Leverandøroppfølging sett i lys av GDPR og NIS2

Digdir

Nettverk for informasjonssikkerhet
7. mai 2025

John A. Horve
Personvernombud

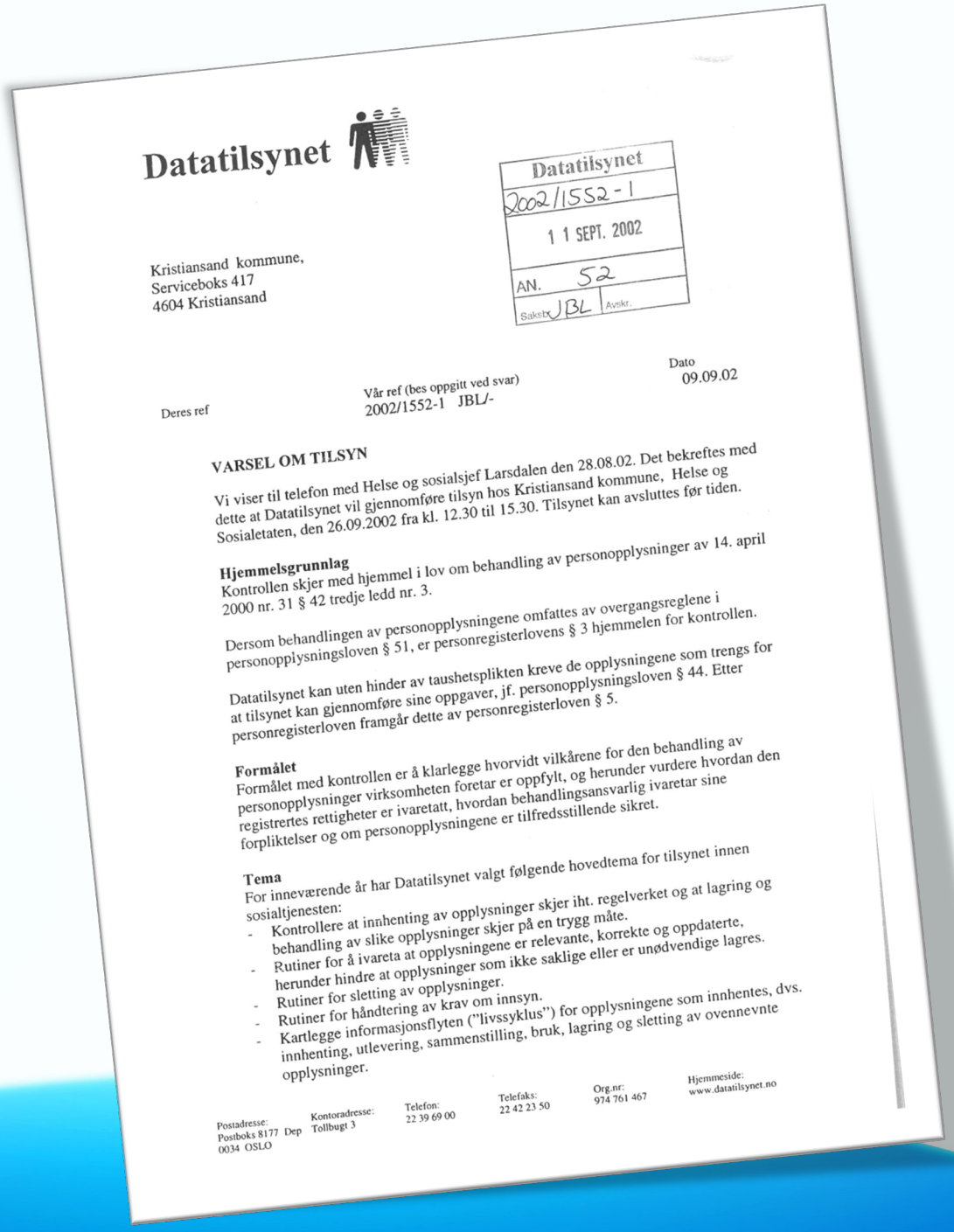
PECB Data Protection Officer
PECB ISO/IEC 27001 Lead Auditor
PECB ISO/IEC 27701 Senior Lead Implementer
PECB NIS 2 Directive Senior Lead Implementer

ikt.agder
Enklere hverdag

DISCLAIMER

Eventuelle meninger, holdninger o l som fremkommer under foredraget er foredragsholders egne meninger og representerer ikke nødvendigvis Digdir eller IKT Agder sine meninger og holdninger.

Hvor mange husker sin første?



Datatilsynet

Datatilsynet
2002/1552-1
11 SEPT. 2002
AN. 52
Saksb JBL Avskr.

Kristiansand kommune,
Serviceboks 417
4604 Kristiansand

Deres ref

Vår ref (bes oppgitt ved svar)
2002/1552-1 JBL/-

Dato
09.09.02

VARSEL OM TILSYN

Vi viser til telefon med Helse og sosialsjef Larsdalen den 28.08.02. Det bekreftes med dette at Datatilsynet vil gjennomføre tilsyn hos Kristiansand kommune, Helse og Sosialetaten, den 26.09.2002 fra kl. 12.30 til 15.30. Tilsynet kan avsluttes før tiden.

Hjemmelsgrunnlag
Kontrollen skjer med hjemmel i lov om behandling av personopplysninger av 14. april 2000 nr. 31 § 42 tredje ledd nr. 3.

Dersom behandlingen av personopplysningene omfattes av overgangsreglene i personopplysningsloven § 51, er personregisterlovens § 3 hjemmelen for kontrollen.

Datatilsynet kan uten hinder av taushetsplikten kreve de opplysningene som trengs for at tilsynet kan gjennomføre sine oppgaver, jf. personopplysningsloven § 44. Etter personregisterloven framgår dette av personregisterloven § 5.

Formålet
Formålet med kontrollen er å klarlegge hvorvidt vilkårene for den behandling av personopplysninger virksomheten foretar er oppfylt, og herunder vurdere hvordan den registrertes rettigheter er ivaretatt, hvordan behandlingsansvarlig ivaretar sine forpliktelser og om personopplysningene er tilfredsstillende sikret.

Tema
For inneværende år har Datatilsynet valgt følgende hovedtema for tilsynet innen sosialtjenesten:
- Kontrollere at innhenting av opplysninger skjer iht. regelverket og at lagring og behandling av slike opplysninger skjer på en trygg måte.
- Rutiner for å ivareta at opplysningene er relevante, korrekte og oppdaterte, herunder hindre at opplysninger som ikke saklige eller er unødvendige lagres.
- Rutiner for sletting av opplysninger.
- Rutiner for håndtering av krav om innsyn.
- Kartlegge informasjonsflyten ("livssyklus") for opplysningene som innhentes, dvs. innhenting, utlevering, sammenstilling, bruk, lagring og sletting av ovennevnte opplysninger.

Postadresse: Postboks 8177 Dep 0034 OSLO
Kontoradresse: Tollbugt 3
Telefon: 22 39 69 00
Telefaks: 22 42 23 50
Org.nr: 974 761 467
Hjemmeside: www.datatilsynet.no

ikt.agder

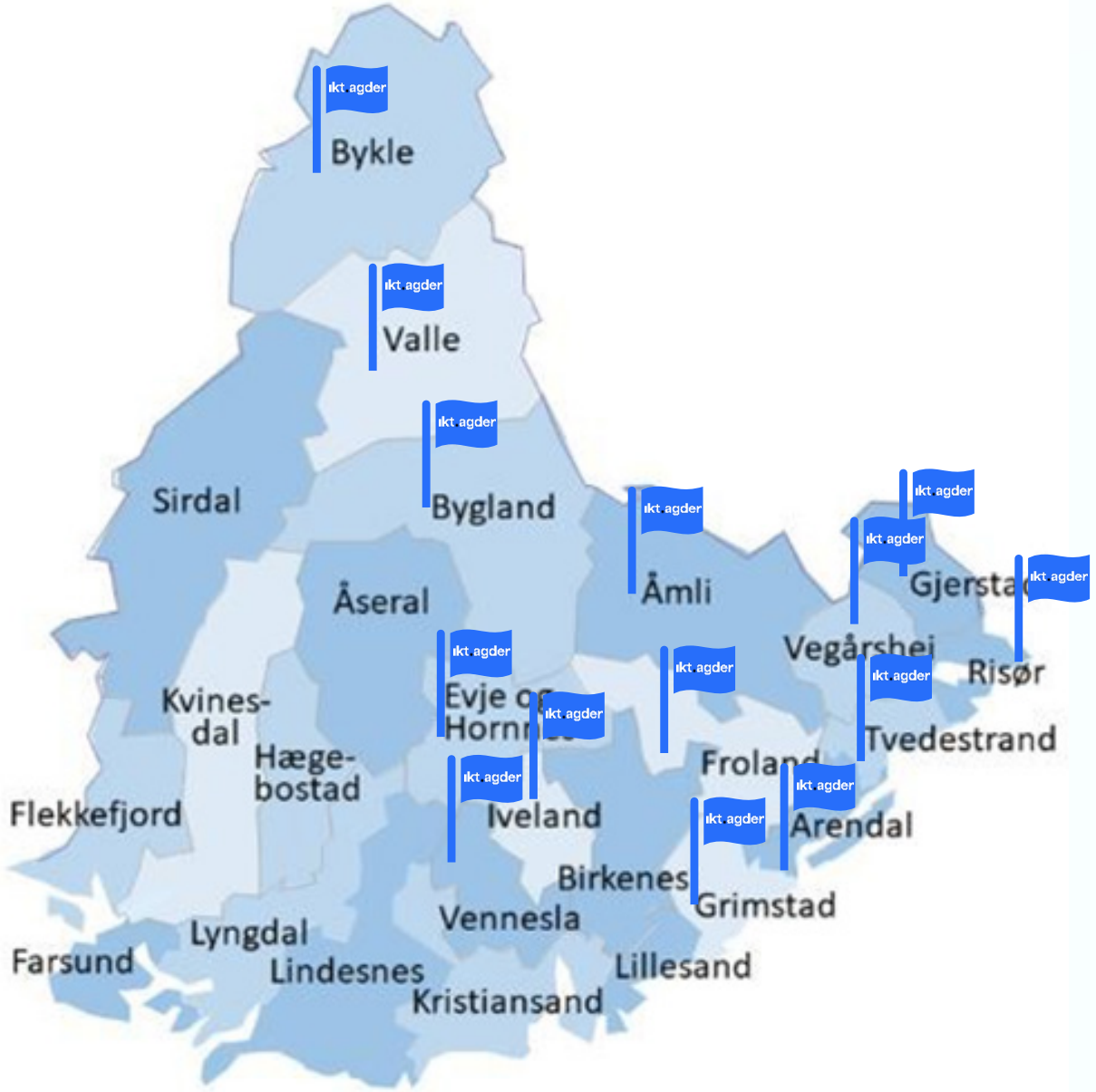
Hvem er ikt.agder ?

