EUROPEISKA
KOMMISSIONEN

Bryssel den 13.9.2017
COM(2017) 495 final

2017/0228 (COD)

Förslag till

EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING

om en ram för det fria flödet av icke-personuppgifter i Europeiska unionen

{SWD(2017) 304 final}
{SWD(2017) 305 final}

MOTIVERING

1. BAKGRUND TILL FÖRSLAGET

• Motiv och syfte med förslaget

Ny digital teknik, exempelvis molntjänster, stordata, artificiell intelligens och sakernas internet (*Internet of Things*, IoT), är utformad för att maximera effektiviteten, möjliggöra stordriftsfördelar och utveckla nya tjänster. Den erbjuder fördelar för användarna, såsom smidighet, produktivitet, snabbare användning och autonomi, *t.ex.* genom maskininlärning[1].

Som framgår av 2017 års meddelande ”Att skapa en europeisk dataekonomi”[2] uppskattades värdet av EU:s datamarknad 2016 till nästan 60 miljarder euro, vilket är en ökning med 9,5 % jämfört med 2015. Enligt en studie skulle EU:s marknad kunna uppgå till mer än 106 miljarder euro 2020[3].

För att frigöra denna potential syftar förslaget till att ta itu med följande frågor:

- Förbättra rörligheten för icke-personuppgifter över gränserna på den inre marknaden, vilken är begränsad i dag i många medlemsstater genom lokaliseringsbegränsningar eller rättslig osäkerhet på marknaden.
- Säkerställa att de behöriga myndigheternas befogenhet att begära och få tillgång till information för reglerings- och tillsynsändamål, t.ex. för inspektion och verifiering, inte påverkas, och
- Göra det lättare för yrkesmässiga användare av datalagring eller andra databehandlingstjänster att byta tjänsteleverantör och att portera data, samtidigt som man inte skapar en alltför stor börda för tjänsteleverantörerna eller snedvrider marknaden.

I halvtidsöversynen om genomförandet av strategin för den digitala inre marknaden[4] meddelades ett lagstiftningsförslag om ett samarbete kring fritt flöde i EU av data.

Det allmänna politiska målet med initiativet är att skapa en mer konkurrenskraftig och integrerad inre marknad för datalagring och andra databehandlingstjänster och databehandlingsverksamheter genom att ta itu med ovannämnda områden. I detta förslag används datalagring och annan databehandling i vid bemärkelse, och omfattar användning av alla typer av it-system, oavsett om de finns i användarens lokaler, eller är utkontrakterade till en leverantör av datalagrings- eller andra databehandlingstjänster[5].

• Förenlighet med befintliga bestämmelser inom området

Förslaget bidrar till att uppfylla de mål som anges i strategin för den digitala inre marknaden[6], i dess nyligen genomförda halvtidsöversyn, samt i de politiska riktlinjerna för den nuvarande

---

1 Maskininlärning är en tillämpning av artificiell intelligens (AI) som gör det möjligt för systemen att automatiskt lära sig och förbättras av erfarenheter utan att uttryckligen programmeras.

2 COM(2017) 9, ”Att skapa en europeisk dataekonomi”, den 10 januari 2017. Se även kommissionens arbetsdokument som åtföljer meddelandet SWD (2017) 2 av den 10 januari 2017.

3 IDC and Open Evidence, European Data Market, Final Report, 1 februari 2017 (SMART 2013/0063).

4 Meddelande från kommissionen som antogs den 10 maj 2017 (COM(2017) 228 final).

5 Andra databehandlingstjänster inbegriper leverantörer av databaserade tjänster såsom dataanalys, förvaltningssystemen osv.

6 COM/2015/0192 final.

kommissionen ”En ny start för EU: Mitt program för sysselsättning, tillväxt, rättvisa och demokratisk förändring”[7].

Detta förslag är inriktat på tillhandahållandet av datavärdskap (lagring) och andra databehandlingstjänster, och är förenligt **med befintliga rättsliga instrument**. Initiativet syftar till att skapa en effektiv inre europeisk marknad för sådana tjänster. Därmed är det i linje med **e-handelsdirektivet**[8], som syftar till en heltäckande och effektiv inre europeisk marknad för bredare kategorier av informationssamhällets tjänster, och med tjänstedirektivet[9], som främjar en fördjupning av EU:s inre marknad för tjänster inom ett flertal sektorer.

Ett antal relevanta sektorer undantas uttryckligen från tillämpningsområdet för denna lagstiftning (dvs. e-handels- och tjänstedirektiven), så att endast de allmänna bestämmelserna i fördraget skulle vara tillämpliga för allt datavärdskap (lagring) och andra databehandlingstjänster. De befintliga hindren för dessa tjänster kan emellertid inte avlägsnas på ett effektivt sätt endast genom att förlita sig på en direkt tillämpning av artiklarna 49 och 56 i fördraget om Europeiska unionens funktionssätt (EUF-fördraget). Skälet till det är för det första att det skulle bli ytterst svårt för de nationella institutionerna och unionens institutioner att ta itu med de hindren från fall till fall genom överträdelseförfaranden mot de berörda medlemsstaterna. För det andra skulle det krävas särskilda regler för att ta itu med såväl offentliga som privata hinder och fordras ett administrativt samarbete, för att undanröja många av hindren. Dessutom verkar den ökade rättssäkerheten vara särskilt viktigt för användare av ny teknik[10].

Eftersom detta förslag gäller elektroniska uppgifter förutom personuppgifter, påverkar det inte unionens rättsliga ram för dataskydd, särskilt förordning nr 2016/679 (den allmänna dataskyddsförordningen)[11], direktiv 2016/680 (polisdirektivet)[12] och direktiv 2002/58/EG (direktivet om integritet och elektronisk kommunikation)[13], som säkerställer en hög skyddsnivå för personuppgifter och det fria flödet av sådana uppgifter inom unionen. Tillsammans med den ovannämnda rättsliga ramen syftar förslaget till att införa en övergripande och samstämmig EU-ram för att möjliggöra fri rörlighet för data på den inre marknaden.

---

7 Inledningsanförande vid Europaparlamentets plenarsammanträde, Strasbourg den 22 oktober 2014

8 Europaparlamentets och rådets direktiv 2000/31/EG av den 8 juni 2000 om vissa rättsliga aspekter på informationssamhällets tjänster, särskilt elektronisk handel, på den inre marknaden (”Direktiv om elektronisk handel”) (EGT L 178, 17.7.2000, s. 1).

9 Europaparlamentets och rådets direktiv 2006/123/EG av den 12 december 2006 om tjänster på den inre marknaden (EUT L 376, 27.12.2006, s. 36).

10 LE Europe Study (SMART 2015/0016) och IDC Study (SMART 2013/0063).

11 Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning) (EUT L 119, 4.5.2016, s. 1).

12 Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF (EUT L 119, 4.5.2016, s. 89).

13 Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (EGT L 201, 31.7.2002, s. 37).

Förslaget kommer att kräva anmälan av förslag till åtgärder avseende datalokalisering enligt öppenhetsdirektivet (2015/1535)[14] för att möjliggöra en bedömning av huruvida dessa lokaliseringsbegränsningar är motiverade.

När det gäller samarbete och ömsesidigt stöd mellan behöriga myndigheter föreslås det i förslaget att alla sådana mekanismer bör tillämpas. Om inga samarbetsmekanismer finns införs genom förslaget åtgärder som syftar till att möjliggöra för behöriga myndigheter att utbyta och få tillgång till uppgifter som lagras eller på annat sätt behandlas i andra medlemsstater.

- **Förenlighet med unionens politik inom andra områden**

Mot bakgrund av den digitala inre marknaden syftar detta initiativ till att minska hindren för en konkurrenskraftig datadriven ekonomi i Europa. I överensstämmelse med meddelandet om översynen efter halva tiden av den digitala inre marknaden undersöker kommissionen separat frågor som rör tillgång och vidareutnyttjande av offentliga och offentligt finansierade uppgifter och privatägda uppgifter som är av allmänt intresse och ansvar i händelse av skador orsakade av dataintensiva produkter[15].

De politiska åtgärderna bygger också vidare på **Digitalisering av den europeiska industrin** det politiska paket som inbegrep det **europeiska initiativet för molnbaserade tjänster**[16] som syftar till att bygga upp en molnbaserad lösning med hög kapacitet för lagring, delning och vidareutnyttjande av vetenskapliga data. Dessutom bygger initiativet på en översyn av **det europeiska ramverket för interoperabilitet**[17], som syftar till att förbättra det digitala samarbetet mellan offentliga förvaltningar i Europa, och det kommer att ha direkt nytta av det fria flödet av uppgifter. Det bidrar till EU:s engagemang för ett **öppet internet**[18].

2. RÄTTSLIG GRUND, SUBSIDIARITETSPRINCIPEN OCH PROPORTIONALITETSPRINCIPEN

- **Rättslig grund**

Förslaget ingår i ett område där delad befogenhet gäller i enlighet med artikel 4.2 a i fördraget om Europeiska unionens funktionssätt (EUF-fördraget). Syftet är att uppnå en mer konkurrenskraftig och integrerad inre marknad för datalagring och andra databehandlingstjänster genom att garantera det fria flödet av uppgifter inom unionen. I förslaget fastställs bestämmelser om krav på datalokalisering, tillgången till uppgifter för behöriga myndigheter och dataportering för yrkesmässiga användare. Förslaget grundar sig på artikel 114 i EUF-fördraget som är den allmänna rättsliga grunden för att anta sådana regler.

- **Subsidiaritetsprincipen**

Förslaget är förenligt med subsidiaritetsprincipen i artikel 5 i fördraget om Europeiska unionen. Syftet med detta förslag är att säkerställa en väl fungerande inre marknad för dessa tjänster, som inte är begränsad till en enda medlemsstats territorium och det fria flödet av

---

[14] Europaparlamentets och rådets direktiv (EU) 2015/1535 av den 9 september 2015 om ett informationsförfarande beträffande tekniska föreskrifter och beträffande föreskrifter för informationssamhällets tjänster (EUT L 241, 17.9.2015, s. 1).

[15] COM(2017) 228 final.

[16] COM(2016) 178 final, ”Europeiskt initiativ för molnbaserade tjänster – Att skapa en konkurrenskraftig data- och kunskapsekonomi i Europa”, 19 april 2016

[17] COM(2017) 134 final, ”Europeiska interoperabilitetsramen – genomförandestrategi”, 23 mars 2017

[18] COM(2014) 72 final, ”Internetpolitik och förvaltning av internet – Europas roll i utformningen av framtidens internetförvaltning”, http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM:2014:0072:FIN

icke-personuppgifter inom unionen kan inte uppnås av medlemsstaterna på nationell nivå, eftersom huvudproblemet är gränsöverskridande datarörlighet.

Medlemsstaterna kan minska antalet och omfattningen av deras egna datalokaliseringsbegränsningar, men de kommer troligen att göra det i olika utsträckning och på olika villkor, eller inte alls.

Olika metoder skulle emellertid leda till att för många lagstadgade krav i EU:s inre marknad och konkreta extra kostnader för företag, särskilt små och medelstora företag.

- **Proportionalitetsprincipen**

Förslaget är förenligt med proportionalitetsprincipen enligt artikel 5 i EU-fördraget eftersom det består av ett effektivt regelverk som inte går utöver vad som är nödvändigt för att lösa de problem som konstaterats och är proportionerligt för att uppnå sina mål.

I syfte att avlägsna hindren för det fria flödet av icke-personuppgifter inom unionen som begränsas av lokaliseringskrav och att öka förtroendet för gränsöverskridande dataflöden och datalagring och andra databehandlingstjänster kommer förslaget i hög grad att bygga på EU:s befintliga instrument och ramar: öppenhetsdirektivet för anmälan av förslag till åtgärder om krav på datalokalisering, olika ramar som säkrar tillgången till uppgifter för reglering och tillsyn av medlemsstaterna. Det är bara om det saknas andra samarbetsmekanismer, och när andra former av kontakt har uttömts, som samarbetsmekanismen i förslaget kommer att användas för att hantera frågor som rör tillgänglighet för data för nationella behöriga myndigheter.

I det föreslagna tillvägagångssättet för flödet av uppgifter mellan medlemsstaternas gränser och mellan olika tjänsteleverantörer/interna it-system eftersträvas en balans mellan EU:s lagstiftning och allmänna säkerhetsintressen i medlemsstaterna samt en balans mellan reglering och självreglering av marknaden.

För att lindra svårigheterna för yrkesmässiga användare att byta tjänsteleverantör och portera data, uppmuntrar initiativet till självreglering genom uppförandekoder om uppgifter som ska lämnas till användarna av datalagring eller andra databehandlingstjänster. Även villkoren för byte och portering bör hanteras genom självreglering för att fastställa bästa praxis.

I förslaget påminns det om att säkerhetskrav som införs genom nationell rätt och unionsrätten också ska säkerställas när fysiska eller juridiska personer utkontrakterar sina uppgifter, lagring eller andra behandlingstjänster, även i en annan medlemsstat. I förslaget påminns också om de genomförandebefogenheter som kommissionen tilldelas genom direktivet om nät- och informationssäkerhet för att åtgärda säkerhetsproblemen, vilket också bidrar till denna förordnings verkan. Även om det i förslaget skulle krävas åtgärder från de offentliga myndigheterna i medlemsstaterna till följd av anmälnings-/granskningskrav, kraven på insyn och det administrativa samarbetet är förslaget utformat för att minimera sådana åtgärder till de viktigaste samarbetsbehoven och därmed undvika onödiga administrativa bördor.

Genom att upprätta en tydlig ram tillsammans med samarbete mellan och med medlemsstaterna, samt genom självreglering, syftar förslaget till att förbättra rättssäkerheten och öka förtroendet, samtidigt som det är fortsatt relevant och effektivt på lång sikt på grund av flexibiliteten i den samarbetsram som bygger på de gemensamma kontaktpunkterna i medlemsstaterna.

Kommissionen avser att inrätta en expertgrupp som ska ge råd i frågor som omfattas av denna förordning.

- **Val av instrument**

Kommissionen lägger fram ett förslag till en förordning som kan säkerställa att enhetliga regler om det fria dataflödet av icke-personuppgifter är tillämpliga inom hela unionen vid samma tidpunkt. Detta är särskilt viktigt för att avlägsna befintliga hinder och förhindra att nya kommer att införas av medlemsstaterna, för att garantera rättssäkerheten för de berörda tjänsteleverantörerna och användarna och därmed öka förtroendet för gränsöverskridande dataflöden samt datalagring och andra databehandlingstjänster.

3. RESULTAT AV EFTERHANDSUTVÄRDERINGAR, SAMRÅD MED BERÖRDA PARTER OCH KONSEKVENSBEDÖMNINGAR

- **Samråd med berörda parter**

Under den **första omgången av uppgiftsinsamling** genomfördes 2015 ett **offentligt samråd** om regelverket för plattformar, mellanhänder på internet, data och molntjänster samt delningsekonomi. Två tredjedelar av de svarande – jämt fördelat över alla intressentgrupper, inklusive de små och medelstora företagen – ansåg att begränsningarna av datalokalisering har påverkat deras affärsstrategi[19]. Annan uppgiftsinsamling skedde i form av möten och evenemang, riktade workshopar med viktiga intressenter (t.ex. *Cloud Select Industry Group*) och särskilda workshoppar inom ramen för studier.

En **andra omgång av uppgiftsinsamling**, från slutet av 2016 till andra halvåret 2017, omfattade ett **offentligt samråd som inleddes i samband med kommissionens meddelande ”Att skapa en europeisk dataekonomi”** den 10 januari 2017. Enligt svaren på det offentliga samrådet ansåg 61,9 % av intressenterna att begränsningarna för datalokalisering borde avskaffas. En majoritet av intressenterna (55,3 % av de svarande) ansåg att lagstiftningsåtgärder är det lämpligaste instrumentet för att ta itu med oberättigade begränsningar för lokalisering, och vissa av dem efterfrågade uttryckligen en förordning[20]. Stödet för lagstiftningsåtgärder är störst bland it-tjänsteleverantörerna, såväl stora som små, inom och utanför EU. En del av intressenterna konstaterade även negativa effekter med restriktioner för datalokalisering. Förutom att de leder till ökade kostnader för företagen påverkar de tillhandahållandet av en tjänst till privata eller offentliga parter (69,6 % av de deltagande intressenterna identifierade denna negativa effekt som ”stor”) eller möjligheten att ta sig in på en ny marknad (73,9 % av de svarande intressenterna identifierade denna negativa effekt som ”stor”). Intressenternas svar hade en snarlik procentuell fördelning, oavsett deras bakgrund. Det framgick också av det offentliga samrådet på internet att problemet med att byta tjänsteleverantör är utbrett: 56,8 % av de svarande små och medelstora företagen uppgav att de hade stött på svårigheter när de vill byta leverantör.

Mötena med medlemsstaterna inom ramen för den strukturerade dialogen underlättade en samsyn om utmaningarna. 16 medlemsstater har uttryckligen efterfrågat ett lagstiftningsförslag i ett brev till ordförande Donald Tusk.

En rad påpekanden från medlemsstaterna och näringslivet betraktas i förslaget, särskilt behovet av en övergripande princip om fri rörlighet för uppgifter för att skapa rättssäkerhet,

---

19 Ytterligare ekonomiska uppgifter inhämtades genom en undersökning av de ekonomiska effekterna av molntjänster i Europa (SMART 2014/0031, Deloitte, *Measuring the economic impact of cloud computing in Europe*”, 2016).

20 Denna flervalsfråga i det offentliga samrådet besvarades av 289 intressenter. De svarande ombads inte besvara vilken *typ* av lagstiftningsåtgärd de önskade, men 12 intressenter utnyttjade möjligheten att på eget initiativ uttryckligen efterfråga en förordning i en skriftlig kommentar. Denna intressentgrupp var heterogen och bestod av 2 medlemsstater, 3 näringslivsorganisationer, 6 it-tjänsteleverantörer och en advokatbyrå.

framsteg när det gäller tillgången till data för regleringsändamål, att göra det lättare för yrkesmässiga användare att byta leverantör av datalagring eller andra databehandlingstjänster och portering av data genom att uppmuntra till ökad öppenhet i de tillämpliga förfarandena och villkoren i avtalen, utan att införa särskilda standarder eller krav på tjänsteleverantörerna i det här skedet.

- **Insamling och användning av sakkunnigutlåtanden**

Rättsliga och ekonomiska studier har använts för att belysa olika aspekter av datarörlighet, inbegripet krav på datalokalisering[21], byte av leverantör/dataportering[22] och datasäkerhet[23]. Ytterligare undersökningar har beställts om konsekvenserna av molntjänster[24] och spridningen av molntjänster[25], samt om den europeiska datamarknaden[26]. Studier har också genomförts av sam- eller självregleringsåtgärder i sektorn för molntjänster[27]. Kommissionen har även grundat sig på andra externa källor, bl.a. marknadsöversyner och marknadsstatistik (t.ex. Eurostat).

- **Konsekvensbedömning**

En konsekvensbedömning har genomförts för detta förslag. Följande uppsättning alternativ beaktades i konsekvensbedömningen: Ett grundscenario (inga åtgärder) och tre alternativ. Alternativ 1 utgjordes av riktlinjer och/eller självreglering för att ta itu med de identifierade problemen och den därpå följande skärpningen av verkställighetsbefogenheterna i fråga om olika kategorier av oberättigade eller oproportionerliga hinder för datalokalisering som införs av medlemsstaterna. Alternativ 2 består i att fastställa rättsliga principer för de olika problem som ringats in och innebär att medlemsstaterna ska utse gemensamma kontaktpunkter och inrätta en expertgrupp, för att diskutera gemensamma strategier och praxis samt ge vägledning om de principer som införts enligt det här alternativet. Ett underalternativ 2a övervägdes också för att man skulle kunna bedöma en kombination av lagstiftning bestående av ramen för det fria flödet av uppgifter, de gemensamma kontaktpunkterna och en expertgrupp, samt självregleringsåtgärder rörande dataportering. Alternativ 3 utgörs av ett detaljerat lagstiftningsinitiativ för att fastställa bl.a. fördefinierade (harmoniserade) bedömningskriterier för vad som utgör (o)berättigade och (o)proportionella restriktioner för datalokalisering och en ny rättighet om dataportering.

Den 28 september 2016 avgav nämnden för lagstiftningskontroll sitt första yttrande om konsekvensanalysen, och den begärde att en omarbetad konsekvensbedömning lades fram.

---

[21] SMART 2015/0054, TimeLex, Spark and Tech4i, ”Cross-border Data Flow in the Digital Single Market: Study on Data Location Restrictions”, D5. Final Report (pågående) [TimeLex Study (SMART 2015/0054)]; SMART 2015/0016, London Economics Europe, Carsa and CharlesRussellSpeechlys, ”Facilitating cross border data flow in the Digital Single Market”, 2016 (pågående) [LE Europe Study (SMART 2015/0016)].

[22] SMART 2016/0032, IDC and Arthur's Legal, ”Switching between Cloud Service Providers”, 2017 (pågående) [IDC and Arthur's Legal Study (SMART 2016/0032)].

[23] SMART 2016/0029 (pågående), Tecnalia, ”Certification Schemes for Cloud Computing”, D6.1 Inception Report.

[24] SMART 2014/0031, Deloitte, “Measuring the economic impact of cloud computing in Europe”, 2016 [Deloitte Study (SMART 2014/0031)].

[25] SMART 2013/43, IDC, ”Uptake of Cloud in Europe. Follow-up of IDC Study on Quantitative estimates of the demand for Cloud computing in Europe and the likely barriers to take-up ”, 2014. Tillgänglig på följande länk: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=9742; SMART 2011/0045, IDC, ”Quantitative Estimates of the Demand for Cloud Computing in Europe and the Likely Barriers to Uptake” (juli 2012).

