NOTAT
27. marts 2017

BREXIT KAN SLÅ KNUDE PÅ BRITISK STRØM AF DATA

Kontakt:
Analytiker, Sarah Vormsby
+45 21 81 56 30
sav@thinkeuropa.dk

RESUME *Op imod 800 danske datterselskaber i Storbritannien kan blive afskåret fra at udveksle altafgørende data med EU, hvis briterne ikke får en smidig aftale efter Brexit. Det store spørgsmål er, om briterne vil acceptere at leve op til EU's høje databeskyttelsesniveau, eller forsøge at dumpe persondatabeskyttelsen med henblik på at tiltrække digitale virksomheder. Hvis EU accepterer en aftale, der giver briterne lov til at sænke standarderne, kan det betyde, at digitale virksomheder vil forbigå EU-landene og i stedet søge til Storbritannien. Samtidig kan det medføre ringere databeskyttelse til danske og europæiske forbrugere.*

It-sektoren er, sammen med den finansielle sektor, nogle af Storbritanniens erhvervsmæssige førerpositioner. Den fortsatte udveksling af data er derfor en stor prioritet for briterne, som ikke ønsker at sætte deres førerposition over styr ved at kappe forbindelsen til den digitale del af det indre marked. Ønsker briterne fortsat at kunne udveksle data over kanalen, skal de have en dataudvekslingsaftale med EU.

En barriere for dataudveksling kan opstå, hvis Kommissionen ikke anser databeskyttelsesniveauet i Storbritannien som tilstrækkeligt, eller hvis EU-Domstolen ved en eventuel sag kommer til samme konklusion. Nogle frygter, at en britisk aftale – ligesom den amerikanske Safe Harbour-aftale – i yderste konsekvens kan blive underkendt, hvorved der helt sættes en stopper for dataudvekslingen.

Med mange danske datterselskaber i Storbritannien er det i dansk interesse at sikre ens regler for databeskyttelse på tværs af kanalen efter Brexit. Det vil både være til gavn for den danske industri og for de danske forbrugere.

HOVEDKONKLUSIONER:

- Fælles regler for databeskyttelse er fundamentet for fri dataudveksling mellem virksomheder i EU.
- Skal virksomheder i Storbritannien – herunder op mod 800 danske datterselskaber – fortsat kunne udveksle data med resten af EU efter Brexit, skal briterne have samme høje databeskyttelsesstandarder. Her bliver det helt afgørende, hvilken aftale EU og Storbritannien forhandler på plads.
- Får Storbritannien en tilknytningsaftale, der ligner EU's aftale med Canada, er der frygt for, at databeskyttelsesniveauet i Storbritannien falder. Det kan betyde at digitale virksomheder vil vælge at placere sig i Storbritannien frem for resten af EU, og at datasikkerheden svækkes for forbrugere i Danmark og resten af EU.
- Hvis Storbritannien spekulerer i at udarbejde mere lempelige regler for databeskyttelse og på den baggrund få en dataudvekslingsaftale med EU kan det fragmentere det indre marked og skabe ulige konkurrence.
- Der er desuden risiko for, at dataudvekslingen mellem Storbritannien og EU helt stoppes, hvilket kan få endnu større økonomiske konsekvenser. Det kan blive tilfældet, hvis Storbritannien må forlade forhandlingerne helt uden en aftale, eller hvis en evt. aftale erklæres ugyldig af EU-Domstolen, ligesom det skete med den amerikanske Safe Harbour-aftale.
- Det er i dansk interesse at der sikres ens regler for databeskyttelse på tværs af kanalen efter Brexit. Det vil være det bedste scenarie for både dansk erhvervsliv og danske forbrugere.

Når Theresa May den 29. marts 2017 aktiverer artikel 50, starter de lange og komplekse forhandlinger mellem EU og Storbritannien om landets fortsatte tilknytning til EU. Her har især adgangen til det indre marked været et springende punkt for briterne, som ønsker fortsat at kunne handle frit med EU-landene. Men det indre marked kommer med en lang række regler om f.eks. fælles standarder. Ét af regelsættende drejer sig om fælles standarder for databeskyttelse, og er en grundsten for dataudvekslingen mellem EU-landene i det indre marked.

