POLICY FOR BEHANDLING AV PERSONOPPLYSNINGER

Fearnleys Pensjonskasse

Pensjonskassen er behandlingsansvarlig for de personopplysninger behandles om pensjonskassens medlemmer i forbindelse med forvaltning av deres pensjonsrettigheter. Pensjonskassen har definert følgende retningslinjer for behandling av personopplysninger

Innhold

1. Definisjoner

Med ***leverandør*** menes her foretak som leverer tjenester gjennom eventuell utkontraktert funksjon til pensjonskassen som behandlingsansvarlig. Leverandøren vil som regel være hovedleverandør av tjenesten til pensjonskassen, men vil også kunne benytte seg av eventuelle underleverandører i forbindelse med tjenesteleveransen. Der personopplysninger som pensjonskassen er behandlingsansvarlig for behandles av en underleverandør vil sistnevnte bli en underdatabehandler til leveredøren som databehandler.

Med ***personopplysninger***[1] menes her enhver opplysning om en identifisert eller identifiserbar fysisk person («***den registrerte***[2]»), 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 online-identifikator eller ett eller flere elementer som er spesifikke for nevnte fysiske persons fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sosiale identitet. Det enkelte medlemmet i pensjonskassen er eksempel på den «registrerte», det samme er pensjonskassens ansatte.

Med ***særlige kategorier personopplysninger***[3] ***(sensitive)*** menes her personopplysninger om

- rasemessig eller etnisk opprinnelse, politisk oppfatning, religion, overbevisning eller fagforeningsmedlemskap,
- behandling av genetiske opplysninger og biometriske opplysninger med det formål å entydig identifisere en fysisk person,
- helseopplysninger eller opplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering.

Med ***behandling av personopplysninger***[4] menes her enhver operasjon eller rekke av operasjoner som gjøres med personopplysninger, enten automatisert eller ikke, f.eks. innsamling, registrering, organisering, strukturering, lagring, tilpasning eller endring, gjenfinning, konsultering, bruk, utlevering ved overføring, spredning eller alle andre former for tilgjengeliggjøring, sammenstilling eller samkjøring, begrensning, sletting eller tilintetgjøring.

Med ***behandlingsansvarlig***[5] menes her en fysisk eller juridisk person, en offentlig myndighet, en institusjon eller ethvert annet organ som alene eller sammen med andre bestemmer formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes. I denne instruksen vil den enkelte pensjonskasse være behandlingsansvarlig.

Med ***databehandler***[6] menes her en fysisk eller juridisk person, offentlig myndighet, institusjon eller ethvert annet organ som behandler personopplysninger på vegne av den behandlingsansvarlige. I denne instruksen vil leverandør være databehandler. Der databehandleren benytter seg av en underdatabehandler som underleverandør skal sistnevnte pålegges de samme pliktene til vern av personopplysninger som er fastsatt i databehandleravtalen med pensjonskassen. Databehandleren har det fulle ansvar for at underdatabehandleren oppfyller sine forpliktelser overfor pensjonskassen som behandlingsansvarlig.

Med ***brudd på personopplysningssikkerheten***[7] menes her et brudd på sikkerheten som fører til utilsiktet eller ulovlig tilintetgjøring, tap, endring, ulovlig spredning av eller tilgang til personopplysninger som er overført, lagret eller på annen måte behandlet.

---

[1] Se GDPR art 4 nr 1
[2] Se GDPR art 4 nr 1
[3] Se GDPR art 9 nr 1 og 10
[4] Se GDPR art 2 nr 4
[5] Se GDPR art 4 nr 7, 24 og 26
[6] GDPR art 4 nr 8, 27 og 28
[7] GDPR art 4 nr 12

2. Pensjonskassens lovlige behandling av personopplysninger[8]

Pensjonskassen kan behandle personopplysninger så lenge det er lovlig grunnlag for behandlingen. Personopplysninger skal som prinsipp[9]:

- behandles på en lovlig, rettferdig og gjennomsiktig måte
- samles inn for spesifikke, uttrykkelig angitte og berettigede formål og ikke viderebehandles på en måte som er uforenlig med disse formålene
- være adekvate, relevante og begrenset til det som er nødvendig for formålene de behandles for
- være korrekte og om nødvendig oppdaterte
- ikke lagres lenger enn det som er nødvendig for formålene som personopplysningene behandles for
- behandles på en måte som sikrer tilstrekkelig sikkerhet for personopplysninger ved bruk av egnede tekniske eller organisatoriske tiltak.

