DANSK ERHVERV
BØRSEN
DK-1217 KØBENHAVN K
WWW.DANSKERHVERV.DK

T. +45 3374 6000
F. +45 3374 6080
–
INFO@DANSKERHVERV.DK

Erhvervsstyrelsen
Att.: Jens Kasper Greven Rasmussen jekara@erst.dk og Mette Schiøtz Sørensen mescso@erst.dk

3. marts 2017

Dansk Erhvervs bemærkninger til høringen om Kommissionens meddelelse "Opbygning af en Europæisk dataøkonomi"

Generelle bemærkninger

Dansk Erhverv takker for muligheden for at kommentere på Kommissionens meddelelse "Opbygning af en Europæiske dataøkonomi".

Dansk Erhverv ser det som positivt, at Kommissionen med meddelelsen sætter fokus på vigtigheden af data i nutidens digitaliserede økonomi. Dansk Erhverv hilser det velkomment, at Kommissionen gennemfører høringen om disse komplekse emner, som vil have stor indflydelse på erhvervslivets fremtid. Vi havde dog gerne set, at Kommissionen ikke havde ventet med at fremsætte et lovforslag der skal sikre frie data strømme i EU.

Specifikke bemærkninger

Ad. Punkt 2 Free Flow of Data
Dansk Erhverv deler Kommissionens analyse om, at et effektivt og barrierefrit indre marked for data kan bidrage markant til vækst og beskæftigelse i EU, og underbygger den frie bevægelighed for services og friheden til at etablere sig. Vi er ligeledes enige i, at de databeskyttelseshensyn der tidligere har været ikke længere er aktuelle efter vedtagelsen af den nye databeskyttelsesforordning og NIS direktivet. I dag afhænger databeskyttelse ikke af hvor data opbevares, men hvordan.

Netop derfor er Dansk Erhverv bekymrede over, den udvikling vi har set imod flere og flere datalokaliseringskrav globalt og internt i EU[1]. Det er en ny form for "digital" protektionisme, som rammer små åbne økonomier som Danmark ekstra hårdt, og som fører til en suboptimal placering af datacentre. Det resulterer i højere priser på bl.a. cloud løsninger som særligt SMVer og start-ups benytter sig af, og skader miljøet, da der skal bruges meget energi på bl.a. nedkøling.

De seneste års store investeringer i datacentre i Danmark viser at Danmark ligger godt med i konkurrencen om at tiltrække disse milliard investeringer og de medfølgende arbejdspladser, men

[1] http://ecipe.org/publications/unleashing-internal-data-flows-in-the-eu/

denne attraktive position kan blive truet, hvis store medlemslande indfører flere lokaliseringskrav, som der i øjeblikket lægges op til i nogle lande.
Dansk Erhverv hilser derfor Kommissionens ide om at indføre et princip om frie data strømme i EU velkommen. Vi støtter fuld op om, at eventuelle undtagelser til dette princip skal kunne hjemles i Traktaten og skal være så begrænsede og klare som muligt.

Dansk Erhverv mener, at der hurtigst muligt er behov for en forordning der stadfæster princippet om frie data strømme i EU. Med en sådan forordning i hånden, vil det ligeledes blive nemmere for EU at argumenterer imod datalokalisering i tredjelande. Lokaliseringskrav fra tredjelande er et stigende problem og skader europæiske virksomheders muligheder for at konkurrere på globalt plan.

Adskillige krav til datalokalisering er allerede blevet identificeret af Kommissionen og europæiske erhvervsorganisationer. En række eksempler er listet i annex I, herunder den danske såkaldte Krigsregel. Et andet og lige så stort problem som de lovmæssige krav om datalokalisering er den opfattelse mange har af, at lokalisering kan bruges som en proxy for sikkerhed. Denne opfattelse er meget forkert, men sætter ikke desto mindre barrierer for at datainfrastrukturen i EU kan blive etableret mest optimalt.

