Orange
Cyberdefense

1. RAPPORT FOR NORSK ÅPENHETSLOV 2022

1.1. Introduksjon

I henhold til åpenhetsloven skal Orange Cyberdefence AS gjennomføre due diligence-vurderinger og tilgjengeliggjøre en rapport om vurderingene.

"Loven skal fremme virksomheters ***respekt for grunnleggende menneskerettigheter og anstendige arbeidsforhold*** *i forbindelse med produksjon av varer og levering av tjenester, og sikre allmennheten tilgang til informasjon om hvordan virksomheter håndterer negative konsekvenser for grunnleggende menneskerettigheter og anstendige arbeidsforhold.*

Denne rapporten er en redegjørelse for due diligence-vurderinger som er utført fra 1. juli 2022 og frem til i dag, inkludert vurderinger av eventuelle tiltak som er iverksatt.

1.2. Kontaktinformasjon

Ved spørsmål knyttet til denne rapporten kontakt oss gjerne på Kontakt og support (orangecyberdefense.com).

1.3. Rapporteringsplikt

Orange Cyberdefense Norge AS sitt hovedkontor ligger på Lysaker Torg 25, 1366 Lysaker.

Selskapet er rapporteringspliktig etter åpenhetsloven, paragraf 2 og 3.

2. SELSKAPET

2.1. Om selskapet

Orange Cyberdefense Norge AS er 100 % eid av Orange Business S.A, en del av ORANGE SA, Paris, Frankrike.

Orange Cyberdefense er cybersikkerhetsekspertens forretningsenhet i Orange Group, som tilbyr rådgivning, løsninger og tjenester til organisasjoner over hele verden. Som Europas beste sikkerhetsleverandør streber vi etter å beskytte frihet og bygge et tryggere digitalt samfunn. Orange Cyberdefense Norge AS tilbyr en rekke cybersikkerhetstjenester til sine kunder, slik som, men ikke begrenset til, etisk hacking, endepunkt sikkerhet, informasjonssikkerhet, OT-sikkerhet, SASE, skysikkerhet og infrastruktur.

Selskapet opererer i et svært konkurranseutsatt og stadig voksende og skiftende marked. Hovedkundene er bedrifter og offentlige organisasjoner i Norge. Kundetilbudene består av både videresalg av tredjeparts maskinvare og programvare, og ulike tjenester levert av Orange Cyberdefense.

Selv om det er et teknologiselskap, jobber Orange Cyberdefense Norge AS for å møte våre kunders forretningsutfordringer, og leverer tjenester fra idé til løsning (fra strategirådgivning til drift). Selskapets fokus på å være lokalt og å jobbe i tett samarbeid med kunden er grunnlaget for å levere det høyeste nivået av ytelse og kvalitet som kundene krever for å bygge et generelt, tryggere digitalt samfunn.

Selskapet er sertifisert i henhold til ISO27001.

2.2 Ansvarlig innkjøp hos Orange Cyberdefense Norge AS

Orange Cyberdefense Norge AS tar veiledning av Orange Group sin retningslinje for bærekraftig utvikling og samfunnsansvar (CSR) i sine styrings- og anskaffelsesprosesser og etablerer tillits- og lojalitetsforhold med sine leverandører (kontraktsmessig forpliktelse, evaluering av CSR-aspekter og revisjon), for å overholde:

- Sosiale lover med hensyn til mennesket, internasjonale regler knyttet til arbeidsrett, barnevern, helse og sikkerhet.
- De miljømessige, sosiale og etiske kriteriene som vurderes under selskapets prosess for valg av leverandør.

Administrerende direktør i Orange Cyberdefense Norge, med støtte fra Orange Cyberdefense Group compliance officer, har ansvaret for at selskapet følger mottatt veiledning og retningslinjer.

2.3 Etikk, kampen mot svindel og korrupsjon, internasjonale sanksjoner

Orange Group er forpliktet til å forhindre og bekjempe alle former for korrupsjon (Orange Group Anti-Corruption Policy), medvirkning, utpressing, underslag og enhver upassende fordel. Etikk er et viktig tema på alle nivåer av vår aktivitet, spesielt i forholdet vårt til våre ansatte, våre leverandører og våre underleverandører: (The Group Code of Ethics). Utover de regulatoriske begrensningene, er Orange forpliktet til å utføre sine aktiviteter på en rettferdig og ærlig måte.

2.4 Våre etiske retningslinjer

Etiske retningslinjer for leverandører beskriver de etiske, sosiale og miljømessige forpliktelsene som forventes av Orange Group, som krever følgende av leverandører og deres underleverandører:

- Overhold nasjonale, europeiske og internasjonale regler knyttet til standarder for etisk og ansvarlig atferd, inkludert de som omhandler menneskerettigheter, miljøvern, bærekraftig utvikling, korrupsjon og barnevern.
- Vedta og anvende Group's etiske standarder og forpliktelser og fremgang på disse områdene

Orange støtter sine leverandører i kontraktuelle og kontraktsmessige forhold for effektiv implementering av disse etiske retningslinjene (Supplier Code of Conduct).