Pensjonskassens behandling av alle typer personopplysninger er beskrevet i behandlingsprotokollen vedlagt under i pkt 13. Lovlig grunnlag for pensjonskassens behandling etter GDPR art 6 er:

- Samtykke fra den registrerte
- Nødvendig for å oppfylle avtale som den registrerte er part i eller gjennomføre tiltak på den registrertes anmodning før avtaleinngåelse
- Oppfylle rettslig forpliktelse som påhviler den behandlingsansvarlige
- Verne den registrertes eller annen persons vitale interesser
- Utføre en oppgave i allmennhetens interesse eller utøve offentlig myndighet
- Formål knyttet til berettiget interesse dersom registrertes interesse eller grunnleggende rettigheter går foran/krever vern (interesseavveining)

Ved behandling av særlige kategorier av personopplysninger som helseopplysninger eller opplysninger om et medlems fagforeningsmedlemskap etter GDPR art 9, skal behandlingen være i tråd med denne instruksen, gjeldende personvernregelverk og beskrevet i behandlingsprotokollen.

3. Oppstart og opphør av behandling av personopplysninger

Pensjonskassen har som policy å utsette drift av pensjonskassen til ekstern part. Før oppstart av behandling av personopplysninger utført av den eksterne part som databehandler skal det inngås databehandleravtale i henhold til GDPR art 28 og denne instruksen. Pensjonskassen har satt ut behandlingen av personopplysninger til en databehandler, men vil kunne få spørsmål fra databehandleren om enkeltsaker. I de fleste tilfellene vil personopplysningene som mottas i saken være anonymiserte, men personopplysninger kan i enkelte sjeldne tilfeller bli kommunisert mellom daglig leder og databehandler eller daglig leder og styret i Pensjonskassen. All behandlingsaktivitet skal være beskrevet i pensjonskassens behandlingsprotokoll etter GDPR art 30 før oppstart. I protokollen vil det også være beskrevet når pensjonskassens behandling av personopplysninger opphører.

4. Personopplysningers riktighet[10]

Dersom det er behandlet personopplysninger som er uriktige, ufullstendige eller som det ikke er adgang til å behandle, skal den behandlingsansvarlige av eget tiltak eller på begjæring av den registrerte rette de mangelfulle opplysningene.

[8] GDPR art 6
[9] Se personvernprinsippene i GDPR art 5
[10] GDPR art 5

Retting av uriktige eller ufullstendige personopplysninger som kan ha betydning som dokumentasjon, skal skje ved at opplysningene tydelig markeres og suppleres med korrekte opplysninger.

Sletting bør suppleres med registrering av korrekte og fullstendige opplysninger. Dersom dette ikke er mulig, og dokumentet som inneholdt de slettede opplysningene av den grunn gir et åpenbart misvisende bilde, skal hele dokumentet slettes.

5. Den registrertes rettigheter

5.1 Informasjon til den registrerte uavhengig av henvendelse

Pensjonskassens hovedleverandør og databehandler sørger for å informere om behandlingen i tråd med GDPR art 14 gjennom en personvernerklæring.

