Datatilsynet

Foreløpig kontrollrapport		
Saksnummer: 20/03293 Dato for kontroll: 09.11.2021 04.04.2022 06.04.2022 07.04.2022 Rapportdato: 24.06.2022	Kontrollobjekt: Kriminalomsorgen Sted: Kriminalomsorgsdirektoratet, Lillestrøm, Oslo friomsorgskontor, Oslo, Bredtveit fengsel- og forvaringsinstitusjon, Oslo, Romerike fengsel, Kløfta	Utarbeidet av: Embla Helle Nerland Camilla Nervik Maren Vaagan

Sammendrag

Datatilsynet har kontrollert kriminalomsorgens etterlevelse av personvernregelverkets sentrale krav til behandlingsansvar, sikkerhetsledelse og internkontroll. Tilsynet begynte som en brevkontroll med Kriminalomsorgsdirektoratet (KDI). I løpet av tilsynet har Datatilsynet vært på stedlige tilsyn med Kriminalomsorgsdirektoratet og tre lokale enheter. Våre vurderinger legges frem samlet i denne kontrollrapporten.

Følgende hovedfunn trekkes frem fra den foreliggende rapporten:

- Plasseringen av behandlingsansvaret i Kriminalomsorgen har vært uklar. Kriminalomsorgsdirektoratet har, underveis i tilsynsperioden, utarbeidet en instruks som avklarer ansvarsforholdene knyttet til behandling av personopplysninger. Denne instruksen har ennå ikke fått fotfeste i hele organisasjonen, og det er fremdeles uklart for flere av enhetene hvem som har ansvaret for oversikt og regelverksetterlevelse for sentrale systemer.
- Kriminalomsorgens internkontroll er mangelfull. Internkontrollen er delvis gammel og ikke oppdatert. Det meldes få avvik fra personvernregelverket i eksisterende avvikssystem, og Datatilsynets inntrykk er at dette kan skyldes manglende opplæring og kultur for personopplysningssikkerhet i organisasjonen.

Innholdsfortegnelse

1 Innledning

Datatilsynet gjennomførte vinteren 2021 og våren 2022 kontroller med kriminalomsorgen. Kontrollene ble gjennomført ved Kriminalomsorgsdirektoratet, Oslo friomsorgskontor, Bredtveit fengsel- og forvaringsanstalt, avdeling B2, og Romerike fengsel, avdeling Ullersmo. Kontrollene ble gjennomført i medhold av personopplysningsloven av 2018 § 20 og personvernforordningen artikkel 58 nr. 1.

Datatilsynet påbegynte kontrollen ved varsel om brevkontroll av 10. desember 2020. Gjennom våren 2021 kommuniserte Datatilsynet med Kriminalomsorgsdirektoratet per brev. 28. juni 2021 påla Datatilsynet direktoratet å fremlegge en oversikt over behandling av personopplysninger som gjøres i etaten, samt å redegjøre for organiseringen av behandlingsansvaret. KDI måtte også oversende gjeldende internkontroll for etaten.

På bakgrunn av de mottatte dokumentene besluttet Datatilsynet å gjennomføre stedlig tilsyn med Kriminalomsorgsdirektoratet. Tilsynet fant sted i direktoratets lokaler i Lillestrøm 9. november 2021.

Videre besluttet Datatilsynet å verifisere funnene hos Kriminalomsorgsdirektoratet ved å gjennomføre stedlige tilsyn ved tre enheter på Østlandet. Disse ble gjennomført i løpet av uke 14 i april 2022 (4., 6. og 7. april).

Datatilsynet har sett på forståelsen og organiseringen av behandlingsansvaret, samt internkontroll og sikkerhetsledelse.

Rapporten inneholder en overordnet gjennomgang av gjeldende regelverk, og hvilke funn Datatilsynet har gjort hos kriminalomsorgen sett i lys av gjeldende regelverk. Kontrollrapporten danner grunnlag for Datatilsynets videre vurderinger og eventuelle vedtak.

2 Kort om hvordan tilsynet er avgrenset

Kriminalomsorgen er en lovregulert og statlig etat, som per dags dato består av tre organisatoriske nivåer. *Kriminalomsorgsdirektoratet* utgjør ledelsen i etaten. Det andre nivået i organisasjonen er *regionene*. Etatens laveste organisatoriske nivå er *enhetene.* Her finner vi fengsler, både med lav sikkerhet og høy sikkerhet, friomsorgskontorer og overgangsboliger.

Datatilsynet avgrenset tilsynet til kriminalomsorgens tiltak og organisering i lys av personopplysningsreglene om behandlingsansvar og internkontroll.

Temaene for tilsynet omfatter organisatoriske tiltak, og det er derfor relevant å se ulike deler av organisasjonen i sammenheng. Datatilsynets fokusområde var i første omgang Kriminalomsorgsdirektoratet (KDI), som leder *etaten* kriminalomsorgen. Under det stedlige tilsynet med KDI ble det klart at temaene som tilsynet skulle belyse, også omfatter underordnede enheter. Det fremsto derfor som hensiktsmessig å stille spørsmål til flere enn øverste nivå i organisasjonen. Datatilsynet besluttet derfor å undersøke etterlevelsen av regelverket i tre lokale *enheter*.

Enhetene ble valgt ut på bakgrunn av variasjonen i ansvarsområder og størrelse. Datatilsynets hypotese var at variasjonen ville medføre ulik etterlevelse av regelverket, på grunn av ulike

lovpålagte oppgaver med tilhørende forskjellige former for behandling av personopplysninger, registrerte, og kategorier av opplysninger.

Alle enhetene befant seg i samme region, region Øst. Enhetene ble valgt på bakgrunn av sin geografiske beliggenhet (nærhet til Datatilsynets stedlige plassering).

3 Kort om kriminalomsorgen

Kriminalomsorgen er en statlig etat med ansvar for gjennomføring av straff. Oppgaver og ansvar er lovbestemt, og følger av straffegjennomføringsloven. Organiseringen av etaten følger av straffegjennomføringsloven § 5.

Kriminalomsorgen består av 33 fengsler fordelt på 58 lokasjoner, samt elleve friomsorgskontorer med 32 lokasjoner. Videre er det fire «sammenslåtte enheter» som skal sørge for sømløs straffegjennomføring, og to sentre for narkotikaprogram med domstolskontroll. Lokalt nivå omfatter også overgangsboliger.

Mellom lokalt nivå og direktorat befinner regionene seg. Det er fem regionskontorer. Kriminalomsorgens høgskole og utdanningssenter, forkortet KRUS, er også en del av etaten.

Til sammen er det omtrent 5000 ansatte i kriminalomsorgen. I 2020 var det 2932 innsatte, mot 3218 i 2019. 50 % av straffegjennomføringen skjer gjennom elektronisk kontroll, som er en form for gjennomføring av straff i samfunnet. I 2020 ble det iverksatt 5336 saker om straffegjennomføring i samfunnet, hvorav 3178 var soning med elektronisk kontroll.

KDI befinner seg i en omorganiseringsprosess, med en ny formell avdelingsstruktur fra 1. mars 2021. KDI har informert om at organisasjonen er i gang med arbeidet for å avklare interne prosesser og grensesnitt.

4 Regelverket

Behandling av personopplysninger for straffegjennomføring er ikke en del av EØS-avtalen, og heller ikke en del av de europeiske politisamarbeidet (Schengen-regelverket). Da EUs personvernforordning trådte i kraft i 2018, valgte Stortinget å videreføre personopplysningsloven av 2000 for visse typer behandlinger, herunder for straffegjennomføringsformål. Siden 2018 har Justis- og beredskapsdepartementet varslet at et lovarbeid for ny lov om behandling av personopplysninger for straffegjennomføring er underveis.

Kriminalomsorgens behandling av personopplysninger for andre formål enn straffegjennomføring omfattes av personopplysningsloven av 2018 og personvernforordningen.

I tilsynet har Datatilsynet konsentrert spørsmålene rundt behandling av personopplysninger ved gjennomføring av straff. Gjeldende relevant regelverk for tilsynet er

personopplysningsloven av 2000 med forskrift, samt straffegjennomføringsloven med forskrifter.

5 Kort om arbeidet med kontrollen før de stedlige tilsynene

I brev av 10. desember 2020 varslet Datatilsynet brevkontroll med kriminalomsorgen, ved Kriminalomsorgsdirektoratet. Datatilsynet ba om å få oversendt behandlingsprotokoll for behandlinger i kriminalomsorgen, og dersom denne ikke eksisterte, en forklaring på hvorfor denne mangler. Datatilsynet ba KDI om en forklaring av behandlingsansvaret internt i etaten.

KDI besvarte brevet 28. mars 2021. I brevet opplyste KDI at de i 2019 utarbeidet en oversikt over IKT-systemer som brukes i kriminalomsorgen, hvor det behandles personopplysninger. KDI påpekte selv at denne ikke tilfredsstilte kravene til behandlingsprotokoll. Oversikten var vedlagt brevet. KDI opplyste videre at de ikke har en samlet behandlingsprotokoll, men at KDI i 2020 gikk til innkjøp av datasystemet DraftIt, som skulle danne grunnlag for en fullverdig behandlingsprotokoll. KDI informerte om at det har blitt gjennomført DPIA for de sentrale systemene (KOMPIS (fagsystemer)). Disse systemene skal skiftes ut med et nytt, mer funksjonelt system, KODA. DPIA-en som ble gjennomført for KOMPIS inneholder en oversikt over hvilke personopplysninger som registreres. KDI skrev at det var gjort tilsvarende for arkivsystemet Doculive, GAT-timeregistrering, og Fellesområdet. På spørsmålet om behandlingsansvar opplyste KDI:

> *«Øverste behandlingsansvarlige i kriminalomsorgen er KD direktør, som er direktør for hele virksomheten. Denne myndigheten er delegert i tråd med ordinær fullmaktsstruktur i linjen, dvs til avdelingsdirektører KDI, regiondirektører og til enhetsledere (fengsel, friomsorgsledere).»*

Som vedlegg til redegjørelsen mottok Datatilsynet KDI behandlingsprotokoll som da var under arbeid. Datatilsynet mottok to versjoner av et dokument for systemoversikt og ansvar, en uferdig versjon, og en revidert versjon. Dokumentet inneholdt sentralt forvaltede systemer, men også oversikt over det KDI i dokumentet kaller «skyggesystemer». «Skyggesystemene» er systemer som KDI kjenner til at brukes i fengsler og regioner. Den reviderte versjonen av dokumentet inneholdt uavklarte spørsmål. Systemeiere var benevnt med navn, ikke roller.

