

Cirkulæreskrivelse om fælles dataansvar vedrørende Økonomistyrelsens fællesoffentlige systemer

Indledning

Denne cirkulæreskrivelse er udarbejdet efter aftale mellem Økonomistyrelsen og Datatilsynet under henvisning til databeskyttelsesforordningen og bekendtgørelse om statens regnskabsvæsen mv. (regnskabsbekendtgørelsen). Datatilsynet har på vegne af institutionerne ligeledes godkendt udformningen af cirkulæreskrivelsen.

Økonomistyrelsen er ansvarlig for at levere fællesoffentlige systemer på økonomi-, betalings-, HR- og lønområdet, som en række statslige myndigheder og selvejende institutioner er forpligtet til at benytte i henhold til § 2 og § 11 i regnskabsbekendtgørelsen.

Når selvejende institutioner efter aftale, jf. § 12 i regnskabsbekendtgørelsen, benytter de af Økonomistyrelsen leverede systemer, sker det derfor på samme vilkår, som gælder for de institutioner, der er forpligtet til at anvende systemerne.

Oplysninger om, hvilke systemer Økonomistyrelsen leverer, hvilke processer disse systemer understøtter, samt hvilke data der findes i systemerne, fremgår af Økonomistyrelsens hjemmeside.

Aftale om fælles dataansvar efter Databeskyttelsesforordningen

Efter databeskyttelsesforordningens artikel 26 foreligger der fælles dataansvar, når to eller flere dataansvarlige i fællesskab fastlægger formålene med og hjælpemidlerne til behandling af persondata. Dette er tilfældet for de fællesoffentlige systemer på økonomi-, betalings-, HR- og lønområdet, som Økonomistyrelsen leverer i henhold til regnskabsbekendtgørelsen.

Foreligger der fælles dataansvar, skal de fælles dataansvarlige ifølge forordningen på en gennemsigtig måde fastlægge deres respektive ansvar for overholdelse af forpligtelserne i henhold til forordningen, navnlig hvad angår udøvelse af den registreredes rettigheder og deres respektive forpligtelser til at fremlægge de oplysninger, der er omhandlet i artikel 13 og 14, ved hjælp af en ordning imellem dem, medmindre og i det omfang de dataansvarliges respektive ansvar er fastlagt i EU-ret eller medlemsstaternes nationale ret, som de dataansvarlige er underlagt.

Det er på denne baggrund, at Økonomistyrelsen og Datatilsynet har indgået en aftale om fælles dataansvar for de systemer, der stilles til rådighed af Økonomistyrelsen. Datatilsynet har herefter sanktioneret, at aftalen bliver ophøjet til retsregler i form af indeværende cirkulæreskrivelse.

Aftalen er gældende for alle institutioner, som i henhold til § 11, jf. § 2 i bekendtgørelse om statens regnskabsvæsen mv. anvender de nævnte systemer, der stilles til rådighed af Økonomistyrelsen.

De enkelte institutioner er som led i deres efterlevelse af databeskyttelsesforordningens regler derfor forpligtet til at gøre sig bekendt med indholdet af aftalen og følge den i forbindelse med deres behandling af personoplysninger ved hjælp af de nævnte systemer.

1. Aftale om fælles dataansvar for systemer på økonomi-, betalings-, HR- og lønområdet, som stilles til rådighed af Økonomistyrelsen

- 1.1. I denne aftale fastsættes bestemmelser om ansvarsfordelingen mellem Økonomistyrelsen og de institutioner, der anvender de systemer på økonomi-, betalings-, HR- og lønområdet, der stilles til rådighed af Økonomistyrelsen efter bekendtgørelse om statens regnskabsvæsen mv. (regnskabsbekendtgørelsen).

Personoplysninger, som institutionerne behandler i systemerne, bliver ligeledes behandlet, herunder indsamlet til Økonomistyrelsens formål, fordi Økonomistyrelsen har behov for oplysningerne til en viderebehandling, som Økonomistyrelsen foretager uden instruks fra institutionerne.