[26] SMART 2013/0063, IDC and Open Evidence, ”European Data Market. Data ownership and Access to Data - Key Emerging Issues”, 1 februari 2017 [IDC Study (SMART 2013/0063)].

[27] SMART 2015/0018, TimeLex, Spark, ”Clarification of Applicable Legal Framework for Full, Co- or Self-Regulatory Actions in the Cloud Computing Sector” (pågående).

Den ändrades därefter och lades fram på nytt till nämnden för lagstiftningskontroll den 11 augusti 2017. I sitt andra yttrandet noterade nämnden för lagstiftningskontroll den utvidgning av tillämpningsområdet som skett till följd av kommissionens meddelande (2017) 9 ”Att skapa en europeisk dataekonomi”, samt det ytterligare materialet om intressenternas synpunkter och om bristerna hos den nuvarande ramen. Nämnden avgav ett andra negativt yttrande den 25 augusti 2017, där den i synnerhet noterade bristande belägg för att det behövs en ny rättighet om molntjänstportabilitet. I enlighet med operativ praxis betraktade nämnden yttrandet som slutligt.

Kommissionen ansåg att det var lämpligt att lägga fram ett förslag och samtidigt ytterligare förbättra sin bedömning av konsekvensanalysen genom att ta vederbörlig hänsyn till synpunkterna i det andra yttrandet från nämnden för lagstiftningskontroll. Räckvidden hos förslaget är begränsad till fritt flöde av icke-personuppgifter i Europeiska unionen. I enlighet med nämndens konstaterande att beläggen tycks peka mot ett mindre strängt alternativ i fråga om dataportering har man övergett det rekommenderade alternativ som ursprungligen föreslogs i konsekvensanalysen om en skyldighet för leverantörerna att underlätta byte eller portering av användarnas uppgifter. I stället bibehöll kommissionen ett mindre betungande alternativ som består av självregleringsåtgärder som underlättas av kommissionen. Förslaget är proportionellt och mindre strängt, eftersom det inte skapar en ny rätt till portering mellan leverantörer av datalagringstjänster eller av andra databehandlingstjänster, utan bygger på självreglering för att skapa transparens i de tekniska och driftsmässiga villkoren för portabilitet.

Förslaget beaktar även nämndens yttrande för att säkerställa att det inte sker överlappningar eller dubbleringar i förhållande till översynen av mandatet för Europeiska unionens byrå för nät- och informationssäkerhet (Enisa) och införandet av en europeisk ram för IKT-cybersäkerhetscertifiering.

Konsekvensanalysen visade att det rekommenderade alternativet, underalternativ 2a, skulle medföra att befintliga oberättigade begränsningar för lokalisering undanröjdes och att framtida hinder förebyggdes genom en tydlig rättslig princip i kombination med prövning, anmälning och transparens, samtidigt som det skulle öka rättssäkerheten på och förtroendet för marknaden. Bördan för medlemsstaternas offentliga myndigheter skulle bli måttlig, vilket leder till en årlig kostnad på ungefär 33 000 euro i fråga om personalresurser för att upprätthålla de gemensamma kontaktpunkterna samt en årlig kostnad på mellan 385 och 1 925 euro för utarbetande av anmälningar.

Förslaget kommer att ha positiva effekter på konkurrensen, eftersom det kommer att stimulera innovation i datalagrings- eller andra databehandlingstjänster, locka fler användare till tjänsterna och göra det avsevärt mycket lättare, särskilt för nya och små tjänsteleverantörer, att ta sig in på nya marknader. Förslaget kommer också att främja gränsöverskridande och sektorsövergripande användning av datalagrings- eller andra databehandlingstjänster och utvecklingen av datamarknaden. Därför kommer förslaget bidra till att omvandla samhället och ekonomin samt skapa nya möjligheter för europeiska medborgare, företag och offentliga förvaltningar.

- **Lagstiftningens ändamålsenlighet och förenkling**

Förslaget gäller medborgare, nationella förvaltningar och alla företag, inbegripet mikroföretag och små och medelstora företag. Alla företag gynnas av bestämmelserna om åtgärder mot hinder för datarörligheten. Särskilt de små och medelstora företagen kommer att gynnas av förslaget, eftersom fri rörlighet för icke-personuppgifter direkt kommer att sänka deras

kostnader och gynna en starkare konkurrensposition. Om de små och medelstora företagen undantogs från reglerna, skulle reglernas ändamålsenlighet undergrävas, eftersom de små och medelstora företagen utgör en stor andel av leverantörerna av datalagring och annan lagring och är drivkrafter för innovation på de marknaderna. Eftersom kostnaderna till följd av reglerna dessutom sannolikt inte kommer att bli betydande, bör mikroföretag och små och medelstora företag inte undantas från deras tillämpningsområde.

- **Grundläggande rättigheter**

Det här förslaget till förordning respekterar de grundläggande rättigheter och principer som erkänns bland annat i Europeiska unionens stadga om de grundläggande rättigheterna. Den föreslagna förordningen skulle ha en positiv effekt på näringsfriheten (artikel 16), eftersom den skulle bidra till att undanröja och förhindra omotiverade eller oproportionerliga hinder för användning och tillhandahållande av datatjänster, exempelvis molntjänster, samt utformning av interna it-system.

4. BUDGETKONSEKVENSER

Det kommer att uppstå en måttlig administrativ börda för medlemsstaternas offentliga myndigheter, till följd av behovet av personalresurser för samarbetet mellan medlemsstaterna i de gemensamma kontaktpunkterna, och för att följa bestämmelserna om anmälan, översyn och öppenhet.

5. ÖVRIGA INSLAG

- **Genomförandeplaner samt åtgärder för övervakning, utvärdering och rapportering**

En omfattande utvärdering ska äga rum fem år efter det att tillämpningen av reglerna inletts för att bedöma deras ändamålsenlighet och proportionalitet. Den utvärderingen kommer att ske i enlighet med riktlinjerna för bättre lagstiftning.

Den måste särskilt omfatta en undersökning av om förordningen har bidragit till att minska datalokaliseringbegränsningarnas antal och omfattning, och till att öka rättssäkerheten om de återstående (motiverade och proportionerliga) begränsningarna och öppenheten i dessa. Utvärderingen måste också rymma en bedömning av om initiativet har bidragit till att förbättra förtroendet för det fria flödet av icke-personuppgifter, om medlemsstaterna rimligen kan få tillgång till uppgifter lagrade i utlandet för kontrolländamål och om förordningen har lett till ökad öppenhet i villkoren för dataportering.

De gemensamma kontaktpunkterna i medlemsstaterna planeras tjäna som en värdefull informationskälla vid efterhandsutvärderingen av lagstiftningen.

Särskilda indikatorer (såsom föreslås i konsekvensanalysen) skulle användas för att mäta framstegen på dessa områden. Även uppgifter från Eurostat och indexet för digital ekonomi och digitalt samhälle planeras användas. En specialutgåva av Eurobarometern kan också övervägas för detta ändamål.

- **Ingående redogörelse för de specifika bestämmelserna i förslaget**

I **artiklarna 1–3** anges förslagets **syfte**, förordningens **tillämpningsområde** och de **definitioner** som används i förordningen.

I **artikel 4** fastställs **principen om fri rörlighet för icke-personuppgifter** i unionen. Denna princip förbjuder varje krav på datalokalisering, såvida den inte berättigas av hänsyn till

allmän säkerhet. Vidare föreskrivs en översyn av de nuvarande kraven, en anmälan av kvarvarande eller nya krav till kommissionen samt åtgärder för ökad öppenhet.

Artikel 5 syftar till att säkerställa **behöriga myndigheters tillgång till data för kontroll**. Användare får därför inte vägra att ge behöriga myndigheter tillgång till data på grund av att data lagras eller på annat sätt behandlas i en annan medlemsstat. Om en behörig myndighet har uttömt alla möjligheter att få tillgång till uppgifterna, **får den behöriga myndigheten begära bistånd** från en myndighet i en annan medlemsstat, om det inte finns någon specifik samarbetsmekanism.

I **artikel 6** föreskrivs att kommissionen ska uppmuntra **tjänsteleverantörer och yrkesmässiga användare att utveckla och införa uppförandekoder**, och det anges vad som ska ingå i den detaljerade, tydliga och öppna information om villkoren för dataportering (inbegripet tekniska och operativa krav) som leverantören ska förse de professionella användarna med innan ett avtal ingås. Kommissionen ska se över utarbetandet och det faktiska genomförandet av sådana uppförandekoder senast två år efter det att denna förordning börjar tillämpas.

I **artikel 7** föreskrivs att varje medlemsstat ska utse en **gemensam kontaktpunkt** som ska upprätthålla kontakt med de gemensamma kontaktpunkterna i andra medlemsstater och kommissionen vad gäller tillämpningen av denna förordning. I artikel 7 fastställs också de förfaranderegler som gäller för sådant stöd mellan behöriga myndigheter som avses i artikel 5.

Enligt **artikel 8** ska kommissionen biträdas av kommittén för fritt dataflöde i den mening som avses i förordning (EU) nr 182/2011.

I **artikel 9** föreskrivs en **översyn** inom fem år efter det att förordningen börjar tillämpas.

Enligt **artikel 10** ska förordningen börja tillämpas sex månader efter dagen för dess offentliggörande.

2017/0228 (COD)

Förslag till

EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING

om en ram för det fria flödet av icke-personuppgifter i Europeiska unionen

EUROPAPARLAMENTET OCH EUROPEISKA UNIONENS RÅD HAR ANTAGIT DENNA FÖRORDNING

med beaktande av fördraget om Europeiska unionens funktionssätt, särskilt artikel 114,

med beaktande av Europeiska kommissionens förslag,

efter översändande av utkastet till lagstiftningsakt till de nationella parlamenten,

med beaktande av Europeiska ekonomiska och sociala kommitténs yttrande[28],

med beaktande av Regionkommitténs yttrande[29],

i enlighet med det ordinarie lagstiftningsförfarandet, och

av följande skäl:

(1) Digitaliseringen av ekonomin ökar. Informations- och kommunikationstekniken (IKT) är inte längre en specifik sektor, utan grunden för alla moderna innovativa ekonomiska system och samhällen. Elektroniska uppgifter står i centrum för dessa system och kan skapa stort värde när de analyseras eller kombineras med tjänster och produkter.

(2) Datavärdekedjor bygger på olika verksamheter som rör data: skapande och insamling av data; sammanställning och organiserande av data; datalagring och databehandling; analys, marknadsföring och distribution av data; användning och återanvändning av data. En effektiv och ändamålsenlig datalagring och annan databehandling är en grundläggande byggsten i alla datavärdekedjor. Den effektiviteten och ändamålsenligheten samt utvecklingen av den datadrivna ekonomin i unionen hämmas dock, i första hand av två typer av hinder för datarörlighet och för den inre marknaden.

(3) Etableringsfriheten och friheten att tillhandahålla tjänster enligt fördraget om Europeiska unionens funktionssätt gäller för datalagringstjänster och andra databehandlingstjänster. Tillhandahållandet av dessa tjänster försvåras eller hindras i vissa fall av vissa nationella krav på att lokalisera data på ett visst territorium.

(4) Sådana hinder för den fria rörligheten för datalagringstjänster eller andra databehandlingstjänster, och etableringsrätt för leverantörer av datalagringstjänster eller andra databehandlingstjänster härrör från krav i medlemsstaternas lagstiftning att lokalisera data i ett visst geografiskt område eller territorium för lagring eller annan behandling. Andra bestämmelser eller administrativ praxis har liknande verkan genom att de inför särskilda krav som gör det svårare att lagra eller på annat sätt behandla data utanför ett visst geografiskt område eller territorium inom unionen, till exempel krav på användning av tekniska anläggningar som är certifierade eller godkända i en

[28] EUT C , , s. .
[29] EUT C , , s. .

specifik medlemsstat. Rättslig osäkerhet när det gäller lagliga och olagliga krav på datalokalisering begränsar marknadsaktörernas och den offentliga sektorns valmöjligheter ytterligare när det gäller lokalisering av datalagring eller annan databehandling.

(5) Samtidigt begränsas datarörligheten i unionen av privata restriktioner: rättsliga, avtalsrättsliga och tekniska aspekter som hindrar eller stoppar användare av datalagringstjänster eller andra databehandlingstjänster från att portera sina data från en tjänsteleverantör till en annan eller tillbaka till sina egna it-system, inte minst vid uppsägning av avtal med en tjänsteleverantör.

(6) Av rättssäkerhetsskäl och på grund av behovet av lika villkor inom unionen är det mycket viktigt att det finns en samlad uppsättning regler för alla marknadsaktörer för att den inre marknaden ska fungera väl. För att avlägsna handelshindren och snedvridningen av konkurrensen beroende på skilda nationella regelverk, samt för att förhindra uppkomsten av framtida liknande handelshinder och snedvriden konkurrens, är det därför nödvändigt att anta enhetliga regler som ska tillämpas i alla medlemsstater.

(7) För att skapa en ram för den fria rörligheten för icke-personuppgifter i unionen och grunden för att utveckla den datadrivna ekonomin och stärka den europeiska industrins konkurrenskraft, är det nödvändigt att fastställa en tydlig, omfattande och förutsägbar rättslig ram för lagring eller annan behandling av andra uppgifter än personuppgifter på den inre marknaden. En principbaserad strategi för samarbete mellan medlemsstaterna, samt självreglering, bör säkerställa att systemet är flexibelt så att det kan ta hänsyn till förändrade behov hos användare, tjänsteleverantörer och nationella myndigheter i EU. För att undvika risken för överlappning med befintliga mekanismer och således undvika ökade bördor för både medlemsstater och företag, bör man inte fastställa detaljerade tekniska regler.

(8) Denna förordning bör tillämpas på juridiska eller fysiska personer som tillhandahåller datalagringstjänster eller andra databehandlingstjänster till användare som är bosatta eller etablerade i unionen, inbegripet de som tillhandahåller tjänster i unionen utan att vara etablerade i unionen.

(9) Den rättsliga ramen om skydd för fysiska personer med avseende på behandling av personuppgifter, särskilt förordning (EU) 2016/679[30], direktiv (EU) 2016/680[31] och direktiv 2002/58/EG[32], bör inte påverkas av denna förordning.

(10) Enligt förordning (EU) 2016/679 får medlemsstaterna varken begränsa eller förbjuda det fria flödet av personuppgifter inom unionen av skäl som har anknytning till skydd för fysiska personer med avseende på behandling av personuppgifter. I den förordningen fastställs samma princip om fri rörlighet inom unionen för andra

---

30 Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning) (EUT L 119, 4.5.2016, s. 1).

31 Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF (EUT L 119, 4.5.2016, s. 89).

32 Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (EGT L 201, 31.7.2002, s. 37).

uppgifter än personuppgifter, utom om en begränsning eller ett förbud skulle vara motiverat av säkerhetsskäl.

(11) Denna förordning bör gälla för datalagring eller annan databehandling i vid bemärkelse, och omfatta användning av alla typer av it-system, oavsett om de finns i användarens lokaler eller är utkontrakterade till en leverantör av datalagringstjänster eller andra databehandlingstjänster. Den bör omfatta databehandling på olika nivåer, från datalagring (Infrastructure-as-a-Service (IaaS)), till databehandling på plattformar (Platform-as-a-Service (PaaS)), eller i tillämpningar (Software-as-a-Service (SaaS)). Dessa olika tjänster bör omfattas av tillämpningsområdet för denna förordning, såvida inte datalagring eller annan databehandling endast är en hjälptjänst till en tjänst av en annan typ, t.ex. att tillhandahålla en elektronisk marknadsplats som fungerar som förmedling mellan tjänsteleverantörer och konsumenter eller företagsanvändare.

(12) Krav på datalokalisering utgör ett tydligt hinder för det fria tillhandahållandet av datalagringstjänster eller andra databehandlingstjänster i unionen och för den inre marknaden. Sådana krav borde därför förbjudas såvida de inte är motiverade på grund av den allmänna säkerheten, enligt definitionen i unionslagstiftningen, särskilt artikel 52 i fördraget om Europeiska unionens funktionssätt, och är förenliga med proportionalitetsprincipen som fastställs i artikel 5 i fördraget om Europeiska unionen. I syfte att tillämpa principen om fritt flöde av icke-personuppgifter över gränserna, för att säkerställa ett snabbt undanröjande av existerande krav på datalokalisering och för att av operativa skäl möjliggöra datalagring eller annan databehandling på flera platser i hela EU, och eftersom det i denna förordning föreskrivs åtgärder för att säkerställa tillgången till data för kontrolländamål, bör medlemsstaterna inte kunna åberopa andra grunder än hänsyn till allmän säkerhet.

(13) För att säkerställa en effektiv tillämpning av principen om fritt flöde av personuppgifter över gränserna och förhindra att det uppstår nya hinder för en väl fungerande inre marknad, bör medlemsstaterna till kommissionen anmäla förslag till rättsakter som innehåller ett nytt krav på datalokalisering eller ändrar ett befintligt krav på datalokalisering. Dessa anmälningar bör lämnas in och bedömas i enlighet med det förfarande som anges i direktiv (EU) 2015/1535[33].

(14) För att undanröja eventuella befintliga hinder, under en övergångsperiod på 12 månader, bör medlemsstaterna dessutom genomföra en översyn av befintliga nationella krav på datalokalisering och till kommissionen anmäla, tillsammans med en motivering, eventuella krav på datalokalisering som de anser överensstämmer med denna förordning. Dessa anmälningar bör göra det möjligt för kommissionen att bedöma efterlevnaden av eventuella kvarvarande krav på datalokalisering.

(15) För att säkerställa transparensen när det gäller krav på datalokalisering i medlemsstaterna för fysiska och juridiska personer, såsom tjänsteleverantörer och användare av datalagringstjänster eller andra databehandlingstjänster, bör medlemsstaterna offentliggöra information på nätet via en gemensam informationspunkt och regelbundet uppdatera informationen om sådana åtgärder. För att på lämpligt sätt informera juridiska och fysiska personer om krav på datalokalisering i hela unionen, bör medlemsstaterna meddela kommissionen

[33] Europaparlamentets och rådets direktiv (EU) 2015/1535 av den 9 september 2015 om ett informationsförfarande beträffande tekniska föreskrifter och beträffande föreskrifter för informationssamhällets tjänster (EUT L 241, 17.9.2015, s. 1).

adresserna till sådana kontaktpunkter. Kommissionen bör offentliggöra dessa uppgifter på sin webbplats.

(16) Krav på datalokalisering motiveras ofta av ett bristande förtroende för gränsöverskridande datalagring eller annan databehandling, som beror på att behöriga myndigheter i medlemsstater antar att data inte är tillgängliga, t.ex. för kontroll och revisioner i samband med tillsyn eller övervakning. Denna förordning bör därför klart och tydligt fastställa att den inte påverkar de behöriga myndigheternas befogenhet att begära och få tillgång till data i enlighet med unionslagstiftningen eller nationell lagstiftning, och att behöriga myndigheter inte får vägras tillgång till data på grundval av att datalaring eller databehandling sker i en annan medlemsstat.

(17) Fysiska eller juridiska personer som omfattas av skyldigheter att lämna uppgifter till behöriga myndigheter kan uppfylla dessa skyldigheter genom att tillhandahålla och garantera en effektiv elektronisk tillgång i rätt tid för behöriga myndigheter, oberoende av på vilken medlemsstats territorium data lagras eller behandlas på annat sätt. Sådan tillgång kan säkerställas genom konkreta villkor i avtal mellan den fysiska eller juridiska person som omfattas av skyldigheten att ge tillgång och leverantören av datalagringstjänster eller andra databehandlingstjänster.

(18) Om en fysisk eller juridisk person som omfattas av skyldigheter att lämna uppgifter inte uppfyller dem och under förutsättning att en behörig myndighet har uttömt alla möjligheter att få tillgång till data, bör den behöriga myndigheten ha möjlighet att begära hjälp från behöriga myndigheter i andra medlemsstater. I sådana fall bör behöriga myndigheter använda särskilda samarbetsinstrument i unionslagstiftningen eller internationella avtal, exempelvis, när det rör sig om polissamarbete, om straffrättsliga eller civilrättsliga fall eller om administrativa ärenden, rambeslut 2006/960[34], Europaparlamentets och rådets direktiv 2014/41/EU[35], Europarådets konvention om it-brottslighet[36], rådets förordning (EG) nr 1206/2001[37], rådets direktiv 2006/112/EG[38] och rådets förordning (EU) nr 904/2010[39]. Om det inte finns några sådana specifika samarbetsmekanismer bör de behöriga myndigheterna samarbeta med varandra för att ge tillgång till efterfrågade data, genom utsedda kontaktpunkter, såvida detta inte strider mot allmän ordning i den anmodade medlemsstaten.

(19) Om en begäran om hjälp innebär att den tillfrågade myndigheten ska få tillträde till en fysisk eller juridisk persons lokaler, inbegripet till eventuell utrustning och medel för datalagring eller annan databehandling, måste sådant tillträde ske i överensstämmelse med unionens eller medlemsstaternas processrättslagstiftning inklusive eventuellt krav på förhandstillstånd från rättsliga myndigheter.

---

[34] Rådets rambeslut 2006/960/RIF av den 18 december 2006 om förenklat informations- och underrättelseutbyte mellan de brottsbekämpande myndigheterna i Europeiska unionens medlemsstater (EUT L 386, 29.12.2006, s. 89).

[35] Europaparlamentets och rådets direktiv 2014/41/EU av den 3 april 2014 om en europeisk utredningsorder på det straffrättsliga området (EUT L 130, 1.5.2014, s. 1).

[36] Europarådets konvention om it-brottslighet , CETS nr 185.