2.5 Vurdering av leverandørers samfunnsansvar

For leverandører som tilhører høye CSR-risikokategorier og/eller med en betydelig årlig ordreverdi, utfører Orange Group systematisk CSR-vurderinger for å

- bedre forstå leverandørenes initiativ,
- sikre at de er forpliktet til miljøet, sosiale rettigheter og menneskerettigheter og god etisk praksis,
- oppfylle regulatoriske forpliktelser, for eksempel The Duty of Care law,
- iverksette og følge opp korrigerende handlingsplaner.

CSR-vurderinger er basert på internasjonale CSR-standarder, som Global Compact og ISO 26000, og utføres under kontraktsforhandlinger og gjennom kontraktens levetid

2.6 Ledelsesforankring og bevissthet

Selskapets retningslinjer og rutiner er forankret i ledelsen og kommuniseres til ansatte:

- som en del av ansettelsesprosessen
- regelmessige bevisstgjøringskampanjer på vårt intranett
- årlig opplæring, og signering, av relevante retningslinjer.

2.7 Varsling

Enhver oppførsel eller situasjon som bryter loven eller forskriftene (svindel, korrupsjon, alvorlige brudd på menneskerettigheter, fare for fysisk helse og sikkerhet eller miljøet osv.), og våre interne retningslinjer eller prosedyrer (anti-korrupsjonspolicy, etiske retningslinjer osv.) skal rapporteres. Det er en pågående prosess for implementering av et verktøy for dette formål.

2.8 Mål og fremgang

Orange Cyberdefense Norge AS jobber kontinuerlig med å vurdere risiko knyttet til våre aktiviteter og forretningsforbindelser (leverandører og partnere).
Åpenhetsloven ga en ny dimensjon til dette arbeidet og fokuset fremover vil være å tilpasse Orange group sine rutiner og prosesser til kravene og rapporteringen i åpenhetsloven.

2.8.1 Mål fremover

Tilpassing av eksisterende prosesser til åpenhetsloven	Pågående
Videreutvikling av vår due diligence med hele forsyningskjeden som omfang	Pågående
Automatiserte CSR-vurderinger	Pågående
4. TILTAK FOR Å STOPPE, FORHINDRE ELLER BEGRENSE NEGATIVE KONSEKVENSER	Pågående
5. MÅLING AV TILTAK – IMPLEMENTERING OG RESULTATER – rutiner mm.	Planlagt
6. KOMMUNIKASJON MED BERØRTE PARTER OG INTERESSENTER	Pågående

2.8.2 Iverksatte tiltak i 2022

- Forbedret analyse av nye leverandører
- Forbedret Orange Cyberdefense Group Compliance Officer function

3 DUE DILIGENCE-VURDERING

3.1 Due diligence

Orange Cyberdefense Norge AS vurderer fortløpende risikoen for at vår virksomhet får negative konsekvenser for grunnleggende menneskerettigheter og anstendige arbeidsforhold.

Samlet sett utføres due diligence-vurderingen på følgende måte:

a) legge inn ansvarlig forretningsatferd i virksomheten sine retningslinjer
b) identifisere og vurdere faktiske og potensielle negative innvirkninger på grunnleggende menneskerettigheter og anstendige arbeidsforhold som virksomheten enten har forårsaket eller bidratt til, eller som er direkte knyttet til virksomhetens virksomhet, produkter eller tjenester via leverandørkjeden eller forretningspartnere
c) iverksette egnede tiltak for å stanse, forhindre eller dempe uheldige påvirkninger basert på virksomhetens prioriteringer og vurderinger i henhold til (b)
d) Dokumentere og følge opp gjennomføringen og resultatene av tiltak i henhold til (c)
e) kommunisere med berørte interessenter og rettighetsinnehavere angående hvordan ugunstige virkninger håndteres i henhold til (c) og (d)
f) sørge for, eller medvirke til, utbedring og erstatning der dette er påkrevd.

Relevante vilkår for due diligence-vurdering knyttet til selskapets virksomhet og forretningsforbindelser inkluderer:

- selskapets kontekst
- posisjon i forsyningskjeden
- type produkt og tjenester

3.2 Våre leverandører

Orange Cyberdefense Norge AS har totalt 223 leverandører og produsenter innen utgangen av 2022.

I 2022/2023 har vi for å optimalisere ressursene valgt å se nærmere på alle leverandører og produsenter som er kritiske til driften og/eller med en omsetning på over 0,5 millioner kroner, som tilsvarer mer enn 95 % av hele forbruket vårt.