Økonomistyrelsen indsamler institutionernes data fra en række systemer til statistikformål og analyser, lovbestemt afrapportering og lignende samt til udvikling og videreudvikling af fællesoffentlige systemer

Ovennævnte viderebehandling sker til Økonomistyrelsens egne formål og med Økonomistyrelsen som ene dataansvarlig. Økonomistyrelsens viderebehandling af oplysningerne er derfor ikke omfattet af indeværende cirkulæreskrivelse.

- 1.2. Det væsentligste indhold af den ordning, der fastsættes i denne cirkulæreskrivelse, skal gøres tilgængeligt for de registrerede.

Den registrerede kan dog, uanset ordningens udformning, udøve sine rettigheder i medfør af databeskyttelsesforordningen med hensyn til og over for den enkelte dataansvarlige.

- 1.3. I forbindelse med institutionernes anvendelse af de af Økonomistyrelsen administrerede systemer foreligger der et fælles dataansvar. Ved vurderingen heraf er der bl.a. lagt vægt på, at de behandlinger af personoplysninger, som finder sted i systemet, sker til begge parter formål og med fælles hjælpemidler (systemet).

2. Overordnet ansvarsfordeling

- 2.1. Som bruger af systemerne er den enkelte institution bl.a. ansvarlig for den behandling af personoplysninger, som finder sted i forbindelse med anvendelsen, herunder korrekt indsamling og registrering af oplysninger. Den enkelte institution er ligeledes – i vidt omfang – ansvarlig for udøvelsen af den registreredes rettigheder.
- 2.2. Som ansvarlig myndighed for systemerne er Økonomistyrelsen bl.a. ansvarlig for at foretage passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til risiciene for behandlingen i de forskellige systemer.

3. Principper og behandlingshjemmel

- 3.1. Den enkelte institution er ansvarlig for, at der foreligger en hjemmel til behandling af de personoplysninger, som institutionen registrerer og behandler i systemerne.
- 3.2. Den enkelte institution er ligeledes ansvarlig for at kunne dokumentere en gyldig behandlingshjemmel, eksempelvis såfremt hjemlen er baseret på et samtykke fra den registrerede.
- 3.3. Den enkelte institution og Økonomistyrelsen er hver især ansvarlige for at overholde principperne for behandling af personoplysninger samt god databehandlingsskik, i det omfang at reglerne finder anvendelse på den pågældendes ansvarsområder ifølge denne aftale.
- 3.4. Økonomistyrelsen er ansvarlig for at fastsætte slettefrister for personoplysninger, der behandles i de fællesoffentlige systemer. Dette indebærer, at Økonomistyrelsen skal sikre, at slettefristerne er i overensstemmelse med databeskyttelsesforordningen og gældende national lovgivning samt er hensigtsmæssige i forhold til de formål, hvortil personoplysningerne behandles.

4. De registreredes rettigheder

- 4.1. Den enkelte institution er ansvarlig for sikringen af de registreredes rettigheder gennem iagttagelse af nedenstående regler i databeskyttelsesforordningen:
 - oplysningspligt ved indsamling af personoplysninger hos den registrerede,
 - oplysningspligt, hvis personoplysninger ikke er indsamlet hos den registrerede,

- den registreredes indsigtsret,
- ret til berigtigelse,
- ret til sletning (retten til at blive glemt),
- ret til begrænsning af behandling,
- underretningspligt i forbindelse med berigtigelse eller sletning af personoplysninger eller begrænsning af behandling, og
- ret til indsigelse mod en behandling.

- 4.2. Den enkelte institution er ansvarlig for egne data og ansvarlig for behandlingen af anmodninger eller henvendelser fra de registrerede vedrørende de forhold, der er nævnt i punkt 4.1.
- 4.3. Den enkelte institution er ansvarlig for at sikre overholdelse af oplysningspligten over for sine registrerede i relation til den behandling af personoplysninger, der er angivet i pkt. 1.1., herunder for den viderebehandling af oplysningerne, der sker til Økonomistyrelsens egne formål.
- 4.4. Såfremt Økonomistyrelsen modtager en anmodning eller henvendelse fra en registreret vedrørende de forhold, der er nævnt i punkt 4.1., og vedrørende en anden institution, jf. punkt 4.2., oversendes denne til besvarelse hos den relevante institution snarest muligt.
- 4.5. Økonomistyrelsen er ansvarlig for at bistå institutionerne i det omfang, at dette er relevant og nødvendigt for, at institutionerne kan efterleve deres forpligtelser over for de registrerede.