[37] Rådets förordning (EG) nr 1206/2001 av den 28 maj 2001 om samarbete mellan medlemsstaternas domstolar i fråga om bevisupptagning i mål och ärenden av civil eller kommersiell natur (EGT L 174, 27.6.2001, s. 1).

[38] Rådets direktiv 2006/112/EG av den 28 november 2006 om ett gemensamt system för mervärdesskatt (EUT L 347, 11.12.2006, s. 1).

[39] Rådets förordning (EU) nr 904/2010 av den 7 oktober 2010 om administrativt samarbete och kampen mot mervärdesskattebedrägeri (EUT L 268, 12.10.2010, s. 1).

(20) Förmågan att portera data utan hinder är centralt när det gäller användarnas valfrihet och en effektiv konkurrens på marknaderna för datalagring eller databehandlingstjänster. De faktiska eller upplevda svårigheterna i fråga om att portera data över gränser undergräver också förtroendet hos professionella användare i andra EU-länder när det gäller att acceptera gränsöverskridande anbud och därigenom deras förtroende för den inre marknaden. Medan fysiska personer och konsumenter kan dra nytta av befintlig unionslagstiftning, underlättas inte möjligheten att växla mellan tjänsteleverantörer för användare inom ramen för deras närings- eller yrkesverksamhet.

(21) För att utnyttja den konkurrensutsatta miljön fullt ut bör professionella användare kunna göra välinformerade val och på enkelt sätt jämföra enskilda delar av olika datalagringstjänster eller andra databehandlingstjänster på den inre marknaden, bland annat när det gäller avtalsvillkoren för dataportering i samband med uppsägning av avtal. I syfte att anpassa sig till marknadens innovationspotential och beakta den erfarenhet och sakkunskap som finns hos leverantörer och professionella användare av datalagringstjänster eller andra databehandlingstjänster, bör den detaljerade informationen och driftskraven för dataportering fastställas av marknadsaktörer genom självreglering, vilket ska uppmuntras och underlättas av kommissionen, i form av unionsuppförandekoder som kan leda till standardavtalsvillkor. Om sådana uppförandekoder inte införs och tillämpas effektivt inom rimlig tid, bör kommissionen se över situationen.

(22) För att bidra till ett smidigt samarbete mellan medlemsstaterna, bör varje medlemsstat utse en gemensam kontaktpunkt för att hålla kontakt med kontaktpunkterna i övriga medlemsstater och kommissionen när det gäller tillämpningen av denna förordning. Om en behörig myndighet i en medlemsstat begär hjälp från en annan medlemsstat för att få tillgång till uppgifter enligt denna förordning, bör den lämna in en vederbörligen motiverad begäran till den sistnämnda medlemsstatens utsedda gemensamma kontaktpunkt, inbegripet en skriftlig förklaring av sin motivering och de rättsliga grunderna för begäran om att få tillgång till uppgifter. Den gemensamma kontaktpunkt som utsetts av den medlemsstat vars hjälp begärs, bör underlätta hjälpen mellan myndigheter genom att identifiera och överföra begäran till den behöriga myndigheten i den medlemsstat som mottar begäran om hjälp. I syfte att säkerställa ett effektivt samarbete bör den myndighet som mottar begäran om hjälp utan onödigt dröjsmål tillhandahålla hjälp som svar på en viss begäran eller informera om svårigheterna med att uppfylla en begäran om hjälp eller om skälen för att avslå en sådan begäran.

(23) För att säkerställa en effektiv tillämpning av förfarandet för hjälp mellan medlemsstaternas behöriga myndigheter, får kommissionen anta genomförandeakter som fastställer standardformulär, språk för begäran, tidsfrister eller andra närmare uppgifter om förfarandena för begäranden om hjälp. Dessa befogenheter bör utövas i enlighet med Europaparlamentets och rådets förordning (EU) nr 182/2011[40].

(24) Om man stärker tilltron till säkerheten i gränsöverskridande datalagring eller annan databehandling, borde det minska benägenheten hos marknadsaktörerna och den offentliga sektorn att använda datalokalisering som ersättning för datasäkerhet. Det borde också förbättra rättssäkerheten för företag avseende gällande säkerhetskrav när

[40] Europaparlamentets och rådets förordning (EU) nr 182/2011 av den 16 februari 2011 om fastställande av allmänna regler och principer för medlemsstaternas kontroll av kommissionens utövande av sina genomförandebefogenheter (EUT L 55, 28.2.2011, s. 13).

de lägger ut sin datalagring eller annan databehandlingsverksamhet på underleverantörer, vilket även gäller i fråga om tjänsteleverantörer i andra medlemsstater.

(25) Alla säkerhetskrav som gäller för datalagring eller annan databehandling och som tillämpas på ett proportionerligt och motiverat sätt på grundval av unionslagstiftningen eller nationell rätt i överensstämmelse med unionslagstiftningen i hemvist- eller etableringsmedlemsstaten för de fysiska eller juridiska personer vars data berörs, bör fortsätta att gälla för datalagring eller annan databehandling i en annan medlemsstat. Dessa fysiska eller juridiska personer bör kunna uppfylla dessa krav, antingen själva eller genom klausuler i avtal med leverantörer.

(26) Säkerhetskrav som fastställs på nationell nivå bör vara nödvändiga och stå i proportion till de risker som hotar säkerheten för datalagring eller annan databehandling i det område som omfattas av den nationella lagstiftningen där dessa krav fastställts.

(27) Direktiv 2016/1148[41] föreskriver rättsliga åtgärder för att förbättra den övergripande nivån på cybersäkerhet i unionen. Datalagringstjänster eller andra databehandlingstjänster utgör en av de digitala tjänster som omfattas av det direktivet. Enligt artikel 16 i det direktivet måste medlemsstaterna säkerställa att leverantörer av digitala tjänster utarbetar och vidtar ändamålsenliga och proportionella tekniska och organisatoriska åtgärder för att hantera risker som hotar säkerheten i nätverks- och informationssystem som de använder. Sådana åtgärder bör garantera en säkerhetsnivå som är anpassad till den aktuella risken, och bör ta hänsyn till systemens och anläggningarnas säkerhet, hantering av incidenter, driftskontinuitetshantering, övervakning, revision och testning samt efterlevnad av internationella normer. Dessa delar ska anges närmare av kommissionen i genomförandeakter enligt detta direktiv.

(28) Kommissionen bör se över denna förordning med jämna mellanrum, främst i syfte att avgöra behovet av modifieringar med hänsyn till den tekniska utvecklingen eller ändrad marknadsutveckling.

(29) Denna förordning är förenlig med de grundläggande rättigheter och de principer som erkänns särskilt i Europeiska unionens stadga om de grundläggande rättigheterna, och bör tolkas och tillämpas i överensstämmelse med dessa rättigheter och principer, inbegripet rätten till skydd av personuppgifter (artikel 8), näringsfrihet (artikel 16) och yttrandefrihet och informationsfrihet (artikel 11).

(30) Eftersom målet för denna förordning, nämligen att säkerställa den fria rörligheten för icke-personuppgifter i unionen, inte i tillräcklig utsträckning kan uppnås av medlemsstaterna utan snarare, på grund av dess omfattning och verkningar, kan uppnås bättre på unionsnivå, kan unionen vidta åtgärder i enlighet med subsidiaritetsprincipen i artikel 5 i fördraget om Europeiska unionen. I enlighet med proportionalitetsprincipen i samma artikel går denna förordning inte utöver vad som är nödvändigt för att uppnå detta mål.

[41] Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen (EUT L 194, 19.7.2016, s. 1).

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

Artikel 1
Syfte

Denna förordning syftar till att säkerställa den fria rörligheten för andra uppgifter än personuppgifter inom unionen genom att fastställa regler avseende datalokaliseringskrav, tillgång till uppgifter för behöriga myndigheter och dataportering för professionella användare.

Artikel 2
Tillämpningsområde

1. Denna förordning ska tillämpas på lagring eller annan behandling av andra elektroniska data än personuppgifter i unionen, vilken

   (a) tillhandahålls som en tjänst till användare som är bosatta eller etablerade i unionen, utan hänsyn till om leverantören är etablerad i unionen, eller

   (b) utförs av en fysisk eller juridisk person, som är bosatt eller etablerad i unionen, för eget behov.

2. Denna förordning ska inte tillämpas på verksamheter som inte omfattas av unionslagstiftning.

Artikel 3
Definitioner

I denna förordning gäller följande definitioner:

1. *uppgifter*: andra uppgifter än personuppgifter som avses i artikel 4.1 i förordning (EU) 2016/679.

2. *datalagring*: lagring av uppgifter i elektroniskt format.

3. *utkast till akt*: en text som utarbetats i syfte att få den antagen som en lag eller annan författning av allmän karaktär och som befinner sig i det förberedande stadium då väsentliga ändringar fortfarande kan göras av den anmälande medlemsstaten.

4. *leverantör*: en fysisk eller juridisk person som tillhandahåller datalagring eller andra databehandlingstjänster.

5. *datalokaliseringskrav*: varje skyldighet, förbud, villkor, begränsning eller annat krav som föreskrivs i medlemsstaternas lagar eller andra författningar och som föreskriver att datalagring eller annan databehandling ska äga rum på en viss medlemsstats territorium eller hindrar lagring eller annan behandling av data i någon annan medlemsstat.

6. *behörig myndighet*: en medlemsstats myndighet som har befogenhet att få tillgång till uppgifter som lagras eller behandlas av en fysisk eller juridisk person för den personens tjänsteutövning, i enlighet med nationell lagstiftning eller unionslagstiftning.

7. *användare*: en fysisk eller juridisk person som använder eller vill använda en datalagringstjänst eller en annan databehandlingstjänst.

8. *professionell användare*: en fysisk eller juridisk person, inbegripet ett offentligt organ, som använder eller begär en datalagringstjänst eller en annan

databehandlingstjänst för ändamål som är relaterade till personens närings- eller yrkesverksamhet.

Artikel 4
Fri rörlighet för uppgifter inom unionen

1. Lokalisering av data för lagring eller annan behandling inom unionen får inte begränsas till en viss medlemsstats territorium, och lagring eller annan databehandling i någon annan medlemsstat får inte förbjudas eller begränsas, om det inte är motiverat av hänsyn till allmän säkerhet.

2. Medlemsstaterna ska till kommissionen anmäla alla utkast till akter som inför ett nytt datalokaliseringskrav eller gör ändringar i ett existerande datalokaliseringskrav i enlighet med de förfaranden som fastställs i den nationella lag genom vilken direktiv (EU) 2015/1535 genomförs.

3. Inom 12 månader efter det att denna förordning har börjat tillämpas ska medlemsstaterna säkerställa att alla datalokaliseringskrav som inte är förenliga med punkt 1 upphör att gälla. Om en medlemsstat anser att ett datalokaliseringskrav är förenligt med punkt 1 och därför kan fortsätta att gälla ska den anmäla kravet till kommissionen, tillsammans med en motivering till varför kravet ska behållas.

4. Medlemsstaterna ska göra närmare uppgifter om eventuella datalokaliseringskrav som gäller på deras territorier tillgängliga för allmänheten online via en central informationspunkt som de ska hålla uppdaterad.

5. Medlemsstaterna ska meddela kommissionen adressen till sin centrala informationspunkt som nämns i punkt 4. Kommissionen ska offentliggöra länkarna till sådana punkter på sin webbsida.

Artikel 5
Tillgång till uppgifter för behöriga myndigheter

1. Denna förordning ska inte påverka behöriga myndigheters befogenheter att begära och få tillgång till uppgifter för sin tjänsteutövning i enlighet med unionslagstiftning eller nationell lagstiftning. Behöriga myndigheter får inte nekas tillgång till uppgifter på grundval av att uppgifterna lagras, eller behandlas på annat sätt, i en annan medlemsstat.

2. Om en behörig myndighet har uttömt alla användbara möjligheter att få tillgång till uppgifterna får den begära hjälp av en behörig myndighet i en annan medlemsstat i enlighet med det förfarande som fastställs i artikel 7, och den tillfrågade behöriga myndigheten ska tillhandahålla hjälp i enlighet med förfarandet i artikel 7, såvida det inte strider mot den allmänna ordningen i den tillfrågade medlemsstaten.

3. Om en begäran om hjälp innebär att den tillfrågade myndigheten ska få tillträde till en fysisk eller juridisk persons lokaler, inbegripet till utrustning och medel för datalagring eller annan databehandling, måste sådant tillträde ske i överensstämmelse med unionens eller medlemsstaternas processrättslagstiftning.

4. Punkt 2 ska tillämpas endast om det inte finns någon särskild samarbetsmekanism enligt unionslagstiftning eller internationella avtal för utbyte av uppgifter mellan behöriga myndigheter i olika medlemsstater.

Artikel 6
Portering av data

1. Kommissionen ska uppmuntra och underlätta utarbetandet av självreglerande uppförandekoder på unionsnivå, för att fastställa riktlinjer för bästa praxis när det gäller att underlätta byte av leverantörer och för att säkerställa att leverantörerna förser professionella användare med tillräckligt detaljerad, tydlig och öppen information innan ett avtal om datalagring och databehandling ingås, vad gäller följande frågor:

   (a) de processer, tekniska krav, tidsramar och avgifter som gäller om en professionell användare vill byta till en annan leverantör eller portera data tillbaka till sina egna it-system, inbegripet processerna och platsen för eventuell backup av data, tillgängliga dataformat och datastöd, erforderlig it-konfiguration och minsta nätbandbredd; den tid som krävs innan porteringsprocessen inleds och den tid under vilken uppgifterna kommer att förbli tillgängliga för portering; garantierna för tillgång till uppgifter om leverantören gör konkurs;

   (b) de operativa kraven för leverantörsbyte eller dataportering i ett strukturerat, allmänt använt och maskinläsbart format som medger tillräckligt med tid för användaren att byta leverantör eller portera data.

2. Kommissionen ska uppmuntra leverantörer att på ett effektivt sätt tillämpa de uppföranderegler som avses i punkt 1 inom ett år efter det att denna förordning börjar tillämpas.

3. Kommissionen ska se över utarbetandet och det faktiska genomförandet av sådana uppförandekoder och det faktiska tillhandahållandet av information från leverantörer senast två år efter det att denna förordning börjar tillämpas.

Artikel 7
Gemensamma kontaktpunkter

1. Varje medlemsstat ska utse en gemensam kontaktpunkt som ska upprätthålla kontakt med de gemensamma kontaktpunkterna i andra medlemsstater och kommissionen vad gäller tillämpningen av denna förordning. Medlemsstaterna ska underrätta kommissionen om de utsedda gemensamma kontaktpunkterna och alla efterföljande ändringar av dessa.

2. Medlemsstaterna ska säkerställa att de gemensamma kontaktpunkterna har de resurser som krävs för tillämpningen av denna förordning.

3. Om en behörig myndighet i en medlemsstat begär hjälp från en annan medlemsstat för att få tillgång till uppgifter enligt artikel 5.2 ska den lämna in en vederbörligen motiverad begäran till den sistnämnda medlemsstatens utsedda gemensamma kontaktpunkt, inbegripet en skriftlig förklaring av sin motivering och de rättsliga grunderna för begäran om att få tillgång till uppgifter.

4. Den gemensamma kontaktpunkten ska fastställa vilken behörig myndighet som berörs i sin medlemsstat och översända den begäran som mottagits enligt punkt 3 till den behöriga myndigheten. Den sålunda tillfrågade myndigheten ska utan onödigt dröjsmål

   (a) svara den begärande behöriga myndigheten och underrätta den gemensamma kontaktpunkten om sitt svar och

(b) informera den gemensamma kontaktpunkten och den begärande behöriga myndigheten om eventuella svårigheter eller, i händelse av att begäran avslås eller besvaras ofullständigt, om skälen för ett sådant avslag eller ofullständigt svar.

5. All information som utbyts inom ramen för hjälp som begärs och tillhandahålls enligt artikel 5.2 får användas endast med avseende på det ärende för vilket den har begärts.

6. Kommissionen får anta genomförandeakter som fastställer standardformulär, språk för begäran, tidsfrister eller andra närmare uppgifter om förfarandena för begäran om hjälp. Sådana genomförandeakter ska antas i enlighet med det förfarande som avses i artikel 8.

Artikel 8
Kommitté

1. Kommissionen ska biträdas av kommittén för fritt dataflöde. Denna kommitté ska vara en kommitté i den mening som avses i förordning (EU) nr 182/2011.

2. När det hänvisas till denna punkt ska artikel 5 i förordning (EU) nr 182/2011 tillämpas.

Artikel 9
Översyn

1. Senast den [5 år efter det datum som nämns i artikel 10.2] ska kommissionen genomföra en översyn av denna förordning och lägga fram en rapport om de viktigaste slutsatserna för Europaparlamentet, rådet och Europeiska ekonomiska och sociala kommittén.

2. Medlemsstaterna ska förse kommissionen med den information som är nödvändig för utarbetandet av den rapport som avses i punkt 1.

Artikel 10
Slutbestämmelser

1. Denna förordning träder i kraft den tjugonde dagen efter det att den har offentliggjorts i *Europeiska unionens officiella tidning*.

2. Denna förordning ska tillämpas från och med sex månader efter offentliggörandet.

Denna förordning är till alla delar bindande och direkt tillämplig i alla medlemsstater.

Utfärdad i Bryssel den

På Europaparlamentets vägnar	*På rådets vägnar*
Ordförande	*Ordförande*

EUROPEAN
COMMISSION

Brussels, 13.9.2017
SWD(2017) 305 final

COMMISSION STAFF WORKING DOCUMENT

EXECUTIVE SUMMARY OF THE IMPACT ASSESSMENT

Accompanying the document

PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on a framework for the free flow of non-personal data in the European Union

{COM(2017) 495 final}
{SWD(2017) 304 final}

Executive Summary Sheet
Impact assessment on the ***Legislative proposal on a framework for the free flow of data in the EU.***
A. Need for action
Why? What is the problem being addressed?
In the European Union the possibility to build a data economy and to benefit from new technologies which rely on data is undermined by a series of barriers to data mobility, impacting businesses and their operations in the Single Market. In this context, obstacles to data mobility in the EU single market have been identified as the core problem. The underlying problem drivers are legislative and administrative localisation restrictions; data localisation driven by legal uncertainty and a lack of trust in the market; and vendor lock-in practices, which inhibit data mobility across data storage and/or further processing services providers and IT-systems.
What is this initiative expected to achieve?
The objective of the initiative is to achieve a more competitive and integrated EU market for data storage and/or processing services and activities. More specifically this means to reduce the number and range of data localisation restrictions, enhance legal certainty; facilitate cross-border availability of data for regulatory control purposes; improve the conditions under which users can switch data storage and/or processing service providers or port their data back to their own IT systems; enhance trust in and the security of cross-border data storage and/or processing.
What is the value added of action at the EU level?
Building a competitive European Data Economy means benefitting from economies of scale and data storage and processing on a cross-border basis in the EU. Action at Member State level could not achieve the legal certainty required for conducting this business across the EU, or remedy the lack of trust required for a thriving data storage and/or processing sector. EU intervention would also contribute to the development of secure data storage for the whole of the EU.

B. Solutions
What legislative and non-legislative policy options have been considered? Is there a preferred choice or not? Why?
Option 0 – Baseline scenario. This option would entail no EU policy change. **Option 1 – Non-legislative initiatives** This option would provide guidelines on a better enforcement of the existing EU instruments vis-à-vis unjustified data localisation restrictions imposed by Member States. Availability for regulatory control purposes should be facilitated in accordance with the Member States' existing rules. EU-level guidelines on best practices should enable easier switching of cloud service providers and porting data to another service provider or back to users' own IT systems. **Option 2 – Principles-based legislative initiative and cooperation framework.** This option would establish the principle of free flow of data within the EU prohibiting unjustified data localisation measures unless justified on national security grounds and requiring the notification of any new measure on data localisation. Companies which store and/or process their data in another Member State would need to provide data to a regulatory authority if requested in accordance with the law. The switching of cloud service provider and the porting of data to a new provider or back to users' own IT systems should be enabled and reliable common standards and/or certification schemes for the security of storage and/or processing of data should be promoted by dedicated provisions. Single points of contact designated by the Member States and a pan-European policy group comprised of such contact points should enable exchange and cooperation for the development of common approaches and best

practices and an effective implementation of the principles introduced.

A variant: - Sub-option 2a - instead of a legislative provision and co-regulation on data porting, this sub-option would foresee a self-regulatory approach to improve the conditions for data porting upon switching providers or porting data back to users' own IT systems, including the processes, timeframes and charging that may apply. On the intervention area of security of data storage and processing, the Sub-option would entail the clarification that any already applicable security requirements continue to apply to business users when they store or process their data in other Member States of the EU, also when this is subject to outsourcing to e.g. a cloud service provider.

Option 3 – Detailed legislative initiative. This option would establish fully harmonised rules on unjustified data location requirements (white or black lists). A mandatory cooperation framework would allow to enforce cross-border access to relevant data for regulatory authorities. Cloud service providers would be obliged to facilitate the porting of data and disclose with sufficient detail relevant processes, technical requirements and costs. Common standards and a separate European certification scheme for the security of data storage and/or processing for cloud services provided would be developed.

Who supports which option?

61.9% of respondents to the public consultation indicated that data localisation restrictions should be removed and 55.3% argued for a legislative approach in doing so. 16 Member States have explicitly called for a legislative approach in a letter addressed to President Tusk. Stakeholders seem therefore to prefer a legislative approach (Option 2 or 3) in addressing data localisation restrictions and availability for regulatory control to provide more clarity and certainty. However, evidence suggests that legislative action for security and switching and porting data should not be too detailed, as this could have counterproductive effects. Based on evidence-gathering EU businesses users of data storage and processing services prefer option 2 or 3, whereas Cloud service providers prefer option 2a. Member States' public authorities prefer option 2.

C. Impacts of the preferred option

What are the benefits of the preferred option (if any, otherwise main ones)?

