Datatilsynet

BODØ KOMMUNALE PENSJONSKASSE
Postboks 319
8001 BODØ

Deres referanse	Vår referanse	Dato
	20/01865-1 (19/03054) /JHN	21.08.2020

Forhåndsvarsel om irettesettelse

Datatilsynet har mottatt varsel, som omhandler Bodø Kommunale Pensjonskasse (BKP), etter arbeidsmiljøloven § 2a-1 nr. 1 om brudd på personopplysningssikkerheten jf. § 2a-1 nr. 2 bokstav f.

Dokumentene i varselet er unntatt offentlighet også for sakens parter jf. arbeidsmiljøloven § 2a-7. Datatilsynet minner om forbudet mot gjengjeldelse i arbeidsmiljøloven § 2a-4.

I varslingen ble det anført at BKP hadde en praksis i saker om uførepensjon hvor det ble innhentet unødvendige legeerklæringer, manglende kontroll over arkiv og en innsamling og deling av statistikk hvor sensitive personopplysninger ble delt med enheter utenfor BKP.

På bakgrunn av varselet valgte Datatilsynet å iverksette en selvstendig undersøkelse og sendte krav om redegjørelse 06.11.2019 og mottok svar fra BKP 26.02.20. Det ble sendt ytterligere krav om redegjørelse 17.04.2020, som ble besvart 08.05.2020.

1. Varsel om vedtak om irettesettelse

Dette er et forhåndsvarsel etter forvaltningsloven § 16, om at Datatilsynet fatter vedtak om irettesettelse mot Bodø Kommunale Pensjonskasse, org.nr. 940 027 365, for:

- Brudd på personvernforordningen artikkel 6 og 9 ved at BKP har behandlet sensitive personopplysninger i statistikk som ikke fremstår som nødvendig.
- BKP har utlevert sensitive personopplysninger til Bodø Kommune uten rettslig grunnlag i art. 6 og 9.

Vår hjemmel for å utstede irettesettelse er personvernforordningen artikkel 58 nr. 2 bokstav b.

2. Sakens bakgrunn

Saken gjelder anførsler om ulovlig behandling av personopplysninger i Bodø Kommunale Pensjonskasse.

Selv om Datatilsynet har iverksatt sin undersøkelse på bakgrunn av et varsel, så er saksbehandlingen og vedtaket rettet mot BKP, og basert på det faktagrunnlag som har fremkommet fra BKP på bakgrunn av Datatilsynets spørsmål.

Varsler er ikke part i saken da den anførte ulovlige behandlingen av personopplysninger ikke omhandler varsler selv, og det vil kun være BKP som har klagerett jf. fvl. § 28.

Datatilsynet har vurdert tre forhold som sentrale: Innhenting av legeerklæringer, utlevering av personopplysninger til utenforstående og styrets behandling av personopplysninger.

3. Rettslig grunnlag

Datatilsynet fører kontroll med etterlevelsen av personvernregelverket, jf. personvern-forordningen artikkel 57.

3.1. Lovvalg

Personopplysningsloven (2018) og personvernforordningen trådte i kraft 20. juli 2018. Før dette var behandling av personopplysninger regulert av personopplysningsloven av 14. april 2000 nr. 31 og den nå opphevede personopplysningsforskriften av 15. desember 2000 nr. 1265. Overgangsregler finner vi i personopplysningsloven (2018) § 33.

Ifølge personopplysningsloven (2018) § 33, skal reglene «som gjaldt på handlingstidspunktet» legges til grunn når det treffes vedtak om overtredelsesgebyr, med mindre lovgivningen på tidspunktet for avgjørelsen fører til et mer gunstig resultat for den ansvarlige.

Det følger av personopplysningsloven § 28 at adgangen til å ilegge overtredelsesgebyr foreldes fem år etter overtredelsen er opphørt. Fristen avbrytes ved at Datatilsynet gir forhåndsvarsel om eller fatter vedtak om overtredelsesgebyr.

Selv om hoveddelen av den ulovlige behandlingen har foregått før 2015, så er det også forhold i 2015 og fremover som kunne ha medført overtredelsesgebyr etter gammel lov.