5. Dokumentation for overholdelse af databeskyttelsesforordningen

- 5.1. Den enkelte institution er ansvarlig for, under hensyntagen til den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder, at gennemføre passende tekniske og organisatoriske foranstaltninger for at sikre og for at være i stand til at påvise, at behandling er i overensstemmelse med databeskyttelsesforordningen. Foranstaltningerne skal om nødvendigt revideres og ajourføres. Dette kan eksempelvis indebære, at Økonomistyrelsen udarbejder procedurer for håndtering af sikkerhedsbrister, jf. databeskyttelsesforordningens artikel 32.

- 5.2. Økonomistyrelsens foranstaltninger skal, hvis det står i rimeligt forhold til behandlingsaktiviteterne, omfatte implementeringen af passende databeskyttelsespolitikker.
- 5.3. Økonomistyrelsen er ansvarlig for iagttagelse af reglen om databeskyttelse gennem design og databeskyttelse gennem standardindstillinger i databeskyttelsesforordningens artikel 25.
- 5.4. Den enkelte institution er ansvarlig for at gennemføre passende tekniske og organisatoriske foranstaltninger for at sikre og for at være i stand til at påvise, at institutionens behandling af oplysningerne er i overensstemmelse med databeskyttelsesforordningen. Dette kan eksempelvis indebære udarbejdelse af procedurer for anmodninger om indsigt eller opfyldelse af oplysningspligten (databeskyttelsesforordningens artikel 24).

6. Anvendelse af databehandlere og underdatabehandlere

- 6.1. Økonomistyrelsen er berettiget til at anvende databehandlere og eventuelle underdatabehandlere i tilknytning til de omhandlede systemer.
- 6.2. Ved anvendelse af databehandlere og eventuelle underdatabehandlere er Økonomistyrelsen ansvarlig for at efterleve kravene i databeskyttelsesforordningens artikel 28. Økonomistyrelsen er herefter bl.a. forpligtet til
- alene at anvende databehandlere, der kan stille de fornødne garantier for, at de gennemfører de passende tekniske og organisatoriske sikkerhedsforanstaltninger på en sådan måde, at behandling opfylder kravene i denne forordning og sikrer beskyttelse af den registreredes rettigheder,
 - at sikre, at der foreligger en gyldig databehandleraftale mellem Økonomistyrelsen og databehandleren, og
 - at sikre, at der foreligger en gyldig underdatabehandleraftale mellem databehandleren og en eventuel underdatabehandler.
- 6.3. Økonomistyrelsen skal på anmodning fra en institution oplyse om, hvorvidt oplysningerne behandles af databehandlere og evt. underdatabehandlere.

- 6.4. Hvis oplysningerne behandles af databehandlere og evt. underdatabehandlere, kan Økonomistyrelsen efter anmodning fra institutionerne oplyse om indholdet af aftalerne.

7. Fortegnelse

- 7.1. Økonomistyrelsen er ansvarlig for at iagttage kravet i databeskyttelsesforordningens artikel 30 om fortegnelser over behandlingsaktiviteter. Dette indebærer, at Økonomistyrelsen fører fortegnelser over de behandlingsaktiviteter, som foretages i de pågældende systemer.
- 7.2. Økonomistyrelsen orienterer institutionerne om indholdet af ovennævnte fortegnelser.
- 7.3. Den enkelte institution skal – eventuelt på baggrund af indholdet i Økonomistyrelsens fortegnelser – udarbejde egne fortegnelser over de af aftalen omhandlede behandlingsaktiviteter.

8. Behandlingssikkerhed

- 8.1. Økonomistyrelsen er ansvarlig for at iagttage kravet i databeskyttelsesforordningens artikel 32 om behandlingssikkerhed. Dette indebærer, at Økonomistyrelsen skal gennemføre passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til disse risici. Dette skal ske under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder.

Dette indebærer, at Økonomistyrelsen skal foretage en risikovurdering og herefter gennemføre foranstaltninger for at begrænse de identificerede risici.

- 8.2. Den enkelte institution er forpligtet til at gennemføre relevante sikkerhedsforanstaltninger, som knytter sig til institutionens anvendelse af systemerne, herunder f.eks. foranstaltninger i forbindelse med den fysiske sikkerhed.