It would ensure the effective removal of existing unjustified localisation restrictions and the avoidance of future ones by establishing a clear legal principle in combination with a review procedure. As a result of awareness-raising on the legal principles established by the Regulation, it will also enhance legal certainty in the market. Moreover, by encouraging the development of codes of conduct for switching providers and porting data, it would lead to a more competitive internal market for cloud service providers.

What are the costs of the preferred option (if any, otherwise main ones)?

Data storage and processing service providers are most impacted by the initiative in terms of financial costs, albeit still at a moderate level. Compliance costs could arise from legal analysis, the development of new model clauses for contracts for switching of (cloud) data storage and processing service providers, the development of codes of conduct, standard setting, etc. Additional costs would be those for migrating data of ex-customers to a new location and a loss of market share to other/new cloud service providers.

How will businesses, SMEs and micro-enterprises be affected?

Start-ups and SMEs are strongly in favour of legislative action on free flow of data to improve legal certainty and switching, as this will directly cut costs for them and therefore lead to a more competitive market position. Specific costs that could be avoided are costs for duplication of IT-infrastructure, e.g. when an SME is active in multiple Member States and in one or more of those countries data localisation restrictions apply.

Will there be significant impacts on national budgets and administrations?
A moderate administrative burden for Member States' public authorities will emerge, caused by the allocation of human resources for structured cooperation between Member States in the 'single points of contact, and for complying with the notification and review process of the transparency mechanism, as provided for the Single Market Transparency Directive. In total, this could lead to an average annual cost of EUR 34.539 per Member State.
Will there be other significant impacts?
Yes, there will be broad positive impacts on economic development, through the enhancement of the European Data Economy and the creation of a more competitive market for data storage and processing services. This could, for example, lead to cost reductions for business users. The initiative would lead to the reduction of existing costs for business users. These cost reductions can be cost reductions for businesses making use of data storage and processing services and for businesses operating across borders, or intending to do this in the future, and lower costs for launching new products or services.
D. Follow up
When will the policy be reviewed?
A comprehensive evaluation could take place 5 years after the start of application of the rules. This evaluation will be executed in close cooperation with and relying on the information provided by the single points of contact of the Member States.

EUROPEAN
COMMISSION

Brussels, 13.9.2017
SWD(2017) 304 final

PART 1/2

COMMISSION STAFF WORKING DOCUMENT

IMPACT ASSESSMENT

Accompanying the document

Proposal for a Regulation of the European Parliament and of the Council

on a framework for the free flow of non-personal data in the European Union

{COM(2017) 495 final}
{SWD(2017) 305 final}

Table of Contents

1 Context

The political support for an EU free flow of data initiative is very strong, placing it at the centre of the development of digital technologies and services across the EU, rendering it a key element in achieving the Digital Single Market:

A majority of Member States support free flow of data in the EU:

- **16 Heads of State and Government** called for a legislative proposal on free flow of data in December 2016;
- In its Conclusions of 15 December 2016 **the European Council** stressed the need to remove "remaining obstacles within the Single Market, including those hampering the free flow of data";
- Ministers of **15 Member States** reiterated in May 2017 their call to present without delay a legislative proposal to remove data localisation restrictions that cannot be objectively justified.
- Following the structured dialogues, the positions of some **initially reticent Member States** have evolved in the direction of support.

The European Parliament is also a strong supporter of free flow of data:

- In April 2017, a **group of key MEPs** representing different political groups sent a letter to the Commission President calling for a Regulation on the free flow of data.

The **Estonian Presidency of the Council** has identified the free movement of data as a central priority and a key theme of the upcoming (September 2017) **Tallinn Digital Summit of the Heads of State and government**.

Over the last year, the Commission services have carried out further detailed assessment in order to collect as much as possible data and stakeholder's feedback to grasp those elements that represent an obstacle to the correct functioning of Digital single market in the area of free flow of data, through the following key actions:

- the public consultation on Building a European Data Economy (**January - April 2017**);
- structured dialogues with Member States (3 collective meetings and 16 bilateral discussions from **February to May 2017**);
- completion of studies on data flows, localisation restrictions and their economic impacts (including a workshop with stakeholders in **March 2017**); new studies on switching of cloud providers / data porting (including a workshop with stakeholders in **May 2017**) and on cloud certification / security.

These combined inputs have not only provided new evidence on the obstacles to data flows in the EU, but have allowed the scope of the options and of the proposed initiative to be refined in order to better target the problem and its different drivers.

1.1 Technology-driven innovation

New digital technologies, such as cloud computing, big data, artificial intelligence and the Internet of Things (IoT), are transforming our society and economy and are opening up new opportunities for European citizens, businesses and public administrations.

These technologies are designed to gather, manage, distribute and analyse data in order to maximise efficiency, enable economies of scale and develop new services. They offer benefits to users, such as agility, productivity, speed of deployment and autonomy, e.g. through machine learning[1]. For instance, the new generation of data storage and processing services combine cloud and artificial intelligence software. The ability to move data easily to and between these systems - even if they

[1] Machine learning is an application of artificial intelligence (AI) that provides systems the ability to automatically learn from data samples and improve from experience without being explicitly programmed.

are located in different Member States - is a necessary pre-condition for making full use of their potential.

Unlocking this potential requires action, in the short term, on the following issues:

- Improving the mobility of data across borders in the single market, which is limited today in many Member States by localisation restrictions or legal uncertainty in the market;
- Making it clear and ensuring that, as the free flow of data is implemented in Member States, the responsibility of private parties to provide data for regulatory control purposes remains unchanged, as trust is a key element in the development of the data economy;
- Making it easier to switch service providers and to port data, since this is key to the development of a competitive cloud market in the EU, benefiting in particular SMEs;
- Making further progress on the security of data and cloud services in order to enhance trust and to avoid fragmentation of the single market as a result of different approaches in Member States.

Resolving these issues will facilitate the movement of data across borders, across data storage and processing (cloud) services (CSPs)[2] as well as between CSPs and in-house IT systems[3]. It will **create the foundation** upon which future cross-cutting (e.g. re-use of data across borders) and sectoral[4] **data policies can be built**.

Further economic and technological context is provided in **Annex 9** to this Impact Assessment.

1.2 Data flows and data economy

Data is at the heart of all new technologies, and the data market (i.e. the market where digital data is exchanged as products or services derived from raw data)[5] has become a market on its own. In 2016, the value of the EU data market was estimated at almost EUR 60 billion, showing a growth of 9.5% compared to 2015. It could potentially amount to more than EUR 106 billion in 2020[6].

The January 2017 Communication "Building a European Data Economy"[7] set out several issues, the resolution or clarification of which would contribute to a clear framework for data. This would facilitate the rapid evolution of technology, the emergence of data as a key factor of production as well as a competitive differentiator, and create the right conditions for investment and innovation in Europe. These issues include:

- free flow of data (the focus of this initiative);

- data access and transfer (whether 'ownership' rights exist on non-personal data that are generated as part of a business process or that are de facto in the possession of a business; what are the conditions of usability and access to such data);

- liability (how to provide certainty to both users and manufacturers of data technologies and services in relation to their potential liability);

- portability, interoperability and standards (how non-personal data exchange and competitive data markets could be stimulated; partly the focus of this initiative).

Although all these issues are important, it makes sense to address the free flow of data in first instance. The speed with which the market is embracing new technologies is a strong reason to

[2] Although data storage and processing services encompass more than only cloud services (e.g. merely hosting servers), for reasons of brevity the term used hereafter will be 'cloud service providers', or CSPs.
[3] Servers owned and/or operated by enterprises and public sector organisations
[4] E.g. banking and finance, e-health, connected and automated driving, smart grids, etc.
[5] IDC and Open Evidence, European Data Market, Final Report, 1 February 2017 (SMART 2013/0063).
[6] IDC and Open Evidence, European Data Market, Final Report, 1 February 2017 (SMART 2013/0063).
[7] COM(2017) 9, "Building A European Data Economy", 10 January 2017; see also Commission Staff Working Document accompanying the Communication, SWD(2017) 2 of 10 January 2017, https://ec.europa.eu/digital-single-market/en/news/staff-working-document-free-flow-data-and-emerging-issues-european-data-economy.

remove immediately the remaining barriers to the movement of data within the EU and thereby ensuring effective and efficient functioning of data storage and processing, which is at the fundament of any data economy. The resulting legal certainty in the market would stimulate innovation and improve Europe's global competitiveness.

Moreover, the market maturity and opportunities for intervening are different for the different issues. For the barriers to the movement of data, the cause is relatively simple - they spring from the forced storage or processing of certain types of data in electronic format within a geographical zone or IT environment[8].

Other data issues arise from disruptive business models emerging from the digital transformation of the industry, technological advances and a fast-evolving data market, and their implications are still far from clear and need further assessment.

The **public consultation** confirmed that these other data issues, such as data access, transfer and liability, are more difficult topics and less mature topics that deserve further assessment. Indeed, when it comes to potential actions to make more data available for re-use across businesses, most stakeholders call for prudence. They argue that data value chains and business models building on data are of great variety making it difficult to conceive one-size-fits-all solutions. Regarding liability, the need for further assessment taking into account the findings gathered so far also emerges from the public consultation. .[9]

The General Data Protection Regulation (GDPR) provides a single set of rules for the entire EU ensuring a high level of protection of personal data. Businesses and public sector entities processing personal data must comply with these rules. The GDPR will enable people to better control their personal data. At the same time its modernised and unified rules will allow businesses to make the most of the opportunities of the Digital Single Market by cutting red tape and benefiting from reinforced consumer trust.

In line with the DSM Mid-Term Review Communication[10], **the present initiative focuses on aspects of data flows within the EU that are not regulated by the GDPR**: those stemming from decisions of businesses or public sector entities on (i) the choice of a geographical location for data storage or processing and (ii) the choice of a data storage or processing service provider or the choice of in-house IT system(s) for centralised or distributed data storage or processing within a business group.

To the extent that this initiative deals with mixed data sets that include personal data, the applicable provisions of **the GDPR** must be fully complied with in respect to the personal data part of the set.

1.3 Policy background

The policy initiative covered by the present Impact Assessment should be seen in the light of the priority given by the Juncker Commission to creating a connected Digital Single Market (DSM)[11], which aims at maximising the growth potential of the economy, not least by removing the remaining barriers to a competitive data-driven economy in Europe.

The DSM Strategy announced *"a European 'Free flow of data' initiative that tackles restrictions on the **free movement of data** for reasons other than the protection of personal data within the EU and **unjustified restrictions on the location of data** for storage or processing purposes".*[12]

[8] Some of the barriers are also residual from the 'paper era'.
[9] Synopsis Report, Public Consultation on "Building a European Data Economy"
[10] COM (2017) 228, "Mid-Term Review on the implementation of the Digital Single Market Strategy", 10 May 2017.
[11] See: https://ec.europa.eu/priorities/publications/president-junckers-political-guidelines_en.
[12] In the Staff Working Document accompanying the DSM strategy, the Commission had already pointed out that data localisation restrictions can in fact limit the benefits offered by digital services such as cloud computing as they create barriers to EU cross-border data transfers, limiting the competitive choice between providers and raising costs by

The Communication "Building a European Data Economy" stated that in order to "*realise the full potential of the European data economy, any Member State action affecting data storage or processing should be guided by a "**principle of free movement of data within the EU**", as a corollary of their obligations under the free movement of services and the free establishment provisions of the Treaty and relevant secondary legislation*".

The recent **mid-term review of the Digital Single Market strategy**[13]**,** which assessed the progress towards the implementation of the Digital Single Market, re-iterated the importance of the European data economy framework and urged political action, concluding that the Commission will:

> … *"by autumn 2017, subject to Impact Assessment, prepare a legislative proposal on the EU free flow of data cooperation framework which takes into account the principle of free flow of data within the EU, the principle of porting non-personal data, including when switching business services like cloud services as well as the principle of availability of certain data for regulatory control purposes also when that data is stored in another Member State".* It also stated that this framework could, in addition to taking into account these principles, address Member States' legitimate interests on secure storage of data.

The policy intervention also builds upon the **Digitising European Industry** (DEI) policy package that included the **European Cloud initiative**[14] aiming to deploy a high capacity cloud solution for storing, sharing and re-using scientific data. The free flow of data will contribute to an effective functioning of this open environment. Furthermore, the initiative builds upon the revision of **the European Interoperability Framework**[15], which aims to improve digital collaboration between public administrations in Europe and will benefit directly from the free flow of data. It contributes to the EU's commitment to an **open Internet**[16]. The policy initiative also responds to the calls from stakeholders expressed in the **REFIT Platform**[17].

1.4 Scope

The initiative concerns data storage and processing in its broadest sense, encompassing usage of all types of IT-systems, whether located on the premises of the data controller or outsourced to cloud service providers[18]. The initiative also **covers data processing of different levels of intensity**, from mere data 'storage' (Infrastructure-as-a-Service (IaaS) in cloud terminology) to the processing of data on platforms or in applications of different kinds (or, in the jargon, respectively Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS)).

The scope of this initiative is limited in order to **avoid duplication** and to ensure consistency **with existing legal instruments and other Commission initiatives**. In particular, this initiative takes into account the provisions and fields of application of different existing EU legal instruments, such as the GDPR, the e-Commerce Directive, the Services Directive, the Single Market Transparency Directive and the NIS Directive (see sections 3.3 and 8).

It will be **synergetic with the planned initiatives** on the EU ICT security certification framework, online platforms and digital innovation in health and care. It takes into account the forthcoming solutions, including legislative ones, to improve access to e-evidence in criminal matters by law enforcement authorities.

---

forcing organisations and companies to store data on servers physically located inside a particular Member State, SWD(2015) 100 final, 6.5.2015.

[13] COM(2017) 228 final, "Mid-Term Review on the implementation of the Digital Single Market Strategy", 10.5.2017.

[14] COM(2016) 178 final, "European Cloud Initiative - Building a competitive data and knowledge economy in Europe", 19.4.2016.

[15] COM(2017) 134 final, "European Interoperability Framework – Implementation Strategy", 23.3.2017.

[16] COM(2014) 72 final, "Internet Policy and Governance - Europe's role in shaping the future of Internet Governance", 12.2.2014

[17] See Figure 3 - Overview and illustration of the data localisation problem (at the end of section 2).

[18] Other data processing services include data analytics, data management systems, etc.

The territorial scope of the initiative is **limited to the European Union**. It does not address data localisation restrictions put in place by the countries outside the EU or movement of data outside of the EU[19]. This Impact Assessment acknowledges the importance of the international dynamic and of current developments around global data flows, their impacts on EU competitiveness and the importance of protecting fundamental rights[20].

The initiative **does not concern the processing of personal data[21] and the free movement of such data *as governed* by the GDPR and the proposed ePrivacy Regulation**. Specifically, since the GDPR prohibits restrictions on the free movement of personal data within the Union where these are based on reasons connected with the protection of personal data, the initiative deals with data flow restrictions imposed by Member States based on reasons other than the protection of personal data (e.g. security of storage of the data).

For instance, company laws can require local storage of certain corporate information and documents (e.g. registers of shareholders and directors). Those often include personal data, e.g. names of corporate executives. However, the reason for such localisation is to make sure that shareholders and other interested parties can get access to and review the information / documents, and not to protect any personal data. As the GDPR does not address such restrictions, the present initiative will address them.

The initiative also addresses the issue of porting data from one IT environment to another, to the extent that it constitutes a barrier to the movement of data within the EU and the ability to switch cloud service providers or move data back in-house. The initiative will take into account Article 20 of the GDPR, which gives the right to the data subject to receive the personal data concerning him or her from a data controller and the right to transmit those data to another controller. However, this provision cannot be invoked by businesses or public sector entities in B2B data porting scenarios involving personal data, e.g. where a business entity wants to get back or port to another cloud service provider (CSP) all the data sets, including personal data sets.

For instance, a cloud service provider specialising in managing application processes for universities accumulates both personal and non-personal data from the universities using its service (its customer) and stores the data with a major cloud provider (its subcontractor). At some point in time the data service provider wants to switch to another cloud service provider and port all the data it has accumulated to a new subcontractor. This data porting scenario will not fall under Article 20 of the GDPR so that specific issue will be addressed by the initiative.

In this regard the scope of the initiative also differs from the planned online platforms initiative. While the data porting element of this initiative focuses on two-party (cloud provider – cloud user) relationships and seeks to make it easier to port the data provided and controlled by the cloud user, the platforms initiative would focus on the three-party (consumer/business – platform – business) relationship. It would seek to make it easier for businesses offering products or services through platforms to obtain access to the data held by the platform, which has been provided to the platform by the customers of the business concerned while using the platform.

2 Problem Definition

2.1 Relevance of the problem

In an increasingly data-driven economy, data flows are at the core of business processes in

[19] International data flows are dealt with separately under the project team co-managed by Commissioners Jourova, Malmström and Vice-President Ansip and their respective services.
[20] Any transfer of personal data outside the EU must be in compliance with Directive 95/46/EC, which will be replaced by the GDPR on 25 May 2018.
[21] The GDPR defines 'personal data' as any information relating to an identified or identifiable natural person (Art.4.1).

companies of all sizes and in all sectors: from data-intensive ICT companies to manufacturing and agriculture processes, to hospital administration and key electricity infrastructures. In **the public online consultation "European data economy"**, a large number of respondents indicated that they process data in multiple Member States mainly for operational reasons, namely the cross-border character of their activities, the location of subsidiary companies and the satisfaction of consumer expectations in terms of proximity (see further in **Annex 2**). This is equally true for public administrations, not least in supporting data-informed policies and public services delivery within and across borders. Therefore, data is increasingly ubiquitous, supporting all sectors of industry, economy and society.

The nature and role of data in the economy is complex, however. Inherently, data 'travels' across cross-border value chains, where it is generated, collected, curated, processed and analysed, transferred and stored. Its value can increase exponentially when it is aggregated, analysed, or used in innovative ways. Data can become a competitive differentiator and an enabler for innovation and creation of new business models, for example in the fields of data analytics, text and data mining and app development.

However, in the European Union the possibility to build a data economy and to benefit from new technologies which rely on data[22] is undermined by a series of barriers to data mobility, impacting business behaviour in the Single Market.

2.2 Core problem: obstacles to data mobility in the EU single market

"Obstacles to data mobility in the EU single market" is the core problem identified.

"**Data mobility**" refers to the degree in which data can be (re-)located to different IT-systems, regardless of the physical location of such systems in the Union or the owner of such IT-systems, which might be the data holder himself or a data storage and processing service provider/CSP.

A high degree of data mobility is important for realising a European data economy to its full extent, since it is required for core activities of such an economy, for instance data collection, analysis and re-use.

2.3 Problem analysis

Making use of the Better Regulation toolbox[23], the Commission services conducted an extensive analysis of the core problem and its drivers. On the basis of evidence supplied by the public online consultation, the structured dialogues with the Member States and other stakeholders, dedicated support studies, external studies and available data[24], the Commission services have verified the existence of four underlying problems that cause obstacles to data mobility.

Problem 1: Member States' legislative and administrative restrictions

Problem 2: Legal uncertainty

Problem 3: Lack of trust

Obstacles to the movement of data across borders within the EU

Problem 4: Vendor lock-in

Obstacles to the movement of data across IT-systems

Obstacles to data mobility may lead to a large number of negative consequences for European society and economy, hindering the EU's policy objective of creating of a Digital Single Market. Following analysis, the consequences of these obstacles have been divided into four main categories.

Consequence 1: Loss of growth/innovation potential

[22] An estimate shows that 75% of the value added through the Internet (and, implicitly, data flows) rests with traditional industries, see http://europa.eu/rapid/press-release_MEMO-12-759_en.htm.
[23] Specifically, Tool #11: "How to Analyse Problems", http://ec.europa.eu/smart-regulation/guidelines/tool_11_en.htm.
[24] See Annex 1 for a full list of sources used.

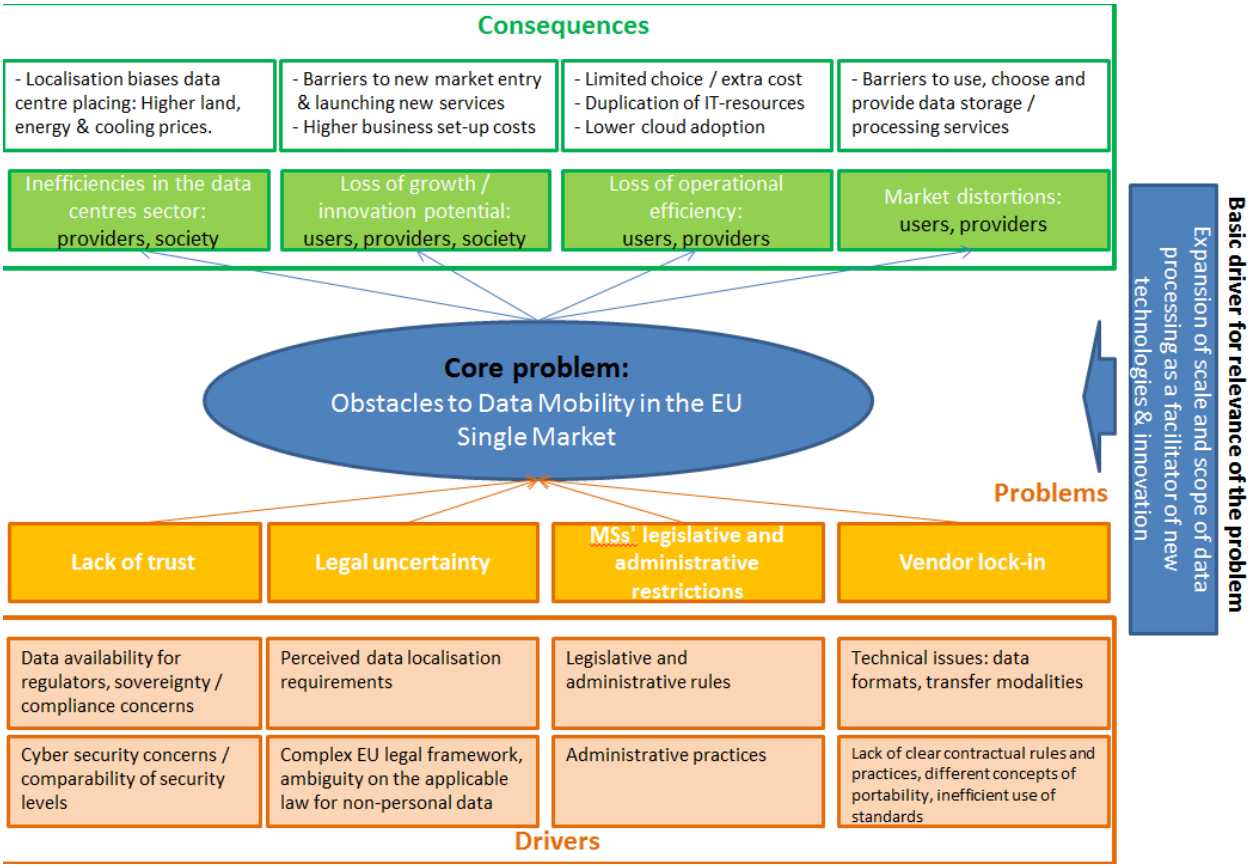
Consequence 2: Loss of operational efficiency

Consequence 3: Inefficiencies in the data centres sector

Consequence 4: Market distortion

For a visual mapping of the problem analysis, see Figure 1: the Problem Tree. In the remainder of this section, the individual problems and consequences will be briefly described, elucidating the many interrelations between them. **For the full problem analysis, comprehensive explanations, examples and extensive references to evidence, the reader is referred to Annex 5**.

