Datatilsynet

KRIMINALOMSORGSDIREKTORATET
Postboks 694
4302 SANDNES

Deres referanse	Vår referanse	Dato
202105340	20/03293-13	26.08.2021

Vedtak om pålegg - Brevkontroll med Kriminalomsorgens behandling av personopplysninger

1. Innledning

Vi viser til vår varsel om vedtak om pålegg, datert 28. juni 2021. Kriminalomsorgsdirektoratet hadde frist til å komme med merknader til varselet 13. august 2021.

Vi har ikke mottatt merknader, og vedtaket er identisk til varselet. For ordens skyld inntar vi den samme teksten som fremgikk av varselet.

2. Vedtak om pålegg

Datatilsynet vedtar følgende pålegg:

> *1. Kriminalomsorgsdirektoratet må i tråd med personopplysningsloven 2000 § 14 og tilhørende forskrift § 2-4 etablere en oversikt over alle behandlingene av personopplysninger som gjøres i direktoratet.*
>
> *2. Kriminalomsorgsdirektoratet må redegjøre for hvordan behandlingsansvaret etter personopplysningsloven er organisatorisk og praktisk plassert og fordelt i organisasjonen, jf. personopplysningsforskriften § 2-7. Vi ber om at gjeldende delegeringsdokumenter vedlegges.*
>
> *3. Kriminalomsorgsdirektoratet må oversende den gjeldende internkontrollen for etaten, jf. personopplysningsloven 2000 § 14.*

Vår hjemmel for å fatte pålegg er personvernforordningen artikkel 58 nr. 2. Vi viser til vår gjennomgang av hjemmelsrekken senere i dette brevet.

Fristen for å gjennomføre påleggene er **21. september 2021.** Innen denne fristen må dere sende oss en skriftlig bekreftelse på at påleggene er gjennomført. Dere må også sende dokumentene som påleggene gjelder.

3. Bakgrunn

3.1 Datatilsynets krav om redegjørelse

Datatilsynet besluttet på eget initiativ å etterspørre informasjon fra Kriminalomsorgsdirektoratet om direktoratets behandling av personopplysninger. I brev datert 10. desember 2020 etterspurte vi følgende:

- Har Kriminalomsorgsdirektoratet en oversikt over behandlinger av personopplysninger (tilsvarende behandlingsprotokoll etter personvernforordningens artikkel 30 og direktiv 2016/680 artikkel 24) som skjer i Kriminalomsorgen for formål etter straffegjennomføringsloven? Dersom dette foreligger ber vi om at denne oversendes til oss. Dersom dette ikke foreligger, ber vi om en forklaring på hvorfor dette mangler.

- Hvem er behandlingsansvarlig for de ulike behandlingene som skjer i kriminalomsorgen? Beskriv ansvarsforholdene internt i etaten.

3.2 Oppsummering av redegjørelse fra Kriminalomsorgsdirektoratet

Kriminalomsorgsdirektoratet skriver i redegjørelsen at det per i dag ikke finnes en sentral oversikt over behandlinger av personopplysninger i direktoratet. Direktoratet gikk i fjor til innkjøp av et datasystem (DraftIt) som skal brukes til i å lage en sentral oversikt. Direktoratet fremla et utkast basert på arbeidet i systemet. Denne behandlingsprotokollen inneholder ti behandlingsaktiviteter. Direktoratet skriver i redegjørelsen at de ikke anser denne for å være en tilstrekkelig oversikt over behandlingsaktiviteter, slik personvernregelverket krever.

I redegjørelsen betoner direktoratet at det behandles mange og til dels svært mange sensitive personopplysninger i forbindelse med straffegjennomføring. Det er derfor viktig at direktoratet har god oversikt og kontroll. Videre skriver direktoratet at det har skjedd en styrking av ressursinnsatsen på IKT-sikkerhet.

4. Nærmere om personopplysningslovens krav

4.1 Datatilsynets kompetanse

Kriminalomsorgsdirektoratets behandling av personopplysninger etter straffegjennomføringsloven kapittel 1A og 1B reguleres fremdeles av lov 14. april 2000 nr. 31 om behandling av personopplysninger med tilhørende forskrift, jf. forskrift om overgangsregler om behandling av personopplysninger § 1 a. Straffegjennomføringslovens

regler gjelder for gjennomføring av fengselsstraff mv., jf. lovens § 1. Straffegjennomføringslovens § 4c angir uttømmende hvilke formål som kan oppnås gjennom behandling av personopplysninger i Kriminalomsorgen.