5.2 Henvendelser fra den registrerte

Pensjonskassens hovedleverandør og databehandler skal ta imot henvendelser knyttet til utøvelse av den registrertes rettigheter, og har videre ansvar for å behandle den registrertes forespørsel i tråd med pensjonskassens instrukser, gjeldende personvernregelverk og den inngåtte databehandleravtale. I tilfeller hvor pensjonskassen selv mottar henvendelser fra registrerte, kan pensjonskassen ved behov videreformidle henvendelsene til databehandler, som i tilfelle skal behandle den registrertes forespørsel i tråd med pensjonskassens instrukser, gjeldende personvernregelverk og den inngåtte databehandleravtale.

5.3 Rettighetene

Databehandler sørger for at rettighetene til de registrerte blir ivaretatt ved eventuell henvendelse, som eksempelvis retten til:

- innsyn[11]
- retting[12]
- sletting[13]
- krav om begrensning av behandling[14]
- innsigelsesrett[15]
- den registrertes motsettelse av eventuelle automatiserte individuelle avgjørelser, herunder profilering[16]

6. Informasjonssikkerhet og ivaretakelse av sikkerheten for personopplysninger[17]

Pensjonskassen og leverandør skal gjennomføre egnede tekniske og organisatoriske tiltak for å sikre og påvise at behandlingen gjennomføres etter personvernforordningen, hensyntatt behandlingens:

- art
- omfang
- formål
- sammenhengen den utføres i

[11] GDPR art 12 og 15
[12] GDPR art 16
[13] GDPR art 17
[14] GDPR art 18
[15] GDPR art 21
[16] GDPR art 22
[17] GDPR art 25 og 32

Det skal sørges for vern av personopplysninger. Godkjente atferdsnormer og sertifiseringsmekanismer skal overholdes. Følgende sikkerhetstiltak er iverksatt:

- Utvekslingen av personopplysninger mellom databehandler og pensjonskassen skal gjøres med sikkerhetstiltak beskrevet i denne instruksen og gjeldende databehandleravtale.
- Pseudonymisering og kryptering av personopplysninger;
    - Utvekslingen av personopplysninger skal være kryptert og tilgang til personopplysningene skal sikres mot uautorisert innsyn. Dette kan gjøres ved bruk av AdminControl eller kryptert oversending av informasjon i e-post, eller annen risikovurdert metode.
- Fortrolighet, integritet, tilgjengelighet og robusthet i behandlingssystemene og – tjenestene
- Kapasitet til å gjenopprette tilgjengeligheten og tilgangen til personopplysninger i rett tid dersom det oppstår en fysisk eller teknisk hendelse
- Prosess for regelmessig testing, analysering og vurdering av hvor effektive behandlingens tekniske og organisatoriske sikkerhetstiltak er
- Dokumenter som utveksles ved bruk av e-post vil være krypterte. Passord vil bli utvekslet over en egen kanal, som sms, og skal ikke lagres sammen med dokumentet.
- Dersom en ukryptert versjon av dokumentet blir lagret, må dette gjøres på et sikkert sted, med tilgangskontroll, slik at uvedkommende ikke kan få tilgang til dokumentet.
- Dokumenter som utveksles gjennom AdminControl vil være beskyttet så lenge det oppbevares i AdminControl og korrekt tilgangskontroll til dokumentet er satt.
- Dersom en versjon av dokumentet blir hentet ut fra AdminControl, må dette lagres på et sikkert sted, med tilgangskontroll, slik at uvedkommende ikke kan få tilgang til dokumentet.

Ved vurderingen av egnet sikkerhetsnivå skal det tas særlig hensyn til risiko forbundet med behandlingen, særlig som følge av utilsiktet eller ulovlig tilintetgjøring, tap, endring eller ikke-autorisert utlevering av eller tilgang til personopplysninger som er overført, lagret eller på annen måte behandlet.

Risikovurdering for behandlingen skal gjennomføres årlig eller ved endringer av betydning for personvernet. Dokumentet for behandlingsprotokoll skal benyttes og risikovurdering for de forskjellige behandlingsaktiviteter skal legges inn her. Risikovurdering skal ta hensyn til den tekniske utviklingen, gjennomføringskostnadene og behandlingens art, omfang, formål og sammenhengen den utføres i, samt risikoene av varierende sannsynlighets- og alvorlighetsgrad for fysiske personers rettigheter og friheter.