Figure 1 - Problem Tree



2.3.1 Underlying problems & drivers

Member States' **legislative and administrative restrictions** form the starting point of the problem analysis, because they represent the most tangible obstacles to data mobility in the EU. To a varying degree, Member States have put in place so-called 'data localisation restrictions'. These are rules that either oblige citizens and businesses to process and store certain categories of data within the territory of the country, or have an equivalent effect. Data localisation restrictions come in many forms, ranging from 'hard law' to 'soft law' measures and administrative practices. National governments are not the only type of actor capable of raising them. Regulatory or supervisory authorities or other sector-level institutions can also do this.

The number of data localisation restrictions has been growing as a response to the digitisation of the economy as a whole and the strong development of the data economy; according to some sources, the number has at least doubled since 2006.[25]

[25] ECIPE, Policy Brief "Unleashing Internal Data Flows in the EU: An Economic Assessment of Data Localisation Measures in the EU Member States", December 2016. Some data localisation measures included in the report fall outside the scope of this initiative.

Member States' reasons for data localisation restrictions

Data localisation measures are adopted by Member States for different reasons, which are prominently data security (in a wide sense, which encompasses concerns like confidentiality, integrity, continuity and accessibility for the controller of the data), and the availability of data for supervisory and regulatory authorities of the Member States.26 This has been confirmed by the bilateral and multilateral exchanges with Member States and private stakeholders, subsequently to the Communication of January 2017.

A study raised that security is a common driver behind data location restrictions imposed by Member States and is often used as "convenient shorthand" for national security, national sovereignty and for security as a public policy task or as a protection of private interests.27 Therefore, some legislative and administrative rules are imposed in order to keep data out of reach of other jurisdictions and limit the access of other governments to specific types of data. Those restrictions reflect concerns to protect the confidentiality of certain types of data, to control access to such data and to oversee legal proceedings in case of unauthorised access, particularly to citizens' data, national sensitive data, privileged information and industrial secrets.

Furthermore, security concerns by Member States are largely unfounded. Localisation is not a proxy for security, but the means of storage is. Contrary to concerns on cyber security, evidence suggests that data stored in large-scale data centres is actually safer than data stored on-site. The economies of scale that are inherent to data centres make it easier to invest in state-of-the-art data security. In addition, CSPs spend much more time and effort on security to be compliant with certain certification schemes as to meet customer expectations and favour demand.

For some legislative and administrative rules, Member States aim at ensuring that the data is immediately available to the national government, administrative authorities and/or law enforcement institutions. A number of the restrictions and requirements are therefore based on considerations that originated in the 'paper era', where documents needed to be physically accessible for scrutiny or where only the original paper version had legal status.

Despite these reasons and objectives, data localisation restrictions often are unjustified or disproportionate, since (i) effective alternative means to achieve the relevant public policy objective are available (e.g. requiring access to accounting and company data could replace outdated measures and obligations requiring accounting and company data to be stored locally) and/or (ii) the scope of a measure is excessive / the measure concerns non-critical data (e.g. requiring all public archives to be stored locally).

One of the main causes for this trend is presumably the attempt by regulators to transfer the given means of control and reassurance tailored for the industrial age to the digital age. According to the OECD, computer services including data storage and data processing services are sensitive to restrictive regulations affecting trade and imposing an additional time burden on companies. It is crucial for these services to be delivered in a timely and agile manner. In view of the fact that all economic activities increasingly depend on them it is understandable why obstacles to such services can generate large economic losses. [28] Therefore respective regulatory barriers have comparatively an even stronger impact on trade, and the progressive emergence of such restrictions is set to increase in gravity in light of the massive expansion of the data economy.

Evidence gathering shows that the data localisation restrictions identified are only part of the core problem. Obstacles to data mobility in the European Union are driven at least as much by market dynamics leading to localisation because of risk-averse behaviour in the face of legal uncertainty.

[26] LE Europe Study (SMART 2016/0016) and TimeLex Study (SMART 2015/0054).
[27] TimeLex (SMART 2015/0054).
[28] Nordås, H., et al. (2014), "Services Trade Restrictiveness Index (STRI): Computer and Related Services", OECD Trade Policy Papers, No. 169, OECD Publishing, Paris.
http://dx.doi.org/10.1787/5jxt4np1pjzt-en

Public and private entities in Europe often assume that they are not allowed to store or process data across borders, while there is actually no restriction in place. This is particular harmful in view of the fact that data services are among the key inputs to any modern economic activity, and that access to such competitive services can help companies - particularly SMEs - integrate into value chains, focus on core competencies and improve productivity.[29]

This phenomenon has several causes. First of all, there is **no explicit prohibition in EU law** against localisation of non-personal data. This gives rise to a large degree of **legal uncertainty** when it comes to cross-border data storage and processing. Several existing EU legislative instruments could be interpreted as prohibiting data localisation, or at least restrictions on services that rely on use of data, but these instruments always apply only to a limited number of cases.

Nearly one quarter of the 45 localisation restrictions identified in the evidence gathering process for this Impact Assessment[30] are exempted from the E-Commerce Directive, and between one quarter and two thirds of the localisation restrictions are excluded from the Services Directive.

Besides, the complexity of applicable legislation also exacerbates legal uncertainty. Apart from the Treaty, different potentially relevant provisions can be found in, among others, the Services Directive, the E-Commerce Directive and the Transparency Directive. This legal patchwork complicates rather than simplifies the matter and does not provide for the robust foundation needed for the emergence of an all-encompassing principle. The result is that European businesses and public sector organisations often store and process their data within the borders of their own Member State.

A data localisation restriction has to be tested against 33 provisions in 5 pieces of EU secondary legislation in order to determine to what extent it is covered by existing EU law.

Legal uncertainty also originates from the manifold and diverse sector-specific guidelines and administrative practices. In highly supervised sectors, such as finance or health, users may have a preference for storing data locally because they assume that it is implicitly required by their regulators.

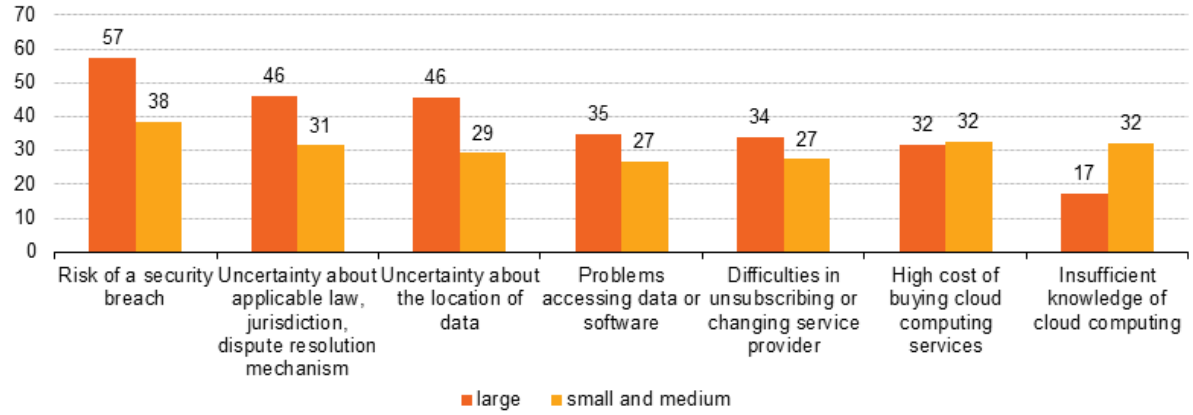
Besides widespread legal uncertainty, the problem of **lack of trust** also constrains data mobility. This lack of trust has two important pillars.

Firstly, there is the broader category of lack of trust in society vis-à-vis certain types of data storage and processing as such (e.g. cloud computing). This type of lack of trust frequently originates from concerns over data security and the protection of sensitive data. It is still rare for customers to rely completely on cloud services for storing their valuable data. Fear of the risk of a security breach is the most common concern, which directly constrains the uptake of cloud services, and which in turn leads to efficiency losses for businesses and, ultimately, society as a whole. Figure 2 below shows that the issue of lack of trust is intertwined with the legal uncertainty problem described above. The combination of both, together with vendor lock-in concerns (referred to below in this section) limits the uptake of cloud services.

[29] Idem

[30] Please refer to Annex 6 for a full list of identified data localisation restrictions.

Figure 2 – factors limiting enterprise use of cloud services



Source: Eurostat (2014)

As indicated above in the textbox on page 8, this type of lack of trust is largely unfounded as evidence suggests that data stored in large-scale data centres is actually safer than data stored on-site.

Secondly, a lack of trust can also be observed in relation to access to data for regulatory/supervisory purposes, when it is stored outside national borders. Certain data localisation restrictions are adopted to ensure the availability of data for inspection/control purposes.[31] The lack of trust surrounding jurisdictional and law enforcement challenges was also raised during the Structured Dialogues with the Member States.[32] Yet, the localisation restriction can be replaced with a functional requirement to ensure data availability for the supervisor, as the data can be made readily available for inspection electronically.[33] This has been exemplified by the amendment to the Danish Bookkeeping Act 2015[34].

In cases where the subject of regulatory oversight does not provide data voluntarily, the Member State might have to resort to issue-specific administrative cross-border access/sharing cooperation mechanisms or judicial cooperation or seek the voluntary assistance of the IT service provider. Cooperation and assistance frameworks have been established in criminal matters, administrative matters, such as taxation, and in financial regulations[35], with different scope of information and entities/supervisors concerned in the various instruments. This variety and the potential delays in judicial cooperation, likely generate uncertainty and lack of trust as to whether a specific (including unforeseen) data availability need could be fulfilled.

Vendor lock-in actions by cloud service providers constitute a form of data localisation restrictions imposed by the private sector, targeting more specifically data mobility across IT-systems instead of data mobility across borders in the EU. This problem occurs when users of data storage or processing services try to switch cloud service providers.

[31] Time.Lex, Spark and Tech4i, "Cross-border Data Flow in the Digital Single Market: Study on Data Location Restrictions", D5. Final Report (SMART 2015/0054) at p.43.
[32] Specifically, workshop held on 23 February 2017.
[33] See to that effect, TimLex Study (SMART 2015/0054) at p. 99: if data should be stored on a server in a specific Member State in order to ensure its accessibility to a national supervisor, then the formal data location requirements can be "recast into a functional accessibility requirement".
[34] Denmark now allows accounting records in electronic format to be stored anywhere without prior application or notification to the public authorities, subject to the requirement on the business to provide online access to the records held abroad at any time. See also Annex 5.
[35] An overview of several sector-specific cooperation frameworks available for public authorities can be found in Annex 8 to this Impact Assessment.

Cloud switching[36] can lead to **prohibitive costs** for cloud customers (and especially SMEs). This includes costs for data transport and licence fees, downtime cost and the need for concurrent services during a transition period, as well as the cost of network use. The aggregate cost can potentially be very high. Numbers vary according to the complexity of each switching scenario, but the Commission has been informed of an anonymised example in which the total costs of data egress for the cloud customer amounted to of EUR 2.700.000 (for more information on the potentially excessive costs of porting data between providers or back in-house, please refer to section 6.2.1.3, the economic assessment of the baseline scenario). Some cloud customers have also reported instances where Cloud Services Providers offer much lower prices for the above cost categories when importing the data on their own systems than when they have to export it to a new destination. Accordingly, they attract customers by offering low thresholds for entry, but 'lock them in' by making switching costly. It is often easier to switch CSPs in the Infrastructure as a Service (IaaS) context, where the services rendered are those of data storage only. Moving into more complex services such as Platform as a Service (PaaS) and especially Software as a Service (SaaS), the difficulties with switching increase. IaaS and PaaS standards can be defined using simple interfaces, but this is mostly not the case with SaaS standards, which at least require more complex interfaces to retrieve the data.

The public online consultation showed that the problem with switching providers is already prevalent, as more than 50% of SME respondents indicated that they experienced difficulties when intending to switch. At the same time, the size and intensity of the problem may become even clearer over time, when the ever-growing cloud services market reaches new stages of dynamism in terms of supply and demand. Today, however, it is already clear that users of storage and processing services are often unaware of technical difficulties, for example in terms of network capacity (bandwidth), which may arise when they want to move their data from one service provider to another or back to their own premises. Also, they often have insufficient or no knowledge of the provisions in their contracts with cloud service providers. Issues at stake here are, for example, the costs of data transfer in the case of termination of contract or what will happen with the data when the service provider ceases to exist as a result of e.g. bankruptcy.

2.3.2 Consequences

Obstacles to data mobility, such as data localisation restrictions, form 'digital border controls' within the European Union and therefore are incompatible with the (digital) single market. They hamper EU businesses that operate cross-border, because certain data would have to be stored in specific and different Member States of activity, therefore leading to multiplication of storage costs. This is disproportionately burdensome for small companies such as start-ups and SMEs. The Scale-Up Europe Manifesto makes a specific reference to this problem: "Enforced data localisation will mean higher costs for the cloud-driven services upon which so many start-ups rely. It will add further uncertainty and immensely greater regulatory burden on fast-growing enterprises, which should rather focus on developing their business…".[37] A direct consequence of this **is a loss in growth and innovation potential** as the (disruptive) innovation potential of start-ups and scale-ups is very high. Next to start-ups and scale-ups, this problem also confronts other SMEs, which in total account for nearly 60% of European GDP and 65% of European employment[38]. Any impact on them would therefore have large implications for the EU economy.

[36] SMART 2016/0032, IDC and Arthur's Legal, "Switching between Cloud Service Providers", 2017 (Ongoing) [IDC and Arthur's Legal Study (SMART 2016/0032)]
[37] The Lisbon Council, Nesta and Open Evidence (2016), "The scale-up Europe manifesto"
[38] Eurostat, "Statistics on small and medium-sized enterprises", September 2015, available at : http://ec.europa.eu/eurostat/statistics-explained/index.php/Statistics_on_small_and_medium-sized_enterprises .

If we assume that SMEs using private cloud services store 50 TB on average and the monthly price per GB of data stored ranges between €0.0224 (low cost location) and €0.5371 (very high cost location), a SME spends between €1010 and €26855 per month.[39] This would mean that an SME would face costs of at least €12120 per year, not considering the administrative costs, if it operates in one Member State. In view of existing and emerging localisation restrictions this cost will potentially duplicate, either fully or partially, for each Member State with respective restrictions where the SME wants to operate in. In particular for start-ups this would undermine cross-border scaling up substantially.

Moreover, a loss in growth and innovation potential will also be incurred because data localisation restrictions form barriers to new types of services that are geographically distributed by design.

The deployment of IoT technologies and applications could suffer from a lack of trust, legal uncertainties or blockages brought by data localisation. With an explosion in the number of connected objects in a variety of application areas – connected cars, manufacturing, energy, agriculture, etc. – data generated by IoT is geographically distributed by design.

According to responses to **the public consultation**, the highest impacts of data localisation restrictions, next to increased costs for business, are on the provision of a service to private or public entities (69.6% of stakeholders responding identified this impact as 'high') or the ability to enter a new market (73.9% of responding stakeholders identified this impact as 'high'). The EU itself is perhaps the most compelling proof that the free provision of services in an internal market leads to growth. Making the provision of cross-border data-based services in the single market more difficult would therefore put a constraint on the European economy.

Moreover, data localisation leads to a **distorted market** for cloud service providers. An important outcome of a dedicated support study showcases that data localisation restrictions force them to make business and investment decisions that lead to suboptimal outcomes in cost, security and operational agility.[40] Already there are large intra-EU price differences for data storage, varying up to 120% between different Member States.

The problem of vendor lock-in also constitutes an obstacle to data mobility; hence it leads directly to market distortions, as it cements the position of larger cloud service providers vis-à-vis new market entrants. Accordingly, vendor lock-in curbs free competition and drives up prices.

Based on the evidence gathered, from the data service (cloud) user perspective, different degrees of impacts caused by obstacles to switching and porting data can be envisaged. These range from very high impact, e.g. where a data service (cloud) provider goes bankrupt without a data porting possibility for the user, and the data is lost; to low, medium or high impact where the possibility to port data exists, but is constrained by technical or contractual issues, and, as a result, the user incurs extra costs and/or decides to port only part of data.

This market failure then leads directly to a **loss of operational efficiency**, which is the consequence caused by, on the one hand, a low-level of cloud adoption in Europe and, on the other hand, a lower level of innovation and efficiency of those cloud services because of the lack of fully free competition in the market. The suboptimal cloud adoption predominantly results from a lack of trust because of data security concerns. Research has confirmed the link between a lack of trust in cloud security and cloud adoption.[41] Also, it may be contended that a lower-than-expected level of cloud adoption derives from vendor lock-in, as this leads to less competitors on the market and therefore

[39] https://azure.microsoft.com/en-us/pricing/details/storage/blobs/ and http://www.telekom.hu/uzleti/szolgaltatasok/informatika/szerverek-adatparkiszolgaltatasok/szerverberles/virtualis-szerverek

[40] SMART 2015/0016, London Economics Europe, Carsa and CharlesRussellSpeechlys, "Facilitating cross border data flow in the Digital Single Market", 2016 [LE Europe Study (SMART 2015/0016)].

[41] Intel and McAffee (2017), "Building trust in a cloudy sky", accessed via: https://www.mcafee.com/us/resources/reports/rp-building-trust-cloudy-sky.pdf

higher prices. To quantify the scale of this problem, one of the Commission's support studies found that all EU businesses can reduce their overall ICT-expenditure by 20% to 50% as a result of adopting cloud solutions.[42] A significantly higher cloud adoption could therefore mean a large leap in the competitiveness of European business.

Finally, **inefficiencies in the data centres sector** are already visible negative consequences of obstacles to data mobility. As a result of intervention (or sometimes: uncertainty about intervention) in the market, cloud service providers locate their data centres in countries with significant markets where data localisation restrictions are in place. If those restrictions would not have been of concern, actors would have been able to base their decisions on different parameters such as energy prices, land prices or the envisaged environmental footprint of data centres in a certain location.

The problems identified in this section have significant (but differing) impacts on various stakeholder groups (see **Annexe 3**). **Annex 2** provides a synopsis report of the public online consultation.