2002
- Arendal kommune
- Grimstad kommune
- Froland kommune
- Aust-Agder fylkeskommune

2018 (DDØ)
- Åmli kommune
- Tvedestrand kommune
- Vegårshei kommune
- Risør kommune
- Gjerstad kommune

2019
- Vennesla kommune
- Agder fylkeskommune

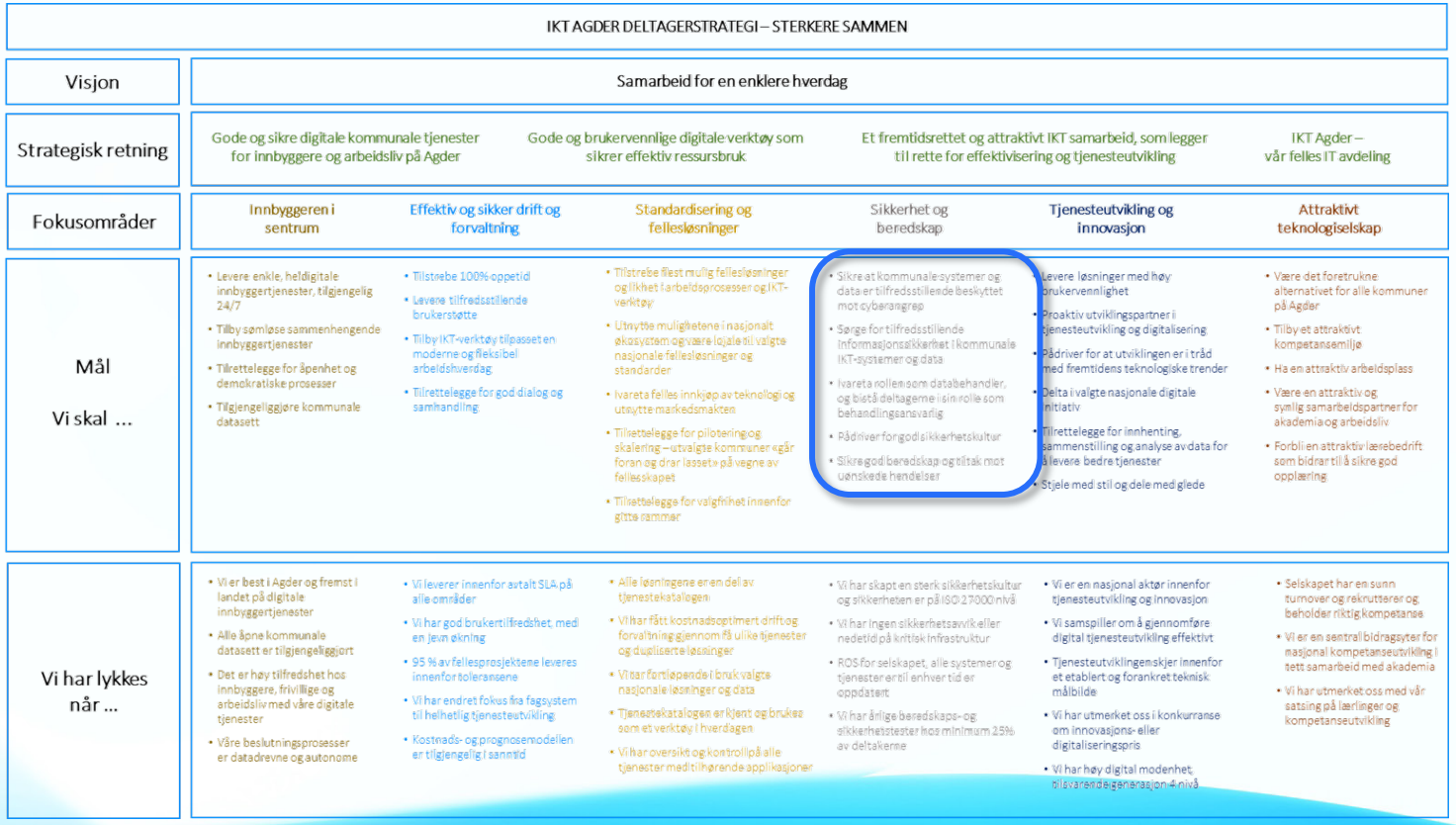
2022 (Setesdal)
- Iveland kommune
- Evje og Hornnes kommune
- Bygland kommune
- Valle kommune
- Bykle kommune



ikt.agder

Representantskapet i IKT Agder IKS

IKT Agder – Deltakerstrategi

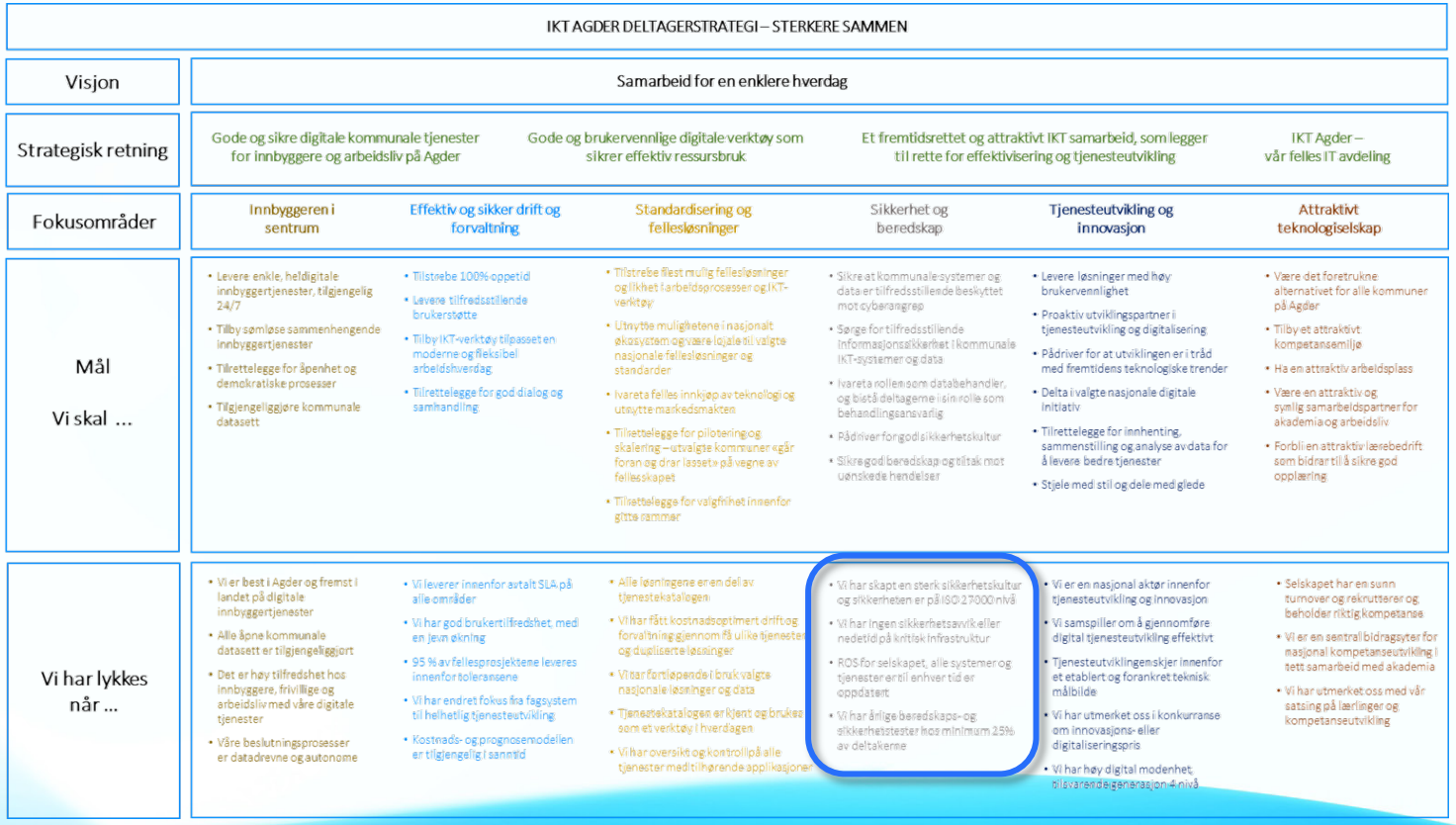


IKT AGDER DELTAGERSTRATEGI – STERKERE SAMMEN						
Visjon	Samarbeid for en enklere hverdag					
Strategisk retning	Gode og sikre digitale kommunale tjenester for innbyggere og arbeidsliv på Agder		Gode og brukervennlige digitale verktøy som sikrer effektiv ressursbruk		Et fremtidsrettet og attraktivt IKT samarbeid, som legger til rette for effektivisering og tjenesteutvikling	IKT Agder – vår felles IT avdeling
Fokusområder	Innbyggeren i sentrum	Effektiv og sikker drift og forvaltning	Standardisering og fellesløsninger	Sikkerhet og beredskap	Tjenesteutvikling og innovasjon	Attraktivt teknologiselskap
Mål Vi skal …	• Levere enkle, heldigitale innbyggertjenester, tilgjengelig 24/7 • Tilby sømløse sammenhengende innbyggertjenester • Tilrettelegge for åpenhet og demokratiske prosesser • Tilgjengeliggjøre kommunale datasett	• Tilstrebe 100%-oppetid • Levere tilfredsstillende brukerstøtte • Tilby IKT-verktøy tilpasset en moderne og fleksibel arbeidshverdag • Tilrettelegge for god dialog og samhandling	• Tilstrebe flest mulig fellesløsninger og likhet i arbeidsprosesser og IKT-verktøy • Utnytte mulighetene i nasjonalt økosystem og være lojale til valgte nasjonale fellesløsninger og standarder • Ivareta felles innkjøp av teknologi og utnytte markedsmakten • Tilrettelegge for pilotering og skalering – utvalgte kommuner «går foran og drar lasset» på vegne av fellesskapet • Tilrettelegge for valgfrihet innenfor gitte rammer	• Sikre at kommunale systemer og data er tilfredsstillende beskyttet mot cyberangrep • Sørge for tilfredsstillende informasjonssikkerhet i kommunale IKT-systemer og data • Ivareta rollen som databehandler, og bistå deltagerne i sin rolle som behandlingsansvarlig • Pådriver for god sikkerhetskultur • Sikre god beredskap og tiltak mot uønskede hendelser	• Levere løsninger med høy brukervennlighet • Proaktiv utviklingspartner i tjenesteutvikling og digitalisering • Pådriver for at utviklingen er i tråd med fremtidens teknologiske trender • Delta i valgte nasjonale digitale initiativ • Tilrettelegge for innhenting, sammenstilling og analyse av data for å levere bedre tjenester • Stjele med stil og dele med glede	• Være det foretrukne alternativet for alle kommuner på Agder • Tilby et attraktivt kompetansemiljø • Ha en attraktiv arbeidsplass • Være en attraktiv og synlig samarbeidspartner for akademia og arbeidsliv • Forbli en attraktiv lærebedrift som bidrar til å sikre god opplæring
Vi har lykkes når …	• Vi er best i Agder og fremst i landet på digitale innbyggertjenester • Alle åpne kommunale datasett er tilgjengeliggjort • Det er høy tilfredshet hos innbyggere, frivillige og arbeidsliv med våre digitale tjenester • Våre beslutningsprosesser er datadrevne og autonome	• Vi leverer innenfor avtalt SLA på alle områder • Vi har god brukertilfredshet, med en jevn økning • 95 % av fellesprosjektene leveres innenfor toleransene • Vi har endret fokus fra fagsystem til helhetlig tjenesteutvikling • Kostnads- og prognosemodellen er tilgjengelig i sanntid	• Alle løsningene er en del av tjenestekatalogen • Vi har fått kostnadsoptimert drift og forvaltning gjennom få ulike tjenester og dupliserte løsninger • Vi har fortløpende i bruk valgte nasjonale løsninger og data • Tjenestekatalogen er kjent og brukes som et verktøy i hverdagen • Vi har oversikt og kontroll på alle tjenester med tilhørende applikasjoner	• Vi har skapt en sterk sikkerhetskultur og sikkerheten er på ISO 27000 nivå • Vi har ingen sikkerhetsavvik eller nedetid på kritisk infrastruktur • ROS for selskapet, alle systemer og tjenester er til enhver tid er oppdatert • Vi har årlige beredskaps- og sikkerhetstester hos minimum 25% av deltakerne	• Vi er en nasjonal aktør innenfor tjenesteutvikling og innovasjon • Vi samspiller om å gjennomføre digital tjenesteutvikling effektivt • Tjenesteutviklingen skjer innenfor et etablert og forankret teknisk målbilde • Vi har utmerket oss i konkurranse om innovasjons- eller digitaliseringspris • Vi har høy digital modenhet, tilsvarende digimaturasjon 4 nivå	• Selskapet har en sunn turnover og rekrutterer og beholder riktig kompetanse • Vi er en sentral bidragsyter for nasjonal kompetanseutvikling i tett samarbeid med akademia • Vi har utmerket oss med vår satsing på lærlinger og kompetanseutvikling