6.1 Sikkerhetstiltak ved styrets behandling av personopplysninger[18]

Styremedlemmer i pensjonskassen vil kunne motta personopplysninger om pensjonskassens medlemmer fra leverandør i forbindelse med styrebehandling av en sak. Et eksempel på en situasjon der styret behandler personopplysninger er dersom en tvistesak tas inn for trygderetten. I et slikt tilfelle vil opplysninger i saken bli behandlet i styremøte.

Følgende tekniske og organisatoriske tiltak etter GDPR art 32 gjøres for å oppnå et tilfredsstillende sikkerhetsnivå ved behandlingen:

- Alle styrets medlemmer må være underlagt taushetserklæring
- Personopplysninger skal oppbevares et samlet sikkert sted og ikke spres til styrets medlemmer. AdminControl kan benyttes, eller annen portal som er risikovurdert.
- Personopplysninger må slettes når saken er avsluttet og formålet med behandlingen oppnådd
- Vanligvis vil behandling av personopplysninger om pensjonskassens medlemmer bli begrenset til lesetilgang i forkant og i styremøte.

[18] GDPR art 32

- Generelt skal det gjelde forbud mot at et styremedlem printer styredokumenter som inneholder personopplysninger om pensjonskassens medlemmer.
- Generelt skal det gjelde forbud mot at et styremedlem lagrer styredokumenter som inneholder personopplysninger på sitt elektronisk utstyr, som PC, mobil, osv.
- Generelt skal det gjelde forbud mot at et styremedlem videresender styredokumenter som inneholder personopplysninger

7. Rutine for bruk av databehandlere[19]

Pensjonskassen skal bare bruke databehandlere som gir tilstrekkelige garantier for at de vil gjennomføre egnede tekniske og organisatoriske tiltak som sikrer at behandlingen oppfyller kravene i personvernforordning og vern av den registrertes rettigheter.

Pensjonskassen skal gjennomføre en vurdering av databehandler basert på de revisjonsrapporter som mottas av databehandler.

Pensjonskassen har rett til å gjennomføre en selvstendig revisjon av databehandler. Det må vurderes om dette er nødvendig for å oppnå en tilstrekkelig garanti. Denne rutinen beskriver hvilke krav som stilles til innhold til databehandleravtale, blant annet krav og plikter til en databehandler som behandler data på vegne av Pensjonskassen. Følgende punkter skal vurderes før inngåelse av databehandleravtale:

1) Fastslå om databehandleravtale er nødvendig
2) Fastslå at databehandler har nødvendig kompetanse

Databehandleravtalen som etableres, eller tilsvarende innhold i en leverandør- eller tjenesteavtale må som minimum inneholde følgende etter GDPR art 28:

- hensikten med behandlingen
- varigheten av behandlingen
- behandlingens formål og art
- typen personopplysninger og kategorier av registrerte som skal behandles
- den behandlingsansvarliges rettigheter og plikter

I tillegg skal det pålegges spesifikke plikter for databehandleren, som at databehandleren skal:

- kun behandle personopplysningene på instruks fra den behandlingsansvarlige (som kan dokumenteres i ettertid)
- ikke overføre personopplysninger til land utenfor EU/EØS (tredjeland) uten etter instruksjon fra den behandlingsansvarlige
- sikre at personer som er autorisert til å behandle personopplysningene har forpliktet seg til å behandle opplysningene fortrolig eller er underlagt en egnet lovfestet taushetsplikt
- treffe alle tiltak som er nødvendig for sikkerhet ved behandlingen, og gjennomføring av tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som hensyntar relevant risiko ved behandlingen etter artikkel 32 i GDPR
- kun engasjere en annen databehandler ("underdatabehandler") dersom det på forhånd er innhentet særlig eller generell skriftlig tillatelse til dette fra den behandlingsansvarlige.
    - Er det gitt en generell tillatelse, skal databehandleren underrette den behandlingsansvarlige om eventuelle planer om å benytte andre databehandlere eller skifte ut databehandlere, og dermed gi den behandlingsansvarlige muligheten til å motsette seg slike endringer.
    - Engasjeres det underdatabehandler, skal denne pålegges de samme forpliktelsene til vern av personopplysninger som er fastsatt i databehandleravtalen.