Figure 3 - Overview and illustration of the data localisation problem

Feedback from stakeholders	Two thirds of respondents to the public consultation said that they had knowledge of the existence of data localisation restrictions. **80%** of them stated that their organisations must comply with these restrictions. The issue was also raised in the REFIT platform in April 2017.[43]	
Scale	**Legislative / administrative requirements**	**Localisation driven by legal uncertainty / lack of trust in the market**
	- 56 identified by the studies[44] - 49 sent to MS for the structured dialogues (measures outside scope of initiative were discarded) - 9 removed or to be removed in the future by MS - 20 new measures identified by the public consultation (specific legal acts not always mentioned, some might coincide with those identified by the studies) - Approximately 60-65 known measures in place at the time of this IA - More than two thirds of the sample of 45 analysed in detail could be considered unjustified or disproportionate at the time of this IA **Further details – Annex 5 for the analysis and Annex 6 for the list of measures per Member State**	37% of IT service providers responding to the public consultation had received requests from customers for local data storage or processing, mostly due to an assumption that they were obliged to do so. The providers stated that they duly inform their clients about the applicable rules, but are still asked by those clients to deliver local storage or processing **Further details – Annex 5**
Illustration – current examples	In a paper presented during the Roundtable 'banking in the digital age', organised by the Commission in November 2016, the European Banking Federation	A software as a service provider specialising in integrated solutions for universities has

[42] Deloitte, "Measuring the economic impact of cloud computing in Europe", 2016 (SMART 2014/0031).
[43] An opinion of the REFIT Platform is expected in September 2017).
[44] LE Europe Study (SMART 2016/0016) and TimeLex Study (SMART 2015/0054). Please note that the numbers, descriptions and categorisation of data localisation measures in the studies and this Impact Assessment might differ, since the measures identified by the studies were verified and discussed with the Member States in the context of the structured dialogues before being analysed in the Impact Assessment.

	clearly pleaded for a legal principle on free flow of data, to enable the banking sector to become more efficient.[45] During the Roundtable, a participating bank presented the Commission with the following problem it is experiencing: X bank, a top-10 EU bank, undertook an initiative to increase efficiency, lower costs and improve security through centralisation of IT infrastructures in one Member State, thereby avoiding IT duplication in subsidiaries of the bank. The project was presented to all the national competent authorities concerned for information / approval. All the Central Banks approved the project with the exception of the National Bank of Member State Y, which insisted on local storage based on considerations of distance, the possibility of change of storage configuration in the future and complexity. X bank provided documentation demonstrating low level of those risks. Still, Y National Bank repeatedly rejected the project. As a result, X bank had to maintain redundant IT operations in country Y.	reported that some of their partner universities "believe" that laws applicable to them force them to keep data in their respective countries.
Consequences	The direct consequence is a loss of operational efficiency for X Bank. IT-costs constitute on average 15% of total bank expenditure, which is the second highest cost category (after staff).[46] Moreover, 70% of this spending concerns the operational expenditure (infrastructure and systems)[47]. Research shows that centralisation of IT-systems can lead to 40% of cost reduction on IT operational expenditure.[48] Combining this information, it may be contented that X Bank misses a total cost reduction potential of 4.2% on **overall costs**, at least for the branch in country Y. Indeed, existing evidence shows that diverging data localisation restrictions in the EU lead to IT-inefficiency. 23% of national financial supervisory authorities in the EU states that cloud should never be used by financial institutions, regardless of the type of activity concerned.[49] Nevertheless the ECB mentions that there is large room for improvement of IT-expenditure by EU banks, as the average EU ratio of cost to total assets is 1.4% whereas in the best performing Member State, Sweden, it is just half of that: 0.7%.[50]	The provider deprived of the possibility to scale-up in an important EU market and the ensuing reduction in competitiveness on global markets.

[45] European Banking Federation (2016), "Innovate. Collaborate. Deploy. The EBF vision on banking in the Digital Single Market"
[46] Zeb (2017), "Cutting IT costs in a smart way", accessed via: https://www.bankinghub.eu/banking/operations/cutting-costs-smart-way-swim-aid-cios-pressure
[47] Ibid,
[48] CIO 2010, "Ensure a smooth transition to centralised IT delivery": http://www.cio.co.uk/it-strategy/ensure-a-smooth-transition-to-centralised-it-delivery-3430109/. Examples from banking show that figures can be comparable when migrating systems to the cloud, as the Commonwealth Bank of Australia saved an estimated 30 to 40% through using Cloud: W Kuan Hon and Christopher Millard (2016), "Use by banks of cloud computing: An empirical study"
[49] ENISA (2015), "Secure use of cloud computing in the finance sector"
[50] ECB (2017), accessed via: https://www.ecb.europa.eu/press/key/date/2017/html/ecb.sp170614.en.html

Illustration – future examples	The Commission is working on a new initiative to promote digital innovation in health and care[51]. One of the 3 pillars is "Connecting and sharing data and expertise to advance research, personalise health and care, and better anticipate epidemics". Specifically, the diagnosis of rare diseases could be substantially improved by applying analytics to large pools of data gathered from all over the EU, including the use of artificial intelligence technologies. Data localisation restrictions in the health sector are likely to undermine such pooling of data.[52]	Blockchain is a promising new technological approach to data storage and processing. Instead of relying on huge data centres, it distributes data storage and processing to a large (and potentially unlimited) number of computing resources called "nodes". Blockchain already underpins crypto-currencies (bitcoin, ether). Numerous start-ups are working on ways to deploy blockchain in other areas, e.g. recording identities of and operations associated with things connected to the Internet, organising land registries, etc. Widespread market assumption that data localisation is required is likely to be an obstacle to innovations based on the multiple-location blockchain approach.
Consequences	The realisation of the full potential of digital technologies in health and care inhibited.	The realisation of the full potential of technological and business innovation inhibited.
Possibility to solve the problem under the existing framework(s)	Very limited as confirmed by the structured dialogues with Member States and the Commission's own analysis. **For further details, please refer to section 6.3.1.1, Annex 5 and Annex 7**	Limited in view of the challenges identified during the structured dialogues with Member States, complexity of existing frameworks and absence of a clear free movement of non-personal data principle. **For further details, please refer to Annex 5**

3 Why should the EU act?

3.1 Does the EU have the right to act?

Article 114 of the Treaty on the Functioning of the European Union (TFEU) confers on the EU the power to adopt measures, including regulations, which have as their object the establishment and functioning of the internal market.

Removing obstacles to the movement of data across borders and obstacles to the movement of data across cloud service providers / in-house IT systems as well as preventing the emergence of the new

[51] European Commission – Press Release, "Commission launches public consultation on Health and Care in the Digital Single Market", http://europa.eu/rapid/press-release_IP-17-2085_en.htm .

[52] As explained in section 1.4 above, if these restrictions are based on reasons connected with the protection of personal data, the prohibition under the GDPR applies. However, if they are imposed for reasons other than the protection of personal data (e.g. security of storage of the data), the free movement of data provisions of this initiative would apply.

ones would contribute to stimulating a competitive and innovative EU single market for data storage and processing services.

3.2 What would be the added value of action at EU level?

An EU level initiative would address the problem of legal uncertainty by establishing a clear free movement of data principle covering the whole Union and fostering common approaches to and awareness of the legal possibilities to store and process data at the location and using the service or IT system chosen by an enterprise or a public sector organisation.

As demonstrated above, both obstacles to the movement of data across borders and obstacles to the movement of data across cloud service providers / in-house IT systems are widespread in the EU. They concern different economic sectors and have been detected in many Member States.

Therefore, the initiative is a precondition for the development of an innovative and competitive European data economy. It is an enabler of efficient allocation of resources and exploitation of the economies of scale. It is an important factor in creating an environment that attracts foreign investment to the EU. Furthermore, the initiative will give an impulse to economic growth in the EU, leading to GDP gains of up to EUR 8 billion or 0.06%) per year, as a dedicated study estimated.[53] To put these benefits in perspective, they would be on par with recently concluded free trade agreements (FTA), such as the FTA between the EU and South-Korea. EU intervention through this initiative would therefore answer directly to the Commission's overall policy objective of creating jobs and growth for the EU.

EU intervention would also contribute to the development of a safe and trustworthy data space, while avoiding the proliferation of potentially different and conflicting requirements to ensure data availability for regulatory control or security of data storage and processing. This is particularly necessary because data value chains are not bound by territorial borders and are increasingly in operation across different Member States.

A survey on the data economy by Noerr LPP (119 replies covering 20 Member States) revealed that a majority consider that "any regulation must be European, not national".

3.2.1 Subsidiarity

The initiative is fully in line with the subsidiarity principle, because there is no possible action at national, regional or local level that could be more effective than EU-intervention.

Obstacles to cross-border data mobility constitute the core problem underpinning the proposed EU-action. As the cross-border element is obviously a fundamental aspect of this problem, the initiative should be supranational in nature and cannot be tackled at Member State-level.

Member States are able to reduce the number and range of their own data localisation restrictions, but are likely to do so to different extents, at different rates and in different ways or not at all.

Similarly, Member States could take initiatives at national level to set the conditions for switching cloud service providers and porting data between providers and/or users' own IT systems. However, none of these separate actions would induce EU-wide principles. Therefore, they would lead to multiplication of regulatory requirements across the EU single market, hence fragmentation, and tangible additional costs for enterprises, especially SMEs. As stated above, the only way to credibly confront these problems is by introducing general legislative principles at European level. This would provide legal certainty regarding the different intervention areas of this initiative, vis-à-vis both Member States public authorities and the private sector.

[53] ECIPE, Policy Brief "Unleashing Internal Data Flows in the EU: An Economic Assessment of Data Localisation Measures in the EU Member States", December 2016.

3.3 Consistency with other EU policies and with the Charter of Fundamental Rights

The initiative pursues the objectives set in the DSM Strategy, its recent mid-term review, as well as the Political Guidelines for the current European Commission - "A New Start for Europe: My Agenda for Jobs, Growth, Fairness and Democratic Change".

Together with the GDPR, the initiative would put in place a comprehensive and consistent EU framework enabling free movement of data in the EU single market as well as movement of data between data cloud service providers and in-house IT systems.

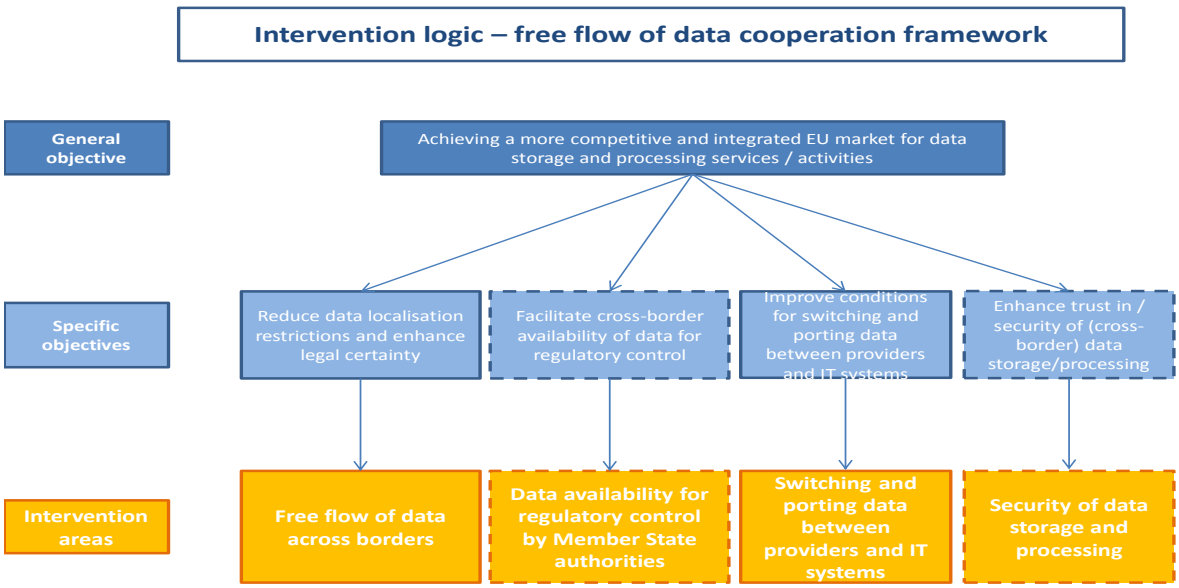
The initiative is consistent with the E-commerce Directive, Services Directive and the Transparency Directive: it pursues the ambition to create an effective EU single market for data-based services, just as those Directives aim at a comprehensive and effective EU single market for services. It is also consistent with the NIS Directive: the NIS Directive provides legal measures to boost the overall level of cybersecurity in the EU; this initiative aims to enhance cyber resilience of cross-border storage and processing of data, relying on the NIS Directive.

The initiative would promote rights enshrined in the Charter of Fundamental Rights. In particular, it would promote the freedom of information (Article 11), since enhancing transparency is an important element of the initiative. The freedom to conduct a business (Article 16) would also be promoted since this initiative would contribute to eliminating and preventing unjustified or disproportionate barriers to the use and provision cloud services as well as configuration of in-house IT systems.

4 What should be achieved?

The following diagram summarises the intervention logic that inspired the proposal, providing the necessary links between the general objective of the intervention, its specific objectives and the intervention areas.

Figure 4 – Intervention logic of the initiative



4.1 General policy objectives

The general policy objective of the initiative is to achieve a more competitive and integrated EU market for data storage and processing services and activities.

4.2 Specific policy objectives

1) Reduce the number and range of data localisation restrictions, enhance legal certainty and transparency of remaining (justified and proportionate) requirements;
2) Facilitate cross-border availability of data for regulatory control purposes, specifically when that data is stored / processed in another Member State, reducing the propensity of Member States to impose data localisation restrictions for that purpose;
3) Improve the conditions under which users can switch data storage and processing (cloud) service providers and port their data to a new provider or back to their own IT systems;
4) Enhance trust in and the security of (cross-border) data storage and processing[54], reducing the propensity of market players and the public sector to use localisation as a default safe option.

The four specific objectives identified are closely linked to the problems described in section 2. In particular:

- The first specific objective targets concrete and existing legal and administrative data localisation restrictions, as well as localisation restrictions that may be adopted by Member States in the future. This would create a more efficient and environmentally friendly data centre sector and effectively address the problem of legal uncertainty as to the existence and scope of application of data localisation restrictions and the extent to which the existing EU rules mandate the free movement of data.
- The second specific objective facilitates the achievement of the first one and is focused on reducing the lack of trust in the free movement of data stemming from Member States' concerns about data availability for regulatory control purposes or data sovereignty.
- The third specific objective targets vendor lock-in situations on the data services (cloud) market.
- The fourth specific objective also facilitates the achievement of the first one. It focuses on enhancing trust through enhanced cyber resilience levels of cloud services in Europe.

4.3 Intervention Areas

To achieve these objectives, four **areas of intervention** have been identified, taking into account the results of the structured dialogue with the Member States and the results of the public consultation:

- Free flow of data across borders;
- Data availability for regulatory control by Member State authorities;
- Switching and porting data between providers and IT systems;
- Security of data storage and processing.

5 What are the various options to achieve the objectives?

Options projecting different levels of intervention are considered: from no EU policy change to low-intensity non-legislative intervention to high-intensity legislative intervention. The nature of the area / objective (core or supportive) is taken into account when formulating and describing the options.

The no change/baseline scenario is being used as the benchmark against which the alternative options should be compared, in line with the provisions in the Better Regulation Guidelines.

[54] In line with but separate from horizontal ICT security frameworks and initiatives.

Discarded options are also mentioned. As prescribed by the Better Regulation Guidelines, section 5 is merely descriptive, while the impacts of the policy options are presented in section 6.

5.1 Discarded options

The option of revising existing EU sectorial legislation (e.g. the INSPIRE Directive[55]) with a view to limiting the scope for unjustified data localisation has been discarded. This is because it would not be able to overcome the significant problem that some data localisation restrictions might not fall within the scope of this legislation, and eventual revisions might not take the free flow of data dimension into account. Limiting the intervention to specific sectors would also ignore the evolving nature of the problem and the need to offer an innovation-friendly legal environment in an expanding data economy.

Other options would be to revise the E-commerce Directive[56], the Single Market Transparency Directive (SMTD)[57] or the Services Directive[58].

However, amending the E-commerce Directive or the Services Directive to introduce the free flow of data provisions would be disproportionate and ineffective. This is because many provisions would have to be modified with the data issue in mind, meaning that such revision would go beyond mere technical adaptation. Secondly the lists of sectors/services excluded from the scope of these Directives, for example important sectors such as transport, telecommunications or healthcare in the case of the Services Directive, would need to be reviewed.

Amending the SMTD would not address data localisation restrictions effectively as the Commission cannot, under that Directive, adopt legally binding decisions requesting the Member States to refrain from adopting the notified requirements.

The GDPR provisions addressing data portability covers only personal data.[59] Provisions would have to be expanded in scope to also cover switching of cloud services providers, which is a different kind of portability as it concerns a change of data processors, which often concerns in practice large volumes of business data. The technical conditions under which portability could take place are therefore distinct in the case of switching cloud providers. Furthermore, cloud services are used in almost every sector. Introducing the principle of switching cloud services providers in sectoral legislation would mean amending a large amount of legislation, and this has not been deemed feasible.

As regards the intervention area of security of data storage and processing, addressing it by means of additional legislative provisions has been discarded in view of the recent adoption of the NIS Directive and the planned initiative on the EU ICT security certification framework.

5.2 Option 0: Baseline scenario - no EU policy change

This option would imply:

- Relying on the Member States to progressively replace data localisation restrictions with less intrusive measures and not to introduce new (unjustified and disproportionate) data localisation restrictions. In practice, notifications under the Transparency Directive would be examined and - although unlikely - infringement proceedings could be launched on a case by case basis where

[55] Directive 2007/2/EC (OJ L 108, 25.4.2007, p. 1–14). The Directive established the Infrastructure for Spatial Information for the purposes of Union environmental policies. See the 2016 Report and REFIT evaluation: http://inspire.ec.europa.eu/news/commissions-inspire-report-and-refit-evaluation-published.
[56] Directive 2000/31/EC (OJ L 178, 17/07/2000, p. 1-16).
[57] Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (Text with EEA relevance) (OJ L 241, 17.9.2015, p. 1).
[58] Directive 2006/123/EC (OJ L 376, 27.12.2006, p. 36–68).
[59] GDPR, Article 20.

strong evidence can be gathered to show that the restriction has a direct and significant impact on the cross-border provision of a service.

- That Member State authorities seeking data stored or processed in another Member State would continue to rely on (i) requests addressed to the subject of regulatory oversight / holder of the data as well as (ii) formal judicial cooperation requests and / or (iii) other cooperation / assistance frameworks where these exist, and which are of varying scope and degrees of effectiveness / efficiency.

- Relying on market players to introduce technical and contractual conditions progressively to enable data portability and facilitate the switching of data (cloud) service providers.

- Relying on the NIS Directive and related instruments to provide a benchmark for a common level of security of data storage and processing.

5.3 Option 1: Non-legislative initiatives to promote trustworthy free flow of data across borders and facilitate switching and porting data between providers and IT systems

This option would:

- Provide guidelines on the existing EU instruments relevant to data localisation restrictions, their scope of application, applicable provisions and exceptions as well as best practices in addressing the functional requirements underpinning data localisation (including guidelines on data availability for regulatory control by Member State authorities and security of data storage and processing).

- Imply a strengthened enforcement of existing EU legislation vis-à-vis different categories of unjustified or disproportionate data localisation restrictions imposed by Member States, e.g. by giving priority to the preparation of this type of cases.

- Encourage Member States, e.g. by means of transparency mechanisms under existing legislation, to enhance the transparency of (justified and proportionate) data localisation restrictions as well as any requirements concerning data availability for regulatory control by Member State authorities and security of data storage and processing.

- Foster regular discussions between Member State representatives and the Commission on issues that may be identified regarding the availability of data for regulatory control by Member States' authorities and ways to resolve them, using existing (sectoral) guidelines, and cooperation mechanisms such as these listed in **Annex 8**.

- Provide EU-level guidelines on best practices in facilitating switching cloud service providers and porting data to a new provider or back to users' own IT systems.

- Encourage self- and co-regulation by market players to work out the technical and contractual conditions of switching / data porting, as well as data security.

5.4 Option 2: Principles-based legislative initiative and cooperation framework to ensure trustworthy free flow of data across borders and facilitate switching and porting data between providers and IT systems

This option would:

- Lay down the principle of free flow of data within the EU requiring Member States not to put in place unjustified or disproportionate data localisation restrictions. Under this Option, in principle all data localisation restrictions for reasons other than protecting public security would be considered unjustified or disproportionate restrictions. It would require Member States to notify any new data localisation restriction they intend to put in place by means of the existing notification scheme of the Transparency Directive and to carry out a review of / notify existing measures during a transitional period; ensure transparency and proportionality of remaining (justified) data localisation restrictions.

- Lay down the principle whereby a user of a data storage and/or processing service that is subject to regulatory oversight or regulatory compliance obligations shall not deny access to data to a competent authority of a Member State that has the right to obtain the data for regulatory control purposes when the data is stored and/or further processed in another Member State. It would provide for cooperation between the Member States on obtaining access to the data where existing cooperation / mutual assistance frameworks cannot be relied on as well as an implementing act laying down details of the procedures for the cooperation on obtaining access to data.

- Lay down the principle that data storage and/or processing service providers should facilitate data porting for switching providers or porting data back to users' own IT systems; require that cloud service providers explain in a sufficiently detailed, clear and transparent manner (including in contracts) the processes (e.g. scope, exit plan and support services), technical requirements (e.g. data formats and supports), timeframes and charges that apply in those situations as well as the extent of a data return guarantee in the case of bankruptcy; encourage self-regulation to work out the detailed technical and legal conditions of switching / data porting.

- Identify and develop reliable common standards and/or requirements for the security of storage and/or processing of data. In particular, a cloud-specific EU-level set of binding requirements could be established in an implementing act. In practice, the Commission would work with the DSM cloud stakeholder platform[60] to prepare ground for the future cloud-specific requirements.

- Envisage the designation by each Member State of a single point of contact, who shall be responsible for coordinating the application of this Regulation in the Member State and, specifically, coordinate the cooperation on access to data.

- Establish an expert group composed of the single contact points. The group could advise on a consistent application of the principles in all Member States. It could exchange experience and good practice regarding the removal of data localisation requirements and the cooperation of competent authorities for the purpose of ensuring data availability for regulatory control purposes as well as give opinions on, and develop model contracts or guidelines facilitating data availability. It could meet and coordinate with data protection and cyber security authorities and sectoral regulators as needed. It could discuss and engage in raising awareness of the free movement of data principle.

The principles-based legislation would be detailed and made operational using several instruments: the notification and transparency requirements, implementing acts (in all the intervention areas of this initiative except for the free flow of data across borders), advice and opinions of the expert group and self-regulation.

Sub-option 2a

In view of the different nature of the various intervention areas of this initiative (as defined in section 4.3), a sub-option to Option 2 was developed to allow for the assessment of a combination of binding substantive provisions establishing the free flow of data principle and ensuring access to data for regulatory control purposes on the one hand, and softer measures for data porting and security of data storage and processing on the other hand.