- Sikre at kommunale systemer og data er tilfredsstillende beskyttet mot cyberangrep
- Sørge for tilfredsstillende informasjonssikkerhet i kommunale IKT-systemer og data
- Ivareta rollen som databehandler og bistå deltakerne i sin rolle som behandlingsansvarlig
- Pådriver for god sikkerhetskultur
- Sikre god beredskap og tiltak mot uønskede hendelser

ikt.agder

IKT Agder – Deltakerstrategi



IKT AGDER DELTAGERSTRATEGI – STERKERE SAMMEN						
Visjon	Samarbeid for en enklere hverdag					
Strategisk retning	Gode og sikre digitale kommunale tjenester for innbyggere og arbeidsliv på Agder	Gode og brukervennlige digitale verktøy som sikrer effektiv ressursbruk		Et fremtidsrettet og attraktivt IKT samarbeid, som legger til rette for effektivisering og tjenesteutvikling		IKT Agder – vår felles IT avdeling
Fokusområder	Innbyggeren i sentrum	Effektiv og sikker drift og forvaltning	Standardisering og fellesløsninger	Sikkerhet og beredskap	Tjenesteutvikling og innovasjon	Attraktivt teknologiselskap
Mål Vi skal …	• Levere enkle, heldigitale innbyggertjenester, tilgjengelig 24/7 • Tilby sømløse sammenhengende innbyggertjenester • Tilrettelegge for åpenhet og demokratiske prosesser • Tilgjengeliggjøre kommunale datasett	• Tilstrebe 100% oppetid • Levere tilfredsstillende brukerstøtte • Tilby IKT-verktøy tilpasset en moderne og fleksibel arbeidshverdag • Tilrettelegge for god dialog og samhandling	• Tilstrebe flest mulig fellesløsninger og likhet i arbeidsprosesser og IKT-verktøy • Utnytte mulighetene i nasjonalt økosystem og være lojale til valgte nasjonale fellesløsninger og standarder • Ivareta felles innkjøp av teknologi og utnytte markedsmakten • Tilrettelegge for pilotering og skalering – utvalgte kommuner «går foran og drar lasset» på vegne av fellesskapet • Tilrettelegge for valgfrihet innenfor gitte rammer	• Sikre at kommunale systemer og data er tilfredsstillende beskyttet mot cyberangrep • Sørge for tilfredsstillende informasjonssikkerhet i kommunale IKT-systemer og data • Ivareta rollen som databehandler, og bistå deltagerne i sin rolle som behandlingsansvarlig • Pådriver for god sikkerhetskultur • Sikre god beredskap og tiltak mot uønskede hendelser	• Levere løsninger med høy brukervennlighet • Proaktiv utviklingspartner i tjenesteutvikling og digitalisering • Pådriver for at utviklingen er i tråd med fremtidens teknologiske trender • Delta i valgte nasjonale digitale initiativ • Tilrettelegge for innhenting, sammenstilling og analyse av data for å levere bedre tjenester • Stjele med stil og dele med glede	• Være det foretrukne alternativet for alle kommuner på Agder • Tilby et attraktivt kompetansemiljø • Ha en attraktiv arbeidsplass • Være en attraktiv og synlig samarbeidspartner for akademia og arbeidsliv • Forbli en attraktiv lærebedrift som bidrar til å sikre god opplæring
Vi har lykkes når …	• Vi er best i Agder og fremst i landet på digitale innbyggertjenester • Alle åpne kommunale datasett er tilgjengeliggjort • Det er høy tilfredshet hos innbyggere, frivillige og arbeidsliv med våre digitale tjenester • Våre beslutningsprosesser er datadrevne og autonome	• Vi leverer innenfor avtalt SLA på alle områder • Vi har god brukertilfredshet, med en jevn økning • 95 % av fellesprosjektene leveres innenfor toleransene • Vi har endret fokus fra fagsystem til helhetlig tjenesteutvikling • Kostnads- og prognosemodellen er tilgjengelig i sanntid	• Alle løsningene en del av tjenestekatalogen • Vi har fått kostnadsoptimert drift og forvaltning gjennom få ulike tjenester og dupliserte løsninger • Vi har fortløpende i bruk valgte nasjonale løsninger og data • Tjenestekatalogen er kjent og brukes som et verktøy i hverdagen • Vi har oversikt og kontroll på alle tjenester med tilhørende applikasjoner	• Vi har skapt en sterk sikkerhetskultur og sikkerheten er på ISO 27000 nivå • Vi har ingen sikkerhetsavvik eller nedetid på kritisk infrastruktur • ROS for selskapet, alle systemer og tjenester er til enhver tid er oppdatert • Vi har årlige beredskaps- og sikkerhetstester hos minimum 25% av deltakerne	• Vi er en nasjonal aktør innenfor tjenesteutvikling og innovasjon • Vi samspiller om å gjennomføre digital tjenesteutvikling effektivt • Tjenesteutviklingen skjer innenfor et etablert og forankret teknisk målbilde • Vi har utmerket oss i konkurranse om innovasjons- eller digitaliseringspris • Vi har høy digital modenhet, tilsvarende digeneration 4 nivå	• Selskapet har en sunn turnover og rekrutterer og beholder riktig kompetanse • Vi er en sentral bidragsyter for nasjonal kompetanseutvikling i tett samarbeid med akademia • Vi har utmerket oss med vår satsing på lærlinger og kompetanseutvikling

- Vi har skapt en sterk sikkerhetskultur og sikkerheten er på ISO 27000 nivå
- Vi har ingen sikkerhetsavvik eller nedetid på kritisk infrastruktur
- ROS for selskapet, alle systemer og tjenester er til enhver tid er oppdatert
- Vi har årlige beredskaps- og sikkerhetstester hos minimum 25% av deltakerne

ikt.agder

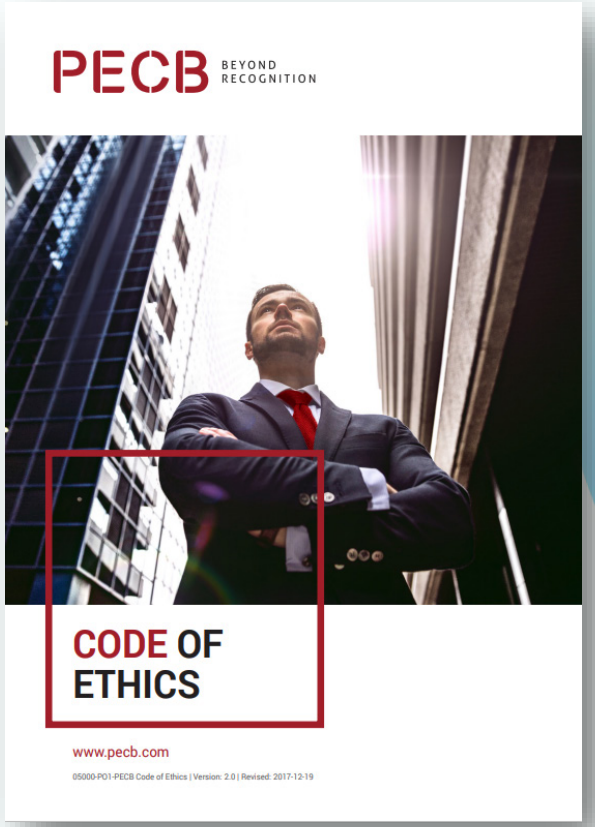
Kan dessverre ikke gå i detalj på eventuelle funn

Personopplysningsloven § 18

Forvaltningsloven § 13

Straffeloven § 209

Straffeloven § 210



ikt.agder

Personopplysningsloven § 18 –Personvernombudets taushetsplikt

Personvernombud1 plikter å hindre at andre får adgang eller kjennskap til det de i forbindelse med utførelsen av sine oppgaver får vite om

a. noens personlige forhold

b. **tekniske innretninger**, produksjonsmetoder, forretningsmessige analyser og beregninger og forretningshemmeligheter ellers når opplysningene er av en slik art at andre kan utnytte dem i sin egen næringsvirksomhet

c. **sikkerhetstiltak etter personvernforordningen artikkel 32**

d. enkeltpersoners varsling om overtredelser av loven her.

Taushetsplikten gjelder ikke dersom personvernombudet får samtykke fra den opplysningene gjelder, til å legge dem frem, eller dette er nødvendig for gjennomføring av personvernombudets lovpålagte oppgaver.

Taushetsplikten gjelder også etter at personvernombudet har avsluttet tjenesten eller arbeidet. Opplysninger som nevnt i denne paragraf kan heller ikke utnyttes i egen virksomhet eller i tjeneste eller arbeid for andre.

Forvaltningsloven § 13

Enhver som utfører tjeneste eller arbeid for et forvaltningsorgan, plikter å hindre at andre får adgang eller kjennskap til det han i forbindelse med tjenesten eller arbeidet får vite om:

1. noens personlige forhold, eller
2. **tekniske innretninger og fremgangsmåter** samt drifts- eller forretningsforhold som det vil være av konkurransemessig betydning å hemmeligholde av hensyn til den som opplysningen angår.

Som personlige forhold regnes ikke fødested, fødselsdato og personnummer, statsborgerforhold, sivilstand, yrke, bopel og arbeidssted, med mindre slike opplysninger røper et klientforhold eller andre forhold som må anses som personlige. Kongen kan ellers gi nærmere forskrifter om hvilke opplysninger som skal reknes som personlige, om hvilke organer som kan gi privatpersoner opplysninger som nevnt i punktumet foran og opplysninger om den enkeltes personlige status for øvrig, samt om vilkårene for å gi slike opplysninger.

Taushetsplikten gjelder også etter at vedkommende har avsluttet tjenesten eller arbeidet. Han kan heller ikke utnytte opplysninger som nevnt i denne paragraf i egen virksomhet eller i tjeneste eller arbeid for andre.

NSM Risiko 2023

«Rikets sikkerhet avhenger også av private virksomheter og individer. Når disse opplever en svakere økonomi, risikerer vi at sikkerheten nedprioriteres samtidig som det oppstår sårbarheter som trusselaktører vet å utnytte. Vår avhengighet av leverandører som understøtter viktige samfunnsfunksjoner må vurderes i lys av den sikkerhetspolitiske utviklingen. **Sikkerheten vår blir ikke bedre enn det svakeste leddet i leverandørkjeden**.»