Datatilsynet varslet i brev av 28. juni 2021 pålegg og ytterligere krav om opplysninger. KDI ble pålagt å etablere en oversikt over alle behandlingene av personopplysninger som gjøres i direktoratet, redegjøre for hvordan behandlingsansvaret er organisatorisk og praktisk plassert og fordelt i organisasjonen, samt å oversende gjeldende internkontroll.

KDI besvarte det siste pålegget med brev av 21. september 2021. I brevet beskrev KDI nærmere arbeidet med behandlingsprotokoller.

> *- Endelig databehandleravtale (DBA) når det gjelder behandlingen i systemene KIKS og DocuLive er under arbeid. Endringer i regelverk for overføring av personopplysninger til utlandet underveis i prosessen har komplisert dette arbeidet.*

- Vedrørende systemer hvor vi har brukt leverandørs anbefalte DBA eller personvernerklæring: Noen av de større databehandlerne har avtaler eller erklæringer som er designet for deres systemer, og vi har i protokollene henvist til lenker hvor disse befinner seg.

- Når det gjelder interne og sikrede systemer er det lagt til grunn at det ikke kreves DBA eller personvernerklæring, da dette gjelder kontorstøttesystemer eller infrastrukturtjenester som ansatte må benytte seg av for å overholde sine arbeidskontrakter. Dette gjelder eksempelvis signert erklæring om taushetsplikt, brukererklæring og leders bekreftelse av tjenestemessig behov for tilgang til systemer.

- Utdanningsmyndighetene og kriminalomsorgen har et system til bruk ved undervisning under varetekt og straffegjennomføring i fengsel. Dette systemet er basert på søknad og samtykke fra innsatte.

- Kriminalomsorgen har et system for behovs- og ressurskartlegging av innsatte og domfelte, BRIK. Det ble før innføring av dette søkt konsesjon hos Datatilsynet og systemet er forskriftsregulert. I ettertid er strgjfl. kap 1A vedtatt. Behandlingen av personopplysninger i ved bruk av systemet er i tillegg basert på skriftlig samtykke fra innsatte.

- Kriminalomsorgen utvikler for tiden flere systemer. Disse er prosjektfasen og ikke er med i protokollene, men de vil bli behandlet før de tas i bruk.

- KDI har nylig gjennomført en omorganisering av direktoratet. I tillegg utredes en større omorganisering av hele kriminalomsorgen. Dette vil kunne medføre en del endringer når det gjelder behandlingsansvarlige, men KDI legger likevel til grunn at grunnstrukturen i dagens system opprettholdes. (Se nedenfor under punkt 2).

KDI oversendte nylig utarbeidede protokoller for behandling av personopplysninger for innsatte og domfelte, og for behandling av personopplysninger for andre grupper.

KDI beskrev organiseringen av behandlingsansvaret i lys av straffegjennomføringsloven, og viste til at forarbeidene til loven uttrykker at behandlingsansvaret kan deles med ulike deler av organisasjonen. KDI opplyste videre at de har avdekket et behov for formalisering av behandlingsansvaret i uttrykkelige fullmakter/instrukser, og at de ville prioritere dette arbeidet.

KDI oversendte rammeverket for internkontrollen, og opplyste at dette ville bli oppdatert i pågående prosess med gjennomgang av informasjonssikkerheten i kriminalomsorgen.

KDI beskrev sitt videre arbeid med personvern og informasjonssikkerhet slik:

KDI vil prioritere arbeidet med ferdigstillelse av databehandleravtaler. Det vil også bli prioritert å gi en uttrykkelig delegering av ansvar til regionalt og lokalt nivå når det gjelder oppgaver under behandlingsansvaret. KDI er, som nevnt ovenfor, i en prosess

hvor det arbeides for å ta i bruk et digitalt verktøy som vil lette arbeidet med informasjonssikkerhet.

6 Funn og avvik fra lovbestemte krav til behandling av personopplysninger

6.1 Behandlingsansvar

6.1.1 Behandlingsansvar som tema for tilsynet

Datatilsynet hadde til hensikt å kontrollere hvordan kriminalomsorgen forstår og ivaretar behandlingsansvaret i etaten.

6.1.2 Krav i regelverket

6.1.2.1 Generelt om regelverket

Avklaring av hvem som har ansvar for behandling av personopplysninger, er et grunnleggende krav og premiss etter personvernregelverket. Behandlingsansvarlig er det primære pliktsubjektet etter personopplysningsloven.

Klarhet i ansvarsfordeling er særlig viktig i sammensatte organisasjoner, hvor det praktiske og daglige ansvaret kan pulveriseres som følge av uklare ansvarsforhold. I ytterste konsekvens kan uklare ansvarsforhold medføre ulik praktisering av personvernregelverket i forskjellige deler av organisasjonen.

Klarhet i ansvarsfordeling er avgjørende både for at for at den registrerte skal kunne gjøre bruk av sine rettigheter etter loven, og for at tilsynsmyndigheten skal vite hvem som har ansvaret for etterlevelse av personvernregelverket.

Personopplysningsloven § 2 nr. 4 definerer behandlingsansvarlig som «den som bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler som skal brukes».

Databehandler er i § 2 nr. 5 definert som «den som behandler personopplysninger på vegne av den behandlingsansvarlige».

Personopplysningsforskriften § 2-7 stiller krav om at det skal etableres klare ansvars- og myndighetsforhold for bruk av informasjonssystemet. Forholdene skal dokumenteres.

Straffegjennomføringsloven § 4b slår fast at med «behandlingsansvarlig menes den som etter lov eller forskrift, alene eller sammen med andre, bestemmer formålet med behandlingen og hvilke hjelpemidler som skal brukes.»

I straffegjennomføringsloven § 4 a er det presisert at personopplysningsloven gjelder utfyllende til reglene i straffegjennomføringsloven kapittel 1 A, «Behandling av personopplysninger i kriminalomsorgen». I forarbeidene til straffegjennomføringsloven kapittel 1 A, Prop. 151 L (2009-2010) er det lagt til grunn at behandlingsansvaret i kriminalomsorgen kan være delt.

Forskrift om behandling av personopplysninger i kriminalomsorgen regulerer enkelte behandlingsaktiviteter nærmere. [1] Retten til retting, sperring og sletting av opplysninger er presisert i forskriften § 6, og ansvaret for å håndtere begjæringer om slike personvernrettigheter er i § 8 lagt til lokalt nivå i kriminalomsorgen. Etter forskriften § 9 er regionalt nivå klagemyndighet etter beslutninger fattet av lokalt nivå i medhold av § 8.

6.1.2.2 Behandlingsansvar i offentlig virksomhet

Personvernregelverkets definisjon av behandlingsansvar er todelt. Den behandlingsansvarlige bestemmer formålet og midlene med behandlingen. For offentlige virksomheter, som kriminalomsorgen, er formålet i stor grad lovfestet. Det kan tenkes behandlinger av personopplysninger som ikke følger av sektorlovgivning eller forvaltningsretten, og som dermed overlater større grad av frihet til den behandlingsansvarlige til å bestemme formålet. For alle praktiske formål er det likevel slik at formålet med behandling av personopplysninger for utøvelse av offentlig myndighet i offentlige virksomheter bestemmes i lov eller forskrift.

Ved å undersøke hvem som bestemmer hvilke midler som brukes for behandlingen av personopplysninger, vil det fremkomme tydelige indikasjoner på hvem som faktisk er behandlingsansvarlig i en offentlig virksomhet. Spørsmålene som ble stilt under kontrollen reflekterer denne forståelsen av problemstillingen.

6.1.3 Faktiske forhold

6.1.3.1 Generelt hos KDI

Ledelsen i Kriminalomsorgsdirektoratet uttalte under tilsynet at to ulike regelsett kompliserer arbeidet med personvern i kriminalomsorgen. Nye regler har vært ventet i lengre tid, og KDI ser frem til fremtidig regulering. I mellomtiden søker KDI å harmonisere regelverket ved å sørge for én forståelse av behandlingsansvaret og ved utarbeidelse av protokoller.

Ledelsen i Kriminalomsorgsdirektoratet har organisert behandlingsansvaret etter følgende prinsipper:

- *Direktør KDI når det gjelder behandlinger i direktoratet og ellers gjennomgående etatssystemer og direktoratets ansvar knyttet til informasjonssikkerhet på overordnet nivå.*
    - *Regiondirektørene ivaretar oppgaver for å sikre ivaretakelse i regionene*
    - *Fengselsleder og friomsorgsleder ivaretar oppgaver for å sikre ivaretakelse på enhetsnivå.*
    - *Direktør ved KRUS ivaretar oppgaver for å sikre ivaretakelse ved KRUS.*

Ledelsen i Kriminalomsorgsdirektoratet anser at lovreguleringen av etatens organiseringen medfører at behandlingsansvaret må sees i sammenheng med organiseringen av etaten. Det er direktoratet som har totalansvar for å styre etaten, slik at det også er direktoratet som har det overordnede behandlingsansvaret. Det er imidlertid en praksis for at enhetene selv har ansvar

[1] FOR-2013-09-20-1099, jf. straffegjennomføringsloven § 4e

for oppgavene de er tillagt i tråd med organiseringen. Dette medfører at direktoratets ledelse anser at direktoratet har et «selvstendig» behandlingsansvar for personopplysningene som behandles direkte av dem. Samtidig er det klart at KDI er etatsleder, og har et spesielt ansvar med hensyn til styringen.

