Sikkervarsling.no

GJELDENDE TEKNISK WHITEPAPER

FRA FØRSTE URO TIL DOKUMENTERT OPPFØLGING

Trygg teknologi. Lavere terskel. Bedre prosess.

En detaljert beskrivelse av tjenestemodell, varslingsløp, støtte til varsler og virksomhet, sikkerhetsmekanismer, modenhet og anbefalt kommersiell modell.

DOKUMENT
SV-WHITEPAPER-2026-07

DATERT
20. juli 2026

TEKNISK GRUNNLAG
Sikkervarsling produksjonsgrunnlag

DOKUMENTETS ROLLE

Hva dette whitepaperet dokumenterer

Sikkervarsling er utviklet for å gjøre det enklere å si ifra, tryggere å følge opp og vanskeligere å gi flere personer tilgang enn saken krever. Dokumentet beskriver både den tekniske motoren og den menneskelige tjenestemodellen rundt den.

Dokumentert mot faktisk løsning

Funksjonene i dette dokumentet finnes i kildekoden og inngår i automatiserte, syntetiske eller nettleserbaserte kontroller. Før inntaket åpnes for reelle saker skal den uavhengige sikkerhetsgjennomgangen bekrefte at personvern- og kryptografikontrollene virker som beskrevet.

3

DEFINERTE VARSLINGSLØP

Fortrolig formidling, dobbelt anonym sikker innboks og vanlig varsel.

0 kr

FOR VARSLEREN

Ingen skal måtte betale for å forstå, formulere, sende eller følge opp et varsel.

2FA

FOR VIRKSOMHETSMOTTAK

Personlige kontoer med obligatorisk TOTP før tilgang til saksinnhold.

Kort konklusjon

Sikkervarslings sterkeste kommersielle idé er kombinasjonen av gratis varslerlos, lokal forberedelse før innsending, flere tydelige personvernmodeller, saksavgrenset tilgang for virksomheten og et beskyttelsesspor som fortsetter etter at varselet er levert. Den undersøkte markedskombinasjonen er særpreget; hvert enkelt element finnes også i andre løsninger.

INNHOLDSFORTEGNELSE

Finn riktig detaljnivå

BRUKSRAMME

Whitepaperet er produkt- og systemdokumentasjon. Det erstatter ikke juridisk rådgivning, virksomhetens varslingsrutine, DPIA, databehandleravtale, beredskapsplan eller konkret vurdering av kontradiksjon og innsyn i den enkelte saken.

KAPITTEL 1

Formål og designprinsipper

En varslingskanal må både beskytte mennesker og gjøre ansvarlig oppfølging mulig.

1.1 Formålet

Sikkervarsling skal hjelpe en person å forstå situasjonen, formulere et ryddig varsel, velge riktig grad av identitetsskjerming og følge opp det som skjer videre. Samtidig skal virksomheten få et avgrenset, dokumenterbart arbeidsrom for mottak, vurdering, undersøkelse og tilbakemelding.

1.2 Fem styrende prinsipper

Trygg første avklaring.

Veiviseren hjelper varsleren å skille type bekymring, egne observasjoner og mulige neste steg uten å avsi en juridisk eller faktisk konklusjon.

01

Varsleren først

Hjelp før innsending er ikke betinget av at arbeidsgiveren er kunde.

02

Minst mulig data

Forberedelsen forblir lokal til brukeren aktivt velger mottaker og bekrefter sending.

03

Minste privilegium

Virksomhetsbrukere får bare de sakene rollen og den konkrete tildelingen krever.

04

Lavest forsvarlige eskalering

Prosessen skal støtte avklaring og tidlig løsning uten å redusere alvorlige forhold til en uformell samtale.

05

Ettervern

Levering er starten på oppfølgingen, ikke slutten på tjenesten.

1.3 Tjenesten avgjør ikke saken

Motoren kategoriserer ikke automatisk om et forhold juridisk er et varsel, avgjør ikke om en påstand er sann, rangerer ikke varslerens troverdighet og fatter ikke automatiserte personalavgjørelser. Klassifisering, risikonivå og foreslåtte beskyttelsestiltak er strukturering og beslutningsstøtte.

KAPITTEL 2

Det som skiller Sikkervarsling

Det særpregede ligger i sammenhengen mellom støtte, personvern, overlevering og oppfølging.

2.1 En hel prosess – ikke bare et skjema

1 Sortere
Hva gjelder bekymringen?

→

2 Formulere
Fakta, observasjon og ønsket handling.

→

3 Beskytte
Identitetsnivå og tiltak mot gjengjeldelse.

→

4 Levere
Lokalt, via Sikkervarsling eller direkte.

→

5 Behandle
Riktig og habil mottaker.

→

6 Følge opp
Status, tidslinje og kontrollpunkter.

2.2 Særpreget kombinasjon

Element	Praktisk verdi	Teknisk status
Gratis varslerlos	Den som vurderer å si ifra får hjelp uavhengig av arbeidsgiverens avtale.	Implementert grunnflyt
Lokal forberedelse og lokal varselpakke	Brukeren kan forberede og ta med seg dokumentet uten serverinnsending.	Implementert og testet
Valg av første mottaker	Direkte kundemottak eller Sikkervarsling først.	Implementert
Saksavgrenset virksomhetstilgang	En ikke-kunde kan åpne én sak med innholdsfri lenke og separat telefonkode.	Implementert og testet
Dobbelt anonym overlevering	Ingen identitet oppgis, og nye meldinger etter overleveringen kan bare dekrypteres av varsleren og virksomhetens sikre innboks.	Implementert og testet
Vern og oppfølging etter innsending	Støtter forebygging, private kontrollpunkter og rask hjelp ved mulige negative reaksjoner.	12 varslerverktøy implementert