Da Storbritannien er et stort marked for it-sektoren, er dataudveksling et væsentligt element i Brexit-forhandlingerne. Alt efter hvilken aftale EU og Storbritannien kommer frem til, kan det få konsekvenser for danske virksomheder og forbrugere. Spørgsmålet er, om briterne vil implementere lempelige regler for databeskyttelse, og om det i så fald vil være i strid med reglerne for det indre marked? For dansk industri lempelige regler det betyde, at flere it-selskaber vælger at lægge deres virksomhed i Storbritannien. Samtidig kan lempeligere databeskyttelsesregler på den anden side af kanalen betyde, at danske forbrugeres data er dårligere beskyttet, når de udveksles med Storbritannien efter Brexit.

Storbritannien skal følge EU's databeskyttelsesregler

Når briterne træder ud af EU, mister de deres nuværende status som et sikkert land for persondataudveksling, fordi de ikke længere er en del af EU's regler på området. Det betyder, at der skal indgås en aftale, som tillader den fortsatte frie udveksling af data fra systemer og services mellem EU og Storbritannien. Det skyldes de nye regler for databeskyttelse i EU.

EU's nye persondataforordning (GDPR) indeholder nemlig et princip om en "long arm approach" til andre jurisdiktioner, som går ud på, at GDPR har eksterritorial effekt. Dvs., at enhver britisk virksomhed, der handler i EU, skal overholde GDPR, såfremt de behandler persondata om EU-borgere. Det gælder alle virksomheder, uanset hvor i verden de er placeret, såfremt de behandler EU-borgeres persondata eller overvåger aktiviteter, hvor disse indgår. Vil briterne fortsat have datadrevne virksomheder, som opererer i og handler med EU, skal de overholde GDPR.

Ikrafttrædelsen af GDPR i maj 2018 betyder dog, at Storbritannien vil være underlagt GDPR, indtil landet endeligt træder ud af EU. Der er imidlertid uvished om, hvorvidt Storbritannien vil ændre sine databeskyttelsesregler efter Brexit. Som den britiske informationskommissær, Elizabeth Denham, udtalte sidste år, kan der meget vel blive tale om et "start and stop regulatory environment".[1] Det vil

[1] Commissioner: UK 'must avoid data protection Brexit', BBC, 29. september 2016, http://www.bbc.com/news/technology-37512419.

dog være uhensigtsmæssigt for britiske virksomheder, men også for danske virksomheder med forretninger eller afdelinger i Storbritannien. Det vil nemlig skabe usikkerhed om virksomhedernes forpligtelser ift. databeskyttelse, når de sender data til Storbritannien. Landet er imidlertid førende når det gælder grænseoverskridende dataforbindelser, og stod for 11,5 pct. af den globale grænseoverskridende dataudveksling i 2015. Samtidig går 75 pct. af Storbritanniens dataudveksling til europæiske lande.[2] Det gælder også Danmark. I 2015 havde danske virksomheder 756 datterselskaber i Storbritannien.[3] Danske virksomheder deler i dag frit data med deres datterselskaber og samarbejdspartnere i Storbritannien på samme måde, som var hjemmehørende i Danmark. Danske virksomheder vil altså blive direkte påvirket af Storbritanniens kurs ift. databeskyttelse.

Derudover er Storbritannien et af de største markeder for *cloud services* i EU. Hver femte virksomhed i Europa benyttede sig i 2014 af *cloud services*, mens det gjaldt 38 pct. af danske virksomheder. Endelig er Storbritannien det land i Europa, hvor flest datacentre er placeret. Storbritannien huser 250 fælles location datacentre, hvor Tyskland, som har næst flest, kun har 184.[4] Konsekvenserne af et stop for dataudvekslingen mellem EU og Storbritannien kan således få betydning for Danmark såvel som resten af EU.

