Sjøfartsdirektoratet
Norwegian Maritime Authority

Sjøfartsdirektoratet er utpekt myndighet for sektortilsyn med digitalsikkerhetsloven for rederier

Justis- og beredskapsdepartementet hadde lov om digital sikkerhet og forskrift om digitalsikkerhet på høring høsten 2024. Den nye digitalsikkerhetsloven og digitalsikkerhetsforskriften trådte i kraft 1. oktober 2025. I anledning at Sjøfartsdirektoratet nå er utpekt myndighet for sektortilsyn for de rederier som faller inn under lovens virkeområde veileder vi om kravene i digitalsikkerhetsloven med tilhørende forskrift[1].

Rederier må selv vurdere om de tilbyr samfunnsviktige tjenester og dermed er omfattet av regelverket.

Rederier som er etablert i Norge og som har skip med fast anløp eller som transporterer minst fem prosent av passasjerantallet eller godsomslaget i en havn med godsomslag på 100 000 tonn per år over en femårsperiode, eller som håndterer 100 000 passasjerer per over en femårsperiode, vil kvalifisere for å være en tilbyder av samfunnviktig tjeneste etter regelverket om digital sikkerhet.

Rederier som tilbyr samfunnsviktige tjenester, vil måtte varsle både NSM og Sjøfartsdirektoratet om at de anser seg for å være omfattet. I tillegg må nærmere krav til digital sikkerhet innarbeides, herunder blant annet styringssystem, risikovurdering, risikohåndtering, sikkerhetstiltak, beredskapstiltak, oppfølgings- og varslingsrutiner. Se veiledning nedenfor og NSM sin veileder om regelverket her:

Introduksjon til digitalsikkerhetsloven og -forskriften.pdf

1. Digitalsikkerhetsloven

Digitalsikkerhetsloven skal forebygge, avdekke og motvirke uønskede hendelser mot nettverks- og informasjonssystemer– enten de er tilsiktet (f.eks. et cyberangrep) eller utilsiktet (f.eks. teknisk svikt, naturkatastrofer, strømstans). På engelsk kalles dette «all hazards approach». Hvis virksomheten deres er underlagt loven, skal dere derfor arbeide for å forhindre og håndtere alle typer hendelser som kan true nettverks- og informasjonssystemene deres.

Loven gjelder både informasjonsteknologi og operasjonell teknologi, og har en bred definisjon av nettverks- og informasjonssystemer. Både informasjonsteknologi (IT) og operasjonell teknologi (OT) er omfattet. Bakgrunnen for den brede definisjonen er at mange samfunnsviktige tjenester er avhengige av digitale driftskontrollanlegg og produksjonsutstyr (OT). OT-systemene trenger ikke å være koblet sammen med IT-systemene for å være omfattet eller for å være sårbare. Men hvis de er det, øker sårbarheten. Dere må derfor se IT- og OT-systemene under ett når dere vurderer sikkerhet og risiko.

Det er ingen overgangsperiode, og virksomheter som omfattes må etterleve kravene fra første dag.

Vi vil nedenfor gi informasjon om hvilke rederier loven gjelder for, hvilke krav som stilles, hvilke sanksjoner som kan komme ved manglende etterlevelse, og konkrete tiltak virksomheter bør iverksettes nå.

[1] Lov 20. Desember 2023 nr. 108 om digital sikkerhet (digitalsikkerhetsloven), og forskrift 20. Juni 2025 nr. 1131 om digital sikkerhet (digitalsikkerhetsforskriften)

Sjøfartsdirektoratet
Norwegian Maritime Authority

2.Hvilke rederier gjelder loven for?

Loven retter seg mot to hovedgrupper virksomheter. Først og fremst gjelder den tilbydere av samfunnsviktige tjenester etablert i Norge innen sektorer som energi, transport, helse, vannforsyning, bank, finansmarkedsinfrastruktur og digital infrastruktur. De nærmere kriteriene for hvilke tjenester som regnes som samfunnsviktige gis i digitalsikkerhetsforskriften. Herunder er rederier med følgende skip omfattet:

1) skip med fast anløp eller som transporterer minst fem prosent av passasjerantallet eller godsomslaget i en havn som enten har et godsomlag på mer enn 100 000 tonn per år over en femårsperiode, eller
2) skip som går til havner eller havneanlegg som håndterer mer enn 100 000 passasjer per år over en femårsperiode.