Datatilsynet behandler likevel saken etter reglene i personopplysningsloven og personvernforordningen som trådte i kraft 20. juli 2018. Det tidligere regelverket gir ikke adgang for irettesettelse som reaksjonsform. Behandling etter nytt regelverk vil derfor også føre til et mer gunstig resultat for BKP.

3.2 Nærmere om personopplysningslovens krav

Personopplysningsloven gjennomfører den europeiske personvernforordningen i norsk rett.

Reglene i loven og forordningen gjelder ved helt eller delvis automatisert behandling av personopplysninger, jf. personopplysningsloven § 2 og personvernforordningen artikkel 2. Inngangsvilkåret for at forordningen skal komme til anvendelse, er at det skjer en behandling av personopplysninger.

Forordningens artikkel 4 nr. 1 definerer personopplysninger slik:

«enhver opplysning om en identifisert eller identifiserbar fysisk person («den registrerte»); en identifiserbar fysisk person er en person som direkte eller indirekte kan identifiseres, særlig ved hjelp av en identifikator, f.eks. et navn, et identifikasjonsnummer, lokaliseringsopplysninger, en nettidentifikator eller ett eller flere elementer som er spesifikke for nevne fysiske persons fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sosiale identitet».

Definisjonen av personopplysninger er vid. Det relevante er at opplysningene er egnet til å identifisere en person, også med hjelpemidler.

All behandling av personopplysninger må være i tråd med de grunnleggende prinsippene i forordningens artikkel 5. Prinsippene innebærer at behandlingen skal være lovlig, rettferdig og gjennomsiktig (bokstav a). Behandlingen skal kun skje etter forhåndsbestemte formål, og ikke gjenbrukes for nye formål som strider mot de opprinnelige (bokstav b). Behandlingen skal være adekvat, relevant og begrenset til det bestemte formålet (bokstav c). Opplysningene skal være riktige (bokstav d), og de skal kun lagres for en begrenset tidsperiode etter hva som er nødvendig etter formålet (bokstav e). Behandlingen skal skje på en måte som sikrer personopplysningenes integritet og konfidensialitet (bokstav f). Dette prinsippet innebærer at personopplysningene skal sikres mot at utenforstående får uautorisert tilgang, gjennom egnede organisatoriske og tekniske tiltak.

Det er den behandlingsansvarlige som er ansvarlig for å sikre at disse prinsippene og forordningen som helhet, overholdes (artikkel 5 nr. 2).

Et av personvernforordningens krav for at behandlingen skal anses for å være lovlig er at det foreligger et behandlingsgrunnlag. De ulike formene for behandlingsgrunnlag finner vi i forordningens artikkel 6.

Helseopplysninger er en særlig kategori av personopplysninger, jf. personvernforordningen artikkel 9 nr. 1. For at behandling av helseopplysninger skal være lovlig, må behandlingen også oppfylle et av vilkårene i artikkel 9 nr. 2 bokstav a til j. Dette kan for eksempel være at den registrerte har samtykket til behandlingen (bokstav a) eller at behandlingen er nødvendig for å yte eller forvalte helsetjenester (bokstav h).

4. Innhenting av legeerklæringer

BKP opplyser i sin redegjørelse at det har vært praksis i søknader om bruttopensjoner (uførepensjoner) å innhente helseopplysninger/legeerklæring, også i de sakene hvor NAV har kommet til at uføregraden er 50% eller høyere.

Det blir opplyst at man innhentet 27 erklæringer i 2017, 12 i 2018 og 20 erklæringer i 2019. Datatilsynet ba også om tall for 2014, 2015 og 2016, men har ikke mottatt dette.

Det rettslige grunnlaget for denne praksisen blir opplyst å være Hovedtariffavtalen for offentlig sektor, Vedlegg 5 §§ 8-1 (1) og 8-4 (2). Det vises også til et tilsvarende krav til dokumentasjon for Statens Pensjonskasse (SP) etter lov om SP § 20 og folketrygdloven § 21-3.