[19] GDPR art 28

    - Databehandler har fullt ansvar overfor den behandlingsansvarlige for at underdatabehandlere oppfyller sine forpliktelser
- etterkomme pålegg fra den behandlingsansvarlige om å slette eller tilbakelevere alle personopplysninger (inkludert kopier) etter at tjenestene knyttet til behandlingen er avsluttet, med mindre det foreligger lovkrav til at opplysningene fortsatt skal lagres
- gjøre tilgjengelig all informasjon som er nødvendig for å påvise at forpliktelsene ovenfor er oppfylt for den behandlingsansvarlige, samt muliggjøre og bidra til revisjoner og inspeksjoner som gjennomføres av den behandlingsansvarlige eller annen på dennes vegne
- omgående underrette den behandlingsansvarlige dersom en instruks fra den behandlingsansvarlige er i strid med GDPR eller andre bestemmelser om vern av personopplysninger, som personopplysningsloven

Databehandleren skal bistå den behandlingsansvarlige med oppfyllelse av plikter, som skal reguleres i databehandleravtalen. Dette omfatter å bistå den behandlingsansvarlige med å:

- oppfylle pliktene til å svare på anmodninger som de registrerte inngir med henblikk på å utøve sine rettigheter fastsatt i kapittel III i GDPR hensyntatt behandlingens art og i den grad det er mulig ved hjelp av egnede tekniske og organisatoriske tiltak
- sikre overholdelse av forpliktelser etter artikkel 32–36, som er krav til sikkerhet ved behandlingen, melding til tilsynsmyndigheten (Datatilsynet) og eventuelt de registrerte om brudd på personopplysningssikkerheten, vurdering av personvernkonsekvenser (såkalte DPIAs) og ved forhåndsdrøftinger med Datatilsynet før behandling med høy risiko

8. Retting, endring og sletting av personopplysninger[20]

Den registrerte skal ha rett til å få uriktige personopplysninger om seg selv rettet av den behandlingsansvarlige uten ugrunnet opphold. Når formålet med behandlingen av personopplysningene er oppnådd, skal dokumenter slettes[21]. Rutiner for sletting under de forskjellige behandlingsaktivitetene er beskrevet nærmere i behandlingsprotokollen. Kryptert vedlegg i e-post er personopplysninger selv om det er kryptert, og må også slettes.

Personopplysninger skal slettes uten ugrunnet opphold dersom:

- opplysningene ikke er nødvendige for formålet de ble samlet inn for
- samtykke for behandling er trukket tilbake, og det er ikke annet rettslig grunnlag for behandling
- innsigelse mot behandlingen fra den registrerte
- personopplysninger er blitt behandlet ulovlig
- sletting må skje for å oppfylle rettslig forpliktelse

Unntak fra sletteplikten gjelder når opplysningene er nødvendige for å fastsette, gjøre gjeldende eller forsvare rettskrav eller en oppfylle en rettslig forpliktelse.

9. Brudd på personopplysningssikkerheten

Daglig leder alene eller sammen med styret skal sørge for at et brudd på personopplysningssikkerheten blir håndtert i samsvar med kravene i GDPR. Prosessen er beskrevet i dette kapittelet, i leverandørens egen interne instruks for avvikshåndtering ved brudd på personopplysningssikkerheten. Hvis et styremedlem forårsaker et brudd på personopplysningssikkerheten eller får kjennskap til et brudd på personopplysningssikkerheten

[20] GDPR art 16 og 17
[21] Se GDPR art 17

forårsaket av noen andre, skal vedkommende styremedlem umiddelbart melde om bruddet til daglig leder i Pensjonskassen.