«Enkeltpersoner og **tredjepartstjenester** som virksomhetene er avhengige av, **blir utnyttet** fordi de blir ansett som enklere mål enn de egentlige målene.»

ikt.agder

NSM Risiko 2024

«Det nytter ikke med eksempelvis gode fysiske sikringstiltak dersom virksomhetens verdier enkelt kan rammes digitalt eller gjennom **leverandørkjeden**. Bortfall av en underleverandør kan få alvorlige konsekvenser, ikke bare for selskaper med avhengighetsforhold, men også for nasjonal sikkerhet.»

«Det kan være lettere å utnytte en mindre, men like fullt viktig, **underleverandør** for å få tilgang til et egentlig mål.»

«**Kompromittering av slike leverandørkjeder kan få store konsekvenser** for ivaretakelsen av grunnleggende nasjonale funksjoner og nasjonale sikkerhetsinteresser. I tillegg kan trusselaktører benytte bortfall av eller stans i leveranser til virksomheter som et politisk pressmiddel.»

ikt.agder

NSM Risiko 2025

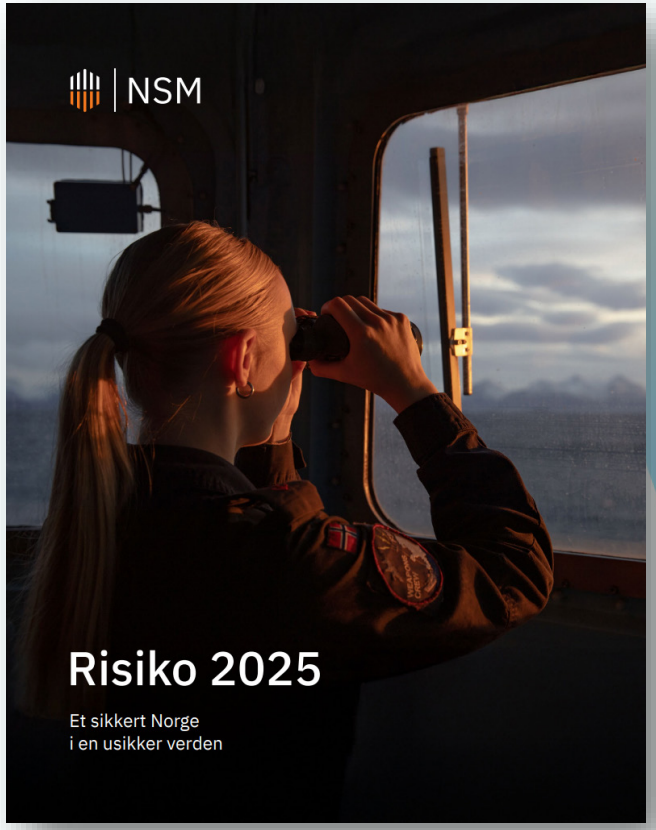
«Trusselaktørene leter langs hele **kjeden av leverandører** for å finne og utnytte sårbarheter og skaffe tilganger som kan svekke norsk forsvarsevne.»

«Gode risikovurderinger er viktig for å avklare beskyttelsesbehov og iverksette **nødvendige sikkerhetstiltak i anskaffelsesprosessen**.»

«I tillegg har virksomheter ansvar for å sørge for at **leverandører** har tilstrekkelig risiko- og sikkerhetsforståelse.»

«Flere cyberangrep utnytter **leverandørkjeder** for å ramme virksomheter»

«**Leverandørene** er ofte ikke fullt klar over egen betydning. Derfor har de heller ikke sikret egne systemer deretter.»



ikt.agder

POLITIET KRIPOS Cyberkriminialitet 2024

«I prinsippet er **alle virksomheter i Norge et potensielt mål for leverandørkjedeangrep**. Hvor utsatte virksomheter er, avhenger av hvor god styring virksomheten har på innkjøp, logistikk, sikkerhet og avhengigheter. Lovverk og reguleringer, som stiller krav til et gitt sikkerhetsnivå hos virksomheter, vil også kunne påvirke dette. Det er observert flere angrep i 2023 hvor **trusselaktør retter seg mot underleverandører** eller selskaper som lager programvare, for å kunne angripe deres kunder.»

«Internasjonal statistikk viser at rundt 1/5 av all cyberrettet kriminalitet **starter hos en tredjepartsleverandør**»

«Cyberkriminelle kan **utnytte dårlig sikkerhet hos underleverandører** i programvare og digitalt utstyr.»

ikt.agder

Cecilie Steensen Skovholt er blant de på Gardermoen som rammes av flykaoset. Foto: Naina Helén Jåma / VG

Flytrafikken rammet av global datatrøbbel

Enn så lenge er det ikke store forsinkelser på Gardermoen, men Avinor forbereder seg på følgeforsinkelser.

Emma Fondenes Øvrebø, Karoline Aga, Naina Helén Jåma (foto) og 3 til
Rapporterer fra Gardermoen

Fredag 19. juli kl. 14:09

Læses lige nu

557 læser
Internet-gigant skærer endnu dybere: Nu kommer årets anden massefyring

417 læser
Nyt Apple Watch ser ud til at blive billigt og rettet mod børn

366 læser
Her er de processorer, som AMD ikke vil sikkerhedsopdatere: Flere hundrede millioner chips berørt af 'Sinkclose'

257 læser
Star søger nye hoved-leverandører: Står klar med 350 millioner kroner til mangeårig kæmpekontrakt

239 læser
Prøvekørt: Den smukke Polestar 4 er en spøjs elbil man let bliver forelsket i

(Foto: Benoit Fraikin/Unsplash)

Tabte 170 milliarder kroner i værdi på 12 dage: Vrede aktionærer sagsøger nu Crowdstrike

Det første aktionær-sagsanlæg på grund af kursfald har ramt Crowdstrike, efter at cybersecurity-selskabets sikkerheds-brist lagde otte millioner computere ned og forårsagede it-kaos verden over.

1. august 2024 kl. 13.48

ANDERS BRUUN
Strategi- og ledelsesredaktør

En gruppe aktionærer har **lagt sag an** ved retten i Texas mod det Austin-baserede it-sikkerheds-selskab Crowdstrike.

Det sker, efter at en brist i selskabets software skabte kaos i blandt andet **lufthavne**, banker og hospitaler verden over.

Ifølge Reuters er det sagsøgernes påstand, at Crowdstrikes forsikringer om dets softwares sikkerhed var falske og misvisende.

Gruppen af sagsøgere går under navnet Plymouth County Retirement Association, Massachusetts. Ifølge gruppen betød it-sammenbruddet et stort tab af dens aktiers værdi på grund af utilstrækkelig test af selskabets software.

SENESTE ARTIKLER RSS

10:58 Norlys indsætter ny topchef: Niels Duedahl fratræder
10:25 Star søger nye hoved-leverandører: Står klar med 350 millioner kroner til mangeårig kæmpekontrakt
09:40 Million-fremgang giver dansk netbetalings-firma blod på tanden: Drømmer om at tredoble markedsandelen i Norden
08:30 Nyt Apple Watch ser ud til at blive billigt og rettet mod børn
07:58 Her er de processorer, som AMD ikke vil sikkerhedsopdatere: Flere hundrede millioner chips berørt af 'Sinkclose'
07:25 Internet-gigant skærer endnu dybere: Nu kommer årets anden massefyring
06:30 Morgen-briefing: Forrige YouTube-CEO dør som 56-årig / Trumps sociale medie bløder penge / Sikker besked-platform blokeres i Rusland
12:00 Ugen i tech: Nye AMD-processorer slippes løs - få overblikket over pris og ydelse / Rigeligt med plads: Nu kan du få svimlende otte terabyte i frimærke-format
09/08 Prøvekørt: Den smukke Polestar 4 er en spøjs elbil man let bliver forelsket i
09/08 Nørgaards vikar: Når cybersikkerhed bliver til statens skjulte magtapparat - kan Danmark så reelt modstå hybridangreb?
09/08 EU-Kommissionen er imod at ændre GDPR-reglerne – vil fokusere på implementeringen

Vis flere artikler

IT-JOB

Udviklings- og Forenklingsstyrelsen
Erfarne generalister til koordinering mellem ledelse, forretning og it-fagligheder

OK a.m.b.a.
OK søger to udviklere til vores IT-finansteam

Udviklings- og Forenklingsstyrelsen
Kontorchef til arkitektur og sikkerhed

IT-JOB

Metro Service A/S
Risk & Cyber Security Expert

Euro Accident
Technical requirement specialist (forsikringsområdet)

Udlændinge- og Integrationsministeriet
Contract Managers til kontrakt- og leverandørstyring

SEGES Innovation
Product Owner til digitale produkter hos SEGES Digital

Arbejdernes Landsbank
Data Governance Specialist

DR
Senior fullstack-udvikler til DR's valgsystem

Unik System Design A/S
Head of Internal IT

SEGES Innovation
Platform Engineer/DevSecOps med lyst til at bygge fremtidens udviklerplatform

VIS FLERE JOBS

EVENTS

Bliv klar til AI Act: Det vil påvirke både din udvikling, drift og organisation
Det Digitale Produktpas
Cyber Security Summit 2024
Cyber Security Summit 2024
Flere events »

WHITE PAPERS

Sådan høster du forretningsfordelene ved Internet of Things
Sådan får du overblik og beskytter dine cloudapplikationer
Sådan gør du: Elektronisk dokumentudveksling i praksis
Nemmere overblik, styring og omkostningskontrol i dit multicloud-miljø

Hva sier GDPR?

Official Journal
of the European Union

L 119

Volume 59
4 May 2016

English edition

Legislation

Contents

(1) Text with EEA relevance

EN

Acts whose titles are printed in light type are those relating to day-to-day management of agricultural matters, and are generally valid for a limited period.

The titles of all other acts are printed in bold type and preceded by an asterisk.

ikt.agder

Artikkel 5 - Prinsipper for behandling av personopplysninger

1. **Personopplysninger skal**
   a. behandles på en lovlig, rettferdig og åpen måte med hensyn til den registrerte («lovlighet, rettferdighet og åpenhet»),
   b. samles inn for spesifikke, uttrykkelig angitte og berettigede formål og ikke viderebehandles på en måte som er uforenlig med disse formålene; viderebehandling for arkivformål i allmennhetens interesse, for formål knyttet til vitenskapelig eller historisk forskning eller for statistiske formål skal, i samsvar med artikkel 89 nr. 1, ikke anses som uforenlig med de opprinnelige formålene («formålsbegrensning»),
   c. være adekvate, relevante og begrenset til det som er nødvendig for formålene de behandles for («dataminimering»),
   d. være korrekte og om nødvendig oppdaterte; det må treffes ethvert rimelig tiltak for å sikre at personopplysninger som er uriktige med hensyn til formålene de behandles for, uten opphold slettes eller rettes («riktighet»),
   e. lagres slik at det ikke er mulig å identifisere de registrerte i lengre perioder enn det som er nødvendig for formålene som personopplysningene behandles for; personopplysninger kan lagres i lengre perioder dersom de utelukkende vil bli behandlet for arkivformål i allmennhetens interesse, for formål knyttet til vitenskapelig eller historisk forskning eller for statistiske formål i samsvar med artikkel 89 nr. 1, forutsatt at det gjennomføres egnede tekniske og organisatoriske tiltak som kreves i henhold til denne forordning for å sikre de registrertes rettigheter og friheter («lagringsbegrensning»),
   f. **behandles på en måte som sikrer tilstrekkelig sikkerhet** for personopplysningene, herunder vern mot uautorisert eller ulovlig behandling og mot utilsiktet tap, ødeleggelse eller skade, ved bruk av egnede tekniske eller organisatoriske tiltak («integritet og konfidensialitet»).