BKP opplyser at de la om praksis i 2017 slik at det ikke lenger innhentes legeerklæringer i saker hvor NAV har innvilget uførepensjon basert på en uføregrad på 50% eller mer, noe som er i tråd med praksis i andre pensjonskasser.

Det er klart at dette er behandling av særskilte kategorier personopplysninger jf. art. 4 nr. 1 jf. art. 9.

Etter Datatilsynet s vurdering vil dette kunne fylle vilkårene for behandlingsgrunnlag i artikkel 6. nr. 1 bokstav b) når behandlingen er nødvendig for å oppfylle en avtale som den registrerte er part i jf. art. 9 nr. 2 bokstav a og b. Spørsmålet er om personopplysningene som behandles har vært adekvat, relevant og begrenset til det bestemte formålet jf. personvernforordningen art. 5 nr. 1 bokstav c.

Formålet med behandlingen har vært å vurdere hvilken uføregrad som skal legges til grunn for utbetaling av pensjon og i den sammenheng vil en legeerklæring være relevant og tilstrekkelig.

Prinsippet om dataminimering er et sentralt prinsipp i personvernretten og man bør alltid søke å behandle så få personopplysninger som mulig, og det fremstår derfor som effektivt og i tråd med dette prinsippet å legge til grunn NAVs vurdering i saker hvor uføregraden er 50% eller mer, noe som er praksis i andre pensjonskasser. Det er likevel vanskelig å si at det foreligger et klart brudd på art. 5 nr. 1 bokstav c da BKP har hjemmel til selvstendig å vurdere uføregraden og har anledning til legge til grunn en uføreprosent som fraviker fra NAVs vurdering noe som åpner for en full behandling i hver enkelt sak.

5. Innsamling av statistikk – deling av personopplysninger med utenforstående

BKP har redegjort for at det fra 2000 til 2015 ble utarbeidet en oversikt som ble oversendt til Bodø Kommune som er pensjonskassens største kunde.

Totalt ble det oversendt opplysninger om 1028 personer som var ansatt i Bodø kommune og 25 personer som var ansatt eksternt.

Opplysningene inneholdt kjønn, alder, diagnosekategori, avdeling i kommunen, stilling. I noen avdelinger var det kun oppgitt en person.

Diagnosene var inndelt i 8 kategorier med ulik grad av presisjon hvor f.eks. kategori F var beinbrudd, mens kategori S var spesielle sykdommer og inneholdt 18 diagnoser for eksempel alkoholisme eller tinnitus. Det var oppgitt 4 avdelinger, men også tre enheter utenfor Bodø kommune.

Et eksempel basert på kategoriene vil kunne være:

Kvinne, 35 år, diagnosekategori D (Depresjon, angst, utbrenthet), …..avdelingen, hjelpepleier

Forordningens artikkel 4 nr. 1 definerer personopplysninger slik:

«enhver opplysning om en identifisert eller identifiserbar fysisk person («den registrerte»); en identifiserbar fysisk person er en person som direkte eller indirekte kan identifiseres

Selv om oppføringene ikke inneholder navn, så vil det på grunn av alder, yrkestittel og tjenestested, som til dels er små enheter, så vil det være enkelt å identifisere den registrerte. I og med oppføringene inneholder helseopplysninger, så vil de falle inn under art. 9 og reglene om særskilte kategorier personopplysninger.

Statistikk som er anonymisert vil ikke falle inn under personvernforordningens regler, men det er ikke tilfelle her i og med statistikken inneholder personopplysninger. I tillegg vil ofte bearbeidelsen av personidentifiserbare opplysninger til statistikk innebære en behandling som faller inn under personvernregelverket. Man må da se på om for det første BKPs interne behandling var i tråd med reglene for behandling av personopplysninger og deretter om det var rettslig grunnlag for å utlevere opplysningene til Bodø kommune.

Behandling av personopplysninger må alltid ha et rettslig grunnlag i art. 6, men for særskilte kategorier opplysninger, så må vilkårene i art. 9 også være oppfylt.

