Statusrapport personvernområdet i DFØ

Direktoratet for forvaltning og økonomistyring

Innholdsfortegnelse

1. Innledning

DFØ er statens fagorgan for økonomistyring, gode beslutningsgrunnlag for statlige tiltak, organisering og ledelse i staten, samt for anskaffelser i offentlig sektor og felles innkjøpsavtaler i staten. DFØ er også leverandør av fellestjenester innenfor lønn og regnskap. Vårt samfunnsoppdrag er å bidra til effektiv ressursbruk i staten, og til at staten når sine mål gjennom god styring, organisering, ledelse og gode beslutningsgrunnlag.

DFØ leverer lønns- og regnskapstjenester til rundt 90 prosent av statsforvaltningen, og har ansvaret for statsregnskapet og statens konsernkontoordning.

Gjennom sin virksomhet behandler DFØ personopplysninger i stor skala. Behandlingen omfatter opplysninger om DFØs egne ansatte, om personer tilknyttet DFØs leverandører og om personer som er tilknyttet de virksomhetene som benytter DFØs tjenester. I den forbindelse opptrer DFØ både i rollen som behandlingsansvarlig og som databehandler. Hovedmengden av personopplysninger behandles i kraft av DFØs rolle som leverandør av lønns- og regnskapstjenester, altså i rollen som databehandler.

Personopplysningsloven og personvernforordningen (personvernregelverket) stiller omfattende krav til virksomheters behandling av personopplysninger. Dette medfører omfattende plikter for DFØ både i rollen som behandlingsansvarlig og databehandler. Tilfredsstillende implementering og etterlevelse av personvernregelverket i praksis er sentrale elementer for å ivareta de registrertes personvern.

2. Bakgrunn og formål

Personvern har lenge vært et prioritert område i DFØ, både før og etter at GDPR trådte i kraft i 2018. I perioden 2017-2019 gjennomførte DFØ et GDPR-prosjekt med ekstern prosjektbistand, hvor hovedformålet var å klargjøre hvilke krav som stilles til DFØ etter personvernforordningen (GDPR), herunder å identifisere hvilke endringer og tiltak som måtte iverksettes for å sikre tilfredsstillende etterlevelse av regelverket. Prosjektet fokuserte særlig på kartlegging av hvilke personopplysninger DFØ behandler i rollen som behandlingsansvarlig og databehandler, inngåelse av databehandleravtaler med kunder og leverandører, samt utarbeidelse av operative rutiner.

For å sikre kontinuitet i arbeidet og ferdigstille etablering av internkontroll på personvernområdet, igangsatte DFØ våren 2020 et nytt GDPR-prosjekt. DFØ har engasjert ekstern, rådgivende bistand i dette personvernarbeidet. Prosjektet har arbeidet systematisk og

målrettet med etablering av helhetlig internkontroll for personvern. Dette for å sikre å sikre god oversikt, systematisk forbedring og etterlevelse av personvernregelverket over tid.

Formålet med denne rapporten er å gi DFØs kunder en statusrapport på arbeidet med personvern. DFØs etablerte internkontroll for etterlevelse av personvernregelverket danner utgangspunktet for gjennomgangen. Videre vil DFØs rolle som databehandler, og da spesielt ivaretakelsen av DFØs forpliktelser etter databehandleravtalen med våre kunder, omtales særskilt der hvor det er relevant.

Sentrale punkter ved vurdering av status er:

- Ajourført styrende dokumentasjon, se punkt 5.1.
- Organisering og roller på personvernområdet, se punkt 5.2.
- Protokoller over behandlingsaktiviteter, se punkt 5.3.
- Databehandleravtaler, se punkt 5.4.
- Oppfølging av underleverandører, se punkt 5.5.
- Bistand til behandlingsansvarlige, se punkt 5.6.
- Rutiner for sletting, se punkt 5.7.
- Rutine for rapportering og håndtering av avvik, se punkt 5.8.
- Egenkontroller og ledelsens gjennomgang, se punkt 5.9.

3. Krav til behandlingsansvarlig og databehandler

Behandlingsansvarlig er definert i personvernforordningen artikkel 4 nr. 7 som “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…”. Den behandlingsansvarlige er det primære pliktsubjektet etter personvernforordningen, og er overordnet ansvarlig for å sikre etterlevelse av personvernregelverket, jf. personvernforordningen artikkel 5 nr. 2.

