Datatilsynet

STATENS PENSJONSKASSE
FORVALTNINGSBEDRIFT
Postboks 10 Skøyen
0212 OSLO

Deres referanse	Vår referanse	Dato
19/029514	20/01893-12	24.11.2021

Vedtak om overtredelsesgebyr

Datatilsynet viser til tidligere korrespondanse i forbindelse med avviksmelding datert 24.09.2019, senest deres svar på varsel om vedtak om overtredelsesgebyr datert 12.05.2021.

Vi beklager den lange saksbehandlingstiden og en til dels uryddig saksgang, jf. vårt brev til dere datert 27.04.2021.

1. Vedtak om overtredelsesgebyr

Datatilsynet ilegger herved Statens pensjonskasse følgende vedtak:

> *Med hjemmel i personvernforordningen artikkel 58 nr. 2 bokstav i, jf. personopplysningsloven § 26, ilegges Statens pensjonskasse et overtredelsesgebyr på 1 000 000 NOK – én million norske kroner – til statskassen, for overtredelse av prinsippene for behandling av personopplysninger i personvernforordningen artikkel 5 nr. 1 bokstav c og e og kravet til nødvendighet etter artikkel 6 nr. 1, jf. artikkel 9 nr. 2.*

2. Beskrivelse av avviket

I avviksmeldingen fremgår det at Statens pensjonskasse (heretter SPK) i perioden 01.07.2015 til 24.09.2019 innhentet større mengder personopplysninger de ikke hadde behov for til det angitte formålet. SPK har angitt at avviket ble oppdaget 15.02.2019.

Avviket knytter seg til innhenting av periodiserte inntektsopplysninger[1] fra Skatteetaten i forbindelse med SPKs årlige etteroppgjør for uførepensjon. Opplysningene brukes til å korrigere utbetalt pensjon (for mye eller for lite).

Overføringen av opplysninger har skjedd i medhold av skatteforvaltningsloven § 3-6 annet ledd, som gir Skatteetaten hjemmel til å utlevere opplysninger om «pensjonsgivende inntekt»

[1] Inntekter som er opptjent i et nærmere angitt tidsintervall innenfor et år.

til SPK, og i tråd med en informasjonsutvekslingsavtale mellom partene. Overføringen har skjedd via et teknisk grensesnitt (API).

Opplysningene Skatteetaten har oversendt er løpende, periodiserte inntektsopplysninger (rådata) fra a-ordningen[2]. Opplysningene er dels særlige kategorier personopplysninger i form av opplysninger om uførepensjon fra andre enn SPK og folketrygden. Ellers er det tale om svært detaljerte inntektsopplysninger, for eksempel skattepliktig del av forsikringer, kjøp av aksjer til underkurs, naturalytelser m.m.

SPK har manglet et filter for å forhindre import og lagring av unødvendige inntektsopplysninger, og man har heller ikke hatt en slettefunksjon for dataene. Ansatte i SPK har hatt tilgang til de overflødige opplysningene på individnivå.

På tidspunktet for avviksmeldingen oppsummerte SPK årsakene til avviket slik:

- utilstrekkelig vurdering av hjemmelsgrunnlaget for behandling av personopplysningene, herunder begrepet «pensjonsgivende inntekt»
- manglende oppfølging av kravet om dataminimering
- manglende sletterutiner/slettefunksjon
- manglende tilgangsstyring i saksbehandlersystemet

SPK vurderer avviket som alvorlig, ettersom det er tale om ulovlig behandling av svært personlige opplysninger om en generelt sårbar gruppe personer (uføretrygdede).

SPK viser også til de mulige konsekvensene av den ulovlige behandlingen av personopplysninger. Etterkontrollen kan utløse krav om tilbakebetaling fra den enkelte mottaker, og krav om tilbakekreving av for mye utbetalt uførepensjon vil utgjøre et tvangsgrunnlag for utlegg. SPKs avgjørelser om tilbakebetaling skjer ved helautomatiserte (maskinelle) vedtak uten hensyn til skyld hos den uføretrygdede.

SPK angir at skatteytere er pålagt en omfattende opplysningsplikt overfor skattemyndighetene. Det er vist til at skattyterne må kunne føle seg trygge på at innrapporterte opplysninger ikke gjenbrukes til uforenlige formål uten rettslig grunnlag.

Videre peker SPK på at de generelt ikke gir aktiv informasjon om hvilke personopplysninger som innhentes, noe som gjør det vanskelig for de registrerte å utøve sin rett etter personvernregelverket til for eksempel sletting av unødvendige opplysninger.