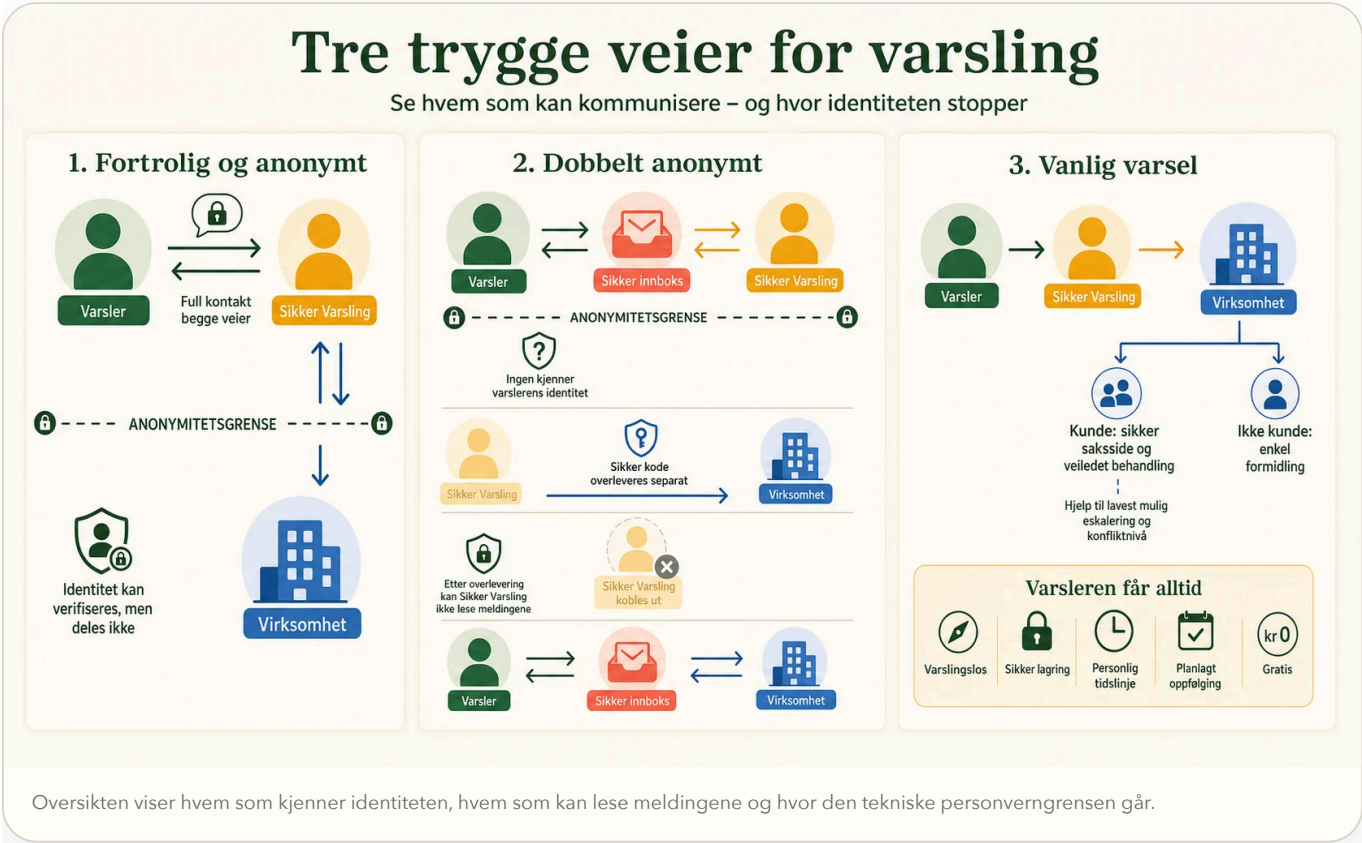
Dokumenterbar USP

Blant løsningene som ble gjennomgått i juli 2026, fant vi ikke en annen offentlig dokumentert tjeneste som kombinerer gratis individuell varslerlos, lokal forberedelse uten innsending, gratis enkel overlevering til ikke-kunde, tre eksplisitte anonymitetsarkitekturer og innebygd ettervern i én sammenhengende modell.

KAPITTEL 3

De tre varslingsløpene

Hvert løp har en annen tillitsmodell og en annen grense for hvem som kan vite hva.



Oversikten viser hvem som kjenner identiteten, hvem som kan lese meldingene og hvor den tekniske personverngrensen går.

3.1 Fortrolig og anonymt overfor virksomheten

01

Sikkervarsling kjenner varsleren – virksomheten gjør det ikke

Varsleren kan ha full dialog med et autorisert mottak. Navn og kontakt lagres autentisert kryptert i et eget kontaktfelt, fysisk adskilt fra saksinnholdet virksomheten kan motta. Ved formidling tømmes identitetsfeltene defensivt en gang til.

- Passer når arbeidsforholdet bør kunne verifiseres.
- Gir mulighet for menneskelig støtte og avklaring før formidling.
- Virksomheten mottar bare et avklart saksinnhold uten navn eller e-post.

Implementert og testet Regresjonstesten kontrollerer både kryptert kontaktlager, formidlet kundepayload og fravær av navn/e-post i rådatabaseklartekst.

Identitetsvern og riktig mottaker.

I det fortrolige løpet kan Sikkervarsling kjenne varsleren og samtidig stoppe identiteten ved grensen mot virksomheten. Identitetsdata og saksinnhold må derfor behandles som to adskilte informasjonsområder.

3.2 Dobbelt anonymt

02

Sikker innboks er bindeleddet – ingen kjenner varslerens identitet

Varsleren kommuniserer gjennom en tilfeldig sikker innboks. Sikkervarsling kan lese den opprinnelige saken i første fase, men mottar ingen identitet. Ved overlevering oppretter virksomhetens nettleser et eget RSA-OAEP-nøkkelpar. Varsleren godkjenner nøkkelfingeravtrykket og pakker samtalens tilfeldige AES-GCM-romnøkkel til virksomhetens offentlige nøkkel. Nye meldinger lagres bare som kryptert innhold.

- Varsleren beholder en toveis kanal uten navn, e-post eller telefon.
- Virksomheten kan be om presiseringer direkte i den sikre innboksen.
- Sikkervarsling kan ikke dekryptere den videre dialogen fordi romnøkkelen ikke finnes på serveren.
- En part kan blokkere dialogen eller frivillig dele én bestemt melding ved misbruksrapportering.

Implementert og testet Inntaket holdes stengt frem til den uavhengige sikkerhetsgjennomgangen har kontrollert nøkkellivsløp og nettlesertrusler.

Toveis uten identitetsdeling.

Illustrasjonen viser tillitsmodellen. I løsningen beskyttes meldingene med AES-GCM, mens virksomhetens romnøkkel overleveres med RSA-OAEP og et synlig nøkkelfingeravtrykk.

3.3 Vanlig varsel

03

Varsleren leverer via Sikkervarsling – virksomheten overtar behandlingen

Varsleren velger selv identitetsnivå og leverer varselet. En kundebedrift kan få saken direkte i sitt mottak. Når virksomheten ikke er kunde, kan Sikkervarsling kontrollere en habil mottaker og formidle saken med en innholdsfri lenke og separat telefonkode.