Dette gir oss 17 leverandører og 10 produsenter. Disse 27 relasjonene er lokalisert som følge:

	Antall leverandører / produsenter
Norge	12
EU	3
UK	1
Israel	1
USA	10

3.3 Due diligence-vurdering av våre tjenester

3.3.1 Managed Services and Professional Services

Orange Cyberdefence Norge AS Managed Services and Professional Services leveres til våre kunder av våre ansatte i Norge eller av ansatte i andre Orange Cyberdefense-enheter innenfor EU. Programvaren som noen ganger brukes til å levere disse tjenestene kjøpes fra nøkkelaktører i Cybersecurity-industrien, med opprinnelse hovedsakelig i USA. Disse leveransene vurderes til lav risiko for brudd på menneskerettigheter og anstendige arbeidsforhold i egen bedrift, i verdikjeden eller hos forretningspartnere.

3.3.2 Underleverandører/eksperter

Når det gjelder underleverandørene som brukes til å utvide kompetanse og kapasitet i oppdrag, er vurderingen at de utgjør en lav risiko. Det dreier seg i hovedsak om kompetansebaserte virksomheter med høyt utdannet personell i et ryddig og oversiktlig norsk arbeidsmarked.

3.3.3 Videresalg av tredjepartsutviklet maskinvare og programvare

Produsenter av maskinvare, som servere, nettverkskomponenter, mobiltelefoner, bærbare datamaskiner og dataskjermer utgjør en høyere risiko for brudd på menneskerettigheter og anstendige arbeidsforhold på grunn av produksjonsrelaterte forhold. Dette er elementer som vurderes i vår anskaffelsesprosess fremover, men det er få alternativer i dagens marked.

Majoriteten av leverandørene av lisensene som vi videreselger til våre kunder er kjente leverandører og ledende i Cyber Security-industrien. Alle, bortsett fra én, har sin opprinnelse fra USA og det må anses rimelig å tro at disse leverandørene er underlagt gjeldende forskrifter i USA og risikoen bør begrenses. Produsenten utenfor USA har opprinnelse i Israel og er et av de ledende selskapene i sin bransje i verden.

3.4 Resultat av due diligence-vurderingen

Orange Cyberdefense Norge AS anser at vi opererer i en bransje og på steder der det er lav risiko for brudd på områder som personvern, forretningsadferd, HMS, menneskerettigheter, arbeidsforhold og korrupsjon. Vi gjør også en tilsvarende vurdering av våre underleverandører.

Internasjonale tilbydere av skytjenester vurderes å representere middels risiko for brudd på menneskerettigheter og arbeidsforhold.

Leverandører innen produksjon av mobiltelefoner, bærbare datamaskiner og dataskjermer utgjør en høy risiko for menneskerettigheter og arbeidsforhold.

Område	Tjeneste	Risiko	Grad av innflytelse
Leverandører/ produsenter			
Programvare	Abonnementslisenser	Moderat	Lav*
Maskinvare	Servers, Firewalls, Laptops etc	Høy	Lav*
	Subcontractors/experts	Lav	Moderat/Høy
Orange Cyberdefense Norge AS / andre europeiske Orange Cyberdefense-enheter	Managed Services and Consulting Services	Lav	Høy

*) Vi vurderer mulighetene våre til å påvirke disse foretakene som lave ettersom vi ikke har noen betydelig innflytelse basert på volumene våre eller posisjonen i markedet.

Identifisert (risiko for) brudd på menneskerettigheter / anstendige arbeidsforhold	Geografi	Kilde
Ansattes rettigheter i forhold til utvinning av råvarer, produksjon av komponenter, og i noen grad montering av mobiltelefoner, bærbare datamaskiner og dataskjermer. Spesielt i form av lav lønn, tvungen overtid, misbruk av studenter som arbeidskraft, oppsigelse av fagforeningsledere.	Kina og andre asiatiske land	Internasjonal media og www.swedwatch.org og www.amnesty.org.
Risiko for brudd på organisasjonsfrihet, lønnsvilkår, arbeidstid, HMS, overvåking av ansatte.	USA	Internasjonal media og Human Rights Watch

4 TILTAK FOR Å STOPPE, FORHINDRE ELLER BEGRENSE NEGATIVE KONSEKVENSER

Vi har ennå ikke iverksatt noen avbøtende tiltak basert på vurderingsfunn for 2022/23 da dette vil kreve mer tid til identifisering, vurdering, utvelgelse og planlegging og gjennomføring.

Fokusområder vil være løpende og forbedret tredjepartsanalyse av nye og eksisterende leverandører og produsenter sammen med forbedret intern opplæring og opplæring for relevante ansatte.

5 OPPFØLGING AV TILTAK – IMPLEMENTERING OG RESULTATER

Planlagt i H2-2023

6 KOMMUNIKASJON MED BERØRTE INTERESSENTER

Planlagt i H2-2023

Oslo 30 Juni 2023

Orange Cyberdefense Norge AS, Styret

Leif Gyllenberg Styreledare	Kaja Narum Styremedlem	Marc Goegebuer Styremedlem