Nedenfor følger noen eksempler på hvilke uønskede hendelser som kan oppstå og som vil automatisk medføre brudd på personopplysningssikkerheten:

- utilsiktet eller ulovlig tilintetgjøring av personopplysninger,
- utilsiktet eller ulovlig tap av personopplysninger,
- utilsiktet eller ulovlig endring av personopplysninger,
- ikke-autorisert eller ulovlig spredning/utlevering av eller tilgang til personopplysninger

9.1 Varslingsplikt for Pensjonskassen (den behandlingsansvarlige)

Varslingsplikten fremgår av GDPR art 33. Ved brudd på personopplysningssikkerheten skal Pensjonskassen ved daglig leder uten ugrunnet opphold og når det er mulig, senest 72 timer etter å ha fått kjennskap til det, varsle bruddet til Datatilsynet, med mindre det er lite trolig at bruddet vil medføre en risiko for fysiske personers rettigheter og friheter. Dersom bruddet ikke meldes til Datatilsynet innen 72 timer, skal årsakene til forsinkelsen oppgis.

9.2 Varslingsplikt for leverandør (databehandler)

Etter å ha fått kjennskap til et brudd på personopplysningssikkerheten skal leverandør uten ugrunnet opphold underrette Pensjonskassen ved daglig leder.

9.3 Melding til Datatilsynet[22]

Meldingen til Datatilsynet skal minst:

a) beskrive arten av bruddet på personopplysningssikkerheten, herunder, når det er mulig, kategoriene av og omtrentlig antall registrerte som er berørt, og kategoriene av og omtrentlig antall personopplysningsposter som er berørt,
b) inneholde navnet på og kontaktopplysningene til personvernrådgiveren (personvernombud) eller et annet kontaktpunkt der mer informasjon kan innhentes,
c) beskrive de sannsynlige konsekvensene av bruddet på personopplysningssikkerheten,
d) beskrive de tiltak som Pensjonskassen (den behandlingsansvarlige) har truffet eller foreslår å treffe for å håndtere bruddet på personopplysningssikkerheten, herunder, dersom det er relevant, tiltak for å redusere eventuelle skadevirkninger som følge av bruddet.

Dersom og i den grad det ikke er mulig å gi all informasjon samtidig, kan den gis trinnvis uten ytterligere ugrunnet opphold. Pensjonskassen (den behandlingsansvarlige) skal dokumentere ethvert brudd på personopplysningssikkerheten, herunder de faktiske forhold rundt nevnte brudd, virkningene av det og hvilke tiltak som er truffet for å utbedre det. Rutine for informasjon til den registrerte

9.4 Underretning av den registrerte

Dersom det er sannsynlig at bruddet på personopplysningssikkerheten vil medføre en høy risiko for fysiske personers rettigheter og friheter, skal Pensjonskassen (den behandlingsansvarlige) uten ugrunnet opphold underrette den registrerte om bruddet.

Underretningen til den registrerte skal inneholde en klar og tydelig beskrivelse av arten av bruddet på personopplysningssikkerheten.

Underretningen skal minst:

a) inneholde navnet på og kontaktopplysningene til personvernrådgiveren (personvernombud) eller et annet kontaktpunkt der mer informasjon kan innhentes,
b) beskrive de sannsynlige konsekvensene av bruddet på personopplysningssikkerheten,

[22] Se GDPR art 33 nr 3

c) beskrive de tiltak Pensjonskassen (den behandlingsansvarlige) har truffet eller foreslår å treffe for å håndtere bruddet på personopplysningssikkerheten, herunder, dersom det er relevant, tiltak for å redusere eventuelle skadevirkninger som følge av bruddet.