KDI skiller mellom begrepene «styringsansvar» og «selvstendig ansvar». «Selvstendig ansvar» er knyttet til oppgavene hvert nivå og enhet har innen straffegjennomføringen.

KDI betonte under tilsynet at de arbeider med å dokumentere behandlingsansvaret. Dette er et arbeid som ble igangsatt etter at tilsynet ble åpnet, men før Datatilsynet var på stedlig kontroll hos KDI.

6.1.3.2 Eksempler på praktisk innretting av behandlingsansvaret

6.1.3.2.1 Anskaffelse av sentrale systemer

KDI har forståelsen av at de beslutter anskaffelse og rutiner for utstyret som brukes og styres av KDI. Eksempler på dette er sporingsteknologi (radiofrekvensteknologi og GPS-sporing) som brukes i forbindelse med gjennomføring av elektronisk kontroll, gjennom elektronisk fotlenke, og teknologi som brukes for å gjennomføre videosamtale av innsatt i fengsel (VIS). Også pust- og bevegelsessensorer som brukes i celler i fengsler er anskaffet av direktoratet.

KDIs begrunnelse for at det er KDI som har ansvar for innkjøp og forvaltning av denne teknologien, er knyttet til det spesielle markedet for innkjøp av programvare og maskinvare for straffegjennomføringsformål.

Gjennomgående systemer i etaten er felles for alle nivåer og enheter. Dette er blant annet journalføringssystemet KOMPIS, og arkivsystemet DocuLive. KDI har ansvar for support og oppfølging av systemene. Dette gjøres gjennom KDIs IT-avdeling.

KOMPIS er kriminalomsorgens fagsystem, og brukes til journalføring og dokumentering. Opplæring gjøres hovedsakelig gjennom utdanningen på Kriminalomsorgens utdanningssenter. Noe opplæring gjøres likevel lokalt. Superbrukere har også noe ansvar for opplæring i lokale enheter. KOMPIS er integrert mot DocuLive, grunnet hensyn til og behov for arkivering og lagring. Dersom det skjer en feil i KOMPIS eller DocuLive vil denne som hovedregel være felles for alle enheter.

Pust- og bevegelsessensor på celler styres fra sentralt hold. Disse er også anskaffet sentralt. Alarmene knyttet til systemet går av lokalt i enheten, og deles ikke med etatens sentralledd. Fysisk adgangskontroll i fengslene skjer gjennom fysiske tiltak. KDI kjenner til at noen enheter bruker dører og døråpnere som er knyttet til elektroniske løsninger.

Tilgangsstyring og tilhørende systemer gjøres gjennom vurderinger av tjenstlig behov, som forestås av lederleddet i enhetene. Disse effektueres og håndteres praktisk av KDI, gjennom etatens IT-avdeling.

6.1.3.2.2 Anskaffelse av systemer som brukes på lokalt og regionalt nivå

KDI har uttrykt i disponeringsbrev at regioner og lokale enheter ikke kan eller skal etablere egne lokale systemer. Dersom det er ønskelig å etablere nye lokale systemer, skal enheter og/eller regioner ta dette opp med KDI.

KDI kjenner likevel til at det eksisterer lokale systemer. For eksempel nevnes et digitalt system for oversikt over celler (med informasjon om hvilken innsatt som befinner seg i hver celle) som brukes som alternativ til «den tradisjonelle magnettavlen på vaktrommet». På sikt er det ønskelig å fjerne eksisterende lokale systemer og erstatte disse med fellessystemer.

I det som omtales av KDI som «større prosesser med anskaffelser», involverer KDI seg i styringen, både ved anskaffelse og implementering. Dette skjer for eksempel ved prosjekter med nyetableringer, som ved oppføring av nye, større fengsler. Etableringen av nye Agder fengsel ble trukket frem som et nylig eksempel.

Beslutninger om gjennomføring av soning med programvare og maskinvare (som overordnet er anskaffet og styres av KDI) gjøres av lokalt nivå (friomsorgskontorer, som har forvaltningsansvar for gjennomføring av denne formen for straff). KDI mottar kopi av alle vedtak som treffes om bruk av ny teknologi for gjennomføring av straff med fotlenke.

Teknologien som brukes ved gjennomføring med elektronisk kontroll, dvs. med fotlenke, åpner for behandling av biometriske opplysninger. Biometriopplysninger lagres ikke i sentrale systemer, men lagres og leses av i utstyr hjemme hos den som gjennomfører straffen. KDI uttaler at det ikke er mulig å benytte annet utstyr enn det som er sentralt anskaffet for gjennomføring av soning med elektronisk kontroll.

Motsatt uttalte KDI, under det stedlige tilsynet, at ansvaret for behandling av personopplysninger gjennom kameraovervåking er delt mellom KDI og enhetene. For denne behandlingen følger det av det rettslige grunnlaget for behandlingen (straffegjennomføringsloven § 28, straffegjennomføringsforskriften § 3-9) at enhetene bestemmer de tekniske hjelpemidlene. Det medfører da en funksjonell deling av ansvaret. Innkjøp av kamera og tilhørende programvare gjøres i lokal enhet.

Det foreligger likevel enkelte sentrale retningslinjer for bruken av utstyret. KDI opplyser om at styringssignaler om personvernvurderinger ble gitt til regionene i 2017.
Det er en oppfatning i KDI at risikovurderinger og systemstyring skal gjennomføres på regionalt nivå. Som eksempel viste KDI frem en veileder i internkontroll for kameraovervåking fra region Sør.

6.1.3.3 Nærmere om instruks for behandlingsansvar i kriminalomsorgen
15. desember 2021, fem uker etter at det stedlige tilsynet hos KDI fant sted, mottok Datatilsynet Kriminalomsorgens nylig utarbeidede instruks for behandlingsansvar i kriminalomsorgen. I oversendelsesbrevet skriver KDI at utkast til instruks ble behandlet i KDIs ledermøte 30. november 2021, og i utvidet etatsledermøte 7. og 8. desember. Det

fremkommer av instruksen at den ble godkjent av assisterende direktør i etaten 16. desember 2021.

Instruksen beskriver regelverket som gjelder for behandling av personopplysninger i kriminalomsorgen. Instruksen har en formålsangivelse, som er å «klargjøre ansvarsforhold mellom de ulike roller i organisasjonen, tydeliggjøre delegert myndighet og fremheve enkelte hovedoppgaver og oppgavenes plassering.» Videre står det: «Denne instruksen må sees i sammenheng med kriminalomsorgens øvrige overordnede og styrende dokumenter som har betydning for informasjonssikkerhet og personvernet. Disse dokumentene finnes i KIKS.»

I instruksens punkt 5.1 fremgår det:

«Straffegjennomføringsloven kapittel 1A og forskrift om behandling av personopplysninger i kriminalomsorgen regulerer ikke hvem som er behandlingsansvarlig i kriminalomsorgen, men ut fra ordlyden i § 4b fremstår det klart at behandlingsansvaret for alle våre systemer tilligger KDI.

Plasseringen av behandlingsansvaret for lokale systemer, anskaffet/utviklet av lokal enhet for lokale formål, har vært noe mindre opplagt ut fra bestemmelsene, men det fastslåes med dette at behandlingsansvaret også for disse systemene tilligger KDI.

KDI har derfor som overordnet myndighet behandlingsansvaret for alle våre systemer frem til annet eventuelt blir besluttet gjennom eget delegeringsbrev.»

Instruksens punkt 7 heter «Oppgaver knyttet til behandlingsansvaret i kriminalomsorgen». Punktet inneholder en tabell med kolonner for oppgaveansvarlig og oppgavebeskrivelse. Instruksen sier at «tabellen er ikke ment å gi en utfyllende oversikt over alle oppgaver knyttet til behandlingsansvaret, men viktige eksempler samt en forståelse av hvilket nivå som håndterer hvilken type oppgaver.»

Tabellen angir at KDI ved direktør har det formelle og overordnede ansvaret for at all databehandling i kriminalomsorgen skjer i samsvar med gjeldende regelverk. Direktoratet har et særlig ansvar for å

- *ivareta etatens internkontroll på personvernets område, herunder avvikshåndtering*
- *vedlikeholde alle nødvendige sentrale dokumenter, herunder rutinebeskrivelser, policyer, instrukser og informative dokumenter,*
- *tilrettelegge for at etaten har tilstrekkelig kunnskap om personvern og de nødvendige ressurser for ivaretagelsen av personvernasvaret*
- *ivareta nødvendige tekniske sikkerhetstiltak for de sentrale systemer etaten bruker*
- *føre og oppdatere behandlingsprotokoll og gjennomføre DPIA (konsekvensvurdering) for sentrale systemer*
- *sikre at det inngås databehandleravtale der dette skal foreligge*
- *ivareta lagringsbegrensning i sentrale systemer, herunder tidsfrister for sletting*
- *sørge for en årlig vurdering av status i form av ledelsens gjennomgang*

Regionadministrasjon ved direktør «har et overordnet tilsynsansvar for behandlingen som finner sted i regionens driftsenheter. Regionene skal være kjent med sentrale bestemmelser/føringer på personvernets område og se til at dette etterleves på underliggende enhet.

Hvis nødvendig skal regionalt nivå gi supplerende/presiserende instrukser, rutinebeskrivelser osv. til underliggende enheter.»

Leder av driftsenhet (herunder «regionene og KDI i funksjonen som driftsenhet», er tillagt de «daglige, operative oppgavene for å ivareta behandlingsansvaret». Videre står det at

«på driftsenhet tas det daglig svært mange beslutninger rundt behandling av personopplysninger. Mye av den operasjonelle utøvelsen av behandlingsansvaret finner sted på dette nivået. Dette nødvendiggjør for leder av driftsenhetene en spesiell bevissthet rundt ivaretagelsen».

Deretter følger en henvisning til pliktene driftsenhet har knyttet til riktighet, formålsbegrensning og dataminimering vedlikehold av tilgangsstyring, opplæring, informasjon og tilrettelegging for den registrerte.