Som følge av avviket hadde SPK planlagt og/eller iverksatt følgende tiltak:

- dialog med Arbeids- og sosialdepartementet om endring av lovhjemmelen for innhenting av opplysninger
- sperre de interne tilgangene til opplysningene
- slette data
- etablere filter for å unngå import av unødvendige data

[2] En elektronisk løsning for samordnet rapportering fra arbeidsgivere.

3. Redegjørelse fra Statens pensjonskasse

I brev av 18.02.2020 ba Datatilsynet om en redegjørelse nærmere for tiltakene som var iverksatt etter avviket. SPK besvarte henvendelsen i brev datert 16.03.2020. SPK har også gitt informasjon i møte den 16.04.2021.

SPK presiserer at etteroppgjør ikke er en kontrollaktivitet for å avdekke forbudte handlinger, men en lovpålagt oppgave der SPK foretar en årlig avregning som kan resultere i et utbetalings- eller tilbakebetalingskrav.

SPK angir også at inntektsopplysninger ble innhentet fra Skatteetaten første gang i oktober 2016 (altså ikke i juli 2015, som tidligere opplyst). Kun SPK-ansatte med tilgang til uførepensjon i saksbehandlersystemet har hatt mulighet for innsyn i opplysningene. Dette utgjør ca. 50 av totalt 450 ansatte.

For ca. 44 000 personer (av totalt ca. 1 000 000) er det innhentet inntektsopplysninger til bruk i etteroppgjør uten tilstrekkelig hjemmelsgrunnlag. For ca. 24 000 av disse er det ikke innhentet overskuddsinformasjon, ettersom personene kun har uførepensjon som inntekt.

SPK understreker at de tar saken svært alvorlig. Som følge av avviket har SPK iverksatt følgende tiltak:

- Lovhjemmelen for innhenting av periodiserte inntektsopplysninger er endret og presisert.
- De interne tilgangene til overflødige opplysninger ble sperret i september 2019.
- Overskuddsopplysninger ble slettet 11.10.2019.
- SPK etablerte en sletterutine der alle inntektsopplysninger som ikke er aktuelle for etteroppgjøret slettes umiddelbart etter innlesing til databasen. I etterkant er et filter for å unngå import av unødvendige data innført i samarbeid med Skatteetaten.

I tiden etter at avviksmeldingen ble sendt har SPK vurdert hjemmelsgrunnlaget for innhentingen av inntektsopplysninger nærmere. SPK vurderer nå at de har hatt hjemmel i skatteforvaltningsloven § 3-6 annet ledd til å hente inn et bredt spekter av inntektsopplysninger. Bestemmelsen var noe uklar når det gjaldt innhenting av *periodiserte* inntektsopplysninger, og SPK tok derfor initiativ til en endring av ordlyden i bestemmelsen. SPK ønsker likevel å presisere at de mener at inntektsopplysninger ikke er innhentet uten hjemmel i særlovgivningen.

En hovedårsak til at SPK har innhentet unødvendige inntektsopplysninger er at SPK fant det formålstjenlig å innhente opplysninger fra Skatteetaten. Inntektsopplysningene fra Skatteetaten var bare tilgjengelig i et predefinert datasett som også inneholdt informasjon SPK ikke hadde behov for i forbindelse med etteroppgjør.

I møtet den 16.04.2021 forklarte SPK at ordningen ble uførepensjon ble lagt om i 2015 («Uføreformen»). Etter omleggingen var det uklart for SPK hvilke inntektsopplysninger som var relevante for det årlige etteroppgjøret. Hvilke opplysninger som har vist seg å være relevante har også endret seg over tid. Dette har medført innhenting av unødvendige inntektsopplysninger. SPK innså ikke implikasjonene av dette på et tidlig nok tidspunkt. SPK

har ikke hatt noe system for gjennomgang og sletting av overskuddsinformasjon i perioden avviket vedvarte.

SPK forklarte videre at det måtte gjøres en nærmere vurdering av hvilke inntektsopplysninger som var nødvendige for etteroppgjør da avviket ble oppdaget. Dette er årsaken til at opplysningene først ble sperret og deretter slettet.

4. Statens pensjonskasses kommentarer til varselbrevet

Statens pensjonskasse har kommet med ytterligere kommentarer og presiseringer i brev datert 12.05.2021.

