

An iceberg floating in the ocean. The tip of the iceberg, which is visible above the water, is relatively small and contains a few people. The much larger part of the iceberg is submerged underwater, representing hidden risks or challenges. The background is a blue sky with a bright sun and clouds.

GDPR- & cybersikkerhed

Compliancestrategi 2022 - 2025

VISION OG MISSION

Kalundborg Forsynings Compliancevision

“Vi udvikler en compliant forsyning, der kan sætte standarden for sikring af persondata og cybersikkerhed i resten af forsyningsbranchen”

Kalundborg Forsynings Compliancemission

“Vores complianceniiveau skaber trygge rammer for kunder, samarbejdspartnere og medarbejdere med fokus på efterlevelse af lovkrav, IT-sikkerhed og oplysning”



PÅ FORKANT MED FREMTIDENS COMPLIANCE

Kalundborg Forsyning har i den overordnede strategi "På forkant med fremtiden" sat som mål, at der skal arbejdes med organisations- og forretningsudvikling. Samtidig skal vi være en bæredygtig og datadreven virksomhed.

Compliance skal understøtte denne strategi. Det er nødvendigt, at der er tillid til Kalundborg Forsyning overholder de formelle lovkrav, og kan sikre en stærk cybersikkerhed.

Virksomheder i alle størrelser udsættes i disse år i stigende grad for cyberangreb, og metoderne er mange og avancerede.

Det gælder alle brancher overalt i verden – og derved også alle vores kunder og samarbejdspartnere.

Kalundborg Forsyning er en del af den kritiske infrastruktur i Danmark. Det betyder, at forsyningssikkerheden er i fokus. Vi skal være ekstra agtpågivende, når eksempelvis konflikter og krig truer sikkerheden i Europa, som det er tilfældet i 2022.

Derfor kan vi kun formode, at kravene til især cybersikkerhed vil blive kraftigt skærpet i de kommende år.

Det betyder, at vi skal indtage en aktiv rolle, der håndterer GDPR-relaterede emner, men som også sikrer forsyningen mod truslen fra cyberkriminelle. En trussel, der også sætter medarbejderne under et stadig stigende pres, når de

skal forholde sig til mere og mere kreative og udspekulerede cybertrusler. Trusler, der involverer alt fra phishing, hacking til Social Engineering.

Alt dette mærkede Kalundborg Forsyning i august 2021, da forsyningen blev ramt af et voldsomt ransomware-angreb.

Angrebet var ikke kun en bekostelig affære. Det viste også vigtigheden af at sikre, at driften kommer op at køre igen så hurtigt som muligt, men også at en solid strategi på compliance-området spiller en stor rolle.

Kalundborg Forsyning er inde i en digital omstilling. Vi skal være datadrevne, og det sætter store krav til håndtering af data.

At være datadreven har afgørende økonomisk og udviklingsmæssig betydning for virksomheden, men kan også have vidtrækkende konsekvenser ved cyberangreb i form af tabt data og omfattende tab af anseelse og image.

Disse trusler sætter større og større krav til viden, forebyggelse og ikke mindst træning af den enkelte medarbejder. Det vil denne strategi adressere. Den vil lægge kimen til en robust og sikker forsyning på cyberområdet.

Det vil sikre os en placering i forsyningsbranchen som den ypperste standard inden for GDPR og cybersikkerhed, som resten vil stræbe efter.



COMPLIANCE

GO

STRATEGISKE RAMMER

Rammerne for den strategiske udvikling skal sikre en organisatorisk robusthed inden for cyber-sikkerhed. De skal også sikre, at de databeskyttelige regler (GDPR) overholdes.

Der arbejdes allerede med flere tiltag. Udover sekventering, geoblocking og to-faktor-godkendelse, der nu er fuldt udrullet, er der ved at blive set ind i digitale værktøjer, der kan hjælpe med systemoprydning, journalisering, samt værktøjer til at understøtte en sund digital kultur.

Rammerne er prioriteret i de nedenstående pejlemærker.

POLITIKKER OG PROCESSER

Implementering af forståelige politikker og processer

Kalundborg Forsynings interne politikker og processer skal være dækkende i forhold til nuværende og fremtidige lovkrav og reguleringer, og så skal de være forståelige for alle.

GDPR- OG CYBERAWARENESS-TRÆNING

Medarbejderne sikrer kvaliteten af GDPR- og cyberhåndtering

Medarbejderne skal kontinuerligt trænes til solid håndtering af persondata samt at kunne imødekomme cybertrusler udefra

MEDARBEJDERNES IT-KULTUR

En stærk IT-infrastruktur samt solid og vedvarende oprydningsskiltur

En solid og vedvarende oprydning på alle drev, mapper og i e-mailsystemer samt journaliseringssystem vil sikre et højt compliance-niveau, og mindske risikoen for data-læk.