9.5 Tilfeller hvor underretning av den registrerte ikke er påkrevd

Underretningen til den registrerte er ikke påkrevd dersom noen av følgende vilkår er oppfylt:

a) Pensjonskassen (den behandlingsansvarlige) har gjennomført egnede tekniske og organisatoriske sikkerhetstiltak, og disse tiltakene er blitt anvendt på personopplysningene som er berørt av bruddet på personopplysningssikkerheten, særlig tiltak som gjør personopplysningene uleselige for enhver person som ikke har autorisert tilgang til dem, f.eks. kryptering,
b) Pensjonskassen (den behandlingsansvarlige) har truffet etterfølgende tiltak som sikrer at det er lite trolig at den høye risikoen for de registrertes rettigheter og friheter vil oppstå,
c) det vil innebære en uforholdsmessig stor innsats. Dersom dette er tilfellet, skal allmennheten isteden underrettes, eller det skal treffes et lignende tiltak som sikrer at de registrerte underrettes på en like effektiv måte.

10. Overføring av personopplysninger

Overføring av personopplysninger må gjennomføres med tilfredsstillende sikkerhet. Personopplysninger som overføres ved bruk av usikre kanaler skal beskyttes mot innsyn på en tilfredsstillende måte.

Det må tas hensyn til risikobildet om sikkerheten til valgte metoder er tilfredsstillende, herunder hvorvidt:

- Krypteringsalgoritmer tilfredsstiller dagens standard, «state of the art»
- Autentiseringsmetoden er god nok
- Eventuell utveksling av krypteringsnøkkel over en annen kanal er sikker nok
- Oppbevaringen av krypterte eller dekrypterte personopplysninger er god nok
- Muligheten for sletting av dokumenter med personopplysninger kan gjennomføres på en enkel og sikker måte

10.1 Overføring til land utenfor EU/EØS

Leverandør som databehandler for pensjonskassen som behandling ansvarlig skal ikke overføre personopplysninger til land utenfor EU/EØS (tredjeland) uten etter instruksjon fra den behandlingsansvarlige.

11. Dataportabilitet

Dataportabilitet innebærer å gi den registrerte kontroll over egne opplysninger og rett til å ta med seg sine personopplysninger fra en virksomhet til en annen. Rettigheten gjelder kun egne opplysninger som den registrerte selv har gitt til pensjonskassen. Personopplysninger samlet fra andre kilder er ikke omfattet av denne retten. Informasjon eller analyse den behandlingsansvarlige har generert på bakgrunn av opplysningene må ikke utleveres.

Utøvelsen av retten til dataportabilitet må heller ikke krenke andre individers rettigheter eller friheter. Eksempelvis i de tilfeller den registrertes opplysninger er lagret sammen med andre personers opplysninger, må disse skilles ut før utlevering.

Krav på dataportabilitet er betinget av følgende vilkår:

- Behandlingen av personopplysninger skjer på bakgrunn av et samtykke eller en kontrakt. Rettigheten gjelder altså ikke for behandlinger som foretas med andre rettslige grunnlag.

- Behandlingen av personopplysninger skjer elektronisk. Rettigheten gjelder altså ikke personopplysninger som kun finnes på papir.

Personopplysninger er nødvendige for å oppfylle vilkårene i avtalen med Pensjonskassen. Leverandør er databehandler for pensjonskassen. Dersom pensjonskassen velger en annen leverandør utleveres personopplysningene til mottagende leverandør gjennom avtalt format.

12. Utpeking av personvernombud[23]

Virksomheter må opprette personvernombud etter GDPR art 37 dersom:

1) behandlingen utføres av en offentlig virksomhet
2) hovedvirksomheten til virksomheten er en av disse:
    a. Regelmessig og systematisk monitorering av personer i stor skala
    b. Behandling av sensitive opplysninger i stor skala
    c. Behandling av opplysninger om straffbare forhold i stor skala

Pensjonskassen har vurdert om dennes virksomhet vil kunne omfattes av GDPR art 37, om kravet om opprettelse av personvernombud dersom det behandles sensitive personopplysninger i stor skala. Det er på det rene at virksomheten ikke omfattes av de øvrige ovennevnte punkter.