I brevet er det pekt på at uførepensjonen skal justeres ut fra hvor mye en person har hatt i arbeidsinntekt et gitt år. Uførepensjonen utbetales som utgangspunkt på grunnlag hva den uføre tror arbeidsinntekten vil være det kommende år. Det kan være vanskelig for en person å forutsi nøyaktig hva årsinntekten vil bli, og SPK er avhengig av at personen fortløpende melder fra om inntektsendringer. Reformen forutsetter at det gjennomføres et etteroppgjør påfølgende år, der SPK beregner om den uføre skal få etterbetalt, eller må tilbakebetale, en del av ytelsen. Etteroppgjør gjøres i stor grad maskinelt, og det årlige skatteoppgjøret legges til grunn for beregningene.

Skatteoppgjøret skiller imidlertid ikke i tilstrekkelig grad mellom ulike inntektsarter, det vil si hvilke typer inntekt som henholdsvis skal inngå eller holdes utenfor grunnlaget for beregning av uføreytelsen – og dermed også etteroppgjøret. Videre angir skatteoppgjøret inntekter for året samlet og ikke som periodiserte inntektstall.

I etteroppgjøret har SPK behov for opplysninger om skatteoppgjørets pensjonsgivende inntekt fordelt både på inntektsarter og periodisert på måneder. Det vil oftest være krevende og komplisert for den uføre selv å dokumentere dette på riktig måte, og manuell innsending av dokumentasjon vil vanligvis gi overskuddsinformasjon som vanskelig kan sorteres ut. SPK valgte derfor å innhente periodiserte data fordelt på inntektsart data direkte fra Skatteetaten. Etteroppgjøret skjer én gang per år, om høsten etter at skatteoppgjøret for året før er klart. Tilsvarende innhentes dataene fra Skatteetaten én gang per år.

Til tross for mangelen på bedre løsninger, erkjenner SPK at avviket fra personvernregelverket burde vært oppdaget tidligere.

SPK har innhentet og oppbevart overskuddsinformasjon totalt tre ganger: i oktober 2016, 2017 og 2018. To av innhentingene fant sted før ny personopplysningslov trådte i kraft (i juli 2018). I oktober 2019 ble overskuddsinformasjon innhentet, men slettet umiddelbart. I oktober 2020 ble kun nødvendige inntektsopplysninger innhentet.

SPK utviklet et filter som fra juli 2019 sørget for at kun nødvendige opplysninger om pensjonsgivende inntekt var tilgjengelig for saksbehandlere. Før SPK hentet inn data for etteroppgjøret i oktober 2019, ble det implementert en systemløsning som slettet all overskuddsinformasjon fra databasen. Løsningen sikret også at all overskuddsinformasjon

som i 2019 og senere måtte bli hentet inn, ville bli slettet fortløpende og umiddelbart. Et nytt datauttrekk med kun nødvendig informasjon var på plass per 27.08.2020.

SPK påpeker også at de brukte lang tid på avviksmeldingen fordi de var «utrente» i å sende slike meldinger. Avviket ble derfor strengt tolket og utførlig forklart i første melding. SPK angir at de i dag ville fremstilt saken annerledes og mer nyansert.

SPK peker blant annet på at det de uføre som er omfattet av avviket deltar i arbeidslivet i stillinger på mellom 20 og 80 %. Det var ikke SPKs intensjon å stigmatisere gruppen som generelt sårbar. Videre fremgår det at SPK tilstreber å gi de registrerte god informasjon sin gjennom nettside.

Oppsummert erkjenner SPK at avviket burde vært oppdaget tidligere. Det påpekes imidlertid at konsekvensen for de berørte har vært begrenset. Overskuddsinformasjonen var underlagt tilgangskontroll, og SPK har gjort sitt ytterste for å rette opp situasjonen da avviket ble oppdaget. I lys av det dette mener SPK at det varslede overtredelsesgebyret er for høyt i forhold til avvikets karakter.

5. Aktuelt lovgrunnlag for vurderingen

Datatilsynet fører kontroll med etterlevelsen av personvernregelverket, jf. personopplysningsloven § 20 og personvernforordningen artikkel 57.

5.1 Om lovvalg

Den nye personopplysningsloven, som inkorporerer EUs personvernforordning i norsk rett, trådte i kraft 20.07.2018. Loven opphevet samtidig personopplysningsloven (2000) og reglene i personopplysningsforskriften (2000).

