per konto, og serveres bare gjennom programkode som kontrollerer tilgang: for innloggede brukere medlemskap i kontoen og relevant rettighet; for signerings- og forespørselslenker lenkens token, avgrenset til sin egen post. Filtypen kontrolleres før filen serveres.
- Tilgang for plattformadministratorer bruker egen innlogging, egen informasjonskapsel og egen autentiseringstabell, adskilt fra kundekontoer.

Kilder: hrcluster.app/security, punkt 4 og 5

Tilgangskontroll og revisjonslogging

- Passordinnlogging oppretter et tilfeldig sesjonstoken som bare lagres i en informasjonskapsel med attributtene Secure, HttpOnly og SameSite i nettleseren. Databasen lagrer bare en hash av tokenet, og hver innlogget forespørsel kontrolleres mot databasen, med tidsavbrudd ved inaktivitet og en absolutt tidsgrense.
- Rollebasert tilgangskontroll (kontoadministrator, leder, arbeider) med overstyringer per rettighet.
- CSRF-beskyttelse på tilstandsendrende forespørsler fra innloggede brukere: skjemaer og API-kall må ha et token som er bundet til innloggingsøkten, og innloggingsinformasjonskapsler settes med SameSite=Lax. Forespørsler som ikke kommer fra en innlogget nettleser, beskyttes på andre måter: webhooks fra leverandører med en delt hemmelighet eller signatur, stemplingsterminalen med arbeiderens PIN-kode, og passordbeskyttede live-skjermer med passordet sitt. Begrensning av antall forespørsler (rate limiting) på autentiseringsendepunkter.
- Vi logger administrative handlinger, dataeksporter og endringer i rettigheter per konto.

Kilder: hrcluster.app/security, punkt 4 og 7

Sikkerhetskopiering og overvåking

- HR Cluster AS opprettholder lagdelte tiltak for sikkerhetskopiering og gjenoppretting etter katastrofer (disaster recovery) som skal støtte kontinuitet i tjenesten og robusthet i dataene.
- Sikkerhetskopier som lagres utenfor driftsstedet, overføres via SSH til Hetzners lagring for sikkerhetskopier i EU. Separate sikkerhetskopier oppbevares i Norge, innenfor EØS.
- Serverlogger omfatter feil, trege spørringer og autentiseringshendelser. Logger oppbevares av hensyn til sikkerhet og ansvarlighet.

Kilder: hrcluster.app/security, punkt 6 og 7

Oppbevaring av e-post og meldinger

HVOR	HVA SOM OPPBEVARES	HVOR LENGE
Postmark (AC PM, LLC), e-postlevering, USA	Meldingsinnhold og metadata. Behandles i USA under standardavtalevilkår (SCC) og, der det er aktuelt, EU-US Data Privacy Framework.	7 dager, oppbevaringsperioden som er satt for HR Clusters Postmark-konto.
Lettermint B.V., e-postlevering, EU	Meldingsinnhold og vedlegg; leverings- og interaksjonshendelser; gjenværende krypterte sikkerhetskopier. Sporing av åpninger og klikk er slått av.	Innhold og vedlegg: 7 dager. Hendelser: inntil 90 dager. Gjenværende krypterte sikkerhetskopier: inntil 14 dager etter aktiv sletting.
I HR Cluster	Meldingsinnhold (teksten og emnet i SMS- og e-postvarsler og i meldinger sendt via plattformen) og leveringsoppføringene for meldingene.	Innhold: fjernes 90 dager etter sending. Leveringsoppføringer: slettes 90 dager etter at sendingen er ferdig.

- Begge e-postleverandørene kan beholde oppføringer på sperrelister, for eksempel adresser som e-post ikke kunne leveres til eller som meldte seg av, lenger enn meldingsinnholdet. Postmark beholder disse oppføringene på ubestemt tid.
- Meldinger som en leverandør tok imot før leverandørens oppbevaringsinnstilling ble endret 19. november 2026, kan fortsatt følge den tidligere perioden: 45 dager for Postmark og 28 dager for Lettermint.

