JUSTITSMINISTERIET

Folketinget
Udvalget for Digitalisering og It
Christiansborg
1240 København K
DK Danmark

Dato: 29. september 2023
Kontor: Databeskyttelseskontoret
Sagsbeh: Anna Rosdahl Christiansen
Sagsnr.: 2023-0032/51-0036
Dok.: 2962744

Besvarelse af spørgsmål nr. 116 (Alm. del) fra Folketingets Udvalg for Digitalisering og IT

Hermed sendes besvarelse af spørgsmål nr. 116 (Alm. del), som Folketingets Udvalg for Digitalisering og IT har stillet til justitsministeren den 1. september 2023. Spørgsmålet er stillet efter ønske fra Lisbeth Bech-Nielsen (SF).

Peter Hummelgaard

/

Louise Black Mogensen

Slotsholmsgade 10
1216 København K.

T +45 7226 8400

www.justitsministeriet.dk
jm@jm.dk

Spørgsmål nr. 116 (Alm. del) fra Folketingets Udvalg for Digitalisering og IT:

> ”Vil Ministeren redegøre for følgende om EU-Kommissionens tilstrækkelighedsredegørelse og EU-U.S. Data Privacy Framework?
> - Hvad betyder afgørelsen og aftalen konkret for behandling af beskyttelsesniveauet for danske borgeres data?
> - Hvordan adskiller EU-U.S. Data Privacy Framework sig materielt fra henholdsvis Privacy Shield-aftalen fra 2016 og Safe Harbour-aftalen fra 2001?
> - Hvordan er EU-borgere stillet i forhold til FISA 702 (Foreign Intelligence Surveillance Act) og amerikanske efterretningstjenesters adgang til at kræve data udleveret fra virksomheder placeret i EU?”

Svar:

1. Når personoplysninger ønskes overført til et tredjeland (lande uden for EU/EØS), skal dataeksportøren (den der fører personoplysningerne ud af EU/EØS) iagttage de databeskyttelsesretlige regler om tredjelandsoverførsler. Formålet med reglerne om tredjelandsoverførsler er at sikre en tilstrækkelig beskyttelse af personoplysninger, som forlader EU.

Reglerne stiller i den forbindelse krav om, at videregivelse af personoplysninger til en modtager i et tredjeland skal være baseret på et overførselsgrundlag, som skal være på plads, inden personoplysninger kan overføres til et tredjeland. Der er forskellige overførselsgrundlag, der kan anvendes, når en dataeksportør vil overføre personoplysninger til et tredjeland.

Et overførselsgrundlag kan f.eks. bestå i en såkaldt tilstrækkelighedsafgørelse. Det vil sige, at et tredjeland i databeskyttelsesretlig forstand betragtes som sikkert at overføre personoplysninger til. Det er EU-Kommissionen, som træffer afgørelse om, at tredjelandet, et område eller en sektor har et tilstrækkeligt databeskyttelsesretligt niveau, hvilket betyder, at beskyttelsesniveauet for personoplysninger i det pågældende tredjeland i det væsentlige svarer til beskyttelsesniveauet i EU/EØS.

Den 10. juli 2023 traf Kommissionen afgørelse om, at det såkaldte ”EU-U.S. Data Privacy Framework” sikrer et tilstrækkeligt beskyttelsesniveau i forbindelse med overførsel af personoplysninger fra EU til USA.

Data Privacy Framework er en ordning, som indeholder en række principper for behandling af personoplysninger, herunder at enhver behandling af personoplysninger skal være lovlig og rimelig, og at personoplysninger skal indsamles til et specifikt formål og efterfølgende udelukkende anvendes, såfremt dette ikke er uforeneligt med behandlingsformålet.

Tilstrækkelighedsafgørelsen, der bygger på Data Privacy Framework, kan anvendes som overførselsgrundlag, når personoplysninger overføres til organisationer i USA, der har certificeret sig under ordningen hos det amerikanske handelsministerium. Data Privacy Framework bygger således på en ordning, hvor virksomheder i USA frivilligt vælger at tilslutte sig for derved at kunne gøre brug af tilstrækkelighedsafgørelsen.

I det omfang en virksomhed tilslutter sig Data Privacy Framework, forpligter virksomheden sig til at overholde principperne, hvilket giver de registrerede, hvis personoplysninger er blevet overført til virksomheden, en række rettigheder.