2. **Den behandlingsansvarlige er ansvarlig for og skal kunne påvise at nr. 1 overholdes** («ansvar»).

Artikkel 24 – Den behandlingsansvarliges ansvar

1. Idet det tas hensyn til behandlingens art, omfang, formål og sammenhengen den utføres i, samt risikoene av varierende sannsynlighets- og alvorlighetsgrad for fysiske personers rettigheter og friheter, **skal den behandlingsansvarlige gjennomføre egnede** tekniske og **organisatoriske tiltak for å sikre og påvise at behandlingen utføres i samsvar med denne forordning**. Nevnte tiltak skal **gjennomgås på nytt** og skal oppdateres ved behov.

2. Dersom det står i et rimelig forhold til behandlingsaktivitetene, skal tiltakene nevnt i nr. 1 omfatte den behandlingsansvarliges iverksetting av egnede retningslinjer for vern av personopplysninger.

Krav til databehandlere i h h t GDPR

Artikkel 28 – Databehandler

1. Dersom en behandling skal utføres på vegne av en behandlingsansvarlig, skal den behandlingsansvarlige **bare bruke databehandlere som gir tilstrekkelige garantier for at de vil gjennomføre egnede tekniske og organisatoriske tiltak** som sikrer at behandlingen oppfyller kravene i denne forordning og vern av den registrertes rettigheter.
2. Databehandleren skal ikke engasjere en annen databehandler uten at det på forhånd er innhentet særlig eller generell skriftlig tillatelse til dette fra den behandlingsansvarlige. Dersom det er innhentet en generell skriftlig tillatelse, skal databehandleren underrette den behandlingsansvarlige om eventuelle planer om å benytte andre databehandlere eller skifte ut databehandlere, og dermed gi den behandlingsansvarlige muligheten til å motsette seg slike endringer.
3. …
4. **Dersom en databehandler engasjerer en annen databehandler** for å utføre spesifikke behandlingsaktiviteter på vegne av den behandlingsansvarlige, **skal nevnte andre databehandler pålegges de samme forpliktelsene** med hensyn til vern av personopplysninger som er fastsatt i avtalen eller i et annet rettslig dokument mellom den behandlingsansvarlige og databehandleren som nevnt i nr. 3, ved hjelp av en avtale eller et annet rettslig dokument i henhold til unionsretten eller medlemsstatenes nasjonale rett, der det særlig gis tilstrekkelige garantier for at det vil bli gjennomført tekniske og organisatoriske tiltak som sikrer at behandlingen oppfyller kravene i denne forordning. Dersom nevnte andre databehandler ikke oppfyller sine forpliktelser med hensyn til vern av personopplysninger, skal den opprinnelige databehandleren overfor den behandlingsansvarlige ha fullt ansvar for at nevnte andre databehandler oppfyller sine forpliktelser.

Artikkel 32 – Sikkerhet ved behandlingen

1. Idet det **tas hensyn til** den **tekniske utviklingen**, gjennomføringskostnadene og behandlingens art, omfang, formål og sammenhengen den utføres i, samt **risikoene** av varierende sannsynlighets- og alvorlighetsgrad for fysiske personers rettigheter og friheter, skal den **behandlingsansvarlige og databehandleren gjennomføre egnede** tekniske og organisatoriske **tiltak** for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen, herunder blant annet, alt etter hva som er egnet,
    a) pseudonymisering og kryptering av personopplysninger,
    b) evne til å sikre **vedvarende konfidensialitet**, **integritet**, **tilgjengelighet** og robusthet i behandlingssystemene og -tjenestene,
    c) evne til å **gjenopprette tilgjengeligheten** og tilgangen til personopplysninger i rett tid dersom det oppstår en fysisk eller teknisk hendelse,
    d) en prosess for **regelmessig testing**, **analysering** og **vurdering av hvor effektive** behandlingens tekniske og organisatoriske **sikkerhetstiltak er**.

Leverandøroppfølging

Dansk privatsykehus – minimum 1 500 000 for å ikke følge opp leverandør

DATATILSYNET

Kontakt Om os Job English Rigsfællesskabet Presse

HVAD SIGER REGLERNE? BORGER AFGØRELSER SIKKERHEDSBRUD INTERNATIONALT

Forside / Afgørelser / Afgørelser / 2024 / feb / Privathospitalet Capio A/S indstilles til bøde

Afgørelser

- Afgørelser
  - 2018
  - 2019
  - 2020
  - 2021
  - 2022
  - 2023
  - 2024
    - jan
    - feb
- Bødesager
- Generelt om tilsyn
- Tilladelser
- Historiske afgørelser

Politianmeldelse

Privathospitalet Capio A/S indstilles til bøde

Dato: 01-02-2024

Afgørelse | Private virksomheder | Politianmeldelse | Tilsyn / egendriftssag | Databehandler | Følsomme oplysninger | Grundlæggende principper

Datatilsynet anmelder Capio A/S til politiet for ikke at have ført tilsyn med databehandlere. Privathospitalet indstilles til en bøde på ikke under 1.500.000 kr.

Datatilsynet har foretaget en undersøgelse af GHP Gildhøj Privathospital ApS' (nu Capio A/S) tilsyn med databehandlere. I den forbindelse udvalgte Datatilsynet tilfældigt tre af privathospitalets databehandlere som genstand for undersøgelsen.

Undersøgelsen af Capio A/S' tilsyn med de tre databehandlere viste, at privathospitalet ikke havde ført tilsyn med databehandlerne. Det første tilsyn med hver enkelt databehandler blev først ført, da Datatilsynet indledte sin undersøgelse af privathospitalet.

På den baggrund har Datatilsynet besluttet at politianmelde Capio A/S for ikke at have handlet i overensstemmelse med det databeskyttelsesretlige princip om ansvarlighed. Det er således Datatilsynets vurdering, at privathospitalet ikke har været i stand til at sikre og påvise, at personoplysninger behandles til lovlige og rimelige formål og på en måde, som sikrer tilstrækkelig sikkerhed for de pågældende personoplysninger. Det gælder også selvom, at privathospitalet bad en anden part (en databehandler) om at behandle oplysningerne på sine vegne.

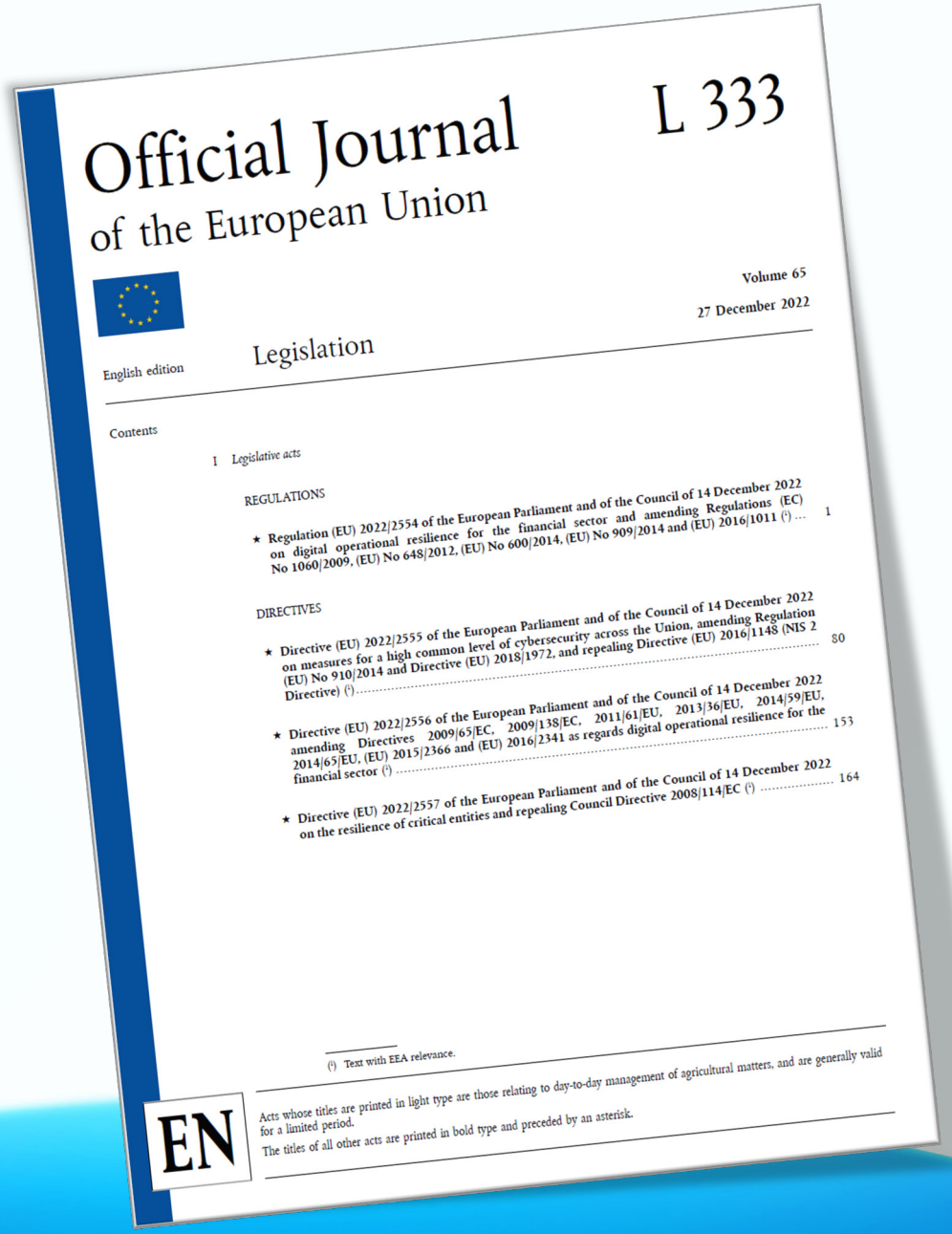
Hvorfor politianmeldelse?

Datatilsynet foretager altid en konkret vurdering af sagens grovhed i medfør af databeskyttelsesforordningens artikel 83, stk. 2, ved vurderingen af, hvilken sanktion der efter tilsynets opfattelse er den korrekte.

Datatilsynet har ved sin vurdering bl.a. lagt vægt på, at der ikke blev ført tilsyn med

ikt.agder

Hva sier NIS2?



Official Journal of the European Union

L 333

Volume 65

27 December 2022

English edition

Legislation

Contents

I Legislative acts

REGULATIONS

DIRECTIVES

(1) Text with EEA relevance.

EN

Acts whose titles are printed in light type are those relating to day-to-day management of agricultural matters, and are generally valid for a limited period.

The titles of all other acts are printed in bold type and preceded by an asterisk.

ikt.agder

Hva slags tiltak kreves i h h t NIS 2

Article 21 – Cybersecurity risk-management measures

2. The measures referred to in paragraph 1 shall be based on an all-hazards approach that aims to **protect network and information systems and the physical environment** of those systems **from incidents**, and **shall include at least the following**:

a) policies on risk analysis and information system security;

b) incident handling;

c) business continuity, such as backup management and disaster recovery, and crisis management;

d) **supply chain security**, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;

e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;

f) policies and procedures to assess the effectiveness of cybersecurity risk-management measures;

g) basic cyber hygiene practices and cybersecurity training;

h) policies and procedures regarding the use of cryptography and, where appropriate, encryption;

i) human resources security, access control policies and asset management;

j) the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate.