Kilder: hrcluster.app/privacy, punkt 11 og 13; hrcluster.app/subprocessors, punkt 2

Databehandleravtale

- Den standard databehandleravtalen er publisert på hrcluster.app/dpa. Den utgjør en del av kontrakten og supplerer vilkårene for bruk og personvernerklæringen.
- En signert PDF fås på forespørsel: send e-post til privacy@hrcluster.com med navnet på organisasjonen din og dens registrerte adresse. Den returneres vanligvis innen to virkedager.
- Kunder varsles på forhånd om enhver vesentlig endring i underleverandørlisten, vanligvis via e-post til kontoadministratoren.

Kilder: hrcluster.app/subprocessors, punkt 5; hrcluster.app/dpa, punkt 1 og 10

Underleverandører og andre leverandører

LEVERANDØR	FORMÅL	LOKASJON	ROLLE OG VERNETILTAK
Hetzner Online GmbH	Hosting, regnekraft, lagring, sikkerhetskopier, databasereplika	Helsinki, Finland og Nürnberg, Tyskland (EU)	Underleverandør. Data behandles i EU. ISO 27001-sertifisert: dette er Hetzners sertifisering, ikke en som HR Cluster selv har.
Postmark (AC PM, LLC)	Levering av transaksjonell e-post	USA	Underleverandør. Standardavtalevilkår (SCC); EU-US Data Privacy Framework der det er aktuelt.
Lettermint B.V.	Levering av transaksjonell e-post	EU; leveres via mottakerens e-postleverandør	Underleverandør. Data behandles i EU i henhold til Lettermints databehandleravtale.
Google Ireland Limited (Google Analytics)	Bruksanalyse på hrcluster.app, også i den innloggede applikasjonen, og på hrcluster.com	USA / global Google-infrastruktur	Underleverandør. Lastes bare etter samtykke i den aktuelle nettleseren. På hrcluster.app mottar Google sidenavn, aldri sideadresser eller identifikatorer for poster; på hrcluster.com mottar Google den offentlige sideadressen og sidetittelen, kampanjeparametere og henvisende side. Reklamefunksjoner og Google-signaler er slått av; standardavtalevilkår (SCC).
Google Ireland Limited (reCAPTCHA Enterprise)	Beskyttelse mot spam og misbruk på skjemaer for tilbakestilling av passord, på innloggingsskjemaet etter gjentatte mislykkede forsøk, på offentlige skjemaer der kunden har slått det på, på stemplingsterminalen og på kontaktskjemaet på hrcluster.com	USA / Googles globale infrastruktur	Underleverandør. Brukes bare som sikkerhetstiltak, ikke til analyse eller reklame; standardavtalevilkår (SCC); EU-US Data Privacy Framework der det er aktuelt.
46elks AB	Levering av SMS sendt fra plattformen, der den aktuelle funksjonen er aktivert	EU, ifølge 46elks; leveres via mottakerens mobiloperatør	Ikke underleverandør. Selvstendig behandlingsansvarlig, ifølge 46elks, som registrert tilbyder av elektronisk kommunikasjon.
Stripe	Kortbetaling for pakker med SMS-kreditter som kjøpes i plattformen	Irland (EU); også USA og andre steder der Stripe har virksomhet	Ikke underleverandør. Behandler betalingsopplysninger for HR Cluster AS' egen fakturering. Kortopplysninger når aldri HR Clusters servere.

Kilder: hrcluster.app/privacy, punkt 11; hrcluster.app/subprocessors, punkt 2, 3 og 4; hrcluster.app/cookies

Selskap og kontakt

- HR Cluster AS, norsk org.nr. 937 565 690. Personvern: privacy@hrcluster.com. Sikkerhet: security@hrcluster.com.
- Databehandleravtalen er underlagt norsk rett. Tilsynsmyndigheten som er nevnt i personvernerklæringen, er Datatilsynet.

Kilder: hrcluster.app/security, punkt 11; hrcluster.app/privacy, punkt 17; hrcluster.app/dpa, punkt 2 og 9