Denne saken gjelder forhold som oppsto i 2016, altså før ikrafttredelsen av personopplysningsloven (2018), men som har vedvart i tiden etterpå. Vi må derfor ta stilling til om saken skal vurderes etter personopplysningsloven (2018) eller personopplysningsloven (2000).

I personopplysningsloven (2018) § 33 første ledd finnes en særskilt overgangsregel om overtredelsesgebyr, som lyder:

> «Reglene om behandling av personopplysninger som gjaldt på handlingstidspunktet, skal legges til grunn når det treffes vedtak om overtredelsesgebyr. Lovgivningen på tidspunktet for avgjørelsen skal likevel anvendes når dette fører til et gunstigere resultat for den ansvarlige».

Spørsmålet om lovvalg må altså vurderes ut fra hva som regnes som handlingstidspunktet.

Det aktuelle avviket oppsto før ikrafttredelsen av nytt regelverk den 20.07.2018, men vedvarte frem til avviket ble oppdaget i september 2019. Handlingstidspunktet i denne saken har altså vedvart over tid og i tiden etter at personopplysningsloven (2018) trådte i kraft. Det følger da av personopplysningsloven (2018) § 33 at saken skal vurderes etter denne loven.

Vi viser også til forarbeidene til personopplysningsloven (2018), Prop. 56 LS (2017-2018) side 196, hvor departementet blant annet uttaler følgende om spørsmålet om lovvalg mellom personopplysningsloven (2000) og personopplysningsloven (2018):

> «Utgangspunktet vil være at vedtak hos Datatilsynet og Personvernnemnda vil måtte fattes på grunnlag av de til enhver tid gjeldende materielle regler».

Det samme følger av Personvernnemndas praksis i saker som ble oversendt nemnda før ny lov trådte i kraft, men som ble behandlet etter ikrafttredelsen; se for eksempel PVN-2018-05 og PVN-2018-06.

På denne bakgrunn er det etter vår vurdering klart at saken må vurderes etter personopplysningsloven (2018) og personvernforordningen.

5.2 Prinsippene for behandling av personopplysninger

Grunnprinsippene for behandling av personopplysninger fremgår av personvernforordningen artikkel 5. De relevante delene av bestemmelsen lyder:

> «1. Personopplysninger skal (…)
> c) være adekvate, relevante og begrenset til det som er nødvendig for formålene de behandles for («dataminimering»), (…)
> e) lagres slik at det ikke er mulig å identifisere de registrerte i lengre perioder enn det som er nødvendig for formålene som personopplysningene behandles for (…) («lagringsbegrensning»),
> f) behandles på en måte som sikrer tilstrekkelig sikkerhet for personopplysningene, herunder vern mot uautorisert eller ulovlig behandling og mot utilsiktet tap, ødeleggelse eller skade, ved bruk av egnede tekniske eller organisatoriske tiltak («integritet og konfidensialitet»)».

5.3 Rettslig grunnlag for behandlingen

Enhver behandling av personopplysninger må ha rettslig grunnlag i personvernforordningen artikkel 6 nr. 1 for å være lovlig. De relevante delene av bestemmelsen lyder:

> «1. Behandlingen er bare lovlig dersom og i den grad minst ett av følgende vilkår er oppfylt: (…)
> c) behandlingen er nødvendig for å oppfylle en rettslig forpliktelse som påhviler den behandlingsansvarlige, (…)
> e) behandlingen er nødvendig for å utføre en oppgave i allmennhetens interesse eller utøve offentlig myndighet som den behandlingsansvarlige er pålagt (…)».

Behandling av såkalt særlige kategorier av personopplysninger, for eksempel helseopplysninger, er som utgangspunkt forbudt, jf. personvernforordningen artikkel 9 nr. 1. For at behandling av slike opplysninger skal være lovlig, må minst ett av vilkårene i artikkel 9 nr. 2 være oppfylt. De relevante delene av bestemmelsen lyder:

«2. Nr. 1 får ikke anvendelse dersom et av følgende vilkår er oppfylt: (…)
b) Behandlingen er nødvendig for at den behandlingsansvarlige eller den registrerte skal kunne oppfylle sine forpliktelser og utøve sine særlige rettigheter på området arbeidsrett, trygderett og sosialrett i den grad dette er tillatt i henhold til unionsretten eller medlemsstatenes nasjonale rett, eller en tariffavtale i henhold til medlemsstatenes nasjonale rett som gir nødvendige garantier for den registrertes grunnleggende rettigheter og interesser. (…)».