Article 21 – Cybersecurity risk-management measures

3. Member States shall ensure that, when considering which measures referred to in paragraph 2, point (d), of this Article are appropriate, entities take into account the **vulnerabilities specific to each direct supplier and service provider** and the overall quality of products and cybersecurity practices of their suppliers and service providers, including their secure development procedures. Member States shall also ensure that, when considering which measures referred to in that point are appropriate, entities are required to take into account the results of the coordinated **security risk assessments of critical supply chains** carried out in accordance with Article 22(1).

4. Member States shall ensure that an entity that finds that it does not comply with the measures provided for in paragraph 2 takes, without undue delay, all necessary, appropriate and proportionate corrective measures.

Fortalepunkt 133

In order to further strengthen the effectiveness and dissuasiveness of the enforcement measures applicable to infringements of this Directive, the competent authorities should be empowered to suspend temporarily or to request the temporary suspension of a certification or authorisation concerning part or all of the relevant services provided or activities carried out by an essential entity and request the **imposition of a temporary prohibition of the exercise of managerial functions by any natural person discharging managerial responsibilities at chief executive officer or legal representative level**. Given their severity and impact on the entities' activities and ultimately on users, such temporary suspensions or prohibitions should only be applied proportionally to the severity of the infringement and taking account of the circumstances of each individual case, including whether the infringement was intentional or negligent, and any actions taken to prevent or mitigate the material or non-material damage. Such temporary suspensions or prohibitions should only be applied as a last resort, namely only after the other relevant enforcement measures laid down in this Directive have been exhausted, and only until the entity concerned takes the necessary action to remedy the deficiencies or comply with the requirements of the competent authority for which such temporary suspensions or prohibitions were applied. The imposition of such temporary suspensions or prohibitions should be subject to appropriate procedural safeguards in accordance with the general principles of Union law and the Charter, including the right to an effective remedy and to a fair trial, the presumption of innocence and the rights of the defence.

Artikkel 32 nr 5 bokstav b)

request that the relevant bodies, courts or tribunals, in accordance with national law, **prohibit temporarily any natural person who is responsible for discharging managerial responsibilities at chief executive officer or legal representative level** in the essential entity **from exercising managerial functions in that entity**.

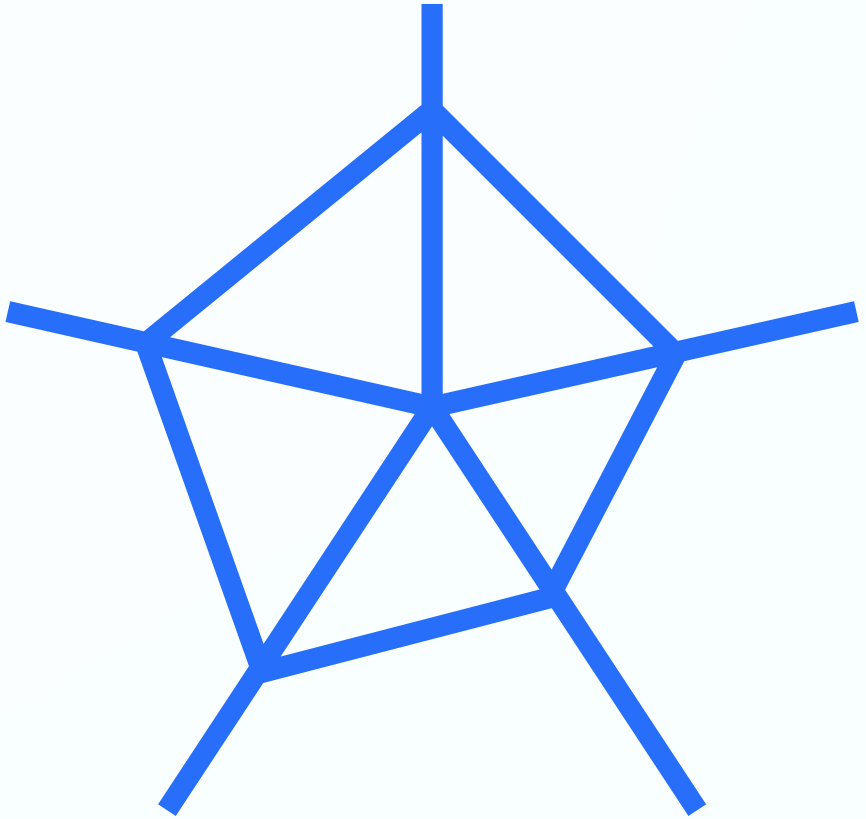
Risikobasert revisjon

Hvilken del av sikkerheten har størst risiko for oss?

-Regulatoriske krav

-Evne til å levere stabile tjenester

-Historikk



Fokusområder for denne revisjonen

Varslingsrutiner (GDPR 72 timer, NIS2 24 timer)

Backup/restore offline backup med tanke på ransomware (Tilgjengelighet)

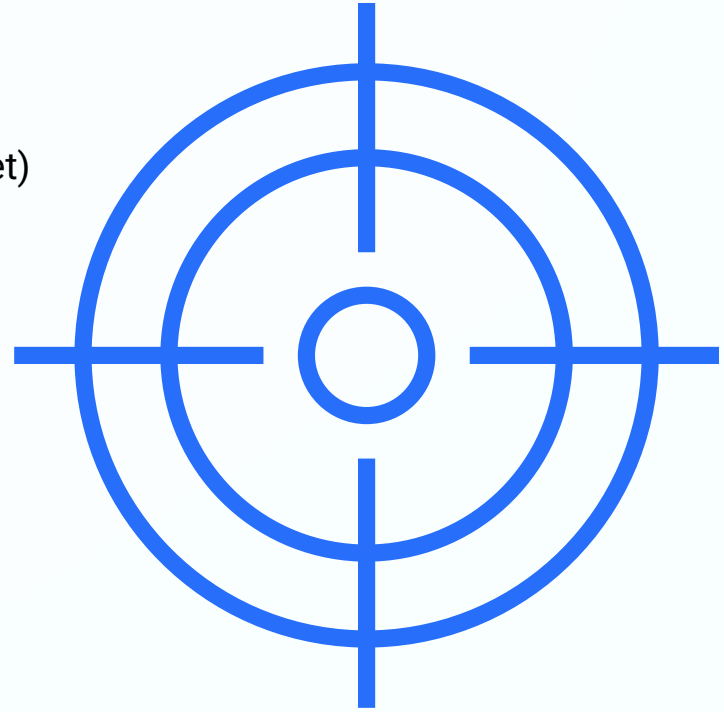
Sporbarhet – logger (analyse av hendelser)

Konfidensialitet

Robusthet i tilgangsstyring

Beskyttelse mot cyberangrep

Virksomhetskultur

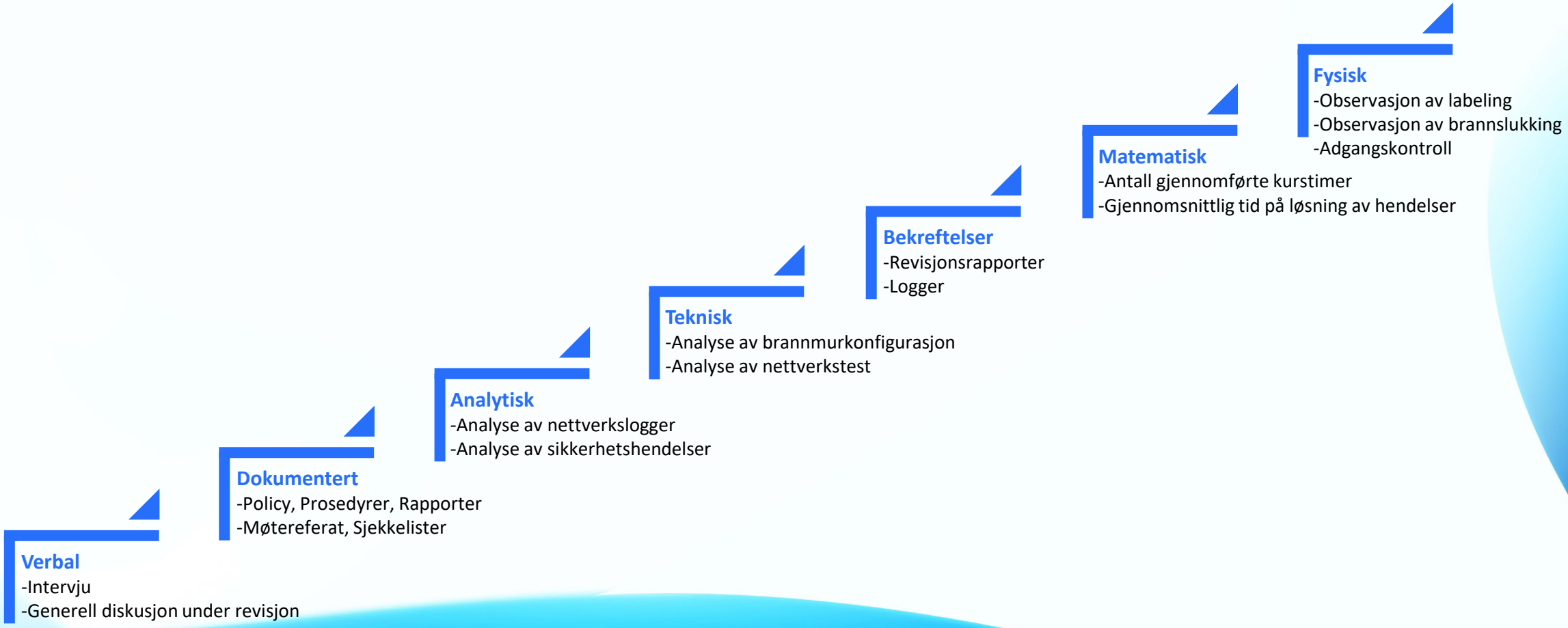


Mål med sikkerhetsrevisjonen

Søke å finne bevis på etterlevelse og tilfredsstillende informasjonssikkerhet og personvern.

ikt.agder

Revisjonsbevis



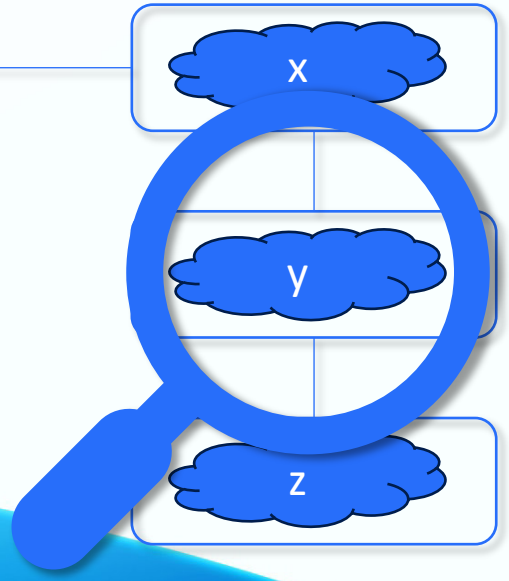
ikt.agder

Deltakere (eiere og kunder)

Andre kunder

1 2 3 4 5 6 7 n

ikt.agder



Opinion 22/2024 on certain obligations following from the reliance on processor(s