Personopplysningsloven av 2018 § 20 tredje ledd bokstav a angir at Datatilsynets myndighet etter personvernforordningen artikkel 58 gjelder tilsvarende for tilsyn med overholdelsen av bestemmelser gitt i loven her og i forskrifter gitt i medhold av loven.

Datatilsynet finner derfor at vår kompetanse til å pålegge tiltak fremgår av personopplysningsloven 2018 § 20 tredje ledd, jf. personvernforordningen artikkel 58 nr. 2.

4.2 Krav til behandlingsprotokoll

Etter personvernforordningen artikkel 30 (og direktiv (EU) 2016/680 artikkel 24) har behandlingsansvarlig en plikt til å ha behandlingsprotokoll.

Tilsvarende plikt til å ha oversikt over behandlingene som finner sted hos en behandlingsansvarlig følger av personopplysningsloven 2000 § 14 og tilhørende forskrift § 2-4. Slik oversikt må regnes som nødvendig for å kunne ha et egnet system for internkontroll.

4.3 Krav til internkontroll

Personopplysningsloven § 14 og personopplysningsforskriften kapittel 3 gir regler om internkontrollsystem. Etter personopplysningsloven § 14 første ledd skal den behandlingsansvarlige «etablere og holde vedlike planlagte og systematiske tiltak som er nødvendige for å oppfylle kravene i eller i medhold av denne loven, herunder sikre personopplysningenes kvalitet». En rekke ulike tiltak kan være aktuelle i denne forbindelse, men en sentral del av internkontrollen vil ofte være å etablere rutiner for å oppfylle pliktene og rettighetene etter loven. Den behandlingsansvarlige skal dokumentere tiltakene, og dokumentasjonen skal være tilgjengelig for medarbeidere hos den behandlingsansvarlige og hos databehandleren, samt for Datatilsynet og Personvernnemnda, jf. § 14 annet ledd.

I henhold til forskriften § 3-1 første ledd skal tiltakene tilpasses virksomhetens art, aktiviteter og størrelse, og det skal legges særlig vekt på etterlevelsen av kravene til informasjonssikkerhet i personopplysningsloven § 13. Kravene om tiltak er konkretisert i forskriften § 3-1 annet ledd, som stiller krav om at den behandlingsansvarlige blant annet skal sørge for kjennskap til gjeldende regler og tilstrekkelig og oppdatert dokumentasjon for gjennomføring av rutiner. Tredje ledd bokstav a til f gir en ikke uttømmende oversikt over plikter og rettigheter den behandlingsansvarlige skal ha rutiner for, blant annet innhenting og kontroll av samtykke, vurdering av formål med behandling og oppfyllelse av begjæringen om innsyn og informasjon.

4.4 Plassering av behandlingsansvar

Straffegjennomføringsloven § 4e bokstav c angir at kongen gir forskrift om hvem som er behandlingsansvarlig.

I forarbeidene til straffegjennomføringslovens kapittel 1a og 1b fremhever departementet at det er særlig viktig å regulere hvem som har behandlingsansvaret. Videre følger det:

> *Eit sentralt spørsmål er kven som skal ha behandlingsansvaret i kriminalomsorga. Behandlingsansvarleg er etter personopplysningslova § 2 nr. 4 den som avgjer formålet med behandlinga av personopplysningar og kva for hjelpemiddel som kan brukast. Den definisjonen departementet nyttar i utkastet § 4b, tek likevel, som framlegget til ny politiregisterlov, utgangspunkt i definisjonen i personverndirektivet i staden for den tilsvarande definisjonen i personopplysningslova. Den behandlingsansvarlege er etter dette definert som den som etter lov eller forskrift avgjer formålet med behandlinga. Når det gjeld bakgrunnen og grunngivinga for dette standpunktet, viser ein til Ot.prp.nr.108 (2008–2009) «Om lov om behandling av opplysninger i politiet og påtalemyndigheten (politiregisterloven)» side 59-60.*
>
> *Når formålet med behandlinga blir fastsett i lov, slik departementet gjer framlegg om, vil hovudoppgåvene til den behandlingsansvarlege vere å sjå til og leggje forholda til rette for at regelverket for behandlinga blir følgt. Den behandlingsansvarlege har for eksempel ansvaret for tryggleik og hjelpemiddel, for at behandlinga blir meld til Datatilsynet, og for trygginga av dei rettane som den registrerte har i kraft av lova, jf. Ot.prp.nr.108 (2008–2009) side 60.*
>
> *Datatilsynet viser til at ein best tek hand om behandlingsansvaret ved å plassere ansvaret i nær tilknyting til sjølve behandlinga, og ber departementet revurdere standpunktet sitt frå høyringsnotatet. Departementet er langt på veg samd i synspunkta frå Datatilsynet og meiner at fengselsleiar og friomsorgsleiar bør vere behandlingsansvarlege på lokalt nivå. Men kriminalomsorga behandlar personopplysningar på fleire nivå – både sentralt ,regionalt og lokalt. Slik departementet ser det, bør den konkrete plasseringa av behandlingsansvaret regulerast i forskrift på same måten som for politiet, sjå nedanfor. Spørsmålet om kven som skal vere behandlingsansvarleg i kriminalomsorga, kjem til å bli vurdert nærmare når forskrifta skal utarbeidast.*