Utarbeidelse av statistikk som inneholder personopplysninger kan ha et rettslig grunnlag art. 6 nr. 1 bokstav f hvis behandlingen er nødvendig for formål knyttet til de berettigede interessene som forfølges av den behandlingsansvarlige eller en tredjepart, med mindre den registrertes interesser eller grunnleggende rettigheter og friheter går foran og krever vern av personopplysninger, særlig dersom den registrerte er et barn.

Her vil man kunne tenke at BKP har i en berettiget interesse til å bruke personopplysningene til å utarbeide statistikk for å effektivt kunne drive pensjonskassen, men det vil fortsatt være spørsmål knyttet til om det er nødvendig at statistikken er i en slik form at de registrerte kan identifiseres.

Når det gjelder vilkårene i art. 9, så vil uttrykkelig samtykke etter bokstav a eller for å oppfylle forpliktelser innen trygderett etter bokstav b kunne være aktuelle grunnlag, men det vil fortsatt kunne stilles spørsmål om det var nødvendig med statistikk som inneholdt personopplysninger og om ikke statistikken kunne vært utarbeidet på en annen måte.

Datatilsynet finner at utarbeidelsen og behandlingen av denne type statistikk ikke er forenelig med reglene i art. 6 og 9.

Når det gjelder utlevering til Bodø kommune som er en kunde av BKP, så kan ikke Datatilsynet se at finnes rettslig grunnlag for utlevering. Bodø kommune er en kunde av BKP og det må derfor både finnes et utleveringsgrunnlag og et rettslig grunnlag for Bodø kommunes behandling. Datatilsynet kan ikke se at dette foreligger.

6. Innsamling av statistikk – behandling av personopplysninger i styret

BKP har opplyst at det i styret har blitt behandlet personopplysninger om pensjonskassens kunder og blitt bedt om å legge frem dokumentasjon på perioden 2014-18 og 2018 til 2019.

Opplysningene har blitt opplyst i følgende form:

Kjønn, fødselsår, stilling, opplysninger om medlemskap og pensjoner, og årsak til pensjon.

Opplysningene om helsetilstand har vært til dels upresise i mangel av konkrete diagnoser, samt svært nærgående f.eks. kreft i lungene, brystkreft, psykisk overbelastning, hjerteproblemer, psykisk lidelse, angst, sykdom etter fødsel etc.

BKP har endret praksis når det gjelder hvilke opplysninger som fremlegges for styret, og fra 15.03.18 har man ikke lenger tatt med arbeidsuførhetens årsak.

Datatilsynet viser til drøftelsen overfor når det gjelder rettslig grunnlag for å utarbeide og behandle statistikk som inneholder personopplysninger og manglene oppfyllelse av vilkårene i art. 6 og 9.

Det kan også her stilles spørsmål om det var nødvendig for styret å behandle statistikk som inneholdt særskilte kategorier personopplysninger, men Datatilsynet kan ikke konkludere at det ikke var nødvendig, men det er klart at enhver virksomhet bør minimere den type behandling.

7. Videre saksgang

Dette brevet er et forhåndsvarsel om vedtak om irettesettelse, jf. forvaltningsloven § 16 jf. personvernforordningen art. 58 nr. 2 bokstav b.

Irettesettelse er forvaltningsmessig reaksjon med formål å markere kritikk av det omtalt bruddet på reglene.

Ileggelse av irettesettelse vil kunne bli lagt vekt på i en eventuell senere vurdering av ileggelse av overtredelsesgebyr hvis det forekommer tilsvarende brudd regelverket jf. personvernforordningen art. 83 nr. 2 bokstav i.

Datatilsynet vil understreke at saken har blitt behandlet under nytt regelverk da det har ført til en mildere reaksjon jf. personopplysningsloven § 33.

Dersom dere har kommentarer til dette varselet, ber vi om at de sendes oss så snart som mulig og senest innen 17.09.2020.

Hvis dere har spørsmål, kan dere ta kontakt med undertegnede saksbehandler (e-post: jani@datatilsynet.no).

Med vennlig hilsen

Jan Henrik Nielsen
juridisk seniorrådgiver

Dette brevet er godkjent elektronisk i Datatilsynet og har derfor ingen signatur.