Dere som rederi må undersøke om dere ut fra 1) deres anløp, 2) de tjenester dere utfører eller 3) antall passasjerer som håndteres av havnene/havneanleggene deres skip anløper, faller inn under virkeområdet.

Loven omfatter også tilbydere av digitale tjenester, i tillegg til tilbydere av samfunnsviktige tjenester. I praksis vil dette si nettbaserte markedsplasser, nettbaserte søkemotorer og skytjenester.

3. Hvilke krav gjelder?

Digitalsikkerhetsloven stiller grunnleggende krav til digital sikkerhet i virksomheter som er særlig viktige for samfunnet.

Formålet er å forebygge, avdekke og motvirke uønskede hendelser i nettverks- og informasjonssystemer som dere bruker for å levere samfunnsviktige tjenester og digitale tjenester.

Hvis deres rederi tilbyr samfunnsviktige tjenester, pålegger loven dere noen plikter. Dette må dere gjøre:

1. Meld fra til både NSM og til Sjøfartsdirektoratet om at deres rederi tilbyr samfunnsviktige tjenester
2. Etabler et forsvarlig sikkerhetsnivå
3. Kartlegg tjenestene, leveransekravene og systemene
4. Gjør en risikovurdering
5. Lag en plan for håndtering av risiko
6. Følg opp samarbeidspartnere og underleverandører og sette samme krav overfor dem
7. Lag en beredskapsplan og øv på den
8. Varsle om hendelser.

Kravene i digitalsikkerhetsloven er minimumskrav. Dere står fritt til å innføre strengere sikkerhetstiltak. Nedenfor forklarer vi pliktene nærmere.

3.1 Meld fra om at dere tilbyr samfunnsviktige tjenester

Rederi som er omfattet skal melde fra både til NSM og til Sjøfartsdirektoratet om at de tilbyr samfunnsviktige tjenester. Dette skal gjøres «snarest», det vil si så raskt det lar seg gjøre uten en saklig grunn for forsinkelsen. Meld inn både virksomheten og tjenesten(e) dere tilbyr.

Innmeldingen til NSM og Sjøfartsdirektoratet sender dere på egne skjema til postmottak@nsm.no og post@sdir.no . Skriv «Innmelding etter digitalsikkerhetsloven» i emnefeltet. Skjemaene finner dere på nsm.no. Merk at det finnes ett skjema for innmelding av virksomhet og ett for innmelding av tjeneste.

Utfører dere flere tjenester skal de meldes inn hver for seg, og også endringer i tjenestene. Følgende informasjon må meldes inn

- virksomhetens navn, organisasjonsnummer, adresse og kontaktinformasjon (inkludert kontaktperson og vakttelefon
- navn på og/eller en kort beskrivelse av de samfunnsviktige tjenestene dere tilbyr
- hvilken sektor dere tilhører
- hvilket geografisk område tjenestene tilbys i
- (om relevant) hvilke andre land tjenestene tilbys i

Videre plikter dere å melde fra om endring som f.eks.:

- bytte av navn eller flytting
- når dere slutter å levere en samfunnsviktig tjeneste
- når dere begynner å tilby en ny samfunnsviktig tjeneste
- når dere begynner å tilby en tjeneste i et nytt geografisk område
- når en tjeneste ikke lenger oppfyller kravene til å være samfunnsviktig

Formålet med innmeldingen er å gi myndighetene en oppdatert oversikt over alle virksomheter som leverer samfunnsviktige tjenester. Oversikten brukes blant annet til beredskapsplanlegging, håndtering av hendelser, planlegging av tilsyn og rapportering til EFTAs overvåkningsorgan (ESA).