Den behandlingsansvarlige er ansvarlig for at personopplysningene behandles på en lovlig, rettferdig og gjennomsiktig måte. I dette ligger det blant annet å påse at det foreligger et behandlingsgrunnlag for behandling av personopplysninger for det enkelte formål, at personopplysningene behandles på en tilfredsstillende sikker måte, og at de registrerte settes i stand til å utøve sine rettigheter. Som behandlingsansvarlig må en derfor sørge for å etablere alle nødvendige organisatoriske og tekniske tiltak for å sikre at regelverket etterleves til enhver tid. Tilsvarende gjelder også med tanke på forsvarlig valg av databehandler.

Databehandler er definert i personvernforordningen artikkel 4 nr. 8 som “en fysisk eller juridisk person, offentlig myndighet, institusjon eller ethvert annet organ som behandler personopplysninger på vegne av den behandlingsansvarlige.” I rollen som databehandler behandles personopplysningene etter instruks fra behandlingsansvarlig, og databehandleren kan derfor ikke beslutte formålet eller andre avgjørende elementer ved behandlingen.

Databehandleravtalen mellom DFØ og våre kunder regulerer DFØs plikter i rollen som databehandler. Databehandleravtalen er en del av avtalen som alle kunder har signert på. Den er i utgangspunktet standard for alle kunder og er tilgjengelig på DFØs nettsider. Avtalen er under revisjon og status på dette arbeidet er nærmere omtalt i punkt 5.4.

4. Overordnet status på personvernarbeidet i DFØ

DFØ arbeider systematisk og målrettet med forbedring av internkontroll for personvern. Dette for å sikre en lovlig behandling av personopplysninger, herunder i rollen som databehandler. Internkontroll for personvern består av overordnede styrende dokumentasjon, samt gjennomførende og kontrollerende rutiner. Internkontrollen skal sikre at etterlevelsen av personvernregelverket dokumenteres.

DFØ har styrende dokumentasjon for behandling av personopplysninger, herunder policy for behandling av personopplysninger og beskrivelse av organiseringen av personvernområdet med tilhørende roller og ansvar. Den styrende dokumentasjonen er forankret og godkjent hos ledelsen, og legger tydelige føringer for DFØs behandling av personopplysninger. DFØ har en protokoll over sine behandlingsaktiviteter, både i rollen som behandlingsansvarlig og databehandler.

DFØ har organisert personvernområdet slik at alle sentrale roller er på plass og oppgaver ivaretas. DFØ har styrket innsatsen på personvernområdet ved å ansette et personvernombud på heltid fra 1. januar 2021.

Når det gjelder det gjennomførende nivået, som operasjonaliserer DFØs overordnede føringer og beskriver hvordan DFØ behandler personopplysninger i praksis, er det utarbeidet en rekke rutiner som samlet sett skal sørge for tilstrekkelige føringer for den daglige håndteringen av personopplysninger. DFØ arbeider kontinuerlig med å implementere rollene og rutinene på personvern i virksomheten.

For å kunne kontrollere og vurdere om etablerte føringer og rutiner fungerer etter sin hensikt, og sørge for at DFØ etterlever regelverket på en tilfredsstillende måte, har DFØ etablert et årshjul med definerte kontrollaktiviteter og rapporteringer. Samlet sett skal etablerte aktiviteter og rapporteringer sikre at DFØs etablerte internkontroll er dekkende og fungerer etter sin hensikt slik at personvernregelverket etterleves. Det er utarbeidet rutine for ledelsens gjennomgang, og neste gjennomføring er satt til 2021. Her vil personvernombudet delta.

Videre har DFØ arbeidet med å etablere en intern kommunikasjon- og opplæringsplan for personvernområdet. Opplæring og bevisstgjøring er sentrale tiltak for å lykkes med personvernarbeidet. Det arbeides løpende med å sikre god kunnskap og bevissthet hos ansatte, slik at de forstår ansvaret som ligger til den enkelte ved behandling av personopplysninger. DFØ vil gjennomføre opplæring for alle nyansatte innenfor personvern. I tillegg vil det avholdes webinarer som er tilpasset for de ulike målgruppene.

I forbindelse med utarbeidelsen av ny databehandleravtale vil vi beskrive rutine for revisjon for DFØs etterlevelse av databehandleravtalen.