På grund af konsekvenserne for virksomhederne påpegede Elizabeth Denham vigtigheden af, at Storbritannien bibeholder et tilsvarende lovregime. Det kunne tyde på, at man er villig til at imødekomme den nye skærpede regulering i GDPR. Den britiske regering har ved en høring i House of Lords i februar understreget, at dens mål i forhandlingerne med EU er at sikre en uhindret dataudveksling mellem Storbritannien og EU.[5] Sammen med finanssektoren er it-sektoren noget af det, briterne satser mest på og lever af. Det er derfor en stor prioritet for den britiske regering, som ikke ønsker at sætte deres førerposition over styr ved at kappe forbindelsen til den digitale del af det indre marked.

Spørgsmålet er dog, om Storbritannien efter Brexit vil blive anset som havende et tilstrækkeligt beskyttelsesniveau til, at EU vil tillade udvekslingen af persondata. En del afhænger her af, hvilken form for aftale briterne får forhandlet på plads med EU, når forhandlingerne går i gang efter aktiveringen af artikel 50.

[2] The UK Digital Sectors After Brexit. An independent report commissioned by techUK, frontier economics, 24. januar 2017, s. 39.
[3] Tal fra Danmarks Statistik.
[4] Colocation Western Europa, Data Center Map, 2017, http://www.datacentermap.com/western-europe/.
[5] On data protectio nBrexit means mirroring EU rules, confirms UK Minister, techcrunch.com, 1. februar 2017, https://techcrunch.com/2017/02/01/on-data-protection-brexit-means-mirroring-eu-rules-confirms-uk-minister/.

En Canada-model skaber mest usikkerhed om databeskyttelse

Selvom EU og Storbritannien nu starter forhandlingerne om briternes udtræden af EU, er det usikkert, hvilken form for tilknytningsmodel man ender med. Det er derfor også svært at spå om, helt præcist hvordan situationen bliver på databeskyttelsesområdet, da det afhænger af den pågældende model. Ser man på de tilknytningsmodeller, som før har været nævnt i forbindelse med Brexit, kan der dog peges på tre scenarier.

For det første kan Storbritannien følge en vej som Den Europæiske Frihandelssammenslutning (EFTA) og forblive medlem af Det Europæiske Økonomiske Samarbejdsområde (EØS)[6] – den såkaldte Norge-model. Det vil betyde, at Storbritannien skal følge de restriktioner og regler, som EU vedtager. For Norge som er medlem af EØS, har det f.eks. betydet, at de har adopteret EU's regelgrundlag, som regulerer databeskyttelse. Ved en Norge-model kan briterne derfor ikke undgå at være underlagt GDPR, og der vil dermed ikke være usikkerheder for danske virksomheder, som handler med eller opererer i Storbritannien.

For det andet er der den schweiziske (og mere usandsynlige) model. Schweiz er ikke medlem af EØS, men kun af EFTA. Schweiz har derfor sine egne love og regler for beskyttelse af data, som er meget lig EU's nuværende regler. De har derfor adgang til det indre marked gennem bilaterale aftaler, som løbende opdateres. Disse regler er anerkendt og godkendt af Kommissionen ved en "tilstrækkelighedsbeslutning". Det betyder, at schweiziske virksomheder godt kan modtage og behandle persondata om EU-borgere, fordi Kommissionen har vurderet, at beskyttelsesniveauet i Schweiz er tilstrækkeligt. Storbritannien vil derfor efter den schweiziske model skulle indrette sin lovgivning sådan, at den kan leve op til GDPR. De kan dog herigennem bestemme deres egne regler, men skal ansøge om en "tilstrækkelighedsbeslutning" fra Kommissionen.