Det indebærer bl.a., at de registrerede skal informeres om de vigtigste elementer i behandlingen af deres personoplysninger, herunder navnlig retten til indsigt i oplysninger, retten til at gøre indsigelse mod behandlingen og retten til at få oplysninger berigtiget og slettet.

Det indebærer også, at de tilmeldte organisationer skal give fysiske personer, der er berørt af manglende overholdelse af principperne i aftalen, mulighed for at klage, dvs. give registrerede i EU mulighed for at indgive klager vedrørende de tilmeldte organisationers manglende overholdelse og om nødvendigt få en afgørelse om effektive foranstaltninger, der kan afhjælpe disse klager.

Det betyder helt konkret, at EU-borgere, hvis oplysninger overføres under Data Privacy Framework, bl.a. vil have ret til indsigt i deres personoplysninger, ret til at få oplysning om, at deres personoplysninger bliver behandlet og ret til at klage over en behandling af deres personoplysninger, ligesom det sikres, at eventuelle afgørelser kan håndhæves, og at den dataansvarlige kan ifalde erstatningsansvar.

2. Kommissionen traf den juli 2000 (2000/520/EF) afgørelse om, at den såkaldte Safe Harbour-ordning sikrede et tilstrækkeligt beskyttelsesniveau i

forbindelse med overførsel af personoplysninger fra EU til USA. Safe Harbour-ordningen indeholdt en række principper, herunder om oplysning, den registreredes valg, ansvarlighed ved videreoverførsel, sikkerhed, integritet og formålsbegrænsning, indsigt og klageadgang, håndhævelse og ansvar.

EU-Domstolen erklærede ved dom af 6. oktober 2015 (den såkaldte Schrems-dom) Kommissionens afgørelse vedrørende Safe Harbor-ordningen ugyldig. EU-Domstolen lagde bl.a. vægt på, at modtagere i USA af oplysninger fra EU var forpligtede til uden begrænsning at se bort fra Safe Harbor-principperne, når disse var i modstrid med krav i amerikansk lovgivning, at der ikke forelå mulighed for effektive retsmidler, herunder domstolsprøvelse, for de europæiske registrerede, og at lovgivning, der tillod masseindsamling af data, der blev overført mellem EU og USA uden nogle former for begrænsninger eller undtagelser, ikke var begrænset til det strengt nødvendige, og det var dermed i strid med EU-retten.

I juli 2016 traf Kommissionen en ny tilstrækkelighedsafgørelse baseret på Privacy Shield-ordningen med det formål at imødekomme manglerne i Safe Harbor-ordningen. Med Privacy Shield blev der bl.a. indført begrænsninger i de amerikanske myndigheders adgang til EU-borgeres personoplysninger, samt indført en ny klagemekanisme for EU-borgere på området for nationale efterretninger i form af en ombudsmand, som var uafhængig af de amerikanske nationale sikkerhedsmyndigheder.

EU-Domstolen erklærede ved dom af 16. juli 2020 (den såkaldte Schrems-II-dom) Kommissionens afgørelse om Privacy Shield-ordningen ugyldig, bl.a. fordi amerikansk lovgivning ikke satte tilstrækkelige rammer for de amerikanske myndigheders adgang til personoplysninger, som blev overført til USA under ordningen.

Det nye Data Privacy Framework er baseret på de tidligere ordninger, men indeholder en række yderligere tiltag. De væsentligste forskelle mellem det nye Data Privacy Framework og de tidligere ordninger er bl.a. en række yderligere begrænsninger i de amerikanske myndigheders adgang til at pålægge virksomheder at udlevere personoplysninger, samt nye klagemuligheder for berørte EU-borgere.

For det første er der indført begrænsninger og foranstaltninger vedrørende de amerikanske myndigheders adgang til personoplysninger med henblik på

strafferetlig håndhævelse og nationale sikkerhedsformål, som bl.a. indebærer, at enhver sådan brug af personoplysninger begrænses til det nødvendige og forholdsmæssige til beskyttelsen af national sikkerhed og skal være proportional i forhold til beskyttelsen af privatliv og frihedsrettigheder i øvrigt.

For det andet vil de amerikanske efterretningstjenester være underlagt tilsyn med henblik på at sikre overholdelse af sikkerhedsforanstaltningerne.

