KIT Sikkerhed 2 (5953)
Økonomiforvaltningen

Orientering

Til Økonomiudvalget

Orientering om status på Schrems II-dommen – nyt overførselsgrundlag mellem EU & USA er vedtaget

25-08-2023

Sagsnummer i F2
2022 - 19986

Dokumentnummer i F2
3662550

Sagsnummer eDoc
2022-0410546

Sagsbehandler
Nelli Schubert Jensen
Stubbe Wissing

Resumé
Den 10. juli 2023 vedtog EU-Kommissionen en tilstrækkelighedsafgørelse med nyt overførselsgrundlag mellem EU/EØS og USA. Den nye tilstrækkelighedsafgørelse for EU-U.S. Data Privacy Framework etablerer et nyt lovligt overførselsgrundlag for persondata til USA, hvilket er positivt.

Det betyder, at Schrems II problematikken vurderes løst og overførsel af personoplysninger til USA isoleret set – igen – kan ske lovligt.

De grundlæggende krav i GDPR skal stadig efterleves og det nye overførselsgrundlag løser ikke problematikken vedr. leverandørernes anvendelse af personoplysninger til egne formål, hvilket stadig vurderes at være en væsentlig udfordring.

Sagsfremstilling
Økonomiudvalget (ØU) er tidligere orienteret om status på Schrems II-dommens betydning for KK som dataansvarlig, senest på aflæggerbordet til ØU-mødet den 25. januar 2023 og igen den 23. maj i forbindelse med fortrolig sag om licensfornyelse af Microsoft 365.

Den 10. juli 2023 blev tilstrækkelighedsafgørelsen for EU-U.S. Data Privacy Framework vedtaget af EU-Kommissionen. Den nye tilstrækkelighedsafgørelse etablerer igen et lovligt overførselsgrundlag for persondata mellem EU og USA.

Tilstrækkelighedsafgørelsen kan dog alene anvendes som overførselsgrundlag, når man agter at overføre personoplysninger til organisationer i USA, der har certificeret sig under EU-U.S. Data Privacy Framework hos det amerikanske handelsministerium.

Det betyder, at både leverandøren og dennes underleverandører skal fremgå af Data Privacy Listen for, at man som dataansvarlig lovligt kan anvende overførselsgrundlaget og dermed overføre personoplysninger til USA.

Overførselsgrundlaget løser ikke problematikken om databehandlernes anvendelse af data til egne formål. Her gælder fortsat de anbefalinger, som databeskyttelsesrådgiveren tidligere har givet, jf. bilag 1. Der afventes fortsat en udmelding fra Datatilsynet om anvendelse af data til egne formål hos databehandlere som Google og Amazon Web Services (AWS), jf. blandt andet den verserende sag om brug af ChromeBooks i Helsingør Kommune.

Anbefalingerne fra kommunens databeskyttelsesrådgiver og Økonomiforvaltningen er, at Københavns Kommune sikrer sig, at hele leverandørkæden optræder på Data Privacy Listen, og at data ikke anvendes til egne formål i hele leverandørkæden, inden der indgås en databehandleraftale. Det anbefales, at det anføres i databehandleraftalen, at det er en forudsætning for aftalen, at leverandøren og dennes underleverandører kan opretholde EU-rettens krav til databeskyttelsesniveau for de registrerede samt at registrering på "Data Privacy Listen" opretholdes. Ifald de to krav misligholdes, betragtes det som lovligt opsigelsesgrundlag af den dataansvarlige (KK). Det anbefales ligeledes, at der udarbejdes en exitstrategi, hvis leverandøren på et tidspunkt efter aftaleindgåelsen, ikke lever op til reglerne i GDPR, eksempelvis hvis leverandøren slettes fra "Data Privacy Listen".

Forvaltningerne bør stadig være opmærksomme på, at de grundlæggende krav i GDPR skal efterleves.

Økonomi
Sagen har ingen økonomiske konsekvenser.

Videre proces
Økonomiforvaltningen vil i samråd med Databeskyttelsesrådgiveren vejlede forvaltningerne om overførselsgrundlaget, og herunder også tage højde for Datatilsynets kommende opdaterede vejledninger om cloud og tredjelandsoverførsler. Det forventes, at Datatilsynet opdaterer deres vejledninger i efteråret 2023.

Bilag
Bilag 1. Databeskyttelsesrådgiverens anbefalinger til håndtering af leverandørens brug af personoplysninger til egne formål

Notat

Databeskyttelsesrådgiverens anbefalinger til håndtering af leverandørens brug af personoplysninger til egne formål

14. april 2023

Sagsbehandler
Christian Cramer Kjelmann
Line Nymann Schoop

Baggrund

Når Københavns Kommune indgår en databehandleraftale med en leverandør, må leverandøren kun behandle personoplysningerne til de formål som Københavns Kommune instruerer leverandøren i.

Det er en kendt problemstilling, at flere cloud-leverandører anvender personoplysninger til deres egne formål, og således i strid med databehandleraftalens instruks.

Databeskyttelsesrådgiveren har været i dialog med Datatilsynet omkring denne problemstilling, og har på baggrund heraf nogle anbefalinger til Københavns Kommunes fremadrettede håndtering af denne problemstilling.