- I kundesaker får både varsleren og virksomheten trinnvise tips, sjekklister, meldingsmaler og kontrollpunkter.
- Kundebedriften får portal, tildeling, habilitet, status og dokumentert dialog.
- Ikke-kunden får en enkel, saksavgrenset side uten tvungen systeminnføring.
- Varsleren beholder statusadgang og 12 varslerrettede verktøy uavhengig av om virksomheten er kunde.

Implementert og testet Den tosidige prosesshjelpen tilpasser innholdet etter saksstatus og opplevd risiko.

Anonymitet er mer enn et navn-felt

Identitet og direkte digitale spor kan skjermes teknisk. Innhold, tidspunkt, rolle, avdeling eller en liten personkrets kan likevel gi indirekte holdepunkter. Tjenesten må derfor kombinere teknisk anonymitet med konkret innholdsveiledning.

KAPITTEL 4

Hjelpen varsleren får

Gratis støtte før, under og etter varsling reduserer terskelen og forbedrer informasjonskvaliteten.

4.1 Før innsending

Varslerlosen

- Skiller mellom lovbrudd/fare, arbeidsmiljø, etikk og usikker kategori.
- Forklarer at kategorien ikke avgjør rettighetene.
- Veileder i å skille observasjoner fra vurderinger.
- Strukturerer tidspunkt, dokumentasjon og ønsket oppfølging.
- Viser akuttveiledning ved høy opplevd risiko.

Kontroll før deling

- Forberedelsen ligger i nettleserøkten før aktiv sending.
- Brukeren kan laste ned en lokal varselpakke.
- Originaldokumenter beholdes hos varsleren til en sikker kanal og riktig mottaker er avklart.
- Mottaker og leveringsmåte vises før bekreftelse.
- Navn og e-post er ikke nødvendig ved anonymt løp.

4.2 Under innsending

Valg	Hva varsleren kontrollerer	Teknisk virkning
Identitetsnivå	Anonym, fortrolig eller i eget navn.	Anonyme saker lagrer ikke navn/e-post i saksinnholdet.
Beskyttelsesønsker	Begrenset identitetsdeling, fast kontakt, støtteperson og vurdering av gjengjeldelsesfare.	Strukturerte felter følger den krypterte saken.
Første mottaker	Lokal pakke, Sikkervarsling først eller registrert kunde direkte.	Serveren avviser ukjent mottakerkode og krever aktiv bekreftelse.
Oppfølgingsnøkkel	QR med separat PIN, QR uten PIN eller manuelle koder.	Rå QR-token/PIN lagres ikke i databasen.

4.3 Etter innsending

Oppfølging over tid.

Saksreferanse, sikker tilgang, status og avtalte kontrollpunkter skal gjøre det mulig å følge fremdriften, forebygge gjengjeldelse og reagere raskt dersom varsleren opplever negative handlinger etter varslingen.

1. **Kvittering**
   Varsleren får saksreferanse og hemmelig tilgangsmekanisme.
2. **Status**
   Mottatt, bekreftet, vurderes, undersøkes, følges opp eller avsluttet.
3. **Melding**
   Virksomheten eller Sikkervarsling kan gi en kryptert statusmelding tilbake.
4. **Vern mot gjengjeldelse**
   En privat tidslinje og planlagte kontrollpunkter hjelper varsleren å oppdage og dokumentere endringer. Virksomheten minnes om å vurdere forebyggende tiltak og følge opp arbeidsmiljøet.

KAPITTEL 5

Hjelpen virksomheten får

Riktig mottaker, tydelige roller og rolig fremdrift gjør det enklere å håndtere alvorlige opplysninger forsvarlig.

5.1 Saksavgrenset grunnmottak

1. Kontrollert mottaker

Sikkervarsling finner et offentlig verifiserbart kontaktpunkt og kontrollerer hvem som er habil til å motta.

TO KANALER

2. Saksavgrenset tilgang

En innholdsfri e-postlenke kombineres med en sekssifret kode gitt separat på telefon.

Mottakeren åpner én saksavgrenset visning og kan bekrefte mottak, velge status, beskrive neste steg og avslutte saken. Grunnløpet fungerer uten virksomhetskonto eller installasjon.

5.2 Kunde: fast mottak og organisatorisk kontroll

ADMIN

Administrator

Ser ufordelte saker, oppretter mottakere, tildeler og fjerner tilgang.

SAK

Saksbehandler

Ser bare tildelte saker og kan oppdatere status og melding.

LES

Lesetilgang

Ser bare tildelte saker og kan ikke endre saksstatus.

5.3 Tosidig prosesshjelp i kundesaker

Rolig saksbehandling.

Mottakeren ledes til å skille påstand, undersøkelse og beslutning, samtidig som habilitet, beskyttelse og neste oppdatering får egne kontrollpunkter.

Saksteg	Hjelp til varsleren	Hjelp til virksomheten	Felles mål
Mottak	Hva skjer nå, hva kan forventes, og hvordan brukes den private tidslinjen?	Bekreft mottak, kontroller habilitet, avgrens tilgang og angi neste oppdatering.	Trygg start uten forhastede konklusjoner.
Avklaring	Skill egne observasjoner, dokumenterte opplysninger og antakelser. Svar på nøytrale presiseringsspørsmål.	Lag en undersøkelsesplan, still åpne spørsmål og skill varsel, påstand og bevist faktum.	Bedre informasjonskvalitet og mindre misforståelse.
Undersøkelse	Følg status, suppler trygt og få råd om hva som bør dokumenteres.	Bruk sjekkliste for habilitet, konfidensialitet, kontradiksjon og forholdsmessig undersøkelse.	Forsvarlig fremdrift med minst mulig unødig belastning.
Tiltak og svar	Forstå hva statusen betyr, hva som kan deles og hvilke muligheter som finnes videre.	Skill funn, vurdering og tiltak; gi en forståelig status uten å dele opplysninger virksomheten må skjerme.	Raskere avklaring og mindre konflikt.
Oppfølging	Kontrollpunkter og privat logg for endringer i arbeidssituasjonen.	Vurder forebyggende tiltak mot gjengjeldelse og følg opp arbeidsmiljøet for alle involverte.	Varig løsning og tidlig reaksjon på nye problemer.