En tredje mulighed er, at Storbritannien indgår aftaler med EU uafhængigt eller igennem organisationer som WTO, som EU har gjort med Canada og USA. Særligt handelsaftalen med Canada har man fra britisk side skelet til som en mulig model for britisk tilknytning til EU efter Brexit. Med den model kan Storbritannien frit vælge hvilke regler og love, som de ønsker at implementere. Det gælder også for databeskyttelse. I både EU's aftale med Canada og med USA er databeskyttelse et element. Problemet med den model er imidlertid, at briterne risikerer en situation som den, USA havde med den nu ugyldige EU-USA Safe Harbour-aftale.

[6] Storbritannien er på nuværende tidspunkt medlem af EØS i kraft af sit EU-medlemskab.

Safe Harbour-aftalen med USA blev kendt ugyldig af EU-Domstolen i Schrems-sagen i oktober 2015, hvor en 28-årig jurastuderende fra Østrig vandt en sag imod Facebook for ikke at give sine europæiske brugere den grad af beskyttelse, som der kræves under EU-retten.[7] Samtidig konkluderede domstolen, at aftalen ikke formåede at sikre EU-borgeres data mod regeringsinstitutioners adgang til data, i f.eks. efterretningsarbejde. Kommissionens nye aftale med USA, Privacy Shield var tænkt som en forbedret udgave af Safe Harbour, men blev allerede inden sin vedtagelse kritiseret for ikke at forbedre datasikkerheden for EU-borgere.[8]

Alt efter hvordan aftalen mellem EU og Storbritannien ender, kan det få konsekvenser for virksomheder i Storbritannien, som potentielt risikerer, at dataudvekslingen mellem EU og Storbritannien sættes på standby, mens en aftale forhandles på plads. Erfaringerne fra USA tyder på, at sådanne forhandlinger kan tage lang tid. Det er her uvist, hvad vil der ske med dataudvekslingen i mellemtiden. Man kan dog formode, at Storbritannien i den situation ville følge retningslinjerne i GDPR.

Kommer Storbritannien og EU frem til en aftale, som betyder, at briterne selv kan bestemme deres databeskyttelsesregler (dvs. Schweiz- eller Canada-modellen), kan det potentielt skabe usikkerhed for danske virksomheder og forbrugere.

Dansk industri ønsker fælles regler på tværs af kanalen

En fremtid med forskellige britiske og europæiske regler for databeskyttelse er en konkret bekymring hos danske virksomheder. Stabiliteten i dataudvekslingen er vigtig for mange sektorer – fra finansielle ydelser til teknologi, it og energi. På nuværende tidspunkt støtter EU-regler dataudvekslingen mellem medlemslandene via fælles standarder og regler, som sikrer lige rettigheder for alle EU-borgere og specificerer fælles forpligtelser for virksomheder, når de behandler og udveksler data. Med forskellige regler risikerer man, at der opstår en barriere for dataudvekslingen fra EU's medlemslande til Storbritannien eller en ulige konkurrence.

Et scenarie med en barriere for dataudveksling kan opstå, hvis Kommissionen ikke finder, at databeskyttelsesniveauet i Storbritannien er tilstrækkeligt, eller hvis EU-Domstolen ved en eventuel sag kommer til samme konklusion. En række britiske kommentatorer frygter, at den nyligt vedtagede britiske Investigatory Powers Act kan betyde, at Kommissionen vil være særdeles forbeholden over for at godtage

[7] Dom i sag C-362-14, Maximillian Schrems v. Data Protection Commissioner, EU-Domstolen, 6. oktober 2015.
[8] Se f.eks. brev til Ms. Isabelle Falque-Pierrotin Chairman, Article 29 Working Party, MEP Claude Moraes Chair of the Committee on Civil Liberties, Justice, and Home Affairs og HE Pieter de Gooijer Amabassador and Permanent Representative of the Netherlands to the EU, https://edri.org/wp-content/uploads/2016/03/PrivacyShield_Letter_Coalition_March2016.pdf.

beskyttelsesniveauet i Storbritannien.[9] Den nye britiske overvågningslov giver britiske regeringsinstitutioner vidtgående beføjelser til at få adgang til persondata i Storbritannien.[10] Risikoen er, at forhandlingerne om at modtage Kommissionens "tilstrækkelighedsbeslutning" kan tage lang tid og i mellemtiden bremse dataudvekslingen. Det vil skabe stor usikkerhed for virksomhederne.