Det fremheves også at «driftsenheter som har anskaffet lokale systemer skal tilrettelegge spesielt for at det totale behandlingsansvaret blir ivaretatt for systemet. Dette forutsetter dialog og oppgaveavklaringer med direktoratet».

6.1.3.4 Faktiske forhold hos enhetene

Oslo friomsorgskontor:

Friomsorgskontoret har ingen dedikert oversikt over hvilke systemer som er i bruk i organisasjonen. Oversikt over systemer, herunder hvilke tilganger som er gitt, er likevel dokumentert gjennom prosedyre og autorisasjonsskjema for tildeling av tilganger ved ansettelse.

Friomsorgskontoret benytter et kameraovervåkingssystem fra leverandør TRYGGE ROM, som er anskaffet lokalt av Oslo Friomsorgskontor. Dette systemet benyttes for realtidsovervåking og ikke for opptak eller lagring. Kameraovervåkingssystemet ble anskaffet lokalt i 2009 ihht. anskaffelsesprotokoll.

Enheten har ennå ikke hatt saker der det er benyttet sporingsteknologi etter bestemmelsene i straffegjennomføringsloven § 16 a fjerde ledd og straffegjennomføringsforskriften § 7-5 tredje ledd. De har imidlertid gjennomført fjernalkoholtesting som et supplement til ordinære kontroller. Kontrollen foretas ved bruk av telefon og alkometer. Det er gitt sentrale retningslinjer for fjernalkoholtesting og telefonen som benyttes til dette formålet er anskaffet av KDI.

Det er ingen lokal instruks for eventuelle anskaffelser. Enheten viste til at det er etatens IT-ansvarlige som er lokalisert i Horten som har ansvaret.

Det er også en ressurs lokalt på enheten som tilrettelegger for daglig og lokal drift, og vedkommende var tilstede under tilsynet.

Enheten opplyste er gitt sentral instruks som gjelder for alle IKT-systemer. Det er ikke gitt egne instrukser for det enkelte system.

For Bredtveit, avdeling B2:

Bredtveit kunne ikke legge frem en dokumentert oversikt over hvilke systemer de hadde i bruk i virksomheten. Det vises til nytt etatssystem (KODA), som er under utvikling. KODA skal bl.a. erstatte dagens internkontrollsystem, KIKS.

Gjennom møtet gikk det likevel klart frem at virksomheten hadde oversikt over hvilke systemer som er i bruk. Det ble vist til KOMPIS, Doculive, EMSYS, KIA/KIF, BRIKK (kartleggingssystem) og banksystemet som brukes for de innsatte.

I tillegg benyttes DSF (Desktop for skole) for innsatte under utdanning. Forvaltningen av systemet er sentralisert, og er et skolesystem som Statsforvalteren i Vestland forvalter.

I løpet av møtet kom det også frem av mappestrukturen på fellesområdet «F» også var i utstrakt bruk ved enheten. Dette beskrives nærmere under rapportens punkt 6.1.3.5.

Det ble vist til at det gjennom de systemene ble brukt tynne klienter, og at det ikke skjedde «lokal lagring», kun hos etatens IT-avdeling som er lokalisert i Horten.

I tillegg bruker virksomheten en kameraløsning for å overvåke bygningens uteområde.

Utstyret som benyttes for overvåking av uteområdet til enheten består av to kameraer. Systemet ble anskaffet i 2006/2007, samtidig som kontoret ble etablert på lokasjonen. Det opplyses at opptak fra kameraovervåkingen kun kan sees av vakta ved enheten. Opptak overskrives etter åtte dager. Systemet er anskaffet lokalt, men det vises til sentrale rutiner for bruk av kamera under straffegjennomføring. Tilgang til bildene fra overvåkingen er begrenset til enheten. Det finnes ingen lokal instruks for bruk av kameraet. Enheten ville benyttet sentrale rutiner for å finne riktig fremgangsmåte ved spørsmål om f.eks. innsyn i kameraløsningen.

Enheten viste til at KDI har sendt en oppdatert instruks for anskaffelser av systemer, hvor det går frem at direktoratet anser seg behandlingsansvarlig og derfor skal være involvert i anskaffelser. Det er ingen lokal instruks for eventuelle anskaffelser.

For Romerike fengsel, avdeling Ullersmo

Fengselet hadde på tidspunktet for tilsynet ingen fullstendig dokumentert oversikt over hvilke systemer de hadde i bruk i virksomheten. Under møtet gikk det likevel klart frem at enheten hadde oversikt over hvilke systemer som er i bruk.

Sentrale systemer som benyttes er Doculive, KOMPIS KIA og KIF, Booking, GAT, KIKS, Wind (for telefoni), Atea (for videosamtale) og Microsoft office.

Virksomheten benytter kameraløsning for overvåkning av inne- og uteområder og system for adgangskort. I tilknytning til produksjon og salg av kjøkken benyttes tegningsprogram og regnskapsprogram.

Mappestrukturen på fellesområdet «:F» var i utstrakt bruk ved enheten. Det ble vist til at sentrale systemer ikke dekker alle behov, og at det det derfor er behov for å lagre dokumenter i mapper på fellesområdet. Arbeidsdokumenter lagres på fellesområdet og skannes inn i Doculive når de er ferdigstilt. Dette gjelder bl.a. liste over besøk. Nytt etatssystem skal rulles ut til høsten, og vil forhåpentligvis redusere behovet for dette. Se nærmere beskrivelse av fellesområdet i rapportens punkt 6.1.3.5.

Enheten har nylig opprettet en protokoll over de behandlingene de opplever at de har ansvar for. Behandlingsprotokollen omfatter fellesområdet, kameraovervåking, samt. tegneprogram kjøkken/kundeliste. Protokollen omfatter ikke opplysninger som lagres under ett døgn. Enhetens behandlingsprotokoll ble vist frem under tilsynet og oversendt i etterkant.

Enheten innhenter vandelsopplysninger fra politiet ved å fylle ut og oversende eget skjema for dette. Skjemaet er utarbeidet av politiet. Det er gjennomført et pilotprosjekt for klarering av besøkende og denne ordningen skal implementeres på Romerike.

Romerike anskaffet system for kameraovervåkning selv i 2016/2017. Anskaffelsen ble gjort i samarbeid med Indre Østfold fengsel gjennom en felles anbudsprosess. Enheten opplyste at dersom det nå var aktuelt å anskaffe et nytt system for kameraovervåkning, ville de hatt dialog med KDI om dette.

Det finnes en lokal instruks som omhandler hvordan Ullersmo avdeling skal håndtere kamerasystemene på Kroksrud avdeling og Ungdomsenhet øst, men det foreligger ingen lokal instruks om bruk av kamerasystemet for Ullersmo avdeling. Enheten planlegger å utarbeide en tilsvarende instruks for bruk av kamerasystemet ved Ullersmo avdeling.

Ullersmo viste til at kriminalomsorgen har en veileder for fengselsbygg med krav til bygg og funksjoner. Videre bistår Statsbygg ved slike anskaffelser. Enheten opplyste at direktoratet inngår rammeavtaler som de benytter seg av ved anskaffelser.

Romerike fengsel har inngått databehandleravtaler for kameraovervåkning (med Caverion), system for adgangskort/nøkler (Traka), samt for programvare for tegningsprogram for kjøkken og kundelister. I tillegg utredes behov for databehandleravtale for regnskapsprogram.

6.1.3.5 Nærmere om bruk av fellesområder (:F)

Under kontrollen med Bredtveit kom det frem informasjon om hvordan «:F-området» i informasjonssystemet brukes i etaten. Fellesmappene brukes i mangel av andre systemer og løsninger som er egnet. Enheten opplyste at det over lang tid er informert om at det vil komme et nytt system som skal erstatte behovet for bruk av fellesmapper.

Fellesmappene er delt inn i et felles område, i tillegg til at hver enkelt har et «privat» område. Bredtveit viste til et nylig mottatt dokument fra KDI som påpeker at bruk av «fellesmapper» er problematisk av flere grunner, og det oppstilles enkelte premisser dersom det er nødvendig å bruke fellesmappene. Dokumentet er oversendt til Datatilsynet etter tilsynet. Dokumentet er udatert og uten tittel.

Rutinen angir at føring av offentlig arkiv i kriminalomsorgen skjer i KOMPIS og Doculive. Deretter står det:

> *Bruk av fellesmapper er problematisk av flere grunner:*
> *- Deler av det det som dokumenteres på fellesmapper blir ikke arkivert. Vi ivaretar dermed ikke et lovbestemt krav om å føre et arkiv.*
> *- Retten til innsyn er vanskelig å praktisere for den registerte (straffedømte)*
> *- Fellesmappene er ikke et offisielt arkivsystem og personopplysninger skal slettes fortløpende (når formålet er oppnådd) og eventuelt dokumenteres i DL.*
>
> *Hvis man er avhengig av å bruke fellesmapper som en midlertidig løsning så gjelder følgende:*
> *- Fellesmapper skal bare benyttes til midlertidige planleggingsoppgaver og ikke inneholde registre eller historiske data.*
> *- Tilgangsstyring, dvs at det bare er de med tjenstlig behov for informasjon som skal ha tilgang til mappene. Det skal etableres et skriftlig system for tilgangsstyring og oversikt over hvem som har tilgang. Tilganger skal sperres når det ikke lenger finnes tjenstlig behov for informasjon.*
> *- Arkivverdig materiale skal overføres til KOMPIS og DL.*
> *- Retten til innsyn gjelder også informasjon som er lagt i fellesmapper.*
>
> *Det beste er å bestemme lagringstiden, tilgangsstyring, formål og overføring til arkiv (KOMPIS, DL) i en egen rutine.*

Bredtveit opplyste at de er avhengige av å registrere opplysninger i fellesmappene for å gjennomføre daglige, fengselsfaglige oppgaver og drifte institusjonen. Praksisen er godt kjent i etaten. Som eksempel på opplysninger som føres i fellesmappene oppgis vaktjournal, beleggslister, oversikt over besøk m.m. På vakta i Bredtveit registreres det opplysninger om besøkende på fellesområdet

De «private» mappene brukes også til registrering av personopplysninger om innsatte. Som eksempel nevnes opplysninger i forbindelse med kontaktbetjentarbeid, kladder og

arbeidsdokumenter. Det er ingen sentrale føringer for bruk av det private området i fellesmappene.