Ad. Punkt 3 Adgang og overførsel
Dansk Erhverv finder spørgsmålene omkring adgang til data interessante og vigtige for udviklingen af en dataøkonomi med mange forskellige aktører.
Dansk Erhverv er som udgangspunkt positiv overfor "genbrug" af data, dog skal dette ske på en afbalanceret måde, så de virksomheder der har investeret i algoritmer, systemer, databaser etc. bliver belønnet for deres investering og ikke bliver tvunget til at afsløre forretningshemmeligheder eller kompromittere beskyttelse af ophavsrettigheder. Det er derudover vigtigt at eventuelle krav om adgang til data ikke er i strid med databeskyttelsesforordningen eller den kommende e-databeskyttelsesforordning.

Dansk Erhverv ser på nuværende tidspunkt ikke noget behov for at lave yderligere lovgivning på området. Det er svært at sige, hvordan den næste forretningsmodel vil se ud, og derfor er kontraktfriheden afgørende. De eksisterende kontraktregler rummer fleksibilitet og Dansk Erhverv ser ikke noget i vejen for, at disse regler kan håndtere kontrakter om data. Dansk Erhverv tager derfor afstand fra Kommissionens forslag om standard kontrakter, "producer's right" og fra forslaget om at offentlige myndigheder skal have adgang til data af almen interesse uden videre. Dette vil være en urimelig form for ekspropriation og fratage virksomheder incitament til at investere.

Kommissionen udpeger ligeledes ulige magtforhold mellem virksomheder i dataværdikæden som et problem. Dansk Erhverv anerkender, at der potentielt kan opstå problemer i denne sammenhæng, men mener ikke at lovgivning nødvendigvis er vejen frem. Frivillige initiativer og symbioser vokser i øjeblikket frem flere sted i EU, og mange store virksomheder ser det som essentielt

for deres konkurrencedygtighed og innovationsevne at samarbejde og dele data med start-ups og SMVer. Et eksempel på et sådant succesfuldt økosystem er "Platform Industrie 4.0" i Tyskland.

Derudover rummer konkurrencereglerne i dag muligheder for at bekæmpe problemer med ulige magtforhold, også når det kommer til data. Disse muligheder er dog endnu ikke udforsket eller udviklet tilstrækkeligt, og Dansk Erhverv opfordre til, at det undersøges nærmere, hvordan de eksisterende konkurrenceregler kan anvendes mere aktivt i sager om data. Et eksempel på et marked hvor der er opstået problemer pga. centralisering af data hos få udbydere er online hotelbooking. Problemstillingen er, at store globale bookingportaler praktisk taget i dag udgør et duopol på markedet for online hotelbookinger, hvilket har indflydelse på adgangen til kundedata. De enkelte hotellerne kan dermed ikke længere opnå et "ejerskab" og en tæt relation til deres kunder, idet de nu er afhængige af de store portaler for at nå ud til kunderne og for at få adgang til data om kunderne.

Dansk Erhverv støtter op om Kommissionens forslag om at understøtte de tekniske løsninger for data deling, f.eks. ved at støtte udviklingen og anvendelsen af APIer gennem tekniske guidelines og identificering af "best practices" både hos virksomheder og offentlige myndigheder.
Dansk Erhverv er heller ikke afvisende overfor, at Kommissionen udvikler ikke-bindende guidelines baseret på den eksisterende lovgivning, for at gøre det lettere for virksomhederne at forstå, hvordan de kan og må dele ikke-personfølsom data. Vi mener således, at det på nuværende tidspunkt er mere passende at øge virksomhedernes incitament til at dele data og udvikle de tekniske muligheder for at gøre det, fremfor at pålægge dem ufleksible regler.

Ad. Punkt 4 Ansvar
Overordnet set mener Dansk Erhverv ikke at der er behov for specifikke regler om IoT produkter, heller ikke angående ansvar. De eksisterende regler i Produktansvarsdirektivet omfatter IoT produkter, og vi ser ingen grund til, at det skal ændres. Mange IoT produkter og services afhænger af en kompleks værdikæde hvor ansvar placeres ved hjælp af kontrakter. Denne løsning giver klarhed for alle involverede og er fleksibel nok til at rumme den hurtige teknologiske udvikling.

Dansk Erhverv tager på denne baggrund afstand fra Kommissionens forslag om, at ansvar skal tilskrives "de markedsaktører der er bedst placeret til at undgå eller minimere risici", da det er meget uklart, hvad det i praksis vil betyde og hvilke kriterier, der vil blive brugt til at vurdere, hvem der bærer ansvaret. Den nuværende praksis med kontrakter er langt mere klar.