Det er identifisert en potensiell konflikt mellom anskaffelsesregelverket og personvernregelverket. Problemstillingen er knyttet til DFØs plikt til å varsle behandlingsansvarlig ved inngåelse av nye avtaler med underleverandører og de behandlingsansvarliges rett til å motsette seg underleverandører, jf. personvernforordningen artikkel 28 nr. 2, sett i sammenheng med at DFØ er bundet av anskaffelsesregelverket ved inngåelse av avtaler med sine underleverandører. DFØ har vært i dialog med Datatilsynet i sakens anledning og oversendt problemstillingen. Datatilsynet skal vurdere problemstillingen nærmere. Oppdaterte databehandleravtaler til kundene vil ikke kunne ferdigstilles før dette er avklart.

Privacy Shield ble som overføringsgrunnlag kjent ugyldig 16. juli 2020. DFØ har oversikt over sine underleverandører og arbeider med å følge opp disse i tråd med anbefalingene fra Det europeiske personvernrådet (EDPB) og Datatilsynet.

DFØ følger med på utviklingen som vil påvirke avtaler som er inngått med Storbritannia. Retningslinjene til EDPB og Datatilsynet ligger til grunn for de videre stegene DFØ vil foreta seg på dette området. En ny midlertidig forskrift sikrer at norske virksomheter fortsatt kan overføre personopplysninger til Storbritannia på en enkel måte.

5. Internkontroll på personvern DFØ

I det følgende vil sentrale temaer gjennomgås.

5.1. Styrende dokumentasjon

Relevant regulering: GDPR kapittel IV jf. artikkel 5 nr. 2

Status
DFØ har utarbeidet “Policy for behandling av personopplysninger”. Policyen omhandler blant annet DFØs rolle som databehandler. Her fremgår det tydelig at DFØ i rollen som databehandler plikter å kun behandle personopplysninger iht. inngåtte databehandleravtaler.

Veien videre

- Sikre jevnlig revisjon og oppdatering av policy for behandling av personopplysninger.

5.2. Organisering og roller på personvernområdet

Relevant regulering: GDPR kapittel IV jf. artikkel 5 nr. 2

Status

DFØ har styrket innsatsen på personvernområdet. Det er etablert og dokumentert en organisering av personvernområdet.

Veien videre

- Sikre tilpasset opplæring for dedikerte roller internt innen personvern.
- Kontinuerlig forbedring på personvernområdet basert på erfaring.

5.3. Protokoller over behandlingsaktiviteter

Relevant regulering: GDPR artikkel 30 jf. artikkel 5 nr. 2

Det følger av GDPR art. 30 nr. 1 at den behandlingsansvarlige skal føre protokoll over "behandlingsaktiviteter som utføres under deres ansvar". Tilsvarende skal databehandler føre en protokoll over alle kategorier av behandlingsaktiviteter som utføres på vegne av en behandlingsansvarlig, jf. GDPR art. 30 nr. 2. Bestemmelsen angir videre hvilke informasjonselementer som skal fremgå av protokollen.

Status

DFØs "Policy for behandling av personopplysninger" omtaler plikten til å føre protokoll i tråd med GDPR art. 30. DFØ har en protokoll over behandlingsaktiviteter, både i rollen som behandlingsansvarlig og databehandler.

Protokoll er etablert, men skal forbedres, og DFØ jobber med utfylling og kartlegging av behandlingsaktiviteter.

Veien videre

- Gjennomgang av protokoll i årlig intern revisjon.

5.4. Databehandleravtaler

Relevant regulering: GDPR artikkel 28

Status

<u>DFØs databehandleravtale med våre kunder:</u>

DFØ har etablert en avtale med kundene våre som ligger tilgjengelig på våre nettsider. Det arbeides med å utarbeide en ny versjon som skal sendes ut til alle kundene. Denne er basert på DFØs (tidligere Digdir) og Datatilsynets mal.

<u>DFØs databehandleravtaler med våre leverandører:</u>

DFØ har en databehandleravtale med alle våre leverandører som behandler personopplysninger. DFØ har etablert en rutine for inngåelse av databehandleravtaler.

Veien videre

- Påse at det blir inngått databehandleravtaler med leverandører som behandler personopplysninger på vegne av DFØ.
- Ferdigstille en ny databehandleravtale med våre kunder.

5.5. Oppfølging underleverandører

Relevant regulering: GDPR artikkel 28

Status
DFØ har etablert rutiner for oppfølging av underleverandører. Der DFØ som databehandler benytter underleverandører skal DFØ påse at avtaleforholdet med underleverandører er innenfor rammene av det som er skriftlig avtalt med kundene.

Veien videre

- Følge opp leverandørene etter anbefalte retningslinjer fra Datatilsynet og Det europeiske personvernrådet (EDPB).