Pensjonskassen behandler enkelte sensitive opplysninger. Her vil helseopplysninger av typen uføregrad være mest relevant, og i noen tilfeller også helseopplysninger utover dette.

Om det behandles sensitive personopplysninger i stor skala er vurdert opp mot:

- Antall personer det behandles opplysninger om
- Mengden og omfanget av personopplysningene som blir behandlet
- Varigheten av behandlingen
- Det geografiske omfanget av behandlingen

Pensjonskassen behandler bare sensitive personopplysninger om sine ansatte. Det er svært få sensitive opplysninger som behandles. Behandlingen av de enkelte helseopplysningene vil være av kort varighet, mens behandlingen av uføregrad vil være av lang varighet. Det geografiske omfanget er svært begrenset.

Pensjonskassen vurderer det dithen at dette ikke kvalifiserer til å være behandling i stor skala.

Pensjonskassen har dermed konkludert med at virksomhetstypen ikke omfattes av art 37 i GDPR med den konsekvens at det ikke vil være påkrevet å utpeke personvernombud.

Pensjonskassens hovedleverandør og databehandler har opprettet et personvernombud. Dette vurderes som et positivt tiltak som vil sikre at rettigheter til Pensjonskassens medlemmer blir ivaretatt. Hvis Pensjonskassen i fremtiden skulle identifisere behov for et personvernombud, vil Pensjonskassen kunne avtale å benytte leverandørens personvernombud eller eventuelt en tilsvarende funksjon hos sitt sponsorforetak.

13. Vurdering av personvernkonsekvenser[24] (DPIA)

Personvernkonsekvensvurdering (DPIA) skal bare gjennomføres for behandlinger som er nye, eller dersom risikobildet vesentlig har endret seg etter ikrafttredelsen av GDPR. Vurdering av om det skal gjennomføres en DPIA vil være en løpende analyse (årlig eller ved endringer av betydning). Hvis det er behov for en ny DPIA-vurdering skal denne tas inn i behandlingsprotokolldokumentet.

[23] GDPR art 37
[24] GDPR art 35

Artikkel 29-gruppen har satt opp 9 punkter - vurderingskriteria - for behandlinger, der noen av punktene kan være aktuelle for enkelte behandlinger som utføres på Pensjonskassens kategorier av personopplysninger. De aktuelle punktene er drøftet og vurdert i det etterfølgende.

Punkt 4) Spesielle kategorier personopplysninger eller andre sensitive personopplysninger av høy personlig karakter.

Vurdering: Pensjonskassen behandler noen sensitive personopplysninger, som uføregrad, og av og til andre helseopplysninger, men behandlingen er svært begrenset og vurderes ikke å kunne medføre høy risiko for en persons rettigheter eller friheter.

Punkt 5) Databehandling i stort omfang.

Vurdering: Selv om Pensjonskassen kan bestå av mange medlemmer og vil utføre behandling over lang tid, vurderes behandling ikke til å kategoriseres som databehandling i stort omfang. Behandlingen har også svært begrenset geografisk tilstedeværelse.

Punkt 6) Kombinering eller sammenføring av datasett

Vurdering: Enkelte behandlinger vil medføre sammenslåing av datasett fra to ulike system, som beregningssystem og lønnssystem eller utbetalingssystem. Sammenslåingen er nødvendig for formålet med behandlingen og behandlingene har samme behandlingsansvarlige.

Vurdering: Ingen behandling som utføres på kategoriene av personopplysninger for Pensjonskassen medfører høy risiko for den registrerte i henhold til anbefalingene for vurdering utgitt av artikkel 29-gruppen. Det behandles enkelte sensitive opplysninger, men denne behandlingen alene medfører ikke krav om en personvernkonsekvensvurdering.

14. Behandlingsprotokoll[25]

Pensjonskassen skal til enhver tid ha en oppdatert behandlingsprotokoll etter GDPR art 30.

[25] GDPR art 30