Endelige dokumenter overføres fra fellesmappene til KOMPIS og Doculive.
Sletting fra fellesmappene må skje manuelt. Enheten opplyste at de nylig gjennomgikk fellesområdet og gjorde en stor opprydding gjennom sletting av eldre dokumenter. Denne prosessen ble initiert av enheten selv.

Ullersmo forklarte at de nylig hadde opprettet en egen behandlingsprotokoll for behandlinger på fellesområdet. Behandlingsprotokollen utarbeidet ved Ullersmo inneholder henvisninger til rettslig grunnlag for behandlingen i personvernforordningen, også for behandlinger som ikke har hjemmel i personopplysningsloven av 2018 og personvernforordningen.

Ullersmo orienterte om at de avgrenset oppføring av behandlinger av personopplysninger mot opplysninger som ble lagret i 24 timer eller lenger. Opplysninger som kun behandles for 24 timer eller kortere er ikke en del av behandlingsprotokollen. Enheten har en overordnet rutine for bruk av fellesområdet. Fellesområdet er delvis tilgangsstyrt ut fra de ansattes tilknytning til avdeling i enheten. Det gis ikke opplæring for bruk. Hver enkelt ansatt har også et eget privat område.

6.1.4 Vurdering

Datatilsynet legger til grunn Kriminalomsorgsdirektoratets egen forståelse av sin stilling som behandlingsansvarlig for all behandling som skjer i kriminalomsorgen, slik dette fremgår av instruks om behandlingsansvar godkjent 16. desember 2021.

Dette er en forståelse som har blitt utviklet i løpet av tilsynsperioden, og som også kom til uttrykk under det stedlige tilsynet hos KDI. Datatilsynets observasjoner under de stedlige tilsynene med enhetene indikerer at denne forståelsen ikke har fått fotfeste i hele organisasjonen, selv om KDI nylig har formulert en instruks til underliggende nivåer. KDI uttalte at de tidligere har uttrykt i disponeringsbrev at regioner og lokale enheter ikke kan eller skal etablere egne systemer.

Det fremstår klart at KDI er behandlingsansvarlig for systemer som KDI selv har anskaffet og har den daglige oppfølgingen med. Dette er journalsystemet KOMPIS, og arkivsystemet DocuLive, samt andre systemer som leverer fellestjenester til organisasjonen. Videre fremstår det klart at KDI er behandlingsansvarlig for systemer som er så spesielle at det kun er KDI som har kompetanse til å anskaffe slike. Dette har etter KDIs oppfatning en funksjonell forklaring knyttet til markedet for programvare og maskinvare. Eksempler på dette er systemer for gjennomføring av straff i frihet, teknologi som brukes for å gjennomføre videosamtale med innsatte, og pust- og bevegelsessensorer til bruk på celler.

Enhetene deler KDIs oppfatning av behandlingsansvaret for sentralt anskaffede og styrte systemer. For disse systemene virker behandlingsansvaret å være tydelig, selv om det i liten grad er fulgt opp, formalisert og tydeliggjort overfor enhetene. Enhetene hadde i varierende

grad en formalisert oversikt over hvilke systemer som var i bruk, selv om det gjennom tilsynene ble avdekket at en uformell oversikt likevel eksisterte i de tre enhetene.

KDI nevnte bruk av fellesmappene i brevet av 23. mars 2021. Enhetene hadde mottatt en uspesifisert og udatert instruks for bruken fellesområdet etter at Datatilsynet var på tilsyn hos KDI.

Enhetenes mottakelse av instruksen var ulik. Romerike fengsel forsto instruksen som at de var behandlingsansvarlige for bruken av fellesområdet. Som følge av dette hadde Romerike fengsel utarbeidet en egen behandlingsprotokoll for informasjonssystemet.

Behandlingsprotokollen var avgrenset på en vilkårlig måte, der kun opplysninger som skulle lagres lenger enn 24 timer, ble oppført. En slik avgrensning vil gjøre at protokollen ikke omfatter all behandling av personopplysninger, noe som gjør den mindre hensiktsmessig. Videre henviser Romerike fengsels behandlingsprotokoll til rettslig grunnlag i personvernforordningen, og ikke til personopplysningsloven av 2000. Datatilsynet anser dette for å trolig være et utslag av manglende styring og retningslinjer fra etatens øverste ledd.

KDI uttrykte under det stedlige tilsynet at behandlingsansvaret for behandling av personopplysninger gjennom kameraovervåking er delt mellom KDI og enhetene. Dette ble begrunnet med henvisning til straffegjennomføringsloven og straffegjennomføringsforskriften, der det er angitt enhetene skal bestemme de tekniske hjelpemidlene.

I instruksen av 16. desember 2021 har KDI forlatt denne oppfatningen, og uttrykker nå at all behandling, også ved kameraovervåking i enhetene, faller inn under KDI som behandlingsansvarlig.

For behandling av personopplysninger ved kameraovervåking inngår enhetene egne avtaler med leverandører av utstyr. Romerike fengsel har inngått databehandleravtale med leverandør av kameraovervåkningssystemet. Hvordan denne databehandleravtalen er forankret i etaten, fremstår som uklart. Romerike fengsel hadde også inngått databehandleravtaler med systemleverandør for adgangskort og nøkler, og for programvare for produksjon av kjøkken.

Datatilsynet oppfatter det som klart at KDI ikke har oversikt over hvilke systemer som benyttes i ulike deler av organisasjonen. KDI involverer seg i prosesser for større prosjekter, både knyttet til anskaffelse og implementering. Direktoratets involvering er ikke formelt angitt gjennom rutiner eller instrukser. Instruks om behandlingsansvar av 16. desember 2021 angir at driftsenheter skal tilrettelegge for at det totale behandlingsansvaret blir ivaretatt for systemet, og at det forutsetter dialog og oppgaveavklaringer med direktoratet. Det fremstår for Datatilsynet som at behovet for, og terskelen for, involvering fra direktoratets side vurderes fra sak til sak, uten at nærmere kriterier er fastsatt. En slik ordning medfører etter vårt syn lite forutberegnelighet for etaten og eksterne.

Datatilsynet viser til at det i Prop. 151 L (2009-2010) ble varslet forskrift om nærmere regulering av behandlingsansvaret, noe departementet ikke har fulgt opp. Samtidig har etaten

selv et ansvar for å sørge for ryddige ansvarsforhold. Dette følger både av kravene til behandlingsansvar, og av internkontrollplikten. Datatilsynet finner at kriminalomsorgen inntil nylig har manglet sentrale dokumenter som avklarer ansvarsforholdene.

Det fremstår å være ulik forståelse av ansvaret i ulike deler av organisasjonen, særlig med hensyn til kameraovervåking. Samtidig har KDI nå forsøkt å klargjøre ansvaret med en instruks for behandlingsansvaret i etaten. Denne instruksen ble utarbeidet underveis i tilsynsperioden.

Datatilsynets kontroll med enhetene skjedde fem måneder etter vedtak og utsendelse av instruksen. Selv etter at enhetene hadde mottatt instruksen om behandlingsansvar, fremsto det for Datatilsynet som forståelsen av behandlingsansvaret og hva dette i praksis innebærer, er ulik. Kravene til klare og dokumenterte ansvarsforhold etter regelverket er dermed ikke oppfylt.

Datatilsynet ser at kriminalomsorgen, ved Kriminalomsorgsdirektoratet, har påbegynt jobben med å avklare ansvarsforholdene knyttet til behandlingsansvaret i etaten. Dette har imidlertid skjedd i løpet av tilsynsperioden, etter at tilsynet overfor etaten ble igangsatt. Datatilsynet vurderer at det gjenstår arbeid før vi kan konkludere med at ansvarsforholdene er tilstrekkelig tydeliggjort og implementert.

6.1.5 Konklusjon

Datatilsynet konkluderer at det foreligger avvik fra regelverkets krav om klarhet i ansvars- og myndighetsforhold, jf. personopplysningsforskriften § 2-7. Det har inntil nylig foreligget avvik fra kravet om dokumentasjon av ansvars- og myndighetsforhold.

6.2 Internkontroll

6.2.1 Internkontroll som tema for tilsynet

Datatilsynet hadde til hensikt å kontrollere hvordan kriminalomsorgen ivaretar sitt ansvar for internkontroll og informasjonssikkerhet i hele organisasjonen.

6.2.2 Krav i regelverket

Personopplysningsloven § 14 stiller krav om at den behandlingsansvarlige gjennom planlagte og systematiske tiltak (internkontroll) sikrer at lovens krav ivaretas. Utfyllende bestemmelser er gitt i personopplysningsforskriftens § 3-1.

Personopplysningslovens § 13 og personopplysningsforskriftens kapittel 2 stiller krav om planlagte og systematiske tiltak (internkontroll) for å oppnå tilfredsstillende informasjonssikkerhet.

Personopplysningsloven § 14 pålegger den behandlingsansvarlige å etablere og holde ved like planlagte og systematiske tiltak som er nødvendige for å oppfylle kravene i eller i medhold av denne loven, herunder sikre personopplysningenes kvalitet.

I personopplysningsforskriftens § 2-3 fastsettes ledelsesansvaret for informasjonssikkerheten, samt at det stilles krav om at sikkerhetsmål og sikkerhetsstrategi fastsettes. I § 2-4 stilles det, foruten krav om risikovurderinger, krav om at virksomheten fører oversikt over personopplysninger som behandles og at det fastsettes kriterier for akseptabel risiko for disse. § 2-7 stiller krav om at ansvars- og myndighetsforhold etableres.

Krav om oppfølging av sikkerhetsarbeidet følger av forskriftens §§ 2-3, 2-5 og 2-6 om henholdsvis ledelsens gjennomgang, sikkerhetsrevisjon og avvikshåndtering.