5.4 Særlig om ileggelse av overtredelsesgebyr

Av personvernforordningen artikkel 58 nr. 2 bokstav i, jf. personopplysningsloven § 26 annet ledd, fremgår det at Datatilsynet kan ilegge offentlige myndigheter og organer overtredelsesgebyr etter reglene i personvernforordningen artikkel 83 ved brudd på bestemmelser i personvernregelverket.

I personvernforordningen artikkel 83 angis vilkårene for ileggelse av gebyr. Bestemmelsen inneholder blant annet en oversikt over hvilke momenter det skal tas hensyn til, både når det vurderes hvorvidt overtredelsesgebyr skal ilegges og i utmålingen av gebyrets størrelse. De relevante delene av artikkel 83 nr. 1 og nr. 2 gjengis under:

«1. Hver tilsynsmyndighet skal sikre at ilegging av overtredelsesgebyr i henhold til denne artikkel for overtredelser av denne forordning nevnt i nr. 4, 5 og 6 i hvert enkelt tilfelle er virkningsfull, står i et rimelig forhold til overtredelsen og virker avskrekkende.

2. (…) Når det treffes avgjørelse om hvorvidt det skal ilegges overtredelsesgebyr samt om overtredelsesgebyrets størrelse, skal det i hvert enkelt tilfelle tas behørig hensyn til følgende:
a) karakteren, alvorlighetsgraden og varigheten av overtredelsen, idet det tas hensyn til den berørte behandlingens art, omfang eller formål samt antall registrerte som er berørt, og omfanget av den skade de har lidd,
b) hvorvidt overtredelsen ble begått forsettlig eller uaktsomt,
c) eventuelle tiltak truffet av den behandlingsansvarlige eller databehandleren for å begrense skaden som de registrerte har lidd,
d) den behandlingsansvarliges eller databehandlerens grad av ansvar, idet det tas hensyn til de tekniske og organisatoriske tiltak de har gjennomført i henhold til artikkel 25 og 32, (…)
f) graden av samarbeid med tilsynsmyndigheten for å bøte på overtredelsen og redusere de mulige negative virkningene av den,
g) kategoriene av personopplysninger som er berørt av overtredelsen,
h) på hvilken måte tilsynsmyndigheten fikk kjennskap til overtredelsen, særlig om og eventuelt i hvilken grad den behandlingsansvarlige eller databehandleren har underrettet om overtredelsen, (…)
k) enhver annen skjerpende eller formildende faktor ved saken, f.eks. økonomiske fordeler som er oppnådd, eller tap som er unngått, direkte eller indirekte, som følge av overtredelsen».

Artikkel 83 angir også rammene for overtredelsesgebyrets størrelse. Vi viser i denne forbindelse til artikkel 83 nr. 4 og 5. De relevante delene av bestemmelsene lyder:

> «4. Ved overtredelser av følgende bestemmelser skal det i samsvar med nr. 2 ilegges overtredelsesgebyr på opptil 10 000 000 euro (…):
> a) den behandlingsansvarliges og databehandlerens forpliktelser i henhold til artikkel 8, 11, 25-39 samt 42 og 43 (…).
>
> 5. Ved overtredelser av følgende bestemmelser skal det i samsvar med nr. 2 ilegges overtredelsesgebyr på opptil 20 000 000 euro (…):
> a) de grunnleggende prinsippene for behandling, herunder vilkår for samtykke, i henhold til artikkel 5, 6, 7 og 9».

6. Datatilsynets vurdering

I det følgende vil vi først vurdere SPKs rettslige grunnlag for å behandle overskuddsinformasjon innhentet fra Skatteetaten til etterkontroll av uførepensjon. Vi vil deretter vurdere om SPK har overholdt prinsippene for behandling av personopplysninger.

6.1 Rettslig grunnlag for behandlingen

SPK har vist til at etteroppgjør for uførepensjon er en lovpålagt oppgave. Et aktuelt rettslig grunnlag etter personvernregelverket kunne dermed være å oppfylle en rettslig forpliktelse etter nasjonal rett, jf. personvernforordningen artikkel 6 nr. 1 bokstav c. Man kan også anse etteroppgjøret som en utøvelse av offentlig myndighet etter nasjonal rett, jf. artikkel 6 nr. 1 bokstav e. Begge bestemmelsene stiller krav om at behandlingen skal være *nødvendig*.