5. Datatilsynets vurdering

Vi legger i det videre til grunn at øverste leder i Kriminalomsorgsdirektoratet har behandlingsansvaret for behandlingen av personopplysninger i etaten.

Datatilsynets finner at Kriminalomsorgsdirektoratet ikke har lagt frem en tilfredsstillende oversikt over direktoratets behandlinger av personopplysninger.

Kravet til oversikt over behandlingene som gjøres i en virksomhet er grunnleggende for å kunne overholde andre forpliktelser etter regelverket. Kriminalomsorgen har ikke gitt noen begrunnelse for at denne sentrale oversikten mangler.

Det foreligger heller ingen dokumentasjon eller beskrivelse av de interne ansvarsforholdene i etaten. Direktoratet har kun vist til sin generelle adgang til å delegere ansvar i styringslinjen i etaten. Dette anses å utgjøre et avvik fra kravene i personvernregelverket som er gjengitt over. Som direktoratet selv fremhever i redegjørelsen, behandler Kriminalomsorgen store mengder personopplysninger. Blant annet behandles mange sensitive personopplysninger, herunder særlige kategorier av personopplysninger. Gjennom det vi har erfart gjennom vår behandling av saker som gjelder ivaretakelse av personvernregelverket i Kriminalomsorgen, som meldinger om brudd på personopplysningssikkerheten, veiledningsforespørsler og klager fra innsatte, mener vi at det foreligger grunn til å kontrollere Kriminalomsorgens etterlevelse nærmere.

For å kunne undersøke Kriminalomsorgens etterlevelse av personvernregelverket, er det nødvendig for Datatilsynet å få tilsendt oversikten over hvilke behandlinger av personopplysninger som gjøres i etaten, se vårt varslede pålegg nr. 1.

Videre finner vi det nødvendig å få tilsendt oversikt over hvordan behandlingsansvaret utøves i praksis i etaten, se vårt varslede pålegg nr. 2. Dette innebærer at dere må sende oss en oversikt over hvor og hvordan ansvar for behandling av personopplysninger, herunder personopplysningssikkerhetskrav, delegeres til de ulike enhetene og underliggende etater til Kriminalomsorgsdirektoratet.

Endelig vurderer vi det også som hensiktsmessig og relevant å pålegge Kriminalomsorgen oversende den samlede dokumenterte internkontrollen som gjelder for etatens behandling av personopplysninger. Vi viser til kravene som følger av personopplysningsloven § 14, jf. tilhørende forskrift kapittel 2 og 3.

Den dokumentasjonen dere oversender vil danne grunnlaget for vår vurdering av eventuell videre kontroll av etatens etterlevelse av personvernregelverket.

6. Avsluttende merknader

6.1 Tvangsmulkt

Vi vil vurdere bruk av tvangsmulkt dersom påleggene ikke er gjennomført innen fristen (jf. personopplysningsloven § 29.)

6.2 Klagemulighet

Dere kan klage på vedtaket. En eventuell klage må sendes til oss **innen tre uker** etter at dette brevet er mottatt (jf. forvaltningsloven §§ 28 og 29). Dersom vi opprettholder vårt vedtak vil vi sende saken videre til Personvernnemnda for klagebehandling.

6.3 Innsyn og offentlighet

Dere har rett til innsyn i sakens dokumenter (jf. forvaltningsloven § 18). Vi vil også informere dere om at alle dokumentene i utgangspunktet er offentlige (jf. offentlighetsloven § 3.)

Dersom dere mener det er grunnlag for å unnta hele eller deler av dokumentet fra offentlig innsyn ber vi dere om å begrunne dette.

Hvis dere har spørsmål, kan dere ta kontakt med Embla Helle Nerland på telefonnummer 22 39 69 54.

Med vennlig hilsen

Camilla Nervik
seksjonssjef

Embla Helle Nerland
juridisk rådgiver

Dokumentet er elektronisk godkjent og har derfor ingen håndskrevne signaturer

Kopi til: KRIMINALOMSORGSDIREKTORATET, Per Ketil Andersen