For det tredje indebærer de supplerende sikkerhedsforanstaltninger etablering af Data Protection Review Court (DPRC), der er en uafhængig klagemekanisme, der skal undersøge og behandle klager fra europæere om amerikanske myndigheders adgang til deres personoplysninger. Alle klager over behandling af personoplysninger til DPRC gennemgås af tre dommere og assisteres af en 'Special Advocate', som skal sikre, at klagers interesser repræsenteres.

3. Justitsministeriet har forstået spørgsmålet således, at der spørges til, hvilke muligheder amerikanske efterretningstjenester har for at indsamle EU-borgeres personoplysninger uden for USA.

Amerikanske efterretningstjenester har under visse betingelser mulighed for at indsamle personoplysninger uden for USA. I Data Privacy Framework reguleres USA's adgang til at foretage efterretningsindsamlinger af data (signalefterretninger) der overføres mellem EU og USA.

Denne adgang til at indsamle data, herunder personoplysninger, der overføres fra EU til USA, fandt EU-Domstolen i Schrems II-dommen, ikke var i overensstemmelse med EU-retten, da adgangen var for vid og uden undtagelser eller begrænsninger. Den 7. oktober 2022 udstedte den amerikanske præsident et præsidentielt dekret (EO 14086 Enhancing Safeguards for United States Signals Intelligence), der fastsætter begrænsninger og garantier for alle amerikanske signalefterretningsaktiviteter. Formålet med dekretet er at indføre nye databeskyttelsesgarantier og klagemuligheder for registrerede EU-borgere, herunder en ny klagemekanisme.

Den nye klagemekanisme skaber rettigheder for enkeltpersoner i EU, og mekanismen skal evalueres af rådet for tilsyn med privatlivets fred og borgerlige rettigheder (PCLOB). Ved Executive Order 14086 fastsættes

også flere garantier for at sikre databeskyttelsesappelrettens ("Data Protection Review Court") uafhængighed sammenlignet med den tidligere ombudsmandsmekanisme, og der indføres mere effektive beføjelser til at afhjælpe overtrædelser, herunder yderligere garantier for registrerede.

Det præsidentielle dekret styrker desuden de betingelser, begrænsninger og garantier, der gælder for alle signalefterretningsaktiviteter uanset hvor de finder sted, og begreberne nødvendighed og proportionalitet med hensyn til USA's signalefterretninger er også indført med dekretet

Kravene i det præsidentielle dekret er bindende, og kravene skal udmøntes i efterretningstjenesternes politikker og procedurer, der omsætter dem til konkrete retningslinjer for de daglige operationer.

Kravene vedrører blandt andet indsamling, anvendelse og videregivelse af personoplysninger og medfører eksempelvis, at aktiviteterne skal være hjemlet ved lov eller præsidentiel bemyndigelse, at der skal være indført passende garantier for at sikre, at hensynet til privatlivets fred og borgerrettigheder integreres i planlægningen af disse aktiviteter, og at enhver signalefterretningsaktivitet kun udføres, efter at det på grundlag af en rimelig vurdering af alle relevante faktorer er fastslået, at aktiviteterne er nødvendige for at fremme en valideret efterretningsprioritet.

Disse overordnede krav underbygges yderligere med hensyn til indsamling af signalefterretninger af en række betingelser og begrænsninger, der sikrer, at indgrebet i fysiske personers rettigheder begrænses til, hvad der er nødvendigt og forholdsmæssigt for at fremme et legitimt mål.

For at sikre overholdelsen af disse generelle krav – som afspejler principperne om lovlighed, nødvendighed og proportionalitet – er signalefterretningsaktiviteter, i tillæg til de i forvejen gældende begrænsninger, desuden underlagt regelmæssige tilsyn.

Det medfører konkret, at registrerede i EU har en række muligheder for at anlægge sag ved en uafhængig og upartisk instans, som har kompetence til at træffe bindende beføjelser, samt mulighed for at få indsigt i deres personoplysninger, få kontrolleret lovligheden af statslige organers adgang til deres oplysninger og, hvis det konstateres, at der er sket en overtrædelse, få en sådan overtrædelse afhjulpet, herunder ved at få berigtiget eller slettet deres personoplysninger.

En registreret i EU, der eksempelvis ønsker at indgive en klage over, at vedkommendes personoplysninger er blevet indsamlet af en efterretningstjeneste i USA, kan indgive den til en tilsynsmyndighed i en EU-medlemsstat, der har kompetence til at føre tilsyn med offentlige myndigheders behandling af personoplysninger (f.eks. Datatilsynet), hvilket sikrer en let adgang til klagemekanismen.