- ✓ **Råd når de trengs:** hjelpen vises underveis i saken, i stedet for som et stort regelverk brukeren må lete i.
- ✓ **Maler som senker temperaturen:** forslag til mottaksbekreftelse, presiseringsspørsmål, neste steg og statusoppdatering bruker et nøytralt språk.
- ✓ **Tydelige grenser:** veiledningen støtter prosessen, men avgjør ikke om påstanden er sann, gir ikke juridisk godkjenning og overtar ikke arbeidsgiverens ansvar.
- ✓ **Bredere arbeidsmiljøkartlegging:** AMIQ kan brukes dersom virksomheten vil undersøke om flere er berørt. Opplysninger fra varslingssaken blir ikke overført.

5.4 Interaktiv beredskap og tilpasset kundereise

Virksomhetssiden lar beslutningstakeren velge situasjon, virksomhetsstørrelse og beredskapsstatus. Svarene behandles lokalt i nettleseren og gir en tilpasset plan i tre tydelige kolonner.

Virksomheten må ivareta	Sikkervarsling hjelper med	Virksomheten trenger ikke
Undersøkelse innen rimelig tid, vern mot gjengjeldelse, forsvarlig arbeidsmiljø, beslutninger og personvernansvar.	Sikker kanal, riktig mottaker, habilitet, minste tilgang, rollebasert saksstøtte, status og dokumenterte neste steg.	Konkludere ved mottak, avvise anonyme varsel, spre saken bredt eller etablere full portal for å følge opp én saksavgrenset henvendelse.

Etter innlogging endres saksstøtten med statusen: mottatt, bekreftet, innledende vurdering, undersøkelse, oppfølging eller avsluttet. Hvert steg viser prioriterte handlinger, en viktig avgrensning og et redigerbart forslag til statusmelding.

Målet med hjelpen

En kundesak skal få raskere avklaring, lavere konfliktnivå og mindre økonomisk og omdømmemessig belastning for de involverte og virksomheten. Det betyr ikke minst mulig alvor eller svakere undersøkelse. En blokkert rømningsvei kan ofte rettes raskt; trakassering, økonomiske misligheter eller alvorlig fare krever et grundigere og mer uavhengig løp.

KAPITTEL 6

Komplett funksjonsoversikt

En etterprøvbar katalog over funksjonene som inngår i løsningen.

Område	Funksjon	Status
Varslerflate	Femstegs veiviser og lokal øktlagring	**Implementert**
	Lokal varselpakke uten serverinnsending	**Implementert**
	Anonym, fortrolig og navngitt innsending	**Implementert og testet**
	Beskyttelsesvalg og risikoskala	**Implementert**
	QR + valgfri separat PIN og manuelle koder	**Implementert**
	QR-rotasjon og sperring av gammel nøkkel	**Implementert**
	Dobbelt anonym toveis meldingshistorikk	**Implementert og testet**
	Personlig tidslinje, ettervern og 12 varslerverktøy	**Implementert og statustilpasset**
Levering	Direkte til aktiv kundekode	**Implementert og testet**
	Sikkervarsling som første mottaker	**Implementert og testet**
	Enkeltmottak med innholdsfri lenke + telefonkode	**Implementert og testet**
	Nøytral attest for identitet/arbeidsforhold	**Valgfri og kryptografisk kontrollert**
	Dobbelt anonym innboksoverlevering	**Implementert og testet**
Virksomhetsmottak	Personlige kontoer og påtvunget passordbytte	**Implementert**
	Obligatorisk TOTP og åtte gjenopprettingskoder	**Implementert**
	Administrator, saksbehandler og leser	**Implementert**
	Saksvis tildeling og tilbakekalling	**Implementert**
	Permanent habilitetsfratreden per sak	**Implementert**
	Status, kryptert melding og statustilpasset veiledning	**Implementert**
	17 lagrede virksomhetsverktøy med frister og oppfølging	**Implementert og statustilpasset**

Område	Funksjon	Status
Drift	Global stoppbryter for nye saker	**Implementert**
	Ratebegrensning med HMAC-pseudonymisert IP-nøkkel	**Implementert**
	Retensjonsjobb med tørrkjøring	**Implementert med kontrollert policy**
	Konsistent backup med manifest, HMAC og integritetstest	**Implementert og øvelsestestet**
	Revisjon uten rå IP og uten saksinnhold i loggen	**Implementert**
	Innholdsfrie mottakerlenker og separat telefonkode	**Implementert og testet**

KAPITTEL 7

Teknisk arkitektur og dataflyt

En liten, forståelig arkitektur reduserer angrepsflate og gjør kontrollene etterprøvbare.

7.1 Lagmodellen

NETTLESER

Lokal veiviser

Forberedelse i `sessionStorage`, lokal QR-generering og lokal varselpakke.

HTTPS + CSP

APPLIKASJON

PHP 8 API

Validering, CSRF, ratebegrensning, roller, økter og tjenestebryter.

Autentisert kryptering

DATA

Privat SQLite

Kryptert saksinnhold, separate tilgangstabeller, revisjon og kontrollstatus.

CLI-only

DRIFT

Operatørverktøy

Formidling, kontroll, backup, retensjon og tjenestestyring utenfor webroot.

7.2 Data som holdes adskilt

Datasett	Innhold	Adskillelse
Saksinnhold	Kategori, beskrivelse, identitetsvalg, beskyttelse, risiko og eventuell sanitert verifikasjon.	Én autentisert kryptert payload uten fortrolig kontakt.

Datasett	Innhold	Adskillelse
Fortrolig varslerkontakt	Navn og valgfri e-post når varsleren ønsker kontakt med Sikkervarsling.	Eget autentisert kryptert felt, avgrenset til mottaket og aldri med i virksomhetens payload.
Oppfølgingsadgang	HMAC av manuell kode eller QR-token; eventuell PIN som passordhash.	Ingen rå hemmelighet i databasen.
Virksomhetsadgang	Bruker, rolle, passordhash, kryptert MFA-hemmelighet og sesjonsversjon.	Separate tabeller og saksvis autorisasjon.
Revisjon	Handling, tid, bruker og pseudonym øktfingeravtrykk.	Ingen rå IP, token eller saksfritekst.
AMIQ-interesse	Virksomhetskontakt og ønsket kartlegging.	Separat kryptert tabell uten saksreferanse.
Dobbelt anonym dialog	Offentlig virksomhetsnøkkel, kryptert privatnøkkel, pakket romnøkkel, IV, chiffertekst og minimale meldingsmetadata.	Serveren mottar ikke romnøkkel eller meldingsklartekst. Frivillig misbruksdeling lagres separat og kryptert.