Når det gjelder behandlingen opplysninger om uførepensjon fra andre enn SPK selv og folketrygden, måtte behandlingen også være tillatt etter personvernforordningen artikkel 9 nr. 2. Opplysninger om at en person mottar uførepensjon, er i seg selv en helseopplysning, ettersom innvilgelse av uførepensjon i seg selv forutsetter nedsatt arbeidsevne på grunn av sykdom/helseproblemer. Vi nøyer oss med å vise til at den aktuelle bestemmelsen i artikkel 9 nr. 2 bokstav b (oppfylle forpliktelser innen området trygderett) også krever at behandlingen er nødvendig.

SPK har opplyst at overføringen av opplysninger har skjedd i medhold av skatteforvaltningsloven § 3-6 annet ledd, som angir at Skatteetaten kan utlevere opplysninger om «pensjonsgivende inntekt» til SPK uten hinder av taushetsplikt.

SPK har angitt at de har hatt hjemmel i skatteforvaltningsloven § 3-6 annet ledd til å innhente et bredt spekter av inntektsopplysninger. SPK har likevel selv meldt fra om og erkjent at unødvendige inntektsopplysninger ble innhentet fra Skatteetaten i det predefinerte datasettet fra Skatteetaten.

Etter Uførereformen i 2015, var det uklart hvilke inntektsopplysninger som var nødvendige for etteroppgjør, og forståelsen endret seg også over tid. Datatilsynet vil likevel peke på at SPK må bære ansvaret for å klargjøre innen rimelig tid hvilke opplysninger de hadde behov for i dette arbeidet, slik at kun nødvendige opplysninger ble innhentet fra Skatteetaten.

Vi legger til grunn at SPK mellom oktober 2016 og oktober 2019 innhentet overskuddsinformasjon ved fire anledninger. I oktober 2019 ble den unødvendige informasjonen innhentet, men slettet umiddelbart.

Datatilsynet har kommet til at SPK har brutt kravet til nødvendighet etter personvernforordningen artikkel 6 nr. 1, jf. artikkel 9 nr. 2, i forbindelse med innhenting av inntektsopplysninger fra Skatteetaten til bruk i etteroppgjør for uførepensjon.

6.2 Prinsippene for behandling av personopplysninger

6.2.1 Prinsippet om dataminimering

Prinsippet om dataminimering fremgår av personvernforordningen artikkel 5 nr. 1 bokstav c. Det fremgår at behandling av personopplysninger skal avgrenses til de opplysningene som er nødvendig for formålet.

I forbindelse med innhentingen av inntektsopplysninger har SPK innhentet overskuddsinformasjon som ikke var nødvendig for etteroppgjøret for uførepensjon. Ettersom en teknisk løsning for innhenting av kun nødvendige opplysninger senere har kommet på plass, legger vi til grunn at det har vært praktisk mulig kun å hente inn opplysninger som SPK har behov for.

Dette utgjør et brudd på prinsippet om dataminimering, jf. artikkel 5 nr. 1 bokstav c.

6.2.2 Prinsippet om lagringsbegrensning

Etter artikkel 5 nr. 1 bokstav e skal ikke personopplysninger lagres lengre enn det som er nødvendig for formålet.

Et skadebegrensende tiltak ved innhenting av overskuddsinformasjon, kan være gode rutiner for å vurdere hvilke opplysninger som er nødvendige og slette unødvendig informasjon. SPK har frem til oktober 2019 ikke hatt rutiner for sletting av unødvendige inntektsopplysninger som ble innhentet fra Skatteetaten.

Dette utgjør et brudd på prinsippet om lagringsbegrensning, jf. artikkel 5 nr. 1 bokstav e.

6.2.3 Prinsippet om konfidensialitet

Prinsippet om konfidensialitet fremgår av personvernforordningen artikkel 5 nr. 1 bokstav f og innebærer blant annet at kun de som har tjenstlig behov skal ha tilgang til personopplysninger.

SPK har redegjort for at man etter Uførereformen i 2015 har måttet gjennomgå inntektsopplysningene for å vurdere hvilke opplysninger som er nødvendige for etteroppgjør. Kun ansatte som arbeider med uførepensjon har hatt tilgang til overskuddsinformasjonen som er innhentet fra Skatteetaten.

Datatilsynet har etter en helhetsvurdering kommet til at SPK ikke har brutt prinsippet om konfidensialitet, jf. artikkel 5 nr. 1 bokstav f.