3.2 Etabler et forsvarlig sikkerhetsnivå

Dere skal etablere et forsvarlig sikkerhetsnivå for alle nettverk og informasjonssystemer dere bruker til å levere samfunnsviktige tjenester. Dette er som nevnt et minimumskrav i digitalsikkerhetsloven – dere står fritt til å innføre strengere sikkerhetstiltak. Det betyr at dere skal:

- etablere et styringssystem for sikkerhet
- skaffe oversikt og gjøre risikovurderinger
- ha en plan for å håndtere risiko
- sette inn teknologiske, organisatoriske, fysiske og personellmessige sikkerhetstiltak som står i forhold til den identifiserte risikoen
- ha en beredskapsplan for håndtering av hendelser og varsling, og gjennomføre øvelser
- følge opp leverandører og andre som utfører arbeid for dere

3.2.1 Hva betyr «forsvarlig sikkerhet»?

Forsvarlig sikkerhet betyr at tjenestene skal fungere og være tilgjengelige selv om uønskede hendelser rammer nettverkene og informasjonssystemene. Forsvarlig sikkerhet innebærer blant annet at systemene er robuste nok til å tåle uønskede hendelser og konsekvensene av dem, og at tjenestene kan opprettholdes til et bestemt nivå under slike hendelser. Hva som er riktig nivå (minimumsnivået), varierer fra tjeneste til tjeneste og fra system til system. Dette må fastsettes i risikovurderingen og har betydning for hvilke tiltak dere skal iverksette, både for å forebygge hendelser og som forberedelse til å håndtere hendelser. Kravet om forsvarlig sikkerhet er en rettslig standard som endrer seg over tid med utviklingen i blant annet teknologi, trusselbilde og samfunnsbehov.

3.2.2 Krav til styringssystemet

Sikkerhetsarbeidet må være en del av den daglige driften. Dere skal derfor ha et styringssystem som gir rammene for hvordan sikkerheten styres i virksomheten.

Styringssystemet skal blant annet:

- dokumentere hvordan sikkerheten håndteres

- vise hvem som har ansvar, hvilke roller som finnes, og hvilken myndighet de har
- beskrive hvordan beslutninger om risiko og tiltak tas, og hvordan sikkerhetsarbeidet følges opp
- bidra til å forebygge, oppdage og håndtere hendelser
- bygge på anerkjente standarder

Styringssystemet skal godkjennes av virksomhetens ledelse og gjennomgås minst én gang i året for å sikre forankring, oppfølging og kontinuerlig forbedring.

3.2.3 Ledelsens ansvar

Virksomhetens øverste ledelse har det overordnede ansvaret for at virksomheten har et forsvarlig sikkerhetsnivå. Ansvaret kan ikke delegeres.

Ledelsen skal sørge for at:

- sikkerhetsarbeidet er organisert og bemannet
- mål og krav for sikkerheten er fastsatt
- sikkerhetstiltak følges opp og forbedres over tid

3.3 Kartlegg tjenestene, leveransekravene og systemene

Før dere kan gjøre en risikovurdering, må dere ha full oversikt. Det får dere ved å kartlegge for eksempel

- hvilke samfunnsviktige tjenester dere tilbyr
- hvilke leveransekrav som gjelder for hver tjeneste
- hvilke systemer som støtter de ulike tjenestene
- hva systemene brukes til for de ulike tjenestene

Med en oppdatert kartlegging har dere grunnlaget dere trenger for å gjøre en korrekt risikovurdering og velge riktige sikkerhetstiltak.

3.4 Gjør en risikovurdering

I risikovurderingen skal dere:

- identifisere trusler og sårbarheter i systemene som leverer de samfunnsviktige tjenestene
- beskrive hvilke hendelser virksomheten kan bli utsatt for, og hvilke konsekvenser disse kan få for tjenestene
- beskrive i hvilken grad dere er avhengige av andre virksomheter eller underleverandører, for eksempel for strømforsyning, lagring eller kjøling

Risikovurderingen skal være så omfattende at dere kan velge riktige organisatoriske, teknologiske, fysiske og personellmessige sikkerhetstiltak. Dere velger selv hvilken metode dere vil bruke for risikovurderingen, men den må være dokumentert, og den må oppdateres jevnlig – og alltid når det skjer endringer som kan påvirke sikkerheten. Dette er essensielt, ettersom risikovurderingen danner grunnlaget for å velge de riktige sikkerhetstiltakene.