7.3 Nøkkelprinsipp

Saksinnhold krypteres med PHP Sodium `secretbox`, en autentisert symmetrisk krypteringsmekanisme med en tilfeldig 24-byte nonce og 256-bit nøkkel. Applikasjonsnøkkelen brukes også til domeneavgrensede HMAC-er. Nøkkelen ligger utenfor offentlig webrot og databasefilen har restriktiv filmodus.

7.4 Separat nøkkelmodell for dobbelt anonym dialog

Den opprinnelige saken og den videre dialogen har forskjellige kryptografiske tillitsmodeller. Den opprinnelige saken kan åpnes av autorisert operatør før overlevering. Den videre dialogen krypteres i nettleseren med en tilfeldig AES-GCM-romnøkkel. Virksomhetens nettleser lager et RSA-OAEP-nøkkelpar og krypterer privatnøkkelen lokalt med en separat gjenopprettingshemmelighet. Serveren lagrer bare chiffertekst, offentlig nøkkel, kryptert privatnøkkel og romnøkkelen pakket til den offentlige nøkkelen.

Kontrollert restrisiko

Server og applikasjonsnøkkel må aldri oppbevares i samme backup. Løsningen bruker separat offsite nøkkelkopi, integritetskontroll og gjenopprettingsøvelse. Den uavhengige gjennomgangen skal kontrollere denne grensen og vurdere videre nøkkelseparasjon ved økt volum.

KAPITTEL 8

Sikkerhetsmekanismer

Kontroller legges i flere lag slik at ett enkelt feilpunkt ikke alene skal gi bred sakstilgang.

8.1 Konfidensialitet

01

Kryptert saksinnhold

Autentisert `secretbox`-kryptering før lagring.

02

Ingen rå adgangskoder

Tilgangskoder og invitasjonstokener lagres som HMAC; PIN og passord som passordhash.

03

Lokal QR

QR-bildet genereres i nettleseren uten ekstern QR-tjeneste.

04

Ingen tredjepartssporing

CSP tillater bare egne ressurser; ingen analyse- eller markedsføringsskript.

05

Nettleserkryptert dialog

AES-GCM-meldinger og RSA-OAEP-overlevering gjør at serveren ikke kan lese den videre dobbelt anonyme samtalen.

8.2 Tilgangskontroll

06

Obligatorisk MFA

TOTP kreves før virksomhetsmottak kan lese saker.

07

Saksvis minste privilegium

Ikke-administratorer ser bare aktivt tildelte saker.

08

Éngangsinvitasjon

Lenke og separat telefonkode åpner én sak og kan bare brukes én gang.

09

Øktgrenser

Inaktivitet og absolutt levetid håndheves for følsomme økter.

8.3 Integritet og misbruksvern

- ✓ **CSRF:** skrivende API-kall krever serverutstedt token.
- ✓ **Ratebegrensning:** innsending, sporing og innlogging begrenses per tidsvindu uten rå IP i tabellen.
- ✓ **Revisjon:** innlogging, visning, oppdatering, tildeling og habilitetsfratreden logges med pseudonym øktfingeravtrykk.
- ✓ **Replayvern:** TOTP-trinn kan ikke brukes på nytt; ekstern attest har HMAC-beskyttet gjenbruksregister.
- ✓ **Selektiv misbruksdeling:** operatøren får ikke generell lesetilgang til E2E-dialogen. En part må selv velge og bekrefte deling av den konkrete meldingen som rapporteres.
- ✓ **Blokkering:** begge parter kan stenge den dobbelt anonyme dialogen, og serveren avviser nye meldinger etter blokkering.
- ✓ **Sikkerhetsheadere:** HSTS, CSP med `object-src 'none'`, `frame-ancestors 'none'`, `Referrer-Policy: no-referrer` og restriktiv Permissions Policy.
- ✓ **Fail-closed:** ny database eller manglende tjenestekontroll betyr stengt inntak til eksplisitt åpning.

8.4 QR-nøkkelens sikkerhetsmodell

QR-tokenet er tilfeldig 256-bit data i URL-fragmentet. Fragmentet sendes normalt ikke som del av HTTP-forespørselen, og klienten fjerner det fra adresselinjen før første API-kall. Serveren lagrer bare HMAC av tokenet. Separat PIN anbefales fordi QR-bildet alene ellers er en bærernøkkel.

KAPITTEL 9

Identitet, tilgang og habilitet

Identitet er et eget risikoområde – ikke bare et felt i varselet.

9.1 Tre identitetsnivåer

Nivå	Hvem kjenner identiteten?	Bruk
Anonym	Ingen identitet lagres i den krypterte saken.	Når skjerming veier tyngst og dialog kan skje pseudonymt.
Fortrolig	Sikkervarslings mottak kan kjenne identiteten. Kontakt lagres kryptert og separat og følger aldri saken til virksomheten.	Når kontroll eller støtte krever kjent identitet, men virksomheten ikke skal få den.
I eget navn	Navn følger saken til valgt mottaker.	Når varsleren ønsker direkte og identifisert oppfølging.

9.2 Nøytral verifikasjon

Løsningen kan lagre en sanitert opplysning om at identitet og eventuelt arbeidsforhold er kontrollert, uten å lagre legitimasjon, fødselsnummer, arbeidsavtale eller kontrollkode i saken. En ekstern attest kan signeres med Ed25519 og bindes til virksomhet, kort levetid og engangskontroll. Attesten bekrefter tilknytning – aldri at påstanden er sann.

9.3 Habilitetsvern

Virksomhetsmottakeren kan erklære standardisert konfliktgrunn. Systemet fjerner da aktiv tildeling, registrerer hendelsen og sperrer ny tildeling av samme bruker i saken. Dette støtter prinsippet om habil behandling, men virksomheten må fortsatt ha en navngitt stedfortreder og prosedyre når administrator eller ledelse er berørt.

Konfidensialitet og kontradiksjon må balanseres

Arbeidstilsynet beskriver konfidensialitet, habilitet og kontradiksjon som grunnleggende prinsipper. Den omvarslede kan ha rett til informasjon og til å imøtegå opplysninger, samtidig som varsleridentiteten ikke skal spres mer enn nødvendig. Det krever konkret saksbehandling – ikke én universell automatisk regel.

KAPITTEL 10

Lagring, sletting, backup og hendelser

Sikker drift handler like mye om livsløpet etter lagring som om kryptering ved mottak.

10.1 Retensjon

Retensjonsverktøyet kjører som standard i tørrmodus. Det kan slette lukkede saker etter valgt frist, fjerne rå saksreferanse fra mottakerrevisjonen og bevare en HMAC-pseudonymisert slettekvittering. SQLite `secure_delete` og WAL-checkpoint brukes for å redusere rester i databasefilen.