6.3 Vurdering av om overtredelsesgebyr skal ilegges

Datatilsynet har kommet til at SPK har brutt personvernforordningen artikkel 5 nr. 1 bokstav c og e samt nødvendighetskravet i artikkel 6 nr. 1, jf. artikkel 9 nr. 2. Det foreligger dermed et lovbrudd som kan gi grunnlag for ileggelse av overtredelsesgebyr.

Lovbruddet har for en stor del skjedd før personopplysningsloven (2018) og personvernforordningen trådte i kraft. Datatilsynet kunne også tidligere ilegge overtredelsesgebyr, jf. personopplysningsloven (2000) § 46, men beløpet var da begrenset til inntil 10 ganger folketrygdens grunnbeløp (p.t. ca. 1 010 000 NOK).

Vi viser imidlertid til drøftelsen under punkt 3.1 og legger til grunn at gebyret skal utmåles etter nytt regelverk. I utgangspunktet er det dermed grunnlag for å ilegge SPK et overtredelsesgebyr på inntil 20 000 000 euro (p.t. ca. 213 000 000 NOK), jf. personvernforordningen artikkel 83 nr. 5. Vi vil likevel se hen til at tre av de fire tilfellene av innhenting av overskuddsinformasjon har skjedd i perioden da tidligere personvernregelverk gjaldt.

Under gjennomgår vi de momentene som vi anser relevante for vurderingen av om overtredelsesgebyr skal ilegges.

a) karakteren, alvorlighetsgraden og varigheten av overtredelsen, idet det tas hensyn til den berørte behandlingens art, omfang eller formål samt antall registrerte som er berørt, og omfanget av den skade de har lidd

Vi har kommet til at SPK har brutt grunnkravene til behandling av personopplysninger – det vil si de grunnleggende prinsippene i personvernforordningen artikkel 5 nr. 1 og kravet til nødvendighet i artikkel 6 nr. 1, jf. artikkel 9 nr. 2. Dette er alvorlig.

Innhentingen av overskuddsinformasjon har pågått i nærmere tre år, fra oktober 2016 til oktober 2019.

Ca. 44 000 personer er berørt. Selv om dette er en forholdsmessig lav andel av SPKs medlemmer, er det likevel et høyt antall personer.

b) hvorvidt overtredelsen ble begått forsettlig eller uaktsomt

SPK ble først klar over avviket i februar 2019. SPK har redegjort for hvorfor det i etterkant tok tid å vurdere konkret hvilke opplysninger som ikke var nødvendige for etteroppgjør, slik at verken sperring eller sletting kunne gjennomføres umiddelbart.

Etter en helhetsvurdering vurderer Datatilsynet at SPK, representert ved administrerende direktør, har vært uaktsom i forbindelse med lovbruddet.

c) eventuelle tiltak truffet av den behandlingsansvarlige eller databehandleren for å begrense skaden som de registrerte har lidd

SPK iverksatte flere tiltak etter at avviket ble oppdaget; tilgangen til opplysningene ble sperret i september 2019, og en løsning for sletting var på plass i oktober samme måned.

Enkelte tiltak har det tatt lenger tid å gjennomføre, herunder en løsning for å filtrere opplysningene som innhentes.

Etter vårt syn har SPK totalt sett gjort et godt arbeid med å iverksette relevante tiltak og vist at de tar situasjonen alvorlig.

d) den behandlingsansvarliges eller databehandlerens grad av ansvar, idet det tas hensyn til de tekniske og organisatoriske tiltak de har gjennomført i henhold til artikkel 25 og 32
SPK har innhentet et predefinert datasett fra Skatteetaten, uten at det ble gjort en gjennomgang av innholdet for å vurdere nødvendigheten av de ulike opplysningene.

SPK har heller ikke hatt rutine for å slette overskuddsinformasjon.

Når det gjelder tilgangsstyring, har kun ansatte med tjenstlig tilgang til uførepensjon kunnet se de overskytende inntektsopplysningene, selv om det har vist seg at heller ikke disse personene skulle hatt tilgang til opplysningene.

g) kategoriene av personopplysninger som er berørt av overtredelsen,
Opplysningene som er innhentet ulovlig er dels særlige kategorier personopplysninger, ettersom de omfatter opplysninger om uførepensjon fra andre enn SPK og folketrygden. Dette gjør lovbruddet mer alvorlig, ettersom særlige kategorier av personopplysninger har et særskilt vern etter personvernforordningen artikkel 9.