Problemstilling

Københavns Kommune har på nuværende tidspunkt flere ulovlige kontrakter med leverandører og vil i den nærmeste fremtid have behov for at forny flere af disse kontrakter, fordi leverandørens løsning ikke udbydes af andre, og fordi systemet er nødvendigt for, at Københavns Kommune kan levere velfærdsydelser til borgere.

Københavns Kommune skal sikre, at de databehandlere, og tilhørende underdatabehandlere, som behandler personoplysninger på kommunens vegne, ikke anvender personoplysningerne til egne formål. Kommunen vil i de fleste tilfælde ikke have hjemmel til at videregive personoplysninger til en leverandør, som behandler disse til egne formål. Der henvises til bilag 1, for en uddybet beskrivelse af en leverandørs behandling til egne formål.

I de situationer, hvor Amazon eller Microsoft anvendes i leverandørkæden, er det meget sandsynligt, at der foretages behandling af de overladte personoplysninger, til leverandørernes egne behandlingsformål. Hvis kommunen indgår eller fornyer en

Databeskyttelsesrådgiveren
Københavns Kommune

EAN-nummer
5798009809964

databehandleraftale med fx Microsoft, hvori der gives Microsoft mulighed for at anvende personoplysninger til fx markedsføringsformål, vil aftalen være ulovlig, da der ikke er hjemmel for kommunen til at videregive personoplysninger.

Exit-planer

I det tilfælde, hvor leverandøren behandler personoplysninger til egne formål, skal der udarbejdes en exit-plan, hvis ikke det er muligt at få leverandøren til at ændre vilkårene i databehandleraftalen.

En exit-plan bør, for hvert system med tilhørende FISKK-id, indeholde en vurdering af nuværende kontraktvilkår, oversigt over, hvornår kontrakten udløber, strategi for markedsafdækning, vurdering af alternative løsninger og en tidsplan for, hvornår kommunen kan udtræde af kontrakten.
Exitplanen skal eksekveres inden for maksimalt to år.

Kommende udbud
Står kommunen overfor et udbud, hvor der ikke vil være nogle bydere, som kan levere en lovlig løsning, kan en ny kontrakt maksimalt løbe i to år. Derfor skal en ny kontrakt udarbejdes, således at kommunen har mulighed for at opsige kontrakten, hvis løsningen ikke er blevet lovliggjort inden da. Perioden skal ikke ses som en stilstandsperiode, og der skal aktivt løbende gøres en indsats for at finde en anden lovlig løsning. Hvis kontrakten er blevet opsagt inden for de to år, grundet en fortsat ulovlig løsning, kan der ikke indgås en ny kontrakt med den pågældende leverandør.

I udbudsmaterialet må det ikke fastsættes som et mindstekrav, at leverandøren ikke må anvende personoplysningerne til egne formål, da leverandøren derved ikke anses for konditionsmæssig egnet – og dermed skal diskvalificeres. I stedet bør det anføres som et evalueringskrav, som derved vil favorisere en leverandør der kan levere en løsning, hvor der ikke sker behandling til egne formål. Samtidig giver det transparens i hvilke leverandører der anvender data til egne formål.

Databeskyttelsesrådgiverens konklusion og anbefaling

Det er Databeskyttelsesrådgiverens anbefaling at:

- Københavns Kommune inden for de næste 2 år sikrer, at alle kommunens databehandlere ikke anvender kommunens personoplysninger til egne formål.

- Der igangsættes initiativer der medvirker til at problemstillingen løses i samarbejde med andre store nationale aktører, såsom KL, regionerne og statslige myndigheder mv.

Der henvises endvidere til "DPO Notat – Schrems problematik og udbud april 2023".

Bilag 1 – Uddybende beskrivelse af en leverandørs behandling til egne formål

Siden Datatilsynet nedlagde behandlingsforbud i Helsingør Kommune brug af Chromebooks, som senere blev suspenderet, har der været fokus på databehandlerens brug af personoplysninger til egne formål.

Det følger af forordningen, at alle persondatabehandlinger skal have et lovligt behandlingsgrundlag, som er understøttende for det grundlæggende behandlingsformål.

De store Cloud-udbydere har ofte ugennemsigtige databehandleraftaler, terms of use m.m – hvor de ofte har givet sig selv "lov" til at behandle Københavns Kommunes borgeres personoplysninger til egne formål.

Det kan f.eks. være markedsføring, produktudvikling, profilering, tracking osv.

Hvis en databehandler, skal have et lovligt grundlag for at behandle personoplysninger til egne formål, skal kommunen lovligt kunne videregive personoplysningerne til dette.

Idet kommunerne er offentlige myndigheder, vil behandlingerne ofte være forbundet med myndighedsudøvelse. Lovgivningen tillader derfor ikke, at borgernes personoplysninger behandles til andre formål, end det der følger af den specifikke myndighedsopgave.

Kommunen vil derfor ikke lovligt kunne tillade en databehandler at behandle kommunens personoplysninger til andet, end kommunens egne behandlingsformål.

Der ligger derfor en væsentlig opgave for kommunen, når der kontraheres med en databehandler, i at sikre behandlingssikkerheden, det konkrete aftalegrundlag og instruksen. Dette krav omfatter også databehandlerens underdatabehandlere.