Personopplysningsforskriftens § 3-1 oppstiller krav om at systematiske tiltak skal tilpasses virksomhetens art, aktiviteter og størrelse i det omfang det er nødvendig. Dette forutsetter kjennskap til gjeldende personvernregler, tilstrekkelig og oppdatert dokumentasjon for gjennomføring av rutiner, og tilgjengelig dokumentasjon for den dette måtte angå.

6.2.3 Faktiske forhold

6.2.3.1 Internkontrollsystemet

6.2.3.1.1 Kriminalomsorgsdirektoratet

Internkontrollsystemet til kriminalomsorgen består av systemet KIKS, og en rekke internkontrolldokumenter. Internkontrollsystemet består av styrende dokumenter, gjennomførende dokumenter, og kontrollerende dokumenter. KDI opplyste om at det er igangsatt en prosess for å utarbeide dokumenter, og gjennomgå eldre versjoner som ikke lenger holder mål. Det foreligger også eldre dokumenter som ikke tidligere har vært godkjent, og som er under arbeid.

Av styrende dokumenter opplyste KDI at de har følgende:

- Styringsdokument for internkontroll er organisasjonens felles rammeverk. Dette er fra 2013.
- Ledelsens sikkerhetsgjennomgang foreligger, senest fra 2021
- Håndbok i risikovurdering foreligger, denne er fra 2014. Håndboken skal benyttes i alle sammenhenger der det er aktuelt med risikovurdering.
- Informasjonssikkerhetspolicy fra 2010.

Styrende dokumenter som kun forelå som utkast på tilsynstidspunktet:

- Dokumenter tilhørende informasjonssikkerhetspolicy, sikkerhetsmål og strategi, og Dokument for organisering

Av gjennomførende dokumenter forelå følgende på tilsynstidspunktet:

- Rutine for risikovurdering av informasjonssikkerhet fra 2009
- Brukerinstruks og taushetserklæring for ansatte, henholdsvis fra 2018 og uten dato
- Sjekkliste for nyansatte og ansatte som slutter, begge fra 2012

- Taushetserklæring, fra 2018
- Sjekkliste ved nyansettelse, uten dato

Følgende gjennomførende dokumenter var under arbeid på tilsynstidspunktet:

- Rutiner for håndtering av personopplysninger
- Utkast fra arbeidsgruppe for informasjonshåndtering
- Sikkerhetsinstruks for sikkerhetsansvarlig
- Beskrivelse av informasjonssystemet
- Driftsrutiner
- Overordnet beredskapsplan for informasjonssystemer

Dokument for fysisk sikkerhet, beredskapsplanverk mv. eksisterer, men var ikke en del av tilsynet.

Av kontrollerende dokumenter viste KDI til rutine for avvikshåndtering fra 2009, avviksskjema i KIKS og ellers til håndtering i KIKS.

Under det stedlige tilsynet beskrev KDI at de er i ferd med å etablere et nytt system for internkontroll, kalt KIKS 2. Det gjenstår både teknisk, organisatorisk og personalmessig arbeid før KIKS 2 vil være ferdig og klart til bruk. KDI beskrev at de skal oppgradere risikomodulen, avviksmodulen og dokumentregister, migrere innhold og dokumenter til ny struktur, samt revidere eksisterende drifts- og forvaltningsrutiner. Det skal også integreres med nytt styringssystem for informasjonssikkerhet. Av organisatoriske tiltak skal eksisterende rammeverk for internkontroll for rammeverk, revidering av eksisterende policyer, roller og ansvar, og opplærings- og implementeringsplan.

Av personelle tiltak var KDI i ferd med å etablere en fagansvarlig gruppe med månedlige statusgjennomganger, for å sikre nødvendig bistand.

KDI opplyste at det foreligger rutiner som delvis står med feil navn i henhold til någjeldende organisering og enhetsnavn, men som ligger oppfyller formålene. Videre er det klart at ulike dokumenter foreligger, som sjekklister for nyansatte, rutiner for ansatte som slutter, samt taushetserklæringen fra 2018.

KDI opplyste at de er i prosess for å avklare mange spørsmål knyttet til sikkerhetsarkitektur, som blant annet berører personvernregelverket, vurdering av skytjenester og overføringer som berører Schrems II-avgjørelsen.

Av andre tiltak som var en del av det videre arbeidet, viste KDI til opplæring i regi av KRUS, måling av sikkerhetskultur og kompetanse, benchmarking av INFOSEC, opplæring i INFOSEC i regi av KRUS, og forberedelse av implementering av ny lovgivning.

KDI uttalte at de er klar over at gjeldende krav til avvikshåndtering har endret seg betydelig. Dette skyldes digitalisering og nye tekniske plattformbehov, endringer i regelverk og risikobilder, samt omorganisering og endrede krav til rollebeskrivelser.

6.2.3.1.2 Internkontrollsystemer hos enheter

Friomsorgskontoret:
Enheten opplyste at den overordnede skriftlige internkontrollen finnes i systemet KIKS. Enheten viser til at utarbeidelsen av rutinene for etaten skjer sentralt og at disse er tilgjengelige i KIKS. I møtet viste enheten frem KIKS og hvordan dette systemet er bygget opp og benyttes.

I KIKS er det også funksjonalitet for å utarbeide lokale rutiner, noe enheten har benyttet muligheten til. Dette er spesielt relevant for friomsorgskontorene som har andre behov enn fengsler.

Bredtveit:
På lik linje med friomsorgskontoret viste Bredtveit til at overordnet skriftlig internkontroll befinner seg i KIKS. Enheten opplyste om at de i en viss utstrekning har benyttet seg av funksjonaliteten for å utarbeide lokale rutiner. For arkivering av dokumenter foreligger egne rutiner.

Ullersmo:
Enheten viste til KIKS, på lik linje med friomsorgskontoret.

Enheten har utarbeidet lokale rutiner for informasjonssikkerhet til bruk for ansatte (prosedyre for håndtering og registrering av avvik).

Det er opprettet et personvernmøte, som skal gjennomføres tertialvis (etter samme modell som LAMU-møter). Møtet skal bl.a. benyttes til å gjennomgå ev. avvik innen informasjonssikkerhet, vurdere behov for ROS-analyser og tiltaksplaner og drøfte problemstillinger knyttet til ivaretakelse av personvernet.

6.2.3.2 Sikkerhetsledelse, personopplysningsforskriften § 2-3, samt sikkerhetsrevisjoner
6.2.3.2.1 KDI

KDI uttalte at det ikke foreligger tvil i organisasjonen om at sikkerhetsstrategien er ledelsesforankret. Sikkerhetsstrategien er godkjent av direktoratets ledelse, som rutinemessig gjennomgår sikkerhetsmessige spørsmål en gang i året. Gjennomganger dokumenteres fra alle ledermøter, og det føres referat.

Ledelsen innrømmer på dette punktet at ikke alle tema vies like mye oppmerksomhet ved ledelsens gjennomgang.

Personvernombudet er ikke rutinemessig tilstede under ledelsens gjennomgang.

6.2.3.2.2 Enhetene
Friomsorgskontoret:
Oslo Friomsorgskontor har selv tatt initiativ til prosesser knyttet til sikkerhetsstrategi og risikovurderinger knyttet til informasjonssikkerhet.

Det ble trukket frem tiltak i etaten som har fokus på sikkerhet, blant annet at det tilbys nettkurs i sikkerhet og at det finnes instrukser for bruk av epost.

Det oppleves at det er større oppmerksomhet på informasjonssikkerhet og personvern etter at Datatilsynet startet kontrollen mot KDI.

Enheten rapporterer årlig til KDI på informasjonssikkerhet. Det er også utarbeidet et årshjul for å sikre etterlevelse av internkontrollplikter i etaten. På området informasjonssikkerhet rapporteres det primært om tekniske forhold.

Bredtveit:
Enheten har ikke utarbeidet en lokal sikkerhetsstrategi, og er ikke kjent med om KDI har en slik strategi. Enheten trakk frem flere tiltak i etaten som har fokus på sikkerhet, blant annet at det tilbys nettkurs i sikkerhet, og at det finnes instrukser for bruk av epost.

Hver oktober markeres i tillegg sikkerhetsmåneden i etaten, hvor enkelte rutiner blir trukket frem og det er oppmerksomhet på informasjonssikkerhet. Enheten opplever at det er større oppmerksomhet på informasjonssikkerhet og personvern etter at Datatilsynet startet kontrollen mot KDI.

Hva gjelder sikkerhetsrevisjoner opplyste enheten at de årlig rapporterer til KDI på informasjonssikkerhet. Det er også utarbeidet et årshjul for å sikre etterlevelse av internkontrollplikter i etaten, men denne inneholder ikke ivaretakelse av personvernregelverket.

På området informasjonssikkerhet rapporteres det primært om tekniske forhold. Internkontrollen konsentreres i hovedsak om fysisk sikring i fengslene.

Ullersmo:
Enheten skriver om informasjonssikkerhet i årsmeldinger. Arbeid med informasjonssikkerhet og personvern skal inkluderes i enhetens årshjul for 2023.

Enheten opplyste også at det skal utarbeides en «lokal» internkontroll for å sikre etterlevelse og oppfølging av plikter knyttet til informasjonssikkerhet og personvern.

Det er også planlagt å avholde tertialvise møter med personvern og informasjonssikkerhet som tema.

6.2.3.3 Risikovurderinger, personopplysningsforskriften § 2-4

6.2.3.3.1 KDI

Som nevnt under punkt 8.2.3.1 foreligger en håndbok i risikovurdering fra 2014. Målgruppen for denne håndboken er prosjekteiere.

KDIs sikkerhetsansvarlig har deltatt for å kvalitetssikre for risikovurderingene som ble gjort i forbindelse med Agder fengsel.

Risikovurderinger gjennomføres tidvis. KDI viste til at det ble gjort risikovurdering av videoløsning for innsatte i 2020, en løsning som ble tatt i bruk som følge av koronapandemien. Denne risikovurderingen ble sendt til Datatilsynet etter det stedlige tilsynet.