Ideen om forsikringsordninger er interessant, men Dansk Erhverv understreger, at en regel om obligatoriske forsikringsordninger på alle IoT produkter virker voldsomt disproportional. IoT produkter og services er meget forskellige, og det bør derfor være frivilligt og op til virksomhederne, om de ønsker at have forsikringsordninger for deres produkter eller services.

Ad Punkt 5 Portabilitet, interoperabilitet og standarder

Som nævnt under punkt 3 støtter Dansk Erhverv denne tilgang. Vi ønsker dog at lægge vægt på at standarder skal være industri-drevne, så det sikres at de ikke hæmmer innovationsmulighederne.

Ad. Punkt 6 Eksperimenter og test
Dansk Erhverv hilser CAD initiativet velkommen og så gerne, at der blev oprettet flere muligheder for at teste ny teknologi i "virkelige" omgivelser. Det er afgørende at foretage denne type af tests og eksperimenter i samarbejde med interessenterne, inden der træffes beslutninger om hvordan den europæiske dataøkonomi eventuelt skal reguleres.

Dansk Erhverv står til rådighed for uddybede kommentarer.

Med Venlig Hilsen

Katinka Clausdatter Worsøe
EU-Konsulent
Dansk Erhverv

Annex 1:

List of examples of current data localisation requirements in Europe[i]

MS	Act/Practice	Description
UK	Companies Act 2006 - Art. 388	*According to the Companies Act 2006, "if accounting records are kept at a place outside the UK, accounts and returns (...) must be sent to, and kept at, a place in the UK, and must at all times be open to such inspection".*
UK	NHS information governance rules	*In the UK, there are no legal prohibitions on exporting NHS patient data outside the country. However, the NHS and associated institutions are bound by strong legal, ethical and regulatory obligations of confidentiality. The location outside the UK of the data recipient is considered a risk factor by the NHS information governance rules and therefore might result in data localisation.*
SW	Local storage requirement	*The Financial Services Authority requires 'immediate' access to data in its market supervision which, according to business, the supervisory body interprets as been given physical access to servers. Accordingly, Swedish financial services providers are de facto required to maintain all their records inside Swedish jurisdiction.*
SW	Local storage requirement	*In relation to specific government authorities, there are certain provisions which might require the data processed by the authority to be held within SW or within the authority. This might affect the supply of cloud computing to public authorities.*
SW	Swedish Accounting Act (BokfÃringslag (1999:1078))	*In SW, documents such as a company's annual reports, balance sheets and annual financial reports must be physically stored in SW for a period of 7 years.*
LUX	Circ. CSSF 12/552 as amended by Circs. CSSF 13/563 and 14/597	*According to Circular CSFF 12/552, financial institutions in Luxembourg are required to process their data within the country. Processing abroad is exceptionally permitted for an entity of the group to which the institution belongs or with explicit consent.*
DK	Consolidated Act No. 528/2000 as changed by Act No. 201/2001 (Executive Order on Security)	*Since 2011, the Danish DPA has ruled in several cases against processing of local authorities' data in third countries without using standard contractual clauses. This is the result of a strict interpretation of the European Directive 95/46/EC. Therefore, services such as Dropbox, Google Apps and Microsoft's Office 365 cannot be used by local authorities unless they have signed an agreement with the processor based on standard contractual clauses.*
SI	Slovenian Personal Data Protection Act	*In Slovenia, transfers of personal data to non-EEA and non-whitelist countries require the approval of the Commissioner. The approval is issued if the Commissioner establishes that a sufficient level of protection is ensured for the transferring of personal data respectively for the data subjects to which this data relates.*
RO	Data protection Law	*In Romania, any outbound transfer of personal data requires prior notification to the National DPA. Moreover, any transfer of personal data to a recipient state not offering an adequate level of protection needs prior approval.*