5.6. Bistand til behandlingsansvarlig

Relevant regulering: GDPR artikkel 28 nr. 3

Gjennom personvernregelverket er DFØ som databehandler pålagt en rekke plikter overfor kundene. De sentrale pliktene er konkret regulert i databehandleravtalen, i tillegg til de lovregulerte oppgavene som følger av personvernforordningen art. 28. DFØ plikter blant annet å bistå kundene med oppfyllelse av de registrertes rettigheter, håndtering- og underretning om brudd på personopplysningssikkeheten, sletting av personopplysninger, samt bistå kunden med nødvendig informasjon for å kunne påvise etterlevelse av forpliktelsene etter personvernforordningens art 28.

Status
I DFØs “Policy for behandling av personopplysninger”, fremgår det tydelig og definert hvilken bistand DFØ i rollen som databehandler plikter å tilfredsstille overfor kundene. Dette er viktige avklaringer som viser at DFØ er bevisst på sin rolle som databehandler. Videre har DFØ et etablert og dedikert kundesenter, som sikrer god dialog med kundene, samt sørger for at kundene får nødvendig bistand på henvendelsene.

Veien videre

- Påse at pliktene regulert i databehandleravtalen, samt de lovregulerte oppgavene som følger av personvernforordningen etterleves.

5.7. Rutiner for sletting

Relevant regulering: GDPR artikkel 5 nr. 2 jf. artikkel 5 nr. 1 bokstav e og artikkel 24, samt artikkel 28

Personopplysninger skal slettes når formålet med behandlingen er oppnådd, jf. personvernforordningen art. 5 nr. 1 bokstav c) og e). Kravet til sletting gjelder med mindre andre rettslige forpliktelser tilsier videre lagring, eksempelvis arkivloven og bokføringsloven. Det er den behandlingsansvarliges ansvar å påse at det gis klare føringer for sletting av personopplysninger når formålet med behandlingen er oppnådd.

Status
For at DFØ skal kunne ivareta sin plikt som databehandler og gjennomføre sletting av personopplysninger etter instruks fra kunden, arbeides det med å etablere sletterutiner for behandling av personopplysninger i hver divisjon i DFØ.

Veien videre
- Fortsette arbeidet med sletterutiner og implementere disse i DFØ.

5.8. Rutine for rapportering og håndtering av avvik

Relevant regulering: GDPR artikkel 5 nr. 2 jf. 31 og 32, samt artikkel 28

Ved brudd på personopplysningssikkerheten skal DFØ uten ugrunnet opphold etter å ha fått kjennskap til bruddet, underrette den behandlingsansvarlige (kunden) skriftlig om eventuelle brudd, slik at kunden kan overholde sin forpliktelse til å melde bruddet til Datatilsynet, jf. personvernforordningen artikkel 33. Videre skal DFØ blant annet bistå kunden med å melde bruddet til Datatilsynet, samt gjennomføre de nødvendige tiltak for å unngå tilsvarende brudd på personopplysningssikkerheten.

Status
DFØ har utarbeidet en prosessbeskrivelse og rutine for hvordan brudd på personopplysningssikkerheten skal rapporteres og håndteres. Rutine for håndtering av avvik ivaretar DFØs rapporteringsplikt til behandlingsansvarlig der hvor DFØ er databehandler.

Veien videre
- Implementere forbedret rutine for avviksrapportering og -håndtering.

5.9. Egenkontroller og ledelsens gjennomgang

Relevant regulering: Relevant regulering: GDPR artikkel 5 nr. 2 jf. artikkel 24

DFØ vurderer løpende om iverksatte tiltak er dekkende og fungerer etter sin hensikt, eller om det er behov for endringer.

Status
I “Policy for behandling av personopplysninger” beskrives det et årshjul med definerte kontrollaktiviteter og rapporteringer. Denne skal sikre at DFØs etablerte internkontroll er dekkende og hensiktsmessig. Videre er det utarbeidet rutine for ledelsens gjennomgang.

Veien videre
- Følge årshjul for kontrollaktiviteter og rutine for ledelsens gjennomgang
- Gjennomføre ledelsens årlige gjennomgang på personvern

6. Oppsummering av status og videre arbeid

DFØ har jobbet løpende med personvernområdet over lang tid. DFØ vil sikre kontinuitet i personvernarbeidet, samt fortsette å arbeide systematisk og målrettet med internkontroll på personvernområdet.

Med vennlig hilsen

Hilde Singsaas
Direktør DFØ