I korrespondansen med Datatilsynet i forkant av det stedlige tilsynet, viste KDI til at det ble gjennomført en DPIA (Date Protection Impact Assessment) for KOMPIS.

6.2.3.3.2 Enhetene

Friomsorgskontoret:

Enheten benytter seg av sentrale rutiner for risikovurdering av informasjonssikkerhet, herunder håndbok og veileder som ligger tilgjengelig i KIKS.

Enheten har selv tatt initiativ til prosesser knyttet til risikovurderinger knyttet til informasjonssikkerhet. De er ikke gjort kjent med eventuelle risikovurderinger som er gjort sentralt av KDI for fellesløsninger.

Bredtveit:

Bredtveit opplyser at de ikke gjennomfører vurderinger av risiko for behandling av personopplysninger lokalt på enheten.

Enheten er kjent med at det ble gjennomført en risikovurdering fra KDI før nettbrett ble tatt i bruk i fengslene for kommunikasjon under pandemien. De er ikke kjent med eventuelle sentrale rutiner for gjennomføring av risikovurderinger.

Ullersmo:

Enheten er godt kjent med risikovurderinger knyttet til HMS og straffegjennomføring. Det foreligger ikke lokale risikovurderinger knyttet til informasjonssikkerhet. Enheten har ikke kjennskap til hvilke vurderinger som er gjort for sentrale systemer.

6.2.3.4 Avvikshåndtering

6.2.3.4.1 KDI

Avvikshåndtering gjøres gjennom KIKS. KDI utarbeider p.t. nytt avvikssystem, KIKS 2.

Bruken av avvikssystemet ble beskrevet under tilsynet. Systemet er satt opp slik at det er en mottaker av avviksmeldinger per enhet eller nivå. I KDI er det sikkerhetskoordinator som er mottaker, og tilsvarende er det en dedikert mottaker i hver region og ved hver enhet. Avviksmottakeren behandler avviket selv eller sender til en annen behandler. I tillegg er enhetsleder satt opp som overordnet, og vil kunne ta ut rapporter for å kontrollere status på avviksbehandlingen i enheten.

Det fremgår av rutine for avviksbehandling at avviksrapportering kan føre til situasjoner hvor avviket krever videre behandling eller bistand fra regionskontoret. Alvorlige brudd skal i henhold til rutinen oversendes KSF. KSF er Kriminalomsorgens sentrale forvaltning, som opphørte å eksistere ved opprettelsen av Kriminalomsorgsdirektoratet, og som nå tilsvarer KDI.

6.2.3.4.2 Enhetene

Friomsorgskontoret:

Det ble vist hvor og hvordan man melder avvik i KIKS, og det ble redegjort for hvordan avvik sorteres og håndteres av kontoret.

Enheten hadde ingen avvik registrert knyttet til personopplysningssikkerhet, men meldingssystemet hadde funksjonalitet for å kunne registrere slike hendelser.

Enheten er kjent med en rutine fra 2009 som omhandler avvik innenfor informasjonssikkerhet, men uttaler at denne er lite hensiktsmessig for bruk av dagens avvikssystem. Det var heller ikke utarbeidet lokale rutiner for bruk av avvikssystemet på dette området.

Bredtveit:

Bredtveit viste hvor og hvordan man melder avvik i KIKS, og beskrev hvordan avvik sorteres og håndteres av forskjellige nivåer i etaten.

Enheten hadde ingen avvik registrert knyttet til personopplysningssikkerhet, men meldingssystemet hadde funksjonalitet for å kunne registrere slike hendelser.

Enheten opplyser at de ikke er kjent med at det finnes sentrale rutiner for hvordan avvikssystemet skal benyttes ved brudd på personopplysningssikkerheten.

Det var heller ikke utarbeidet lokale rutiner for bruk av avvikssystemet på dette området.

Ullersmo:

Ullersmo viste til KIKS, og hvordan KIKS brukes.

Det er ikke mange avvik knyttet til informasjonssikkerhet, noe som ifølge enheten kan skyldes underrapportering. Enheten har ansvar for oppfølging av avvik på lokalt nivå. Alle ansatte har fått opplæring i bruk av avvikssystemet.

Under tilsynet gjennomgikk enheten lokalt arbeid med avvikssystemet og håndtering av innmeldte avvik. Enheten opplyser at det ikke mange avvik på informasjonssikkerhet og at dette kan skyldes underrapportering. De jobbet med opplæring da det kan være usikkerhet om når man skal melde avvik.

På konkret forespørsel om bruk av Fellesområdet, bekreftet enheten at manglende sletting og manglende rutiner for systemet ikke hadde vært meldt inn som avvik.

6.2.3.5 Opplæring av personell

6.2.3.5.1 KDI

Opplæring av personell blir i hovedsak gjort gjennom Kriminalomsorgens utdanningssenter. KDI uttalte at rutiner for opplæring av ansatte skal utarbeides som en del av oppgraderingen av internkontrollsystemet.

6.2.3.5.2 Enhetene

Friomsorgskontoret:

Alle ansatte får nødvendig opplæring for bruk av systemene de bruker for å utføre sine arbeidsoppgaver.

Enheten opplyser at de benytter lokalt tilpassede rutiner for opplæringen av ansatte.

Bredtveit:

Alle ansatte får nødvendig opplæring for bruk av relevante systemer for deres arbeid. Fengselsutdannede får opplæring i KOMPIS under utdanningen. Opplæringen foregår i hovedsak ved noe gjennomgang i forkant og gjennom praktisk arbeid på avdelingen. Enkelte gjennomganger er obligatoriske før de ansatte gis tilgang til systemene.

Enheten opplyser at de ikke benytter sentrale rutiner for opplæringen av ansatte.

Ullersmo:

Nye ansatte får opplæring i bruk av informasjonssystemene ved oppstart. Nærmeste leder har ansvaret for å sikre at opplæring blir gitt. I forbindelse med opplæringen får den ansatte informasjonsmateriell som er relevant.

6.2.3.6 Tilgangsstyring

6.2.3.6.1 KDI

Tilganger gis gjennom nærmeste leder på nivået der det ansatte jobber, og forvaltes av etatens IT-avdeling i Horten.

6.2.3.6.2 Enhetene

Friomsorgskontoret:

Enheten gjennomgikk hvordan ansattes tilgang til relevante system bestilles, endres og slettes [redacted]

[redacted]

Den enkelte ansattes behov ulike tilganger vurderes av nærmeste leder. Det gjøres også jevnlige (årlige) revisjoner av tilganger lokalt i enheten.

Tildeling og bestilling av tilganger dekkes av rutiner for nyansettelser.

Bredtveit:

Enheten gjennomgikk hvordan ansattes tilgang til relevante system bestilles, endres og slettes [redacted]

[redacted]

Den enkelte ansattes behov ulike tilganger vurderes av nærmeste leder. Tildeling og bestilling av tilganger dekkes av rutiner for nyansettelser.

Ullersmo:
Tildeling av tilganger til informasjonssystemer skjer via etatens IKT-avdeling, og bestilles på [redacted] Det er ingen rutinemessig revisjon av tilganger.

6.2.4 Vurdering

Datatilsynet observerer at kriminalomsorgen har et internkontrollsystem. Dokumentene som finnes er gamle, og mange av dem er ikke oppdatert. Det pågår en prosess for å etablere et nytt etatssystem, Kriminalomsorgens Databehandlingssystem (KODA), og et nytt system for internkontroll, KIKS 2. Enhetene var kjent med arbeidet med KODA, og flere uttrykte forventninger til systemet.

Under tilsynet med enhetene undersøkte Datatilsynet hvorvidt enheten kjente til den sentrale internkontrollen. Alle enhetene viste til internkontrollen i KIKS. Enhetene har til en viss grad gjort noe arbeid selv knyttet til internkontroll. Romerike fengsel har utarbeidet rutiner etter at tilsynet ble påbegynt, og planlegger å inkludere informasjonssikkerhet og personvern i årshjulet fra og med 2023.

KDI har en håndbok for risikovurderinger fra 2014. KDIs sikkerhetsansvarlig har deltatt i kvalitetssikring av risikovurderinger med Agder fengsel. Dette fremstår ikke som en gjennomgående tilnærming, men noe som blir gjort dersom prosjektet inviterer til dette. På direkte spørsmål om risikovurderinger informerte KDI om at de gjennomførte risikovurdering av videoløsning for innsatte som ble tatt i bruk som følge av utbruddet av koronapandemien i 2020. I brev av 28. mars 2021 opplyste KDI at det var blitt gjennomført DPIA av KOMPIS. Datatilsynet har ikke undersøkt denne nærmere.

Friomsorgskontoret har selv tatt initiativ til å gjennomføre risikovurderinger for informasjonssikkerhet, og da benyttet seg av de sentrale rutinene og veilederen som befinner seg i KIKS. Enheten kjenner ikke til risikovurderinger som er gjort av KDI. Bredtveit kjenner til at det ble gjennomført en risikovurdering i KDI før nettbrett ble tatt i bruk for kommunikasjon i fengslene under pandemien, men var ikke kjent med sentrale rutiner for gjennomføring av risikovurderinger. Romerike kjente ikke til hvilke vurderinger som var gjort for sentrale systemer.

KDI viste til at avviksbehandling ble gjort i KIKS. Dokumentet som beskrev rutinen for avviksrapportering var gammelt (2009), og viste til navn på etatens tidligere øverste nivå (KSF). Enhetene kjente til KIKS. Det varierte hvorvidt enhetene kjente til rutiner for bruk av

avvikssystemet ved brudd på personopplysningssikkerheten. Romerike fengsel jobbet med opplæring, da det fremsto for enheten at det kunne være usikkerhet om når ansatte skulle melde avvik.

Det er svært uklart hvorvidt avvik knyttet til informasjons- og personopplysningssikkerhet faktisk blir meldt. Noen avvik var meldt ved friomsorgskontoret, og det var også notert noen avvik ved Romerike. Ved Romerike ble det bemerket at mangelen på meldte avvik kan skyldes underrapportering, og ikke nødvendigvis at avvik ikke oppstår. Som eksempel på manglende forståelse av avviksrapportering, vil Datatilsynet trekke frem at identifiserte avvik (manglende sletting) ved bruk av fellesområdet ikke var blitt meldt i KIKS.