> **Frister styres av behandlingsformålet**
>
> Standardpolicyen bruker 365 dager etter lukking for saker og 90 dager for separate AMIQ-henvendelser. Virksomheten dokumenterer eventuelle avvik i behandlingsprotokoll, kundeavtale og legal-hold-prosedyre.

10.2 Backup

1 — Konsistent kopi
`VACUUM INTO` produserer snapshot.

→

2 — Manifest
Filnavn, størrelse og SHA-256.

→

3 — HMAC
Manifestet autentiseres med servernøkkelen.

→

4 — Verifikasjon
Integritet og dekrypterbarhet kontrolleres.

Backupopplegget omfatter kryptert offsite-lagring, separat nøkkelkopi, autentisert manifest og automatisert kontroll av integritet og dekrypterbarhet. Gjenoppretting inngår i driftsøvelsen.

10.3 Hendelsesbryter

Nye varslingssaker kan stanses uten å stenge oppfølgingen av eksisterende saker. Pausen lagres med begrunnelse uten saksinnhold. Lokale varselpakker skal fortsatt kunne lages mens inntaket er stengt.

KAPITTEL 11

Personvern og norske rammer

Produktet skal støtte virksomhetens plikter, men kan ikke overta det juridiske ansvaret gjennom programvare alene.

11.1 Varslingsrutinen

Arbeidsmiljøloven § 2 A-6 krever skriftlige rutiner for virksomheter som jevnlig har minst fem arbeidstakere, og også i mindre virksomheter når forholdene tilsier det. Rutinen skal utarbeides sammen med arbeidstakerne og deres tillitsvalgte og beskrive oppfordring, fremgangsmåte og arbeidsgivers behandling og oppfølging.

11.2 Rollemodell

Flyt	Rollemodell	Dokumentasjon
Direkte kundelevering	Kunden er normalt behandlingsansvarlig; Sikkervarsling teknisk databehandler for kundens instruks.	Kundeavtale, databehandleravtale, underleverandører og behandlingsprotokoll.
Sikkervarsling først	Sikkervarsling er selvstendig behandlingsansvarlig frem til kontrollert overføring; arbeidsgiver er ansvarlig for egen videre behandling.	Eget behandlingsgrunnlag, personverninformasjon, overføringspunkt og rettighetsprosedyre.
Dobbelt anonymt	Rollen følger lesetilgangen i hver fase: Sikkervarsling behandler første innsending, mens partenes videre dialog er ende-til-ende-kryptert.	Rollebeskrivelse, DPIA og dokumentert nøkkel- og tilgangsmodell.

11.3 DPIA

Sakene kan inneholde opplysninger om helse, fagforening, straffbare forhold, trakassering og andre opplysninger med høy konsekvens. DPIA-en følger derfor hele behandlingsløpet. Rettsgrunnlag etter artikkel 6, eventuelt artikkel 9 og 10, fastsettes per aktør og behandling.

11.4 Arbeidsgivers ansvar består

Arbeidsgiveren skal undersøke innen rimelig tid, følge opp også anonyme varsler, beskytte mot gjengjeldelse og sikre forsvarlig arbeidsmiljø for både varsler og andre involverte. Sikkervarsling kan gi struktur, spor og sikker kanal; den kan ikke automatisk oppfylle aktivitetsplikten på virksomhetens vegne.

KAPITTEL 12

Testbevis og modenhet

Påstander bindes til konkrete kontroller, ikke bare til ønsket funksjon.

12.1 Syntetisk ende-til-ende-bevis

Den lokale testpakken har bestått direkte kundeløp, Sikkervarsling-først, dobbelt anonym nettleserdialog, passordbytte, TOTP, mottak, statusmelding, avslutning, varsleroppfølging, sletting og databaseintegritet med kun syntetiske data.

Kontroll	Dokumentert resultat	Videre kontroll
Direkte kundeløp	Kunden får saken; operatørverktøyet avviser direkte sak.	Løpende driftskontroll av mottakerregisteret.
Fortrolig formidling	Kontakt krypteres separat; navn og e-post følger ikke kundepayloaden og finnes ikke i rådatabaseklartekst.	Uavhengig gjennomgang av hele identitetsgrensen.
Dobbelt anonym dialog	Bedriftens QR + PIN, nøkkelfingeravtrykk, RSA-OAEP-pakket romnøkkel, AES-GCM-meldinger begge veier, frivillig misbruksdeling og blokkering. Databasen inneholder ikke romnøkkel eller meldingsklartekst.	Uavhengig kryptografisk og nettleserteknisk gjennomgang.
Retensjon og backup	Lukkede saker slettes med pseudonym kvittering; offsite backup, separat nøkkelkopi og dekrypteringskontroll inngår i testpakken.	Periodisk gjenopprettingsøvelse.
Brukerflater	Mobil og desktop er klikketestet for alle sentrale valg, overflyt, tilgjengelige navn og JavaScript-feil.	Regresjonstest ved hver utgivelse.

12.2 Siste produksjonsport

PORT Uavhengig sikkerhetsgjennomgang uten åpne kritiske eller høye funn.

Kontrollert åpning

Nye varslingssaker holdes stengt med tjenestens fail-closed-bryter frem til den uavhengige kontrollen er godkjent. Eksisterende oppfølging og lokale varselpakker fungerer også mens inntaket er stengt.

KAPITTEL 13

Hva som er gratis – og hvorfor

Betaling skal finansiere beredskap og kvalitet, ikke skape en terskel for å si ifra.

13.1 Alltid gratis for varsleren

0 kr

Varsleren betaler aldri

Varslerlos, lokal varselpakke, innsending, sikker oppfølgingsadgang, grunnleggende status og varslerrettet veiledning skal være gratis.

Begrunnelsen er både etisk og kommersiell: betaling fra en person i et mulig makt- eller avhengighetsforhold reduserer bruken, svekker tillit og gjør tjenesten mindre verdifull også for arbeidsgiveren. Virksomheten har størst økonomisk nytte av tidlig oppdagelse og bør finansiere infrastrukturen.

13.2 Gratis saksavgrenset grunnmottak

Når et varsel allerede finnes, kan virksomheten motta én saksavgrenset lenke, bekrefte mottak og gi en enkel status. Det gir rask oppfølging også når virksomheten ikke har etablert en fast kanal på forhånd.