Specifically, this sub-option is based on the elements described above for Option 2, except that:

- for data porting upon switching providers or porting data back to users' own IT systems, it would not put a legal obligation on data storage and/or processing service providers to facilitate data

[60] The recently created Digital Single Market cloud stakeholder platform will provide for a stakeholder engagement platform with the purpose of interacting with the broadest possible collection of stakeholders in order to ensure valuable and multi-perspective participation and commitment on the various current and emerging issues along the cloud computing value chain. The objective of the DSM cloud stakeholder platform is to contribute to the development of a European cloud ecosystem and provide input for imminent EU policies in the context of the Digital Single Market. Its main workstreams envisaged are data (cloud) security and certification, and portability/switching of cloud providers. The preparatory meeting took place on 29 June 2017. See further http://netfuturesconference.eu/cloud-stakeholders-kick-off-meeting/

porting, but it would require the Commission to encourage service providers to develop self-regulatory codes of conduct.

- for the security of data storage and/or processing, it would merely provide for the clarification that any existing security requirements for companies continue to apply to them, regardless the location in the EU where their data is stored or processed and also when this is subject to outsourcing to a cloud service provider.

5.5 Option 3: Detailed legislative initiative to ensure trustworthy free flow of data across borders and facilitate switching and porting data between providers and IT systems

This option would:

- Establish pre-defined (harmonised) assessments of what constitutes (un)justified and (dis)proportionate data localisation restrictions as well as a detailed mechanism to ensure transparency of white-listed data localisation restrictions (dedicated platform).

- Establish a horizontal, cross-sector mandatory cooperation framework to enforce access rights of public authorities to data when it is stored and/or processed in another Member State: competent authorities, deadlines, common request / response templates would be specified.

- Establish both the obligation to facilitate switching / porting and harmonise the key technical and legal conditions (e.g. concerning types of data, usable formats / structures, timeliness). It would require cloud service providers to explain in a sufficiently detailed and accessible manner (including in contracts) the processes (e.g. scope, exit plan and services), technical requirements (e.g. data formats and supports), timeframes and charges that apply in those situations.

- Develop common standards and a European certification scheme for the security of storage and processing of data and mandate its use.

- Envisage implementing acts in all the intervention areas of this initiative and a dedicated Committee[61].

Figure 5 - Summary of measures envisaged by the options in the four intervention areas:

Intervention areas / Options	Free flow of data across borders	Data availability for regulatory control by Member State authorities	Switching and porting data between providers and IT systems	Security of data storage and processing
0-Baseline	-	-	-	-
1- Non-legislative initiatives	Guidelines, enforcement, transparency	Guidelines	Guidelines, self/co-regulation	Guidelines
2- Principles-based legislative initiative and cooperation framework	Legal principle, notification, review, transparency, awareness	Legal principle, MS cooperation, comitology, awareness raising	Legal principle, transparency, self/co-regulation, , comitology,	Standards, cloud-specific requirements, comitology, awareness

[61] As defined by Regulation No. 182/2011 of 16 February 2011, laying down the rules and general principles concerning mechanisms for control by Member States of the Commission's exercise of implementing powers.

	raising		awareness raising	raising
	← *single contact points, expert group* →			
2a	Same as 2	Same as 2	Self/co-regulation, comitology, awareness raising	Enhancing legal certainty on applicable security requirements.
3- Detailed legislative initiative	Harmonisation, transparency, comitology	Mechanism, comitology	Legal principle and conditions, transparency, comitology	Standards, certification, comitology

5.6 Choice of legal instrument

The realisation of Option 0 does not require a new legislative instrument.

Option 1 could take the form of a new Commission Recommendation(s).

Options 2, 2a and 3 could take the form of either a Directive or a Regulation. They would be best implemented through a Regulation, since it would ensure that the new rules are applicable in all Member States at the same time as well as a uniform approach in the EU's entire single market, which is particularly important to guarantee the legal certainty to enterprises and public sector organisations concerned.

Also, as demonstrated before, at least two of the three drivers to the basic problem of obstacles to data mobility (legal uncertainty and lack of trust) are underpinned by important psychological elements. Therefore, these problem drivers can best be solved by introducing clear principles in a Regulation and subsequently raising awareness about them.

A Directive, while also representing a legislative approach, could solve the lack of trust to a certain degree, maintain some flexibility as regards implementation and would fit with a principles-based approach. However, it would bring less legal certainty, and the time period between adoption and the start of implementation would be longer due to the need to transpose a Directive into the national laws of Member States.

The public consultation showed that a majority of participating stakeholders (55.3% of respondents) believe that legislative action is the most appropriate instrument to tackle unjustified localisation restrictions, with a number of them calling explicitly for a Regulation[62]. IT service providers of all sizes, both from the EU and abroad, show the highest support for regulatory action. In a written answer to the public consultation, one of them explained its position: "Without a concrete legislative instrument, Member States may not be incentivized to change laws to remove existing data localization measures. Worse, they may continue to enact new ones."

Most respondents see a combination of a legislative instrument and increasing the transparency of justified restrictions as the most appropriate option. They generally make the same argument, referring to increased legal certainty and trust.

Respondents also took the view that a Regulation would send the strongest signal to the international community, showing that the EU takes leadership on the free movement of data. As

[62] 289 stakeholders participated in this multiple-choice question of the public consultation. Respondents were not asked about *the type of* legislative action, but 12 stakeholders, on their own initiative, took the possibility to explicitly call for a Regulation in a written comment. This stakeholder group was of a diverse nature, consisting of 2 Member States, 3 business associations, 6 IT service providers and a law firm.

there are already data localisation restrictions currently in place, a number of these respondents also call for transparency on the approach to those existing restrictions.

6 What are the impacts of the different policy options and who will be affected?

6.1 Approach and impact categories

The following impact analysis is based on the results of the public consultation, the structured dialogues with the Member States and other stakeholders, studies funded by the European Commission, several analytical tools developed by the European Commission[63] and publicly available information. Most of these sources provide qualitative rather than quantitative insights. The sections below will assess the impacts of the policy options presented in section 5, considering the following impact categories:

1. Economic impacts
2. Environmental and social impacts
3. Impacts on Member States' public authorities

For each category, impacts are also reflected from stakeholders' points of view, on the basis of feedback received during the various steps of assessment (a more detailed assessment of impacts on specific stakeholder categories is provided in **Annex 3):**.

4. Stakeholder views

6.2 Option 0: Baseline scenario - no EU policy change

6.2.1 Economic impacts

6.2.1.1 Free flow of data across borders

Under this option, Member States would have **wide discretion to put in place new data localisation restrictions and maintain the existing ones**. This discretion is constrained by (i) the Treaty provisions on the free movement of services and the freedom of establishment; (ii) relevant EU secondary legislation, notably the e-Commerce Directive and the Services Directive and (iii) the Commission's actions to ensure the effective implementation of the Treaty provisions and the legislation, notably through infringement proceedings.

These **legal constraints are only partially effective**, since they either (i) do not cover all the types of data storage or processing activities addressed in this Impact Assessment (e.g. many are excluded from the scope of application of the e-Commerce Directive and/or the Services Directive) or (ii) could only produce tangible results in the long term. For example, infringement proceedings take on average 4-5 years[64] until they result in a court ruling. Before such judicial clarification legal uncertainty would prevail, leading users of data-based services to demand local data storage and/or processing from the service provider (60% of European IT service providers who participated in the public consultation of 2017 indicated that their customers have demanded local storage of their data) and harming the prospects of the fast-developing data economy. **See section 6.3.1.1 (infringements text box) and Annex 5 for more details**.

Outcome of the structured dialogues with Member States:

[63] *e.g.* the "Institutional Cost Estimation tool" used to calculate Full Time Equivalent cost parameters, developed in the the support study for the Impact assessment of the European Electronic Communications Code (SMART 2015/0005).

[64] From the launch of the proceeding to the EU first instance court ruling. See http://ec.europa.eu/internal_market/scoreboard/performance_by_governance_tool/infringements/index_en.htm and https://curia.europa.eu/jcms/upload/docs/application/pdf/2017-02/cp170017en.pdf

In the case no substantial EU-level policy action were undertaken, as would be the case under Option 0, some Member States that believe in and support free movement of data across borders can remove some data localisation restrictions, possibly even unilaterally. For instance, Denmark changed its Bookkeeping Act already in 2015 to replace the requirement to obtain an individual authorisation to keep data abroad with a functional requirement to provide an online access to Danish supervisory authorities.

Nevertheless, as a result of the structured dialogues, only a few Member States are expected to do so without any EU-level policy action, depending on their national policies. This would lead to an unequal regulatory landscape and an unequal level playing field for businesses in the EU.

In addition, Member States may have different views on which categories of localisation are unjustified. For example, the same Member State as mentioned above, Denmark, maintains some other localisation restrictions concerning public sector data / registries.

Option 0 implies that when making business decisions about data storage or processing activities (notably, their location) **cloud service providers** have to take into account data localisation restrictions as opposed to a market-driven approach. In particular, cloud service providers have to (i) build local data centres even if the provider could serve its users from a data centre located elsewhere or (ii) choose less ideal locations for planned data centre infrastructures or (iii) outsource processing activities to more expensive local service providers. These factors have a **direct effect** on the choice of location and could result in additional costs for cloud service providers, posing a constraint for the **operational efficiency** of the industry.

Deploying cloud data centres beyond the needs dictated by the market, or limiting choices for the location of a planned data centre can have serious **cost implications**. The table below shows a comparison of typical data centre lifetime[65] costs in the EU 28 Member States (excluding land costs and capital costs associated with servers and other equipment)[66]. The EU average is 276.9 million €, the most expensive location is Belgium (421.4 million €), and the cheapest location is Bulgaria (81 million €). This additional cost cascades down the value chain to the consumer eventually.

Figure 6 - Ten year lifetime costs for cloud data servers in EU28 Member States

	Construction and ten years of operating costs €m	Rank
EU28 average	276.9	
Austria	350.8	7
Belgium	421.4	1
Bulgaria	81.0	25
Croatia	145.0	19
Cyprus	n/a	
Czech Rep.	185.1	16
Denmark	356.9	5
Estonia	144.0	20
Finland	318.4	10
France	339.1	8
Germany	324.8	9
Greece	187.9	15
Hungary	164.9	18
Ireland	356.9	4
Italy	301.3	12
Latvia	127.9	22

[65] The typical lifetime of a data centre is 10 years, with servers being replaced every 3 to 5 years

[66] time.lex, Spark and Tech4i, "Cross-border Data Flow in the Digital Single Market: Study on Data Location Restrictions", D5. Final Report (SMART 2015/0054).

Lithuania	116.8	23
Netherlands	356.8	6
Poland	130.2	21
Portugal	213.1	13
Romania	88.0	24
Slovakia	178.8	17
Slovenia	205.7	14
Spain	306.2	11
Sweden	389.8	2
UK	359.4	3

(Source: Timelex, Spark 2016)

The proliferation of data localisation restrictions would mean that organisations carrying out data processing activities in several Member States and using in-house IT systems for that purpose would need to set up dedicated data storage or processing IT systems for those Member States imposing restrictions.

It could be argued that Option 0 would protect (small) cloud service providers operating in Member States with data localisation restrictions from foreign **competition**. However, the competitiveness of all cloud service providers operating in multiple territories would be curtailed by the lack of possibility to benefit from economies of scale.

Clearly, a much more likely outcome in terms of competitiveness, especially in the medium term, is that large cloud service providers active in multiple territories will serve some of the markets of the Member States imposing data localisation restrictions.[67] The real reduction in competitiveness will be seen by **smaller providers and SMEs** that have spare capacity to serve foreign users and export their services but are not able to do so due to data localisation restrictions.

As regards organisations using in-house data storage or processing IT systems, the reduction in competitiveness is likely to affect those organisations that are based in the Member States where the costs of installing and running such IT systems is relatively high and that compete with market players from other Member States (e.g. banks).

The public consultation highlighted that localisation restrictions drive up the **cost of setting up a new business**. Several respondents maintained that if scaling across Europe is more expensive than scaling globally, start-ups will continue moving to other parts of the world to scale there. A recent study procured by the Commission indicates that 1 out of 7 European scale-ups move their headquarters abroad. 83% of them choose the United States, of which a majority ends up in Silicon Valley.[68] Option 0 would not be able to counter this trend and would therefore lead to a loss of growth and innovation potential for the European economy.

6.2.1.2 Data availability for regulatory control by Member State authorities

The economic impacts of this option are expected to be mostly of qualitative and indirect nature. Option 0 does not foresee any type of cooperation mechanism or legislative action so it is likely to reiterate some of the problems highlighted in section 2 concerning the causes and effects of lack of trust.

Even in the absence of any type of intervention the data market will continue to evolve and cross-border data flows will continue to increase, only at a slower pace. IMF data from 2008 to 2012

[67] See London Economics Europe, "Facilitating cross border data flow in the Digital Single Market", 2016 (SMART 2015/0016), pp..35-36 and this overview http://uk.advfn.com/stock-market/NASDAQ/GOOGL/share-news/U-S-Tech-Firms-Dominate-Cloud-Services-in-Western/72136481

[68] Europe Direct 2017, "Study on transatlantic dynamics of new high growth innovative firms" accessed via: http://ec.europa.eu/research/innovation-union/pdf/expert-groups/rise/transatlantic-dynamics_final-report.pdf

present cross-border information flows as the fastest growing component of US as well as EU trade[69]. For more information on the magnitude of cross-border data flows see **Annex 9**. Governments are likely to face an increase in requests for access to data aimed at other jurisdictions, resulting in increased **administrative burden**.

Under Option 0, the lack of trust via-a-vis cross-border storage would persist, altering market dynamics and the choice of market operators and having an indirect effect on their **operational efficiency**. This lack of trust will foster market fragmentation for data storage, **hampering innovation and competitiveness** of the companies in the market. The upstream market structure (cloud service providers) would be distorted by the survival of less efficient companies exploiting localisation restrictions in order to be able to maintain higher prices. The costs would be passed on to the **downstream market** (business users).

If Option 0 leads to high administrative burdens, the impact on economic operators will be cost inefficiency, suboptimal allocation of resources and hence limited growth and competitiveness.

Switching and porting data between providers and IT systems

Vendor lock-in practices have several economic impacts, as cited in the survey on switching cloud providers[70] and in the responses to the public consultation[71]. These would persist under Option 0.

Macro-economic impacts
In the dedicated study 'Switching Cloud Providers'[72] that was conducted on behalf of the Commission, the possible effect on the growth of cloud computing in Europe is described for Option 0, forecasting demand for public cloud to grow by 18.7 % Compound Annual Growth Rate during the period 2018-2025, and reaching €64.9 billion in 2025. That is less than the baseline market prediction of an authority in the cloud computing sector, projecting a CAGR of 23% annually until 2020 for cloud services.[73] Still, the study predicts this even **lower than baseline growth scenario** under Option 0, as SMEs would continue to lag behind larger companies in the take-up of public cloud, resulting in an unequal level playing field. National governments could also take independent action to support data portability in cloud switching, creating fragmentation in the EU cloud market.

Impacts on business users of data storage and processing services
In the situation currently existing on European markets, which Option 0 leaves unchanged, the technical and contractual difficulties with switching can lead to **excessive portability costs** for business users of cloud services**.** As evidenced by the dedicated study mentioned above, these costs are relatively much heavier for smaller business users, sometimes even higher than the total annual runtime cost of the cloud service itself.

There are different categories of portability costs, such as – but not limited to:

- Data egress cost (i.e. the amount charged for data traffic out of the premises of the CSP);
- Transport fees for transporting the data to its new location;
- Cost of downtime;
- Cost of concurrent cloud use (during the porting process);
- External expertise and/or internal resource costs.[74]

[69] Aaronson, Susan Ariel, "Why Trade Agreements are not Setting Information Free: The Lost History and Reinvigorated Debate over Cross-Border Data Flows, Human Rights and National Security", 2015.
[70] IDC and Arthur's Legal, "Switching Cloud Service Providers", 2017 (SMART 2016/0032).
[71] Public Online Consultation on Building a European Data Economy (10 January 2017 – 26 April 2017).
[72] IDC and Arthur's Legal, "Switching Cloud Service Providers", 2017 (SMART 2016/0032).
[73] IDC, Cloudview 2016
[74] IDC and Arthur's Legal, "Switching Cloud Service Providers", 2017 (SMART 2016/0032).

Whereas the exact portability costs always depend on, firstly, the complexity of the digital architecture used and, secondly, the amount of data stored, one element does not change: the cloud customer is completely dependent on the cloud service provider regarding the technical capabilities of the provider to export the data from its premises. The method of data egress does not only affect the transport costs, but also the costs of downtime and concurrent cloud use, because exporting the data of a mid-sized company, when using 'ordinary' internet-browsing speeds, can take months.

The study provides estimations of the height of these costs, modelled to three different use cases: a **simple** case (a relatively simple application of an entrepreneur running the equivalent of under ten PCs and some simple office programs in the cloud), a **medium-complex** case (a commercial application (cloud capacity of the equivalent of <100 PCs, running a large database such as a CRM system) and a **complex** case (an enterprise application landscape of approximately 350 equivalent PC's with distributed data sources). The following figures extracted from the study's analysis show that the 'simple' case users – representing typically smaller business users such as start-ups or SMEs – relatively face the highest portability costs:

	Portability cost (p.c.)	**Yearly runtime cost (y.r.c.)**	**p.c. relative to y.r.c.**
Simple	18.800 EUR	15.000 EUR	125%
Medium Complex	119.400 EUR	120.000 EUR	99.5%
Complex	231.400 EUR	600.000 EUR	38.6%

This example shows that portability costs may become prohibitive, especially for smaller business users, because they can amount to higher than the yearly runtime cost of the service itself. It can be concluded that this in practice leads to a **high degree of vendor lock-in**.

6.2.1.3 Security of data processing

The baseline scenario in the area of security of data processing entails relying on the NIS Directive and related instruments to provide a benchmark for a common level of security of data storage and processing. The evidence that was gathered points to data being more secure when kept in the larger data centres of cloud service providers, as these are often much better equipped in terms of security systems. Therefore, the negative indirect effect from the status quo is linked to the assumption that companies (especially SMEs) that are affected by data localisation restrictions may choose not to store data in the cloud.

When data is stored on-site, the security risks for business end-users are higher, while at the same time more expensive as well[75]. The NIS Directive provides a risk-based approach to security but does not address the cost problem. Some cloud service providers in more closed economies may therefore exploit the existence of data localisation restrictions to raise their prices, at the expenses of business users in the downstream sector.

Moreover, existing legislation and policy does not address security concerns of data storage/processing specifically, for instance by introducing certification. This would not solve the current uncertainty about the security of cloud use.

Therefore, the presence of data localisation restrictions and the limited degree of collaboration in security matters in the baseline scenario looks unlikely to solve the problems discussed in the problem definition section.

The respondents to **the public consultation** have highlighted the importance of allowing free flow of data without restrictions for keeping data storage and processing secure. As one respondent

[75] London Economics Europe, "Facilitating cross border data flow in the Digital Single Market", 2016 (SMART 2015/0016) and EC Consultation on the regulatory environment for data and cloud computing, May 2016.

noted: "*We deliver two major updates a year and smaller updates on a weekly basis, with all of our customers always on the same version. Enabling cross-border data flows enables greater adoption of cloud computing, with these benefits that are lost with multiple instances or hybrid solutions. Having a single privacy and security model and having everyone on the same version makes it easier to protect data, add new functionality, and reduces complexity enhancing ease of use for customers"*. It seems unlikely that a no-action scenario will help to improve the security of the data processing.

6.2.2 Environmental and social impacts

6.2.2.1 Free flow of data across borders

No positive **environmental impacts** are to be expected under Option 0.

In general, a free flow of data has positive **environmental impacts**, because it will allow cloud service providers to locate their data centres in locations where there are substantive energy efficiency gains to operate such infrastructures. These locations are typically locations in lower temperature zones[76], as they allow energy savings on cooling servers. [77] Cooling may account for up to half of a data centre's power expenditures, so this issue of large importance for the sector and may therefore have sizable impacts in terms of environmental footprint. [78]

It is true that many factors play a role in the decision on where to situate a data centre (such as proximity to clients and access to a pool of human resources who have the skills to operate the data centre). Still, it is important to highlight that data localisation restrictions may have an impact on the location choice, skewing it towards less environmentally optimal locations.

Because the baseline option would allow for the persistence of data localisation restrictions by Member States and through market dynamics, it would therefore have a negative impact on the environment.[79]

Proliferation of data localisation restrictions could also hamper the development of innovative approaches energy optimisation or efficiency in data centres, e.g. maximising the use of renewable energy by shifting the loads of data processing to a data centre where renewable energy is available at a particular moment.

In terms of **social impacts**, the baseline option would lead to an increase in employment in Member States that have introduced or will introduce data localisation restrictions, because of supervision or operating needs of new infrastructure. The positive impact of such jobs is likely to be limited, since cloud service providers deploy only the limited capabilities needed to serve customers in those Member States.

In addition it must be noted that the data skills gap is expected to increase to more than 16% over the next four years totalling a number of unfilled positions of almost 770,000. In particular some of the largest and most advanced EU economies will face a considerable skills gap whereas smaller and less developed economies will witness an oversupply of data workers.[80] Therefore, it can be presumed that non-effective policy measures not sufficiently addressing either, existing or

[76] Time.Lex Study (SMART 2015/0054), Economic analysis of costs for cloud data providers in meeting data location restrictions, p.9

[77] In general, data centres situated in Nordic countries with abundant renewable energy are more environmentally-friendly than the data centres situated within cities in countries with a lot of "brown" energy in the energy mix.

[78] Cooling may account for up to half of a data centre's power expenditures, see Oxford Research "A springboard for green data centers in Southern Norway", p.8. Water is another resource used for cooling, see Justin Morton, "Data Centers' Water Use Has Investors on High Alert", Bloomberg, 5 August 2016, available at: http://www.bloomberg.com/news/articles/2016-08-05/data-centers-water-use-has-investors-on-high-alert

[79] Electricity use by data centres is one of the fastest-growing sources of greenhouse gas emissions globally, see Susanne Goldenberg, "Social media explosion powered by dirty energy, report warns", The Guardian, 2 April 2014, https://www.theguardian.com/environment/2014/apr/02/social-media-explosion-powered-dirty-coal-greenpeace-report

[80] Idem, p.198

potentially emerging limitations to the free flow of data would promote directly or indirectly a concentration of data skills demand. This will consequentially also affect negatively the data skills gap.