9. Anmeldelse af brud på persondatasikkerheden til tilsynsmyndigheden

- 9.1. Økonomistyrelsen er ansvarlig for efterlevelsen af databeskyttelsesforordningens artikel 33 om anmeldelse af brud på persondatasikkerheden til tilsynsmyndigheden.
- 9.2. Den enkelte institution er dog ansvarlig for efterlevelsen af databeskyttelsesforordningens artikel 33, såfremt et brud på persondatasikkerheden skyldes egen uberettiget anvendelse af systemet.

10.Underretning om brud på persondatasikkerheden til den registrerede

- 10.1.Økonomistyrelsen er ansvarlig for iagttagelsen af databeskyttelsesforordningens artikel 34 vedrørende underretning om brud på persondatasikkerheden til den registrerede.
- 10.2.Den enkelte institution er ansvarlig for iagttagelsen af databeskyttelsesforordningens artikel 34 vedrørende underretning til den registrerede om brud på persondatasikkerheden, såfremt et brud på persondatasikkerheden skyldes egen uberettiget anvendelse af systemet. I et sådant tilfælde er Økonomistyrelsen forpligtet til at bistå institutionen med oplysninger, som er nødvendige for, at institutionen kan overholde sine forpligtelser over for den registrerede.

11.Konsekvensanalyse vedrørende databeskyttelse og forudgående høring

- 11.1.Økonomistyrelsen er ansvarlig for iagttagelsen af kravet i databeskyttelsesforordningens artikel 35 om konsekvensanalyse vedrørende databeskyttelse. Dette indebærer, at Økonomistyrelsen forud for behandlingen skal foretage en analyse af de påtænkte behandlingsaktiviteters konsekvenser for beskyttelse af personoplysninger, hvis en type behandling, navnlig ved brug af nye teknologier og i medfør af sin karakter, omfang, sammenhæng og formål, sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder.
- 11.2.Økonomistyrelsen er ligeledes forpligtet til at iagttage kravet i databeskyttelsesforordningens artikel 36 om forudgående høring af tilsynsmyndigheden, når kravet finder anvendelse.

12.Overførsel af personoplysninger til tredjelande eller internationale organisationer

12.1. Økonomistyrelsen er ansvarlig for iagttagelsen af kravene i databeskyttelsesforordningens kapitel V, såfremt der sker overførsel af personoplysninger til tredjelande eller internationale organisationer.

12.2. Den enkelte institution er ansvarlig for iagttagelsen af kapitel V, såfremt overførslen af personoplysninger til et tredjeland eller en international organisation sker i forbindelse med institutionens anvendelse af systemet/på institutionens foranledning.

13. Klager

13.1. Økonomistyrelsen er ansvarlig for behandling af eventuelle klager fra registrerede, såfremt klagerne omhandler overtrædelse af bestemmelser i databeskyttelsesforordningen, for hvilke Økonomistyrelsen efter denne aftale er ansvarlig.

13.2. Den enkelte institution er ansvarlig for behandling af eventuelle klager fra registrerede, såfremt klagerne omhandler overtrædelse af bestemmelser i databeskyttelsesforordningen, for hvilke institutionen efter denne aftale er ansvarlig.

13.3. Såfremt en institution eller Økonomistyrelsen modtager en klage, som rettelig bør behandles af den anden part, oversendes klagen til denne dataansvarlige snarest muligt.

13.4. Såfremt en institution eller Økonomistyrelsen modtager en klage, hvor en del af klagen rettelig bør behandles af den anden part, oversendes denne del til besvarelse hos parten snarest muligt.

13.5. Den registrerede skal, i forbindelse med en institutions eller Økonomistyrelsens oversendelse af en klage eller en del heraf til den anden part, oplyses om det væsentligste indhold af denne aftale.

14. Orientering af den anden part

14.1. Parterne orienterer hinanden om væsentlige forhold, der har betydning for de behandlinger og systemer, der er omfattet af denne aftale.

15.Ikrafttrædelse

15.1.Denne aftale træder i kraft den xx. xx 2025.

Økonomistyrrelsen, den xx. xx 2025

P.M.V.

E.B.

Maria Haugaard

UDKAST