For øvrig er det tale om svært detaljerte inntektsopplysninger som de fleste vil oppfatte som private.

h) på hvilken måte tilsynsmyndigheten fikk kjennskap til overtredelsen, særlig om og eventuelt i hvilken grad den behandlingsansvarlige eller databehandleren har underrettet om overtredelsen
SPK varslet selv Datatilsynet om overtredelsen og har ellers bidratt til sakens opplysning.

Det tok riktignok lang tid før avviket ble meldt, ettersom avviket ble oppdaget i februar 2019, men først ble meldt i september samme år. SPK har riktignok forklart seg om årsakene til forsinkelsen, med det er likevel klart i strid med 72-timersfristen som fremgår av personvernforordningen artikkel 33.

k) enhver annen skjerpende eller formildende faktor ved saken, f.eks. økonomiske fordeler som er oppnådd, eller tap som er unngått, direkte eller indirekte, som følge av overtredelsen
Vi har merket oss at tre av fire innhentinger av overskuddsinformasjon ble foretatt før ny personopplysningslov trådte i kraft i juli 2018.

Datatilsynet har til sammen brukt ca. 1 ½ år på å behandle saken. Dette vil også få noe betydning for saken, jf. Personvernnemndas avgjørelser PVN-2021-09 og PVN-2021-03.

Samlet vurdering
Saken gjelder innhenting av unødvendige inntektsopplysninger, herunder særlige kategorier av personopplysninger, og SPK har brutt flere grunnleggende prinsipper for behandling av personopplysninger. Dette er så alvorlig at Datatilsynet har kommet til at SPK skal ilegges et overtredelsesgebyr.

6.4 Utmåling av gebyret
I vurderingen av gebyrets størrelse, har vi vektlagt at SPK har brutt grunnleggende og prinsipielle bestemmelser i personvernforordningen. SPK har samlet inn inngripende inntektsopplysninger uten at disse var nødvendige for formålet. Videre er særlige kategorier av personopplysninger berørt, ettersom opplysningene gjelder uførepensjon.

Formålet med innsamlingen var etteroppgjør for uførepensjon, noe som kan medføre økonomiske konsekvenser (tilbakebetalingskrav) for de berørte personene. Saken omfatter totalt ca. 44 000 personer, det vil si et betydelig antall uførepensjonister.

Det er også pekt på at innbyggerne generelt har en bred opplysningsplikt til skattemyndighetene. Ulovlig bruk av innsamlede opplysninger kan være skadelig for tilliten til det offentlige.

Avviket vedvarte også i over tre år før det ble oppdaget. SPK har i denne perioden ikke gjort tilstrekkelig for å klarlegge hvilke inntektsopplysninger de har hatt behov for til formålet etteroppgjør uførepensjon.

På den annen side har vi sett hen til at SPK iverksatte relevante tiltak etter at avviket ble oppdaget, og SPK har vist at de tar saken alvorlig.

Vi har også sett hen til at SPK selv meldte avviket til Datatilsynet, om enn mye senere enn regelverket tilsier.

Videre har vi vektlagt at lovbruddet dels har funnet sted før personopplysningsloven (2018) og personvernforordningen trådte i kraft. Etter tidligere gjeldende personopplysningslov (2000) var gebyret avgrenset til maksimalt ca. 1 010 000 NOK.

Datatilsynets saksbehandlingstid på ca. 1 ½ år vil også få noe betydning for gebyrets størrelse, jf. PVN-2021-09 og PVN-2021-03.

Datatilsynet har kommet til at overtredelsesgebyret skal settes til 1 000 000 NOK i denne saken.

Beløpet er nedjustert noe fra det varslede gebyret på 1 500 000 NOK ut fra vår vekting av momentene som fremgår over.

7. Klagerett
Dette vedtaket kan påklages innen tre uker etter at dere har mottatt dette brevet, jf. forvaltningsloven §§ 28 og 29. En eventuell klage sendes til Datatilsynet. Dersom vi ikke tar

klagen til følge, vil saken bli sendt til Personvernnemnda for klagebehandling, jf. personopplysningsloven § 22.

Ved eventuelle spørsmål kan dere ta kontakt med direktør Bjørn Erik Thon eller saksbehandler Susanne Lie (e-post: suli@datatilsynet.no).

Med vennlig hilsen

Bjørn Erik Thon
direktør

Susanne Lie
juridisk seniorrådgiver

Dokumentet er elektronisk godkjent og har derfor ingen håndskrevne signaturer

Kopi til: STATENS PENSJONSKASSE FORVALTNINGSBEDRIFT, Gry-Helen Henriksen
SKATTEETATEN