VIDENDELING, SAMARBEJDE OG NETVÆRK

Gennem øget KCS-integration og andre netværk

Videndeling på et komplekst område, såsom GDPR, vil give stor værdi for både Kalundborg Forsyning og dets samarbejdspartnere. Især i forhold til vores involvering i KCS vil det være et stort løft for GDPR-området i sin enkelthed, og for forsyningsbranchen i særdeleshed.

D-MÆRKET

D-mærket vil understøtte et stærkt complianceniiveau og øge erhvervskundernes tillid til os

Certificeringer vil i stigende grad blive efterspurgt som et krav i fremtiden, da forsyningssikkerhed og sikring af kritisk infrastruktur på sigt vil blive en strategisk ressource. Kalundborg Forsyning har mulighed for at konsolidere sin position som troværdig leverandør ved at arbejde hen imod og efterleve principperne i en D-mærkning/certificering på GDPR og cyberområdet.

STRATEGISKE INDSATSOMRÅDER

COMPLIANCE

De strategiske rammer kræver en fælles compliance-kultur, hvor den enkelte medarbejder spiller en afgørende rolle.

Rammerne for en solid compliance (GDPR og cyber-awareness) kræver fokus på nogle særlige strategiske indsatsområder.

Særligt syv indsatsområder kræver et strategisk fokus.



Beredskab

Politikker og planer skal bære den strukturelle del af forsyningens compliance. Det indebærer en operationel struktur der er gennemskuelig og letforståelig.



Digital omstilling

Medarbejderne er vores største aktiv og det stærkeste forsvar, når det kommer til at imødekomme både nutidens og fremtidens cybertrusler.



Kommunikation

Kommunikation, intern såvel som eksternt, skal tænkes helt ind i kernen af dna'en af vores compliance. Alle i organisationen skal tage ejerskab for sikkerheden, herunder italesættelse af det personlige ansvar i relation til både persondata og cybersikkerhed.



Politikker og processer

Vi tilser, at politikker og processer er lettilgængelige og letforståelige. GDPR og dataopbevaring bliver en integreret del af auditprogrammet, hvor oprydning og kontinuerlig vedligeholdelse skal være en del af både de eksisterende processer, men også en ny digital kultur.



Risikobaseret tilgang

Kalundborg Forsyning anvender et ledelsessystem, der overvåger, evaluerer og identificerer nye risici og forbedre vores kontroller. Samtidig arbejder vi henimod standarden for D-mærket.



Sikkerhedskultur

En stærk, modstandsdygtig sikkerhedskultur skal indlejres i hele organisationen. Når der tænkes sikkerhed, mindskes de fleste risici betragteligt.



Træning og awareness

Medarbejderne skal være rustet til at modstå og håndtere en stadigt stigende cybertrussel. De vil blive trænet i forebyggelse, og blive opdateret om de sidste nye trends. Samtidig vil de blive trænet, og være i stand til at leve op til de gældende GDPR-regler.

Strategien og verdensmålene

Med denne compliancestrategi ønsker vi at tilføje verdensmål nummer 16 til de eksisterende verdensmål, som vi allerede arbejder med.

Det er vigtigt for os, at vi aktivt viser, at vi arbejder på at modstå den stigende trussel fra organiseret og grænseoverskridende kriminalitet, som er et af kendetegnene ved det aktuelle cybertrusselsbillede.

16 FRED, RETFÆRDIGHED OG STÆRKE INSTITUTIONER



Verdensmål 16 handler om retssikkerhed og at bekæmpe organiseret kriminalitet. Dette er fundamentet for en bæredygtig udvikling og verdensmålene i hele taget. Herunder hører også cyberkriminalitet.

I Kalundborg Forsyning arbejder vi med verdensmålene, såvel gennem de små daglige hverdags-opgaver som i de større projekter.



Særligt verdensmål 16, punkt 16.4 er i fokus, når det handler om compliancestrategien.

Målet for punkt 16.4 er, at ulovlige penge- og våbenstrømme væsentligt skal reduceres inden 2030. Samtidig skal indsatsen for inddrivelse og tilbagelevering af stjålne værdier, samt bekæmpelse af alle former for organiseret kriminalitet styrkes.

Netop organiseret kriminalitet blomstrer i disse år gennem grænseoverskridende cyberkriminalitet, heriblandt ransomwareangreb på virksomheder.

For Kalundborg Forsyning betyder det konkret, at vi gennem et fokus på cybersikkerhed, datasikkerhed og -sikring vil gøre det så besværligt som muligt at få ulovlig adgang til forsyningens systemer og derved profitere på vores data.

KALUNDBORG FORSYNINGS FREMTID ER COMPLIANT



Kalundborg Forsyning A/S ▪ Dokhavnsvej 15 ▪ 4400 Kalundborg

Telefon 59 57 17 00 ▪ kundecenter@kalfor.dk ▪ www.kalfor.dk