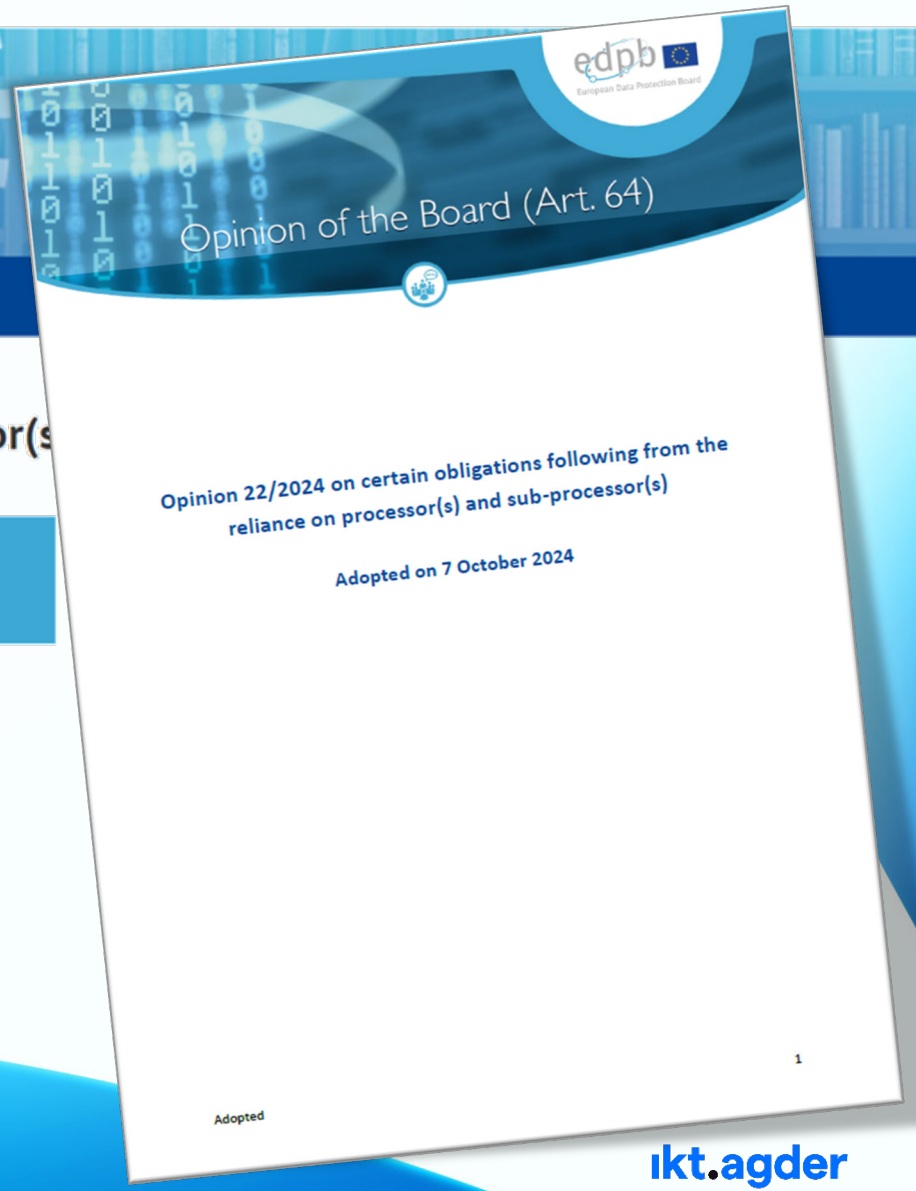
9 October 2024

Opinion 22/2024
652.5KB

Download

Denmark

Controller Processor International Transfers of Data



ikt.agder

39. In this regard, the EDPB highlights that for the purpose of assessing compliance with Articles 24(1) and 28(1) GDPR SAs should consider that the engagement of processors should not lower the level of protection for the rights of data subjects compared to a situation where the processing is carried out directly by the controller. This refers to the engagement of the initial processor, but also to the engagement of additional processors along the processing chain, e.g. sub-processors and sub-sub-processors. Articles 24(1) and 28(1) GDPR should be interpreted as **requiring the controller to ensure that the processing chain only consists of processors, sub-processors, sub-sub-processors (etc.) that provide 'sufficient guarantees to implement appropriate technical and organisational measures**'. In addition the controller should be able to prove that it has taken all of the elements provided in the GDPR into serious consideration. These considerations hold true **even if the chain of processing can be long and complex with different processors, sub-processors, etc. involved at different stages** of the processing activities. The controller should exercise due diligence in their selection of and oversight over their processors.

41. As previously mentioned by the EDPB, the controller should take into account several elements when verifying the guarantees provided by processors, and an exchange of relevant documentation will often be required. In any case, "[t]he guarantees 'provided' by the processor are those that the processor is able to demonstrate to the satisfaction of the controller, as those are the only ones that can effectively be taken into account by the controller when assessing compliance with its obligations". Neither Article 28(1) GDPR itself nor previous EDPB documents provide an exhaustive list of the documents or actions that the processor should show or demonstrate, as this largely depends on the specific circumstances of the processing. For example, **the controller may choose to** draw a questionnaire as a means to gather information from its processor to verify the relevant guarantees, ask for the relevant documentation, rely on publicly-available information and/or certifications or audit reports from trustworthy third parties and/or **perform on-site audits**.

42. The EDPB has already specified that the obligation to use only processors 'providing sufficient guarantees' contained in Article 28(1) GDPR is a continuous obligation, and that **the controller should, at appropriate intervals, verify the processor's guarantees**.

47. The Board considers that **the controller's obligation to verify whether the (sub-)processors present sufficient guarantees to implement the measures determined by the controller should apply regardless of the risk to the rights and freedoms of data subjects**.

69. This said, **the controller does not have a duty to systematically ask for the sub-processing contracts to check whether the data protection obligations provided for in the initial contract have been passed down the processing chain**. The controller should assess, on a case-by-case basis, whether requesting a copy of such contracts or reviewing them at any time is necessary for it to be able to demonstrate compliance in light of the principle of accountability. In the context of exercising its right of audit under 28(3)(h), the controller should have a process in place to undertake audit campaigns in order to check by sampling verifications that the contracts with its sub-processors contain the necessary data protection obligations.

CENTER FOR CYBERSIKKERHED

ikt.agder

Planlægning | Kravstillelse | Leverandør-valg | **Aftalen** | Styring | Afslutning

Kundens ret til at føre kontrol med leverandøren bør omfatte alle forhold relateret til leverandørens opfyldelse af kontrakten, herunder **forhold hos eventuelle underleverandører**, der bidrager til opgaveløsningen. Kontrollen med leverandøren kan udføres på flere forskellige måder (se eksempler i afsnit 5 om styring). Leverandøren bør desuden være forpligtet til at bistå kunden i forbindelse med gennemførelsen af kontrollen, herunder ved at give kunden den fornødne fysiske og logiske adgang til leverandørens lokaliteter, it-systemer og data samt ved at udlevere alt relevant dokumentation.

Cybersikkerhed i leverandørforhold

Planlægning | Kravstillelse | Leverandør-valg | Aftalen | **Styring** | Afslutning

Når aftalen mellem parterne er underskrevet, og samarbejdet går i gang, **bør kunden løbende kontrollere leverandørens efterlevelse af sikkerhedskravene i kontrakten** efter behov. Leverandørstyring giver kunden mulighed for at håndhæve kontrakten og bidrager dermed til at sikre, at leverandøren leverer den aftalte leverance og overholder sine forpligtelser i aftaleperioden.

Planlægning | Kravstillelse | Leverandør-valg | Aftalen | **Styring** | Afslutning

Risici ved utilstrækkelig leverandørstyring

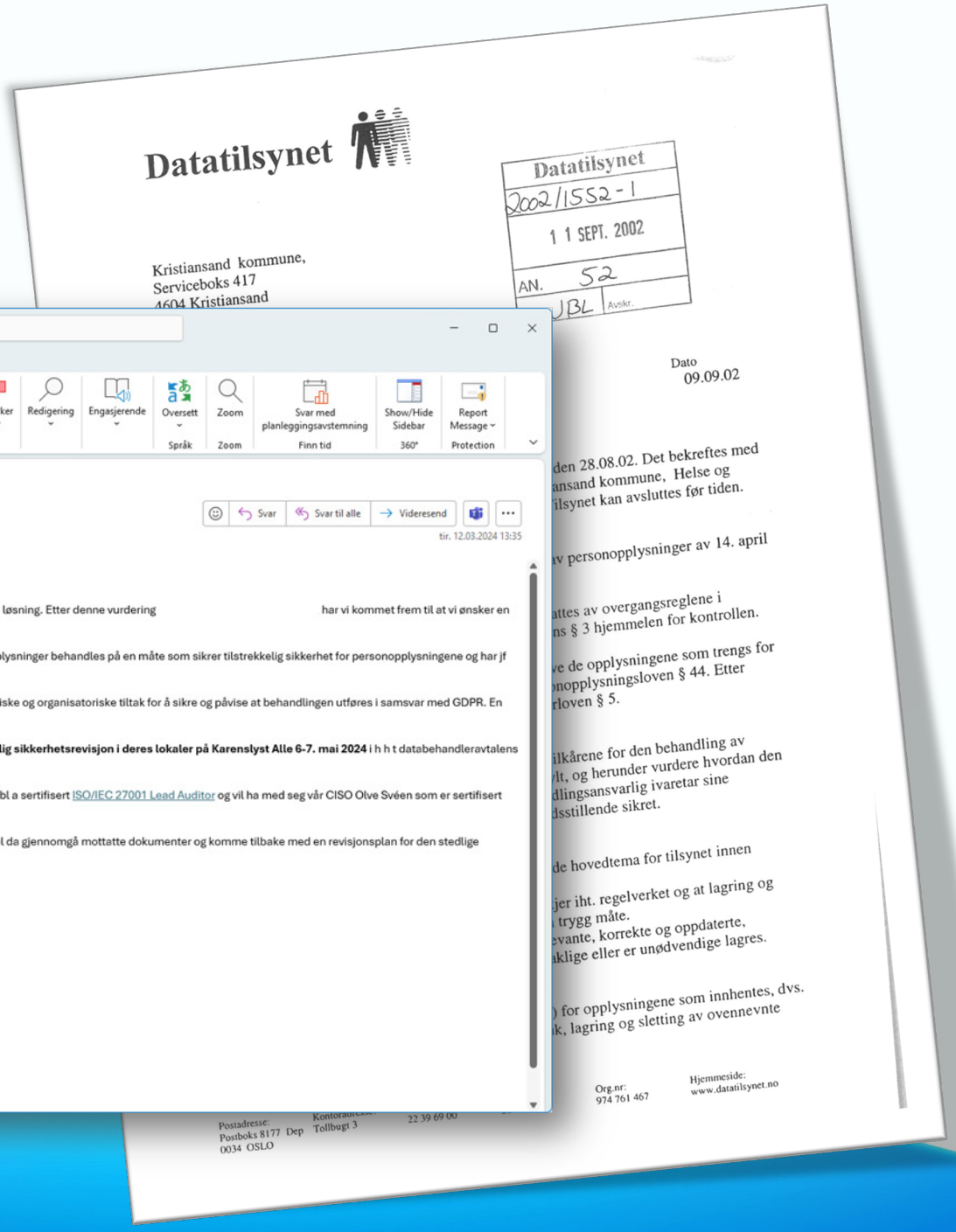
Manglende eller utilstrækkelig leverandørstyring kan blandt andet føre til:

- Utilstrækkelig risikohåndtering hos leverandøren.
- Flere fejl, forsinkelser og mangler i leverancen.
- Leverandørens manglende overholdelse af kontrakten.
- Kundens manglende håndhævelse af kontrakten.
- Leverandørens nedprioritering af kunden til fordel for andre kunder.
- Stigende leverandørafhængighed.