3.5 Lag en plan for håndtering av risiko

Basert på risikovurderingen må dere lage en plan for hvordan dere håndterer risikoene. Formålet er å redusere risikoene til et akseptabelt nivå. Dere har oppnådd et akseptabelt risikonivå når sikkerhetstiltakene til sammen

gir forsvarlig sikkerhet for de samfunnsviktige tjenestene. Det vil si at dere trygt kan levere tjenestene og har evne til å håndtere og raskt gjenopprette driften ved en hendelse. Planen skal inneholde konkrete tiltak i fire kategorier:

- organisatoriske tiltak
- teknologiske tiltak
- fysiske tiltak
- personelltiltak

Tiltakene skal beskytte tilgjengeligheten, autentisiteten, integriteten og tilliten til dataene systemene behandler, og til de tjenestene og funksjonene systemene gjør tilgjengelig. Samlet skal de gjøre det mulig å **forebygge**, **oppdage, håndtere og redusere** konsekvensene av uønskede hendelser.

3.5.1 Organisatoriske tiltak

Dere skal ha oppdaterte og konkrete rutiner, instrukser, prosedyrer og planer for hvordan dere håndterer sikkerheten. Tiltakene skal:

- være tilpasset virksomhetens størrelse og kompleksitet
- kunne settes i verk ved endringer eller hendelser
- være kjent for alle som har relevante oppgaver

3.5.2 Teknologiske tiltak

De teknologiske tiltakene skal være tilpasset hvert enkelt nettverks- og informasjonssystem og minst omfatte:

- sterk autentisering (f.eks. passkey eller multifaktorautentisering)
- kontroll over hvem som har tilgang
- nettverkssegmentering
- evne til å håndtere avbrudd og gjenopprette tjenester
- kapasitet til å tåle belastning
- jevnlig oppdatering og videreutvikling av systemer
- overvåkning for å oppdage hendelser

Er det et tiltak dere ikke kan gjennomføre? Da må virksomhetens leder godkjenne det som et unntak, dokumentere dette i styringssystemet og melde fra til sektormyndigheten. Dere må også sette inn andre tiltak som kompenserer for det manglende tiltaket.

3.5.3 Fysiske tiltak

Dere skal beskytte bygninger, rom og utstyr mot uautorisert tilgang, naturhendelser og andre farer gjennom:

- adgangskontroll til viktige lokasjoner og infrastruktur
- beskyttelse av bygninger og områder
- sikring av strøm og datakommunikasjon
- alarmer, sensorer eller andre systemer som oppdager fysiske hendelser

Tiltakene skal dokumenteres og tilpasses de lokale forholdene.

3.5.4 Personelltiltak

Ansatte, leverandører og andre med tilgang til systemene må få riktig tilgang, basert på hva slags rolle og ansvar de har. De må også få opplæring i sikkerhet og være kjent med alle relevante tiltak. Dere skal fjerne tilgangen fra personer som slutter eller ikke lenger har behov for tilgang. Dette må dere ha rutiner for.

3.6 Følg opp samarbeidspartnere og underleverandører

Hvis dere bruker underleverandører eller andre til å utføre arbeid for eller på vegne av virksomheten og arbeid som kan påvirke sikkerheten i nettverk og informasjonssystemer, er dere ansvarlige for å følge dem opp og sørge for at de oppfyller kravene til forsvarlig sikkerhet. Dere skal følge dem opp løpende – ikke bare kontrollere i etterkant.

Dere må sikre at nødvendige sikkerhetskrav gjelder for hver enkelt leverandør eller underleverandør. Det kan dere gjøre gjennom avtaler eller på andre egnede måter, for eksempel gjennom revisjoner, rapportering og sikkerhetskrav i kjeden. Kravene skal stå i forhold til risikoen og bygge på deres risikovurdering. Denne skal dere dokumentere i styringssystemet.

Oppfølgingsplikten gjelder enten dere har satt bort hele eller deler av en tjeneste. Gå gjennom eksisterende avtaler og revider dem dersom de ikke tilfredsstiller et forsvarlig sikkerhetsnivå.

3.7 Lag en beredskapsplan og øv på den

Dere må ha en beredskapsplan, slik at dere er forberedt på å håndtere hendelser som kan påvirke de samfunnsviktige tjenestene. Planen skal beskrive:

- hvordan dere skal håndtere hendelser
- hvem som skal varsles når
- hvordan varslingen skal skje
- hvilke skjerpede tiltak dere kan sette inn ved behov
- Skjer det en hendelse, skal dere:
- identifisere hva som har skjedd
- iverksette mottiltak for å stanse eller begrense hendelsen gjenopprette sikker tilstand

Dere skal vedlikeholde, dokumentere og teste beredskapsplanen gjennom øvelser.