13.3 Dette finansieres av virksomheten

- ✓ Fast, direkte varslingskanal med virksomhetens mottakerkode.
- ✓ Flerbrukerportal, roller, MFA, saksfordeling og habilitetsspor.
- ✓ 29 lagrede og statustilpassede verktøy for varsler og virksomhet.
- ✓ Dokumentert onboarding, årlig øvelse, rutinemaler og kontroll av mottak.
- ✓ Menneskelig første mottak, prosessbistand, fasilitering og eventuell ekstern utredning.

KAPITTEL 14

Anbefalt prismodell

En tydelig norsk SMB-pris under de tyngste løsningene, uten å underprise sikker drift og menneskelig ansvar.

Kommersiell prismodell

Abonnement faktureres årlig. Månedsbeløpet gjør sammenligningen enkel, mens menneskelig bistand prises separat og forutsigbart.

START

kr 490/mnd

kr 5 880 per år eks. mva.

1–49 ansatte

- Direkte sikker kanal
- Én juridisk enhet
- Administrator + to mottakere
- MFA, tildeling og habilitet
- Standard rutinepakke

STANDARD

kr 990/mnd

kr 11 880 per år eks. mva.

50–249 ansatte

- Alt i Start
- Inntil ti mottakere
- Utvidet onboarding
- Årlig syntetisk mottaksøvelse
- Prioritert støtte

PROFESJONELL

kr 1 990/mnd

kr 23 880 per år eks. mva.

250–999 ansatte

- Alt i Standard
- Flere mottaksgrupper
- Utvidet revisjon/eksport
- Navngitt kontaktperson
- Tilpasset øvelse og SLA

14.1 Enterprise og konsern

Fra kr 3 490 per måned, priset etter antall juridiske enheter, integrasjoner, SSO, databehandlerkrav, språk, beredskap og responstid.

14.2 Oppstart

Tjeneste	Anbefalt pris	Innhold
Standard digital oppstart	Inkludert ved årlig betaling	Mottakere, kanal, standard rutinepakke og 60 min opplæring.
Tilpasset implementering	kr 4 900	Rolleverksted, rutinetilpasning, test, kommunikasjonsplan og dokumentert overlevering.

Tjeneste	Anbefalt pris	Innhold
Ekstra juridisk enhet	fra kr 290/mnd	Eget mottak, roller og rapporteringsgrense.

14.3 Menneskelig bistand

Tjeneste	Anbefalt pris	Avgrensning
Uavhengig første mottak	kr 1 490/mnd + kr 1 900 per åpnet sak	Mottak, habilitetskontroll, første risikovurdering, bekreftelse og sikker ruting. Ikke undersøkelse.
Prosess-start	kr 3 900 per sak	90 minutters oppstart, prosesskart, roller, frister og beskyttelsespunkter.
Veiledet saksbehandling	kr 1 950 per time	Prosessstøtte, dokumentstruktur og møtestøtte. Ikke juridisk konklusjon.
Ekstern utredning	Tilbud etter mandat	Eget habilitetskontrollert oppdrag, separat avtale og kvalifisert fagperson.

Hvorfor disse nivåene?

Startprisen ligger over de enkleste selvbetjeningskanalene og under flere fullverdige norske/internasjonale løsninger. Standard følger et synlig norsk markedsnivå. Menneskelig arbeid prises separat, slik at uforutsigbare saker ikke underfinansieres eller skjules i et for lavt abonnement.

KAPITTEL 15

Markedsgrunnlag og posisjonering

Prisforslaget er kontrollert mot offentlig tilgjengelige priser 20. juli 2026.

Løsning	Offentlig priseksempel	Kommentar
Whitenoise Anonym varsling	Fra kr 200/mnd; «ubegrenset» kr 500	Lavpris, selvbetjent og ende-til-ende-kryptert kanal.
HMSVarsling	kr 599/mnd for 5–49; 990 for 50–249; 1 990 konsern; oppsett 4 990	Norsk modulplattform; ekstern enkeltsak oppgitt til 6 900.
MittVarsel / MyVoice	Ved 100 ansatte: Core 1 950/mnd, Advanced 2 250/mnd; implementering 10 000	Norsk støtte, mange språk og avansert saksbehandling.
Whistlelink	USD 119/mnd for 0–49; 149 for 50–149; 229 for 150–249	Årlig abonnement med omfattende funksjons- og sikkerhetspakke.

15.1 Anbefalt posisjon

Ikke lavest pris

Mer hjelp enn en ren kanal

+

Ikke tung enterprise

Enklere for norske SMB-er

=

Sikker Varsling

Reporter-first trygg prosess

15.2 Budskap

«Varsleren får gratis hjelp til å si ifra på en trygg og ryddig måte. Virksomheten betaler for beredskap, sikker saksbehandling og den støtten som gjør at varselet faktisk kan følges opp.»

KAPITTEL 16

Produksjonskontroll

Tekniske, metodiske og operative kontroller er samlet i en etterprøvbar åpning.

Separat fortrolig kontakt

Navn og e-post krypteres i et eget mottaksfelt og fjernes teknisk fra innholdet virksomheten får.

Dobbelt anonym innboks og toveis dialog

Separat meldingslager, nettleserkryptering, saksavgrenset bedriftsnøkkel, nøkkelfingeravtrykk, misbruksvern og automatiserte kryptografi- og nettlesertester.

Tosidig saksveiledning og ettervern

12 varslerverktøy og 17 virksomhetsverktøy vises etter saksstatus og risiko, med privat tidslinje, 7/30/90-kontrollpunkter og vern mot gjengjeldelse.

Drift, retensjon og gjenoppretting

Fail-closed tjenestebryter, sikkerhetslogger, konsistent backup, separat nøkkelkopi, retensjonsjobb og øvelsestester inngår i utgivelseskontrollen.

Full klikk- og regresjonskontroll

Alle sentrale tastevalg kontrolleres på mobil og desktop sammen med roller, autorisasjon, QR, E2E, personverngrenser og transportvern.

EKSTERN

Uavhengig sikkerhetsgjennomgang

En ekstern kontrollør vurderer nøkkellivsløp, nettlesertrusler, kryptografiske valg, gjenoppretting og misbruksflyt. Inntaket åpnes når kontrollen er godkjent uten kritiske eller høye funn.

FAQ

Ofte stilte spørsmål

Er Sikkervarsling en advokattjeneste?

Tjenesten gir struktur, sikker kanal og prosessveiledning. Juridiske vurderinger utføres av kvalifisert rådgiver under eget mandat når saken trenger det.

Hvordan beskytter tjenesten identiteten?