Litt om vår erfaring

ikt.agder

Hvor mange husker sin første?



ikt.agder

Lærdom – oppdatert databehandleravtale

11. Generelt om revisjon

11.1 Databehandler skal på forespørsel gjøre tilgjengelig for den Behandlingsansvarlige, all informasjon som er nødvendig for å påvise at forpliktelsene fastsatt i personvernforordningen artikkel 28 og denne Databehandleravtalen er oppfylt.

11.2 Databehandler skal muliggjøre og bidra ved inspeksjoner og revisjoner som gjennomføres av eller på oppdrag fra Behandlingsansvarlig. Databehandler skal også muliggjøre og bidra ved inspeksjoner fra aktuelle tilsynsmyndigheter. Den Behandlingsansvarliges tilsyn med eventuelle Underdatabehandler skal skje gjennom Databehandleren med mindre annet er særskilt avtalt. Nærmere rutiner for gjennomføring av revisjoner fremgår av Bilag C, punkt C.5.

11.3 Dersom en revisjon avdekker avvik fra forpliktelsene i Gjeldende personvernregler eller Databehandleravtalen, skal Databehandler så snart som mulig utbedre avviket. Behandlingsansvarlig kan kreve at Databehandleren midlertidig stopper hele eller deler av behandlingsaktivitetene frem til utbedringen er godkjent av Behandlingsansvarlig.

11.4 Hver av Partene dekker sine egne kostnader forbundet med en årlig revisjon. Hvis en revisjon avdekker vesentlige brudd på forpliktelsene etter Gjeldende personvernregler eller Databehandleravtalen, skal Databehandleren likevel dekke Behandlingsansvarliges rimelige kostnader forbundet med revisjonen.

ikt.agder

Lessons learned

Ha en god databehandleravtale !

☐	Behandlingsansvarlig har rett til å utføre revisjon på Databehandlers forretningssted for å verifisere Databehandlers etterlevelse av sine plikter i henhold til denne Databehandleravtalen eller Gjeldende personvernregler. Slike revisjoner skal: • Gjennomføres etter rimelig forhåndsvarsel og maksimalt én gang i året, med mindre sikkerhetsbrudd hos Databehandler eller andre særlige forhold gir grunn for hyppigere revisjoner; • Foregå innenfor normal arbeidstid og ikke forstyrre Databehandlers virksomhet unødvendig; • Utføres av ansatte hos Behandlingsansvarlig eller av tredjepart som er godkjent av Partene og underlagt taushetsplikt. Databehandler plikter å stille til rådighet de ressurser som med rimelighet kan kreves for å gjennomføre revisjonen. Behandlingsansvarlig skal dekke kostnader for eventuelle tredjeparter som benyttes til å gjennomføre revisjonen. For øvrig dekker Partene sine egne kostnader ved gjennomføring av revisjonen. Dersom revisjonen avdekker vesentlige brudd på forpliktelsene etter Gjeldende personvernregler eller Databehandleravtalen, skal Databehandler likevel dekke Behandlingsansvarliges rimelige kostnader ved revisjonen.

dfø

Databehandleravtale

Er inngått mellom:

<Angi navn på virksomhet og organisasjonsnummer>
(heretter kalt Databehandler)

og

<Angi navn på virksomhet og organisasjonsnummer>
(heretter kalt Behandlingsansvarlig)

i fellesskap kalt Partene.

Sted og dato:

nførings- eller

ignerer på vegne av

11 Generelt om revisjon

11.1 Databehandler skal på forespørsel gjøre tilgjengelig for den Behandlingsansvarlige, all informasjon som er nødvendig for å påvise at forpliktelsene fastsatt i personvernforordningen artikkel 28 og denne Databehandleravtalen er oppfylt.

11.2 Databehandler skal muliggjøre og bidra ved inspeksjoner og revisjoner som gjennomføres av eller på oppdrag fra Behandlingsansvarlig. Databehandler skal også muliggjøre og bidra ved inspeksjoner fra aktuelle tilsynsmyndigheter. Den Behandlingsansvarliges tilsyn med eventuelle Underdatabehandler skal skje gjennom Databehandleren med mindre annet er særskilt avtalt. Nærmere rutiner for gjennomføring av revisjoner fremgår av bilag C punkt C.5.

11.3 Dersom en revisjon avdekker avvik fra forpliktelsene i Gjeldende personvernregler eller Databehandleravtalen, skal Databehandler så snart som mulig utbedre avviket. Behandlingsansvarlig kan kreve at Databehandleren midlertidig stopper hele eller deler av behandlingsaktivitetene frem til utbedringen er godkjent av Behandlingsansvarlig.

11.4 Hver av Partene dekker sine egne kostnader forbundet med en årlig revisjon. Hvis en revisjon avdekker vesentlige brudd på forpliktelsene etter Gjeldende personvernregler eller Databehandleravtalen, skal Databehandleren likevel dekke Behandlingsansvarliges rimelige kostnader forbundet med revisjonen.

ikt.agder

Ikke lenge siden jeg ble møtt av denne

Kundens rett til å foreta revisjon (ref. avtalen pkt. 5.8.1.1) skal avtales i avtalen Bilag 6, i henhold til disse prinsippene:

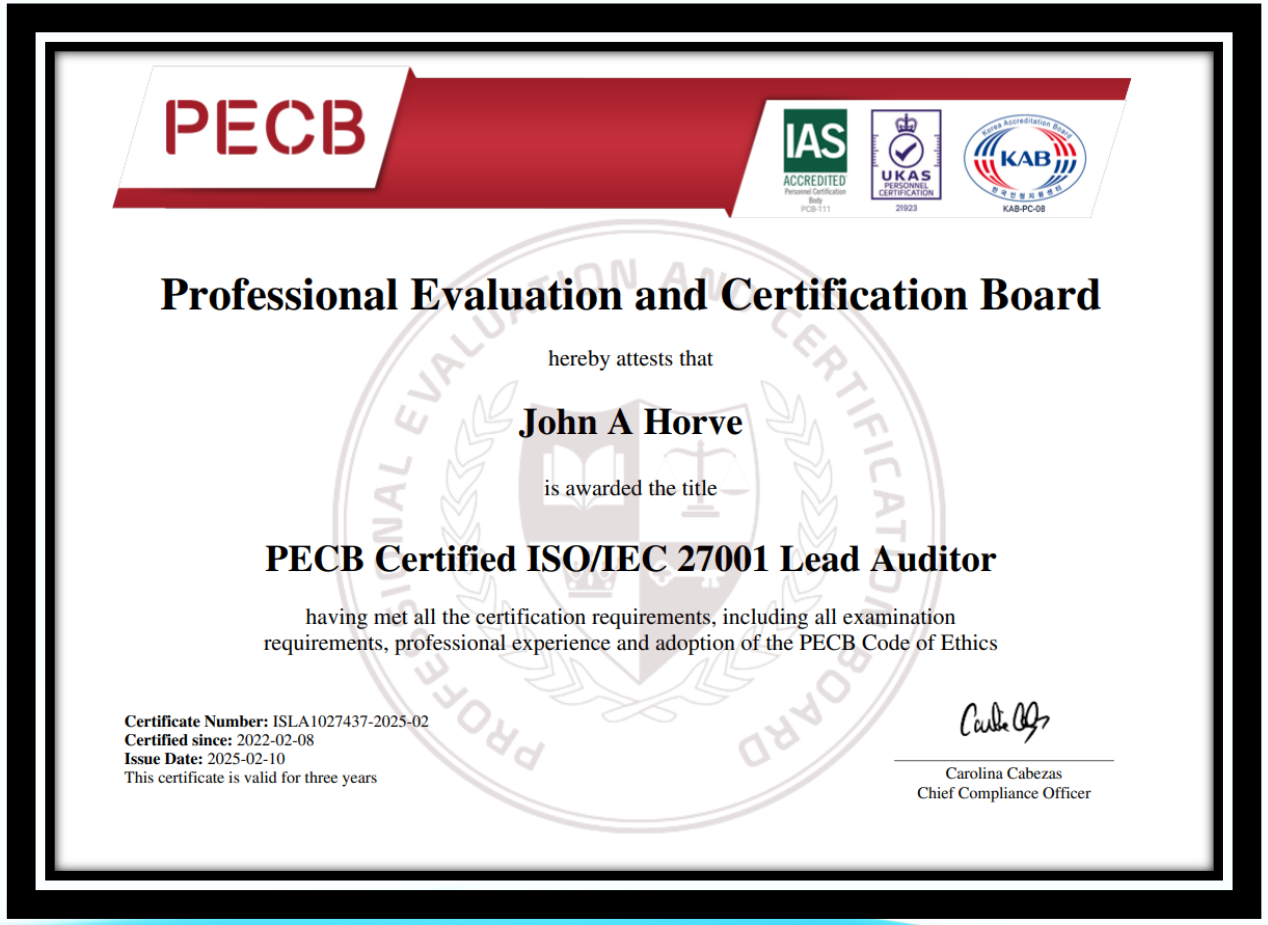
Kunden vil ha rett til å revidere NN's ytelse én gang i året, forutsatt at den oppgir gyldige grunner for å ønske det. Kunden har rett til å bruke enten interne eller anerkjente eksterne revisorer, som ikke er konkurrenter til NN eller som har jobbet i NN for mindre enn to (2) år siden, for å hjelpe til med å gjennomføre slik revisjon. Alle Kundens representanter som deltar i revisjonen, må undertegne en konfidensialitetserklæring om all informasjon som blir gitt dem under revisjonen.

Revisjon skal utføres på en slik måte at NN's forpliktelser overfor Tredjeparter på ingen måte settes i fare.

Partene skal bli enige minst fjorten (14) dager før slike revisjoner, om omfanget, tidspunktet og andre detaljer knyttet til gjennomføringen.

Kunden vil bære alle revisjonsutgifter, inkludert kostnader til eksterne revisorer, og kompensere NN for alle kostnader som følge av NNs arbeidstimer brukt i revisjonen.

Kan anbefale å ha egen revisorkompetanse i virksomheten



PECB

Professional Evaluation and Certification Board

hereby attests that

John A Horve

is awarded the title

PECB Certified ISO/IEC 27001 Lead Auditor

having met all the certification requirements, including all examination requirements, professional experience and adoption of the PECB Code of Ethics

Certificate Number: ISLA1027437-2025-02
Certified since: 2022-02-08
Issue Date: 2025-02-10
This certificate is valid for three years

Carolina Cabezas
Chief Compliance Officer

Ha en god loggfører

09:42 Vi har 5 produktfam
09:43 Strukturen i dag: Mu
09:45 Det har kostet mer e
09:46 Application security
09:46 ISO er fint, men vi m
09:47 VSP fokuserer på n
09:48 Alle produkter har e
09:48 Denne presentasjon
09:49 Security program sk
09:50 Multi er ikke ISO ser
09:51 JH: Påpeker at 340
09:51 Vi har kurs for GDPR
09:53 Sikkerhetsingeniør
09:53 Gjøres beredskapste
09:54 Testet ransomware
09:54 JH: Er det gjort noen
09:54 Ja, vi bruker Micros
09:55 I forhold til backupd
09:56 Alt logges i graylog
09:57 Vi har adferdsanalys
09:58 BCM (business cont
10:00 Om databasen korru

Normkonferansen 2025

ikt.agder

3 dagers besøk til Edinburgh i 2010 – siste budskap var:

Perfect is better than good

But good is better than nothing

Takk for oppmerksomheten

john.a.horve@ikt-agder.no

ikt.agder