Øvelsene skal bidra til å bygge kompetanse, avdekke svakheter i sikkerhetsarbeidet og sikre at dere kan håndtere hendelser riktig og effektivt. Vi anbefaler at dere gjennomfører øvelser minst én gang i året, og at dere inkluderer leverandører eller andre som utfører arbeidet for dere dersom det er relevant. Dere bør også delta i øvelser som sektormyndigheten eller NSM inviterer til.

3.8 Varsle om hendelser

Dere skal varsle myndighetene om hendelser som virker betydelig inn på leveransen av de samfunnsviktige tjenestene deres. Slike hendelser kalles gjerne alvorlige hendelser. Varsling gjør at myndighetene kan følge opp, dele informasjon og rapportere videre. Dere skal varsle selv om det innebærer å dele taushetsbelagt informasjon – loven gir unntak fra taushetsplikten i slike tilfeller.

3.8.1 Hva er en hendelse med «betydelig innvirkning»?

Varslingsplikten gjelder for hendelser som «virker betydelig inn på tjenesteleveransen». Hva som er betydelig, vil variere mellom tjenester. Når dere skal sette grensen, kan det være aktuelt å se til andre lover og regler, internasjonale standarder eller leveranseavtaler. I tillegg skal dere legge vekt på:

- hvor mange brukere som kan bli påvirket
- hvor lenge hendelsen kan vare

- hvor stort geografiske område som kan bli berørt

Definer alltid varslingsgrensen på forhånd.

Dokumenter den i styringssystemet for sikkerhet, og ta den inn i beredskaps- og varslingsplanene.

3.8.2 Slik varsler dere

Bruk eget varslingsskjema tilgjengelig på nsm.no, og send det til Sjøfartsdirektoratet med kopi til NSM på post@sdir.no og postmottak@nsm.no . Skriv «Varsel etter digitalsikkerhetsloven» i emnefeltet.

3.8.3 Dette skal varselet inneholde

Varslet skal:

- angi navn på virksomheten og kontaktinformasjon
- beskrive hvilken tjeneste som er berørt
- beskrive hva som har skjedd, mulige årsaker og konsekvenser
- angi antall berørte brukere
- beskrive om hendelsen har påvirket andre land

Myndighetene kan be om mer informasjon og statusoppdateringer underveis.

3.8.4 Fristene for å varsle og følge opp

Dette er fristene dere må forholde dere til:

- første varsel: innen 24 timer etter at dere oppdaget hendelsen
- oppdatering til myndighetene: innen 72 timer etter at dere oppdaget hendelsen
- hendelsesrapport: innen én måned etter at dere sendte det første varselet

Fristene er absolutte og gjelder også hvis hendelsen skjer hos en samarbeidspartner eller underleverandør.

3.8.5 Dette skal hendelsesrapporten inneholde

Innen én måned etter første varsel skal dere sende en rapport som:

- oppdaterer informasjonen fra det første varselet
- beskriver alvorlighet, virkninger og sannsynlig rotårsak eller type trussel
- gjør rede for hvilke tiltak dere har iverksatt og planlagt
- opplyser om eventuelle grensekryssende virkninger

4 Tilsyn og reaksjoner

Målet med regelverket er å sikre god digital sikkerhet for hele samfunnet – ikke å straffe. Selv om tilsynsmyndighetene kan ilegge reaksjoner, er den viktigste oppgaven å bidra til forbedringer og forebygge feil.

4.1 Hvordan skjer tilsynet?

Både dere som tilbyr samfunnsviktige tjenester (gruppe a), og dersom tilbyr digitale tjenester (gruppe b), kan få tilsyn.

- For gruppe a utføres det både planlagte (regelmessige) og hendelsesbaserte tilsyn (herunder gjelder dette de rederier som omfattes)
- For gruppe b utføres det bare hendelsesbaserte tilsyn.

Hendelsesbasert tilsyn kan skje når tilsynsmyndigheten får informasjon som tyder på brudd på regelverket, eller etter at en hendelse har oppstått. For rederier som er underlagt digitalsikkerhetsloven vil Sjøfartsdirektoratet være tilsynsmyndighet.

Sjøfartsdirektoratet opplyser om at vi for 2026 kun vil foreta hendelsesbaserte tilsyn. Intervaller for regelmessige tilsyn vil fastsettes i løpet av 2026 og regelmessige tilsyn vil først påstartas i 2027.