Navn og direkte digitale identifikatorer holdes utenfor virksomhetens saksinnhold i anonyme løp. Veiledningen minner samtidig om at selve fortellingen kan gi indirekte holdepunkter.

Hvorfor kan varsleren bruke tjenesten gratis?

Fordi betaling reduserer tilgangen for den mest sårbare parten. Virksomheten finansierer beredskap og oppfølging fordi den har plikt og størst nytte av tidlig informasjon.

Må virksomheten være kunde for å motta et varsel?

En ikke-kunde får enkel, saksavgrenset tilgang. Abonnement gir fast kanal, portal, organisasjonskontroller og utvidet støtte.

Hvordan åpnes dobbelt anonymt?

Den tekniske implementasjonen og nettleserflyten har bestått kryptografi- og ende-til-ende-tester. Reell innsending åpnes når den uavhengige sikkerhetsgjennomgangen bekrefter kontrollene.

Kan Sikkervarsling lese krypterte saker?

Autorisert mottak kan lese den opprinnelige saken når Sikkervarsling er første mottaker. I den dobbelt anonyme dialogen kan Sikkervarsling ikke dekryptere nye meldinger etter nøkkeloverleveringen, fordi AES-GCM-romnøkkelen ikke lagres på serveren.

Hvordan håndteres dokumenter?

Originaldokumenter beholdes hos varsleren til riktig mottaker og en sikker kanal er avklart. Det reduserer risiko fra metadata, skadevare og utilsiktede identifikatorer.

Hva skjer hvis tjenesten må stenges?

Nye innsendinger kan pauses, mens lokale varselpakker fortsatt kan lages og eksisterende saker følges opp. Alternative akutt- og myndighetskanaler er alltid synlige.

VEDLEGG A

Datakatalog

Objekt	Eksempler	Beskyttelse	Sletting
Virksomhet	Navn, org.nr., mottakerkode, aktiv status	Tilgangsstyrt konfigurasjon	Etter avtale/opphør
Varslingssak	Beskrivelse, identitetsvalg, beskyttelse, risiko	Secretbox-kryptert payload	Foreslått 365 dager etter lukking
QR-adgang	Token-HMAC, PIN-hash, tid og sperring	Ingen rå token/PIN	Kaskade med saken
Mottakerinvitasjon	Token-HMAC, PIN-hash, utløp og bruk	Éngangsbruk, to kanaler	Kaskade med saken
Mottakerkonto	Navn, rolle, passordhash, kryptert TOTP	MFA og sesjonsversjon	Etter avtale/tilgangsbehov
E2E-rom	Offentlig nøkkel, kryptert privatnøkkel, pakket romnøkkel, nøkkelfingeravtrykk og sperrestatus	Ingen rå privatnøkkel eller romnøkkel på serveren	Kaskade med saken
E2E-melding	Avsenderrolle, tilfeldig IV, chiffertekst og klientgenerert meldings-ID	AES-GCM; ingen meldingsklartekst på serveren	Kaskade med saken
Revisjon	Bruker, handling, tid, pseudonym økt	Ingen rå IP eller saksfritekst	Frist må godkjennes
Slettekvittering	HMAC-pseudonym, policy og tid	Ingen rå saksreferanse	Frist må godkjennes

VEDLEGG B

Sikkerhetskontroller og testdekning

Kontroll	Implementasjon	Test/etterprøving
Autentisert kryptering	PHP Sodium secretbox, tilfeldig nonce	Backupverifikasjon dekrypterer alle krypterte felt
Passord	`password_hash` / `password_verify`	Innlogging, bytte og reset i testløp
TOTP	RFC 6238-modell med replayvern	MFA-innrullering og gjenbrukstest
Autorisasjon	Rolle + saksvis tildeling + konfliktfilter	Receiver-role smoke-test
QR	256-bit token, fragment, HMAC, PIN, rotasjon	QR access smoke-test
Mottakerlenke	256-bit token + separat seks-sifret kode	Case-invite smoke-test
Leveringsgrense	Direkte saker avvises av operatørverktøy	Delivery-route og E2E-test
Dobbelt anonym nøkkeloverlevering	RSA-OAEP-nøkkelpar, AES-GCM-romnøkkel og synlig SHA-256-fingeravtrykk	Double-anonymous E2E smoke-test
Dobbelt anonym dialog	AES-GCM med meldingsbundet AAD, tilfeldig IV, unik klient-ID, blokkering og selektiv misbruksdeling	Full nettlesertest begge veier uten klartekst eller romnøkkel i databasen
Retensjon	Tørrkjøring, secure_delete, WAL checkpoint	Retention smoke-test
Stoppbryter	Fail-closed kontrolltabell	Service-control smoke-test
Backup	Snapshot, SHA-256, HMAC og integritet	verify-backup

VEDLEGG C

Kilder og referanser

1. **Arbeidsmiljøloven § 2 A-6.** Plikt og minimumsinnhold for interne varslingsrutiner. lovdata.no
2. **Arbeidstilsynet: Ansvar, rettigheter og roller.** Oppfølging, anonymitet og bindeleddsrollen. arbeidstilsynet.no
3. **Arbeidstilsynet: Slik bør arbeidsgiver håndtere varsling.** Konfidensialitet, habilitet, kontradiksjon og gjengjeldelse. arbeidstilsynet.no
4. **Datatilsynet: Varsling og personopplysninger.** Anonymitet, identifiseringsfare og roller. datatilsynet.no
5. **Datatilsynet: Innebygd personvern.** Dataminimering, pseudonymisering og tilgangsstyring. datatilsynet.no
6. **PHP Manual: sodium_crypto_secretbox.** Autentisert symmetrisk kryptering. php.net
7. **RFC 6238.** Time-Based One-Time Password Algorithm. rfc-editor.org
8. **OWASP Cheat Sheet Series.** Sesjonshåndtering, autentisering, autorisasjon og sikkerhetslogging. owasp.org
9. **SQLite-dokumentasjon.** `secure_delete`, WAL checkpoint og integrity check. sqlite.org
10. **Whitenoise Anonym varsling – priser.** Offentlig prisinformasjon kontrollert 20.07.2026. varsling.whitenoise.no
11. **HMSVarsling – priser.** Offentlig prisinformasjon kontrollert 20.07.2026. hmsvarsling.no
12. **MittVarsel/MyVoice – priser.** Offentlig prisinformasjon kontrollert 20.07.2026. digitaliq.no
13. **Whistlelink – priser og funksjoner.** Offentlig prisinformasjon kontrollert 20.07.2026. whistlelink.com