Skabes der i sidste ende en barriere for udvekslingen af persondata mellem EU og Storbritannien kan det også få store økonomiske konsekvenser på tværs af kanalen. Et studie estimerer, at de økonomiske konsekvenser for EU som helhed vil være et fald i BNP på 0,4-1,1 pct., et fald i private investeringer på 3,95-1 pct. og et fald i tjenesteydelseseksporten på 1 pct.[11]

En ulige konkurrence kan på den anden side opstå, hvis Storbritannien spekulerer i at udarbejde mere lempelige regler for databeskyttelse og på den baggrund få en dataudvekslingsaftale med EU. Dog forudsat, at Kommissionen giver en "tilstrækkelighedsbeslutning". Så kan de potentielt få en GDPR-light model, hvor man gerne må udveksle data med Storbritannien, men hvor kravene til databehandling ikke er ligeså strenge. Det kan betyde, at it-selskaber eller data-dreven virksomheder vil foretrække at lægge deres datacentre og hovedkontorer i Storbritannien. Det kan trække virksomheder væk fra Danmark.

Derudover vil det med al sandsynlighed medføre en fragmentering af det indre marked, at Storbritannien har særskilte regler for databeskyttelse, hvis landet samtidig har adgang til det indre marked.

Danske forbrugeres data skal sikres efter Brexit

Ud fra et forbrugerperspektiv er lempeligere databeskyttelsesregler i Storbritannien efter Brexit en bekymring. Hvis virksomheder i stigende grad placerer deres datacentre i Storbritannien, hvor persondata er under ringere beskyttelse end i resten af EU, vil persondata om danske forbrugere være mere udsat. Erfaringerne fra aftalerne med Canada og USA viser, at det er svært at garantere det samme databeskyttelsesniveau uden for EU, når der udveksles data om EU-borgere. Og samtidig, at Kommissionen kan være villig til at acceptere lempeligere regler.

Da aftalen med Canada var under forhandling, var Forbrugerrådet Tænk kritisk over for aftalens forhold til databeskyttelse. I deres optik beskytter den ikke

[9] Brexit and data protection, Briefing Paper No. 7838, House of Commons, 15. december 2016, s. 11.
[10] The IP Act: UK's most extreme surveillance law, Aljazeera, 2. december 2016, http://www.aljazeera.com/indepth/opinion/2016/12/ip-act-uk-extreme-surveillance-law-161201141317587.html.
[11] The UK Digital Sectors After Brexit. An independent report commissioned by techUK, frontier economics, 24. januar 2017, s. 38.

forbrugerne tilstrækkeligt, når det kommer til virksomhedernes håndtering af data over grænserne.[12] Samme kritik blev rejst om Privacy Shield-aftalen, som af flere europæiske digitale rettighedsorganisationer blev kritiseret for at lempe databeskyttelseskravene. De mener, at EU-borgernes persondata og dermed deres ret til privatliv ikke er tilstrækkeligt beskyttet ved dataudveksling mellem EU og USA.[13]

Man bør derfor fra dansk side arbejde for at få en garanti fra briterne om, at der bibeholdes et højt databeskyttelsesniveau og skabes ens regler for databeskyttelse efter Brexit. Ud over at komme danske forbrugere til gode, vil det også være en fordel for dansk industri.

[12] Forbrugerråd: EU-aftale med Canada truer forbrugersikkerhed, Berlingske Business, 23. september 2016 (http://www.business.dk/global/forbrugerraad-eu-aftale-med-canada-truer-forbrugersikkerhed).
[13] Se f.eks. "Privacy Shield is the same unsafe harbour, EDRi, 29. februar 2016 (https://edri.org/privacy-shield-is-the-same-unsafe-harbour/).