4.2 Hva kan tilsynsmyndigheten kreve?

Under tilsyn kan myndigheten kreve at dere:

- gir opplysninger og dokumentasjon de trenger for å føre tilsyn – også taushetsbelagt informasjon og personopplysninger, uten hinder av taushetsplikt
- gir dem tilgang til lokaler, utstyr og systemer
- bistår i undersøkelsene
- stiller med relevant personell under tilsynet

Tilsynsmyndigheten kan også sette frister og bestemme hvilket format dere skal gi opplysningene i. Har dere satt bort deler av tjenesten til en underleverandør som ikke er underlagt loven? Da er det deres ansvar – og i deres interesse – å sørge for tilgang til opplysninger og lokaler hos leverandøren.

5 Reaksjoner ved lovbrudd

Hvis tilsynsmyndigheten finner at dere ikke følger loven, kan de reagere med:

- pålegg om å rette opp i forholdet
- tvangsmulkt (for å få pålegget oppfylt)
- overtredelsesgebyr (administrativ sanksjon)

5.1 Pålegg om retting

Tilsynsmyndigheten kan pålegge dere å rette opp i ulovlige forhold. Pålegg kan for eksempel innebære:

- å rette et avvik
- å iverksette tiltak som fjerner årsaken til avviket og hindrer gjentakelse

Myndigheten gir dere en frist for å oppfylle pålegget. Pålegg er en svært vanlig reaksjon etter et tilsyn.

5.2 Tvangsmulkt

Hvis dere har fått et pålegg, men ikke følger det, kan tilsynsmyndigheten ilegge en tvangsmulkt – enten som en løpende mulkt (som fortsetter til forholdet er rettet) eller som et engangsbeløp.

5.3 Overtredelsesgebyr

Tilsynsmyndighetene kan ilegge gebyr ved forsettlige eller uaktsomme brudd. Gebyr kan ilegges:

- virksomheter i gruppe a
- virksomheter i gruppe b
- enkeltpersoner eller virksomheter som handler på vegne av en virksomhet i gruppe a eller b

Også enkeltpersoner kan altså ilegges gebyr i spesielle tilfeller, ved det som beskrives som simpel uaktsomhet.

Når tilsynsmyndigheten vurderer om de skal ilegge gebyr, og hvor stort det i så fall skal være, legger de særlig vekt på:

- hvor alvorlig overtredelsen er
- hvor lenge den har vart
- om den har skjedd gjentatte ganger
- hvor stor virksomheten er
- om virksomheten har fått økonomisk gevinst av å bryte loven
- om virksomheten har samarbeidet med tilsynsmyndigheten
- om overtredelsen har ført til faktiske konsekvenser

5.3.1 Beviskrav, foreldelse og klage

Tilsynsmyndigheten kan ikke ilegge overtredelsesgebyr uten at det er klar sannsynlighetsovervekt for at loven er brutt. De kan heller ikke ilegge gebyr senere enn fem år etter at overtredelsen har opphørt, men denne fristen avbrytes hvis de gir forhåndsvarsel eller gjør vedtak. Et vedtak om overtredelsesgebyr kan påklages etter reglene i forvaltningsloven.

5.3.2 Størrelsen på gebyret

Gebyret skal alltid stå i forhold til overtredelsen og virksomhetens størrelse, men kan aldri overstige disse rammene:

- inntil 25 ganger grunnbeløpet (G) i folketrygden
- inntil fire prosent av årsomsetningen i forrige regnskapsår (gjelder foretak) inntil 50 millioner kroner totalt

Dette er maksimumsgrenser – det konkrete beløpet fastsettes etter en vurdering av alvorlighetsgrad, varighet, konsekvenser og andre relevante forhold.

6 Oppdatert informasjon

Informasjonen som er lagt her er i hovedsak hentet fra «Introduksjon: Digitalsikkerhetsloven og -forskriften, oktober 2025» fra Nasjonal sikkerhetsmyndighet (NSM). Sjekk deres sider for å se om det er kommet oppdatert informasjon.

Når det gjelder informasjon om innmelding og varsling til Sjøfartsdirektoratet, vil eventuelle endringer tilknyttet ønskede kanaler og skjema komme på vår hjemmeside.

Dette er ment som en introduksjon og påminnelse.