KDI forklarte at opplæringen knyttet til informasjonssystemer blir gjort ved KRUS, og uttalte at nye rutiner for opplæring skulle utarbeides i forbindelse med oppgraderingen av internkontrollsystemet. Enhetene utfører egen opplæring i informasjonssystemene ved oppstart. Friomsorgskontoret benytter lokalt tilpassede rutiner for opplæring, mens det ved Bredtveit ikke benyttes sentrale rutiner ved opplæring.

Tilgangsstyring gjøres gjennom sentrale skjemaer, og effektueres av IT-avdelingen i Horten. Det fremsto ikke for Datatilsynet som at KDI gjennomførte jevnlige revisjoner av om gitte tilganger er riktige. Friomsorgskontoret gjennomførte en årlig revisjon, men dette ble ikke gjort ved andre enheter.

Avvik meldes ikke. Datatilsynets oppfatning er at dette mest sannsynlig skyldes underrapportering, og ikke at avvik ikke oppstår. Mangelen på avviksmeldinger og jevnlige revisjoner medfører at det mest sannsynlig er store mørketall i kriminalomsorgen. Risikovurderinger blir ikke gjennomført på en systematisk måte. Hos den enheten som opplyste å gjennomføre egne risikovurderinger, fremsto det som klart for Datatilsynet at dette var personavhengig, og ikke noe som skjer som følge av organisatoriske tiltak og rutiner etablert av behandlingsansvarlig.

Personvernregelverket stiller krav til at internkontrollen og sikkerhetsledelsen skal være systematisk og regelmessig. Dette krever at det er klare ansvarslinjer og regelmessige gjennomganger og oppfølging av internkontrollen. Internkontrollen skal være et levende system, som hele organisasjonen skal kjenne til. Informasjon i organisasjonen må være tydelig.

Resultatet av manglende oppfølging av internkontroll og sikkerhetsledelse vil kunne resultere i alvorlige avvik. Kombinasjonen av mangelfullt system og sårbare registrerte medfører høy risiko for forskjellig praktisering av personvernrettigheter internt i etaten.

For Datatilsynet fremstår det som at kriminalomsorgens tilnærming til informasjonssikkerhet og personopplysningssikkerhet ikke er tilstrekkelig. Selv om det eksisterer et rammeverk for internkontroll, er dette gammelt, og ikke rutinemessig revidert de seneste årene. Dette ble også erkjent under det stedlige tilsynet hos KDI. KDI erkjenner at det gjenstår mye arbeid for å få på plass et tilstrekkelig internkontrollsystem.

6.2.5 Konklusjon

Datatilsynet konkluderer med at det foreligger avvik fra personopplysningslovens og personopplysningsforskriftens krav til internkontroll i form av etablerte og vedlikeholde planlagte og systematiske tiltak, jf. lovens § 14 og forskriftens § 3-1. Videre finner Datatilsynet at det foreligger avvik fra personopplysningsforskriftens kapittel 2 om informasjonssikkerhet, herunder kravene til sikkerhetsledelse, risikovurderinger, sikkerhetsrevisjoner og avvikshåndtering.

7 Tilstede ved gjennomføring av kontrollene

7.1 Kriminalomsorgsdirektoratet

7.1.1 Fra KDI

- Jan-Erik Sandlie, assisterende direktør
- Tone M. Traa, IT-direktør
- Gro Fjellbu Øi, prosjektporteføljeforvalter
- Jan Ove Berg, informasjonssikkerhetsleder
- Maja Karoline Breiby, jurist
- Hans-Gunnar Stey, jurist
- Per Andersen, personvernombud

7.1.2 Fra Datatilsynet

- Embla Helle Nerland, juridisk rådgiver
- Maren Vaagan, juridisk seniorrådgiver
- Eirik Gulbrandsen, senioringeniør
- Camilla Nervik, seksjonssjef

7.2 Oslo friomsorgskontor

7.2.1 Fra friomsorgskontoret

- Johnny Bjørkli, friomsorgsleder/øverste kontorleder
- Stig Tosterud, HMS-ansvarlig/driftsansvarlig

7.2.2 Fra Datatilsynet

- Embla Helle Nerland, juridisk rådgiver
- Maren Vaagan, juridisk seniorrådgiver
- Eirik Gulbrandsen, senioringeniør
- Camilla Nervik, seksjonssjef

7.3 Bredtveit fengsel- og forvaringsanstalt, avdeling B2

7.3.1 Fra Bredtveit

- Doris Bakken, fengselsleder
- Tone Monkerud, avdelingsleder
- Gina Reenskaug, HMS-koordinator
- Trine Nordseth, seniorkonsulent
- Mathis Mjåseth, IKT-medarbeider

7.3.2 Fra Datatilsynet

- Embla Helle Nerland, juridisk rådgiver
- Maren Vaagan, juridisk seniorrådgiver
- Camilla Nervik, seksjonssjef

7.4 Romerike, avdeling Ullersmo

7.4.1 Fra Ullersmo

- Ole Johnny Rydland, fengselsleder
- Marte Bruer-Skarsbø, ass. fengselsleder
- Silvia Strøm, seniorrådgiver
- Linn Kristin Myren, fung. seniorrådgiver
- Vegard Stubberud, inspektør
- Inge Gammeli, fung. inspektør
- Kjetil Hoff, inspektør
- Kenneth Myrstad, fung. IKT-driftsansvarlig

7.4.2 Fra Datatilsynet

- Embla Helle Nerland, juridisk rådgiver
- Maren Vaagan, juridisk seniorrådgiver
- Eirik Gulbrandsen, senioringeniør
- Camilla Nervik, seksjonssjef

8 Dokumentasjon

8.1 Dokumenter fra Kriminalomsorgsdirektoratet

I korrespondansen med Kriminalomsorgsdirektoratet, nevnt under rapportens punkt 7, ble det oversendt dokumenter fra KDI til Datatilsynet før det stedlige tilsynet. I etterkant av det stedlige tilsynet ba vi om å få oversendt ytterligere dokumenter.

Følgende dokumenter er lagt til grunn i tilsynet:

- Behandlingsprotokoll under arbeid, mottatt 16. april 2021
- Kopi av systemoversikt og ansvar, mottatt 19. mai 2021
- Behandlingsprotokoll for KRUS, mottatt 25. mai 2021
- Systemoversikt og ansvar (oppdatert versjon), mottatt 4. juni 2021
- Svar på vedtak om pålegg, mottatt 21. september 2021
- Behandlingsprotokoll for personopplysninger om domfelte, mottatt 21. september 2021
- Behandlingsprotokoll for opplysninger om andre enn domfelte, mottatt 21. september 2021
- Internkontroll i kriminalomsorgen, felles rammeverk, mottatt 21. september 2021

- Risikovurdering for videoløsning for innsatte, mottatt 16. november 2021
- Notat om informasjonssikkerhet for EK-løsningen, mottatt 16. november 2021
- Mandat for forprosjekt – kontroll ved bruk av digital teknologi i EK, mottatt 16. november 2021
- Rutine for avvikshåndtering, mottatt 16. november 2021
- Sjekkliste ved nyansettelse fra KIKS, mottatt 16. november 2021
- Taushetserklæring for nyansatte, mottatt 16. november 2021
- Autorisasjonsskjema for tilganger ved nyansettelser, mottatt 16. november 2021
- Avvikling eller endring av tilganger ved opphør av arbeidsforhold, mottatt 16. november 2021
- Brukerinstruks, mottatt 16. november 2021
- Rutine for risikovurdering av informasjonssikkerhet, mottatt 16. november 2021
- Håndbok i risikovurdering av informasjonssikkerhet, mottatt 16. november 2021
- Policy for informasjonssikkerhet, mottatt 16. november 2021
- Ledelsens gjennomgang av 1. juni 2021, mottatt 16. november 2021
- Veileder i internkontroll for kameraovervåking region sør, mottatt 16. november 2021
- Instruks for behandlingsansvar i kriminalomsorgen godkjent 16. desember 2021, mottatt 15. desember 2021

8.2 Dokumenter fra enhetene

8.2.1 Oslo friomsorgskontor

- Rutiner for informasjonssikkerhet ved Oslo friomsorgskontor, mottatt 19. april 2022
- Brev fra friomsorgskontoret til Region øst av 12. november 2021, mottatt 19. april 2022
- Organisasjonskort Oslo friomsorgskontor, mottatt 19. april 2022
- Fullmaktsskjema gjeldende for ansatte ved friomsorgskontoret, mottatt 19. april 2022
- Opplæringsplan for nyansatte ved friomsorgskontoret, mottatt 19. april 2022
- ROS-analyse og handlingsplan for informasjonssikkerhet med risikovurdering utført 18. mars 2022, mottatt 19. april 2022

8.2.2 Bredtveit fengsel, avdeling B2

- Bredtveits lokale rutiner for behandling av dokumenter, mottatt 20. april 2022
- Udatert instruks uten tittel fra KDI for bruk av fellesområdet, mottatt 20. april 2022
- Internrapportering fra enhet til region, mottatt 20. april 2022
- Brev fra Bredtveit til Region Øst om oppfølging av tilsyn fra Arkivverket, mottatt 20. april 2022
- Kriminalomsorgens arkivplan 2022, mottatt 20. april 2022

8.2.3 Ringerike fengsel, avdeling Ullersmo

- Instruks for bruk av kameraovervåking ved enhetene Kroksrud og Ungdomsenhet Øst, mottatt 26. april 2022
- Oversikt over informasjonssikkerhetsavvik ved Romerike fengsel i perioden 1. januar 2021 til 10. april 2022, mottatt 26. april 2022

- Databehandleravtale med Caverion, mottatt 26. april 2022
- Behandlingsprotokoll for Ullersmos bruk av fellesområdet, mottatt 26. april 2022