RO	Law no. 124/2015, approval of GVT Emergency Ordinance no. 92/2014 regulating fiscal measures	*In Romania, the game server must store all data related to remote gambling services provision, including records and identification of players, stakes placed and winnings. Information must be stored using data storage equipment situated in Romania.*
PT	Data protection law	*In Portugal, all transfer of data outside the EU must be notified and authorized by the relevant Commission, except when directed to whitelisted countries or when using model contract. In 2015 the Portuguese DPA also issued specific guidelines on Intra-Group Agreements ("IGA") involving personal data transfers to non-EEA countries. The DPA considers that such transfers depend on its prior authorisation for the purposes of assessing if IGAs contain sufficient guarantees that the personal data transferred continues to benefit from the same level of protection as in the EEA countries.*
PL	Polish Gambling Act	*According to the Polish Gambling Act, any entity organizing gambling activities is obliged to archive in real time all data exchanged between such entity and the users in an archive device located in Poland.* *Another restriction is the requirement that the equipment (servers) for processing and storing information and data regarding the bets and their participants must be installed and kept on the territory of a member state of the EU or EFTA.*
NL	Public Records Act	*Localisation requirements apply to public records that have to be stored in archives in specific locations in the Netherlands. This applies both to paper and electronic records.*
IT	Presidential Decree No. 633 of 1972	*Article 39 of the Presidential Decree no. 633 of 1972 states state electric archives related to accounting data for VAT declarations might be kept in a foreign country only if some kind of convention has been concluded between Italy and the receiving country governing the exchange of information in the field of direct taxation. Therefore, such limitation does not apply intra-EU.*
GR	National law 3917/2011	*In Greece, the Law No. 3971/2011 goes further in the implementation of the Data Retention Directive (later annulled by the European Court of Justice) by requiring that retained data on traffic and localisation stay within the premises of the Hellenic territory. The Law is still in force.*
DE	German Telecommunications Act, as amended in December 2015	*In October 2015 Germany adopted a new data retention law (entering into force in 2017), replacing the previous law implementing the Data Retention Directive that was declared invalid by the EUCJ In 2014. The new law provides that telecoms providers must retain data such as phone numbers, the time and place of communication (except for emails), and the IP addresses for either 4 or 10 weeks. The data is to be stored in servers located within Germany (Â§113b).*
DE	German Commercial Code – Sect. 257 No. 1, 4 - (Handelsgesetzbuch Â§ 257)	*According to the German Commercial Code, accounting documents and business letters must be stored in Germany.*
DE	Tax Code - Section 146(2) (Abgabenordnung)	*Under the Tax Code, all persons and companies liable to pay taxes that are obliged to keep books and records must keep those records in Germany. There are some exceptions for multinational companies.*

DE	VAT Act - Section 14b (Umsatzsteuergesetz, UStG)	*The Act on Value Added Tax states that invoices must be stored within the country, including when stored electronically. Alternatively, in case of electric storage, they may be stored within the territory of the EU if full online access and the possibility of download are guaranteed. In this case, the entity is obliged to notify the competent tax authority in writing of the location of the electronically stored invoices, and the tax authority may access and download the data.*
DE	Ban to transfer	*There is no European prohibition of data transfer, neither has any EU Member State implemented a national prohibition of data transfer. However, the data protection authority (DPA) at the German federal state of Schleswig Holstein has declared in a position paper that all data protection instruments for the transfer of data to the US after the EUCJ Schrems v Facebook judgment are going to be illegal. The DPA it has not taken any action in this regard, but has threatened to do so.*
FR	Decree 2012-436 amending Electronic Comms Code	*Through a decree amending the Code of Electronic Communications, France has included a territorial restriction requiring that the systems for interception of electronic communications must be established in France.*
FR	Ministerial circular on cloud computing 5 April 2016	*On public procurement states that it is illegal to use a non-"sovereign" cloud for data produced by public (national and local) administration: all data from public administrations have to be considered as archives and therefore stored and processed in France.*
FIN	Accounting Act (1336/1997)	*The Accounting Act requires that a copy of the accounting records in kept within Finland. Alternatively, the records can be stored in another EU country if a real-time connection to the data is guaranteed.*
BG	Gambling Act	*In Bulgaria, an applicant for a gaming license must assure that all data related to operations in Bulgaria is stored on a server located in the territory of Bulgaria. Moreover, the applicant has to assure that the communication equipment and the central computer system of the organizer are located within the EEA or in Switzerland.*

[i] The Digital Trade Estimates (DTE) database, European Centre for International Political Economy (ECIPE)