Another possible negative social impact could incur on the freedom to conduct a business provided for by Article 16 of the European Charter of Fundamental Rights, since it would result in (a growing number of) limitations constraining (i) business choices regarding the location of data storage or processing infrastructures and (ii) the opportunities for cloud service providers to serve customers in other Member States.

6.2.2.2 Data availability for regulatory control by Member State authorities

As there would be no significant action to improve data availability for regulatory control by Member State authorities envisaged by this option, no change in cross-border data mobility can be expected and consequently, no positive environmental impacts. Through inaction, it would mean a missed chance in terms of improving the environmental footprint of data centres.

As explained in section 6.2.2.1 above, a free flow of data is beneficial for the environment through increased liberty for service providers to locate their data centres in more environmentally optimal locations. Policy action on improving data availability to Member State authorities for regulatory control purposes would increase cross-border data mobility because of raised levels of trust, both by market participants and by Member States authorities.

Therefore, the reader is referred to section 6.2.2.1 as it applies similarly for the intervention area of availability.

6.2.2.3 Switching and porting data between providers and IT systems

The baseline option would leave it to the market to implement energy efficient solutions. If the lack of interoperability between cloud services is allowed to persist, this would make it necessary for companies wanting to switch providers to spend more resources and processing power to migrate their data, which could have a negative environmental impact.

Apart from the issues of continued market distortion, and leaving SMEs and start-ups in a weaker position, there are no social impacts of this option, although certain negative regional policy effects of localisation can be quite important on a local level, such as the lack of scaled investments because of fragmented service provision.

6.2.2.4 Security of data processing

Cyber threats pose significant environmental and social risks. As more and more data of critical infrastructure or industry working with dangerous substances are moved to the cloud, state-of-the-art security of data processing and storage facilities is of utmost importance to keep environmental and social dangers to a minimum. In this respect, security breaches could lead to accidents in manufacturing processes and/or the release of dangerous or polluting substances. The policy options presented in this area do not cause direct environmental or social impacts. Nevertheless, it can be argued that because it is most likely that this option will not lead to a higher level of security (through better coordination between Member States' authorities and the establishment of common standards), it will not have the potential positive social and environmental impacts that the other policy options constitute.[81].

[81] Examples of potential environmental impacts are:

- Cyber intrusions that lead to contaminant releases, resulting in damage to human health and the environment
- Cybercrimes causing catastrophic spills, waste discharges and air emissions that result in bodily injury, property damage, environmental remediation expense and significant legal liability claims

See XL Catlin Group, "Environmental Risks: Cyber Security and Critical Industries" (Whitepaper), 2013.

Social impacts concern the disclosure of information that can pose harm to individuals.

As the baseline option does not foresee the development of cloud-specific security guidelines, it may be argued that of all policy options, this option constitutes the highest environmental and social risks.

6.2.3 Impacts on Member States' public authorities

6.2.3.1 Free flow of data across borders

The baseline option would not produce specific impacts on Member States' public authorities in the intervention area of free flow of data across borders (in particular, potential infringement proceedings relating to data localisation restrictions could be dealt with in the context of existing administrative arrangements).

6.2.3.2 Data availability for regulatory control by Member State authorities

There are several inter-state cooperation mechanisms in existence, allowing Member States to exchange information in relation to specific administrative/judicial procedures, and specific data types, subject to various conditions.[82] For scenarios not covered by these instruments, Member States can engage in bilateral or multilateral interaction, with potentially diverging procedures to follow in different exchanges, and multiplied administrative efforts. As outlined above with regard to the economic impacts, without establishing and strengthening obligations on private actors to make the data available and promoting Member States' cooperation, a projected rise in cross-border data services and requests for access to data would exacerbate such administrative burden.

6.2.3.3 Switching and porting data between providers and IT systems

As the baseline option relies on market players to progressively introduce technical and contractual conditions facilitating switching data of cloud service providers, it is not expected to incur direct administrative burden on national public authorities under the baseline option.

However, relying completely on market participant to introduce such conditions could constitute a lack of guidance and therefore cause disproportionately dominant market positions for large tech companies. This could lead to indirect administrative burdens in the form of an increased number of cases referred to Member States' competition authorities.

6.2.3.4 Security of data processing

The baseline scenario does not lead to direct burdens for Member States' public authorities, as it relies on existing instruments like the NIS Directive. It is likely that such existing instruments will not establish specific security benchmarks for cloud services, as their necessary purpose is to create a generic framework. However, if such common security criteria would not be instituted this could in the future lead to burden for Member States authorities as a result of the collective risk this poses to their societies.

6.2.4 Stakeholder views

6.2.4.1 Free flow of data across borders

The majority of stakeholders voiced its support for a legislative principle on the free flow of data. They did so by means of the online public consultation, during the structured dialogues organised by the Commission or by submitting position papers for scrutiny. 61.9% of respondents to the public consultation indicated that data localisation restrictions should be removed and, as mentioned in section 5.6, 55.3% argued for a legislative approach in doing so. Moreover, stakeholders have

[82] Please refer to Annex 8 for a detailed list and analysis of these cooperation mechanisms.

indicated their concern about data localisation restrictions that are currently in place or that are perceived by the market.

As Option 0 would rely on Member States to progressively replace data localisation restrictions with less intrusive measures, this option would not address either of these two concerns raised by stakeholders. It does not propose actions to remove existing and perceived data localisation restrictions, and it would also be unable to avoid the emergence of new data localisation restrictions, following the trend witnessed in the European Data Economy communication of the European Commission.

6.2.4.2 Data availability for regulatory control by Member State authorities

Concerning the intervention area of data availability, stakeholders hold that national competent authorities uphold data localisation restrictions for the objective (in itself legitimate) of keeping data available for supervision or control purposes. In **the public consultation**, 77.4% of respondents indicated that localisation demands were rooted in compliance concerns vis-à-vis local legal or administrative requirements.

As Option 0 neither includes clear EU-level guidance on the abatement of data localisation restrictions, nor provides guidelines or tools for Member States authorities to ensure availability of data processed in another Member State, there is no reason to conclude that these (frequently defined by sector) localisation restrictions would be mitigated by Option 0.

6.2.4.3 Switching and porting data between providers and IT systems

56.8% of SME respondents who intended to switch providers indicated in **the public consultation**[83] that there are important barriers to data portability. This is echoed also by participants from the 18 May 2017 workshop on cloud switching[84], which included representatives of the cloud industry and their business customers. It is evident from the stakeholder engagement that there is an expectation for the EU to act to improve data portability in order to facilitate switching of cloud services providers. Option 0 would not meet this expectation.

6.2.4.4 Security of data processing

Stakeholders have expressed considerable concerns about the security of data processing. The main argument made by stakeholders[85] is that security of data processing would benefit from a free flow of data legal principle. There were zero stakeholders arguing the opposite. The reason behind this is that hosted cyber security services are typically provided remotely, from operation centres located in strategic places around the globe to be able to benefit from 24/7 security incidents reporting. In the case incidents are detected, these services will typically upload security updates at once on IT-systems of many users worldwide.

Considering that stakeholders' views were not conflicting on this issue, their judgment suggests that Option 0 is suboptimal, as it would not include any policy action to ensure enhanced data mobility in Europe.

[83] See Annex 2
[84] Ibid.
[85] This argument was expressed mainly by specialists on the topic, like cyber security service providers, but also by business users.

6.3 Option 1: Non-legislative initiative – guidelines, strengthening enforcement of existing EU rules and enhancing transparency

6.3.1 Economic impacts

6.3.1.1 Free flow of data across borders

The economic impacts of this option **would not vary much compared to the baseline scenario**, as the intervention in this case would be based on a non-legislative and little binding policy action. It does not guarantee any change in data localisation by business actors driven by market dynamics through legal uncertainty and does not promote consistency of treatment across the single market.

Option 1 would foresee strengthened enforcement of existing legal instruments to minimise negative effects of data localisation. However, this would not solve the problem of legal uncertainty and still leave gaps for new localisation restrictions. One IT service provider specifically mentioned this in a written answer to **the public consultation**: "*Only a legislative instrument can remove these barriers; ensure they are not re-instated and that new ones are not introduced; and provide sufficient certainty to providers and users in the longer term. While there are already some relevant legislative instruments in place (e.g., the Services Directive and the E-Commerce Directive), none of these set forth a comprehensive prohibition on the maintenance of unjustified obstacles to the free flow of data. Guidance, or mere identification of the data localisation measures, while helpful, will not be as effective.*"

Also, it would largely **preserve Member States' discretion to put in place new data localisation restrictions and maintain the existing ones**.

Outcome of the structured dialogues with Member States:

Soft approaches could persuade some Member States to lift some data localisation restrictions. For instance, France revised Act number 2002-303 and the French Public Health Code which oblige hosting service providers to be approved by the Shared Healthcare Information Systems Agency within the Ministry of Health in order to be allowed to undertake hosting activity for patient data. From 2019 the strict prior authorisation requirement will be replaced by a certification requirement. In Germany, the initial draft "social network" law contained data localisation restrictions, but those were taken out as deliberations on the draft law progressed.

In particular, as explained below, it would still be **difficult to pursue infringement proceedings** targeting data localisation restrictions.

Factors making infringement proceedings against data localisation restrictions difficult to pursue

The Commission has recently announced that it would pursue infringements "in a strategic way to focus and prioritise its enforcement efforts on the most important breaches of EU law affecting the interests of its citizens and business."[86] In particular, economic and systemic (cross-EU) significance of a particular case are among the factors to be taken into account.

In this vein, the following categories of cases would be easier to pursue:

(i) where a case is underpinned by provisions of EU law clearly targeting the infringement at hand (e.g. the Services Directive clearly precludes Member States from imposing an obligation on the provider to obtain an entry in a register or registration with a professional body or association in their territory); and

(ii) the infringing provisions of laws or practices of Member States are easy to identify (e.g. infringing laws are generally easy to identify).

[86] C(2016) 8600 final, "EU Law: Better Results through Better Application".

In this regard the structured dialogues with Member States point to significant confusion as to how (if at all) the data localisation restrictions identified fall within the scope / could be addressed under the provisions of different existing EU legal instruments (**Annex 5 presents a detailed overview**). Moreover, many restrictions are hidden in outsourcing guidelines, circulars and similar administrative documents.

Also it appears from the structured dialogues with Member States and the Commission's own assessment that it would be more difficult to pursue infringement proceedings against localisation restrictions concerning public data or sensitive private data, such as health data.

Considering the potential cases targeting different categories of data localisation restrictions against the criteria mentioned above, very few cases would satisfy the threshold of addressing "the most important breaches of EU law" while being, at the same time, easy to pursue. For instance, cases targeting restrictions in the financial sector could be said to have sufficient economic significance, however the sector is excluded from the scope of the E-Commerce Directive and the Services Directive. Moreover, the restrictions typically stem from administrative requirements and practices rather than easily identifiable Member States' laws. Cases targeting restrictions in the health sector or those concerning public data could also be regarded as economically important, but the type of data at hand would make such cases difficult to pursue.

In view of these difficulties, it is not surprising that no infringement proceedings against data localisation restrictions imposed by Member States have been launched yet.

Finally, even if proceedings were to be launched, the fact that many data localisation restrictions are context-specific means that several court judgements would be required in order to cover all aspects of such restrictions and establish a cross-cutting set of principles. Since, as explained in section 6.2.1.1 above, infringement proceedings take on average 4-5 years until they result in a court ruling, this would indeed lead to **a long period of legal uncertainty.** As a result, users would continue to demand local data storage and/or processing from the service providers, and the prospects of the fast-developing data economy would continue to be harmed.

This option could have a marginally positive impact on **costs associated with the analysis of the regulatory environment**, at least for SMEs and could also have a marginally positive impact on the **choice and cost of data services** for the organisations using them. This would for instance be the case if an organisation that had erroneously assumed it has to store and/or process data in a particular Member State (i) found out, thanks to transparency measures, that there was no such localisation restriction and (ii) contracted a cheaper (foreign) data service.

Putting in place guidelines and transparency measures is **not expected to affect the competitiveness** of cloud service providers or organisations using in-house data storage or processing IT systems.

6.3.1.2 Data availability for regulatory control by Member State authorities

The introduction of guidelines on data availability for regulatory control by Member State authorities would reduce the negative economic impacts and costs deriving from the **administrative burdens** present in the baseline scenario. Member States will find it useful to have a framework for discussion and a forum where best practices can be discussed and eventually adopted. This could result in a degree of procedural convergence and reduce the human resources cost, thereby increasing **cost efficiency** for public administrations. This remains, however, a simple discussion forum which is not likely to lead to specific improvements or results.

In addition, option 1 is likely to have only **limited impacts on the downstream sector**. Many negative impacts identified for the baseline scenario are likely to persist. A persisting lack of trust could alter **costs and choice** of market operators and have an indirect effect on their **operational efficiency**. **Market fragmentation** would also persist, hampering **innovation and competitiveness**

of the companies in the market as business end-users of data services would in some case be obliged to stay in less competitive markets with **higher prices**.

The impacts on the **upstream market structure** (cloud service providers) would be similar to those envisaged in the baseline scenario.

6.3.1.3 Switching and porting data between providers and IT systems

The development of the EU cloud market is forecast to be somewhat stronger under the Option 1 than under the baseline option[87], putting the **growth in demand for public cloud at 19.7 % Compound Annual Growth Rate between 2018-2025** (6 percentage points higher than in the baseline scenario), amounting to a €68.8 billion market by 2025. This is due e.g. to growing awareness and involvement from industry and increased momentum to build trust and confidence in cloud and reduce the fear of vendor lock-in. Exit strategies by design might be implemented by cloud service providers.

This option would require service providers to explain in a sufficiently detailed and accessible manner the processes, timeframes and charges that apply to switching. The economic impacts of this option therefore include an **increase in variable costs** for the service providers.

Costs in data transmission are already high and sometimes prohibitive[88]. **Transparency** on this type of cost could be helped under this option, e.g. by explicitly stating the cost of bandwidth for data outbound and data inbound in contractual agreements in guidelines or self/co-regulation. This can help cloud customers plan their costs related to migration. This could be **beneficial for SMEs** that have lower bargaining power against cloud service providers, and it could incentivise switching by removing uncertainty.

6.3.1.4 Security of data processing

This option would result in guidelines concerning security of data storage and processing, but would not be binding for the Member States. Nevertheless, clarity would be shed on the security provisions on data storage, and contribute to alleviate the lack of trust and the uncertainty.

Because of enhanced levels of trust, this option would have a positive indirect impact on the business sector, including both upstream (cloud service providers) and downstream markets (business end-users of cloud services). The magnitude of the impact will depend on the uptake and effective implementation of guidelines by Member States. However, it is likely that this impact will be modest because of the voluntary nature of the guidelines, which will configure against a background of a myriad of different voluntary certification schemes.[89] Therefore, Option 1 will not lead to a high degree of clarity.

6.3.2 Environmental and social impacts

6.3.2.1 Free flow of data across borders

As explained in section 6.2.2.1, a free flow of data is beneficial for the environment through increased liberty for cloud service providers to locate their data centres in more environmentally optimal locations. Option 1 would slightly reduce the need to deploy infrastructure in environmentally sub-optimal locations and could have a (limited) positive impact on the environment.

[87] IDC and Arthur's Legal, "Switching between Cloud Service Providers", 2017 (SMART 2016/0032).
[88] Ibid.

[89] Tecnalia SMART 2016/0029, Tecnalia, "Certification Schemes for Cloud Computing" (Ongoing)

Its social impact is likely to be negligible due to (i) the option's non-binding nature and (ii) the absence of a strong link between setting up data storage and processing infrastructures and employment in general.

6.3.2.2 Data availability for regulatory control by Member State authorities

As the option would mostly include discussions / exchange of practices under a non-legislative approach to improve data availability for regulatory control by Member State authorities envisaged by this option, there would be only limited positive environmental impacts in this intervention area.

6.3.2.3 Switching and porting data between providers and IT systems

The impacts would be similar to those under the baseline option. However, with a stronger push from the Commission for market players to cooperate on interoperability, and especially open APIs, a further increase in the efficiency of data migration may be seen.

6.3.2.4 Security of data processing

Guidelines on security of data processing and storage would mean an improvement in terms of cyber security compared with the baseline option. Therefore, potentially negative environmental and social impacts of cyber-attacks, as described in 6.2.2.4 would diminish under Option 1.

6.3.3 Impacts on Member States' public authorities

6.3.3.1 Free flow of data across borders

A strengthened enforcement of existing EU legislation, combined with enhanced transparency on existing data localisation provisions, could lead to administrative burden for Member States, particularly in terms of human resources. As Option 1 is not legislative, the impact would depend greatly on the modalities of its implementation in particular Member States (from low-scale implementation to full-scale implementation) and the degree to which existing mechanisms set up under the *acquis* would be relied on. Any quantitative estimation would also depend on the number of existing data localisation restrictions in a particular Member State. Under this option, therefore, administrative burden is expected to vary greatly by Member State.

Moreover, this option does not provide an avenue for problem resolution regarding data localisation not covered by the existing mechanisms. As such, it is not future-proof and it does not allow for tailoring/further deliberations or implementing rules on issues relating to the free flow of data.

6.3.3.2 Data availability for regulatory control by Member State authorities

Option 1 would have similar implications for burdens on public authorities to those described in 6.3.3.1.

6.3.3.3 Switching and porting data between providers and IT systems

As Option 1 encourages self/co-regulation by the market to establish common conditions for switching cloud service providers, it would pose no direct administrative burden to Member States.

6.3.3.4 Security of data processing

The expected impacts of Option 1 on Member States' public authorities are the same as those of Option 0 for the intervention area security of data processing.

6.3.4 Stakeholder views

6.3.4.1 Free flow of data across borders

In general, stakeholders have indicated *not* to support Option 1. Instead, as argued further below in this section, a majority of different categories of stakeholders has called for a legislative approach to confront the problem.

In first instance, the strengthened enforcement of existing EU legislation vis-à-vis different categories of unjustified localisation restrictions, as foreseen under Option 1, would be welcomed if compared to the baseline option. For, a clear majority of stakeholders (61.9% of respondents to **the public consultation**) believes that data localisation restrictions should be removed. In this regard, strengthened enforcement is expected to have a moderate positive effect as compared to no EU policy change.

However, as introduced above, stakeholders from both the public and private sectors have called for a new legislative instrument. On 13 December 2016, 16 heads of governments of EU Member States sent a letter to President Tusk to call for such a legislative approach. They state "*In our view an early legislative proposal providing for the free flow of data is crucial to avoid market fragmentation and further obstacles to the development of the data economy in the EU*".

The same message appears from **the public online consultation**, in which 55.3% of respondents argue for a legislative approach.[90]

The majority of stakeholders, therefore, would be disappointed with an approach as under Option 1. The different group of stakeholders also provide more in-depth views on why they would prefer a legislative approach. Participants of the structured dialogues with the Member States, for instance, convincingly identified the issues of 'legal uncertainty' and 'lack of trust' as drivers of the problem of obstacles to data mobility. This view was confirmed by respondents to **the public consultation**, who identified the influence of market dynamics on data localisation, even without the presence of data localisation restrictions from the part of public authorities. One respondent to the public consultation referred to such 'perceived restrictions' in a written answer to an open question: "*More concerning than formal obligations are informal/perceived ones. For example, our experience is that many entities in regulated industries want data to be stored in one country. Even without a formal requirement, it is clear from these conversations that entities believe that regulators strongly disfavour or in practice prohibit storing data outside of their home country. More generally even with formal requirements, there is uncertainty as to their application and coverage which complicates market assessment*".

Option 1 would not take away this legal uncertainty, as it proposes to retain the current patchwork of EU-law applicable to data localisation. As no awareness raising campaign would be undertaken under this option, the uninformed market dynamics leading to data localisation and the 'perceived restrictions' mentioned above would retain intact. Accordingly, this approach does not tackle the sectorial administrative requirements that are still in place.

Finally, as evidenced by multiple press reactions to the Digital Single Market Mid-Term Review[91]an initiative under Option 1 could be seen as a negative appreciation of the Commission's promised actions under the Digital Single Market strategy. This is contention is reinforced by the letter of 16 heads of governments of EU Member States to President Tusk on 13 December 2016: "*we note with concern the risk of serious delay with the presentation of a legislative proposal in relation to data localisation under the European 'free flow of data' initiative. The DSM strategy set very clear expectations for presentation in 2016 on an initiative…*"

[90] 289 respondents participated in this multiple-choice question.

[91] See: Politico, http://www.politico.eu/article/digital-single-market-mid-term-report-card-tktkt-percent/ and CBR Online, http://www.cbronline.com/news/verticals/central-government/eu-failing-digital-single-market-says-techuk/.

6.3.4.2 Data availability for regulatory control by Member State authorities

Compared with Option 0, Option 1 does not comprise any significant change in the approach on the intervention area of data availability. It is unlikely that Member State discussions / exchanges of best practices would lead to tangible results in terms of trust either on the part of public authorities or the part of market players. Therefore, Option 1 would not enhance the data availability concerns that were frequently mentioned by stakeholders in their responses to the public online consultation.

6.3.4.3 Switching and porting data between providers and IT systems

There is broad agreement among stakeholders that the identified issues with data portability and switching need to be addressed. Stakeholders have generally been positive towards the different soft law measures suggested, both in the public consultation and in workshops. Especially popular measures are standards development and guidelines. However, many stakeholders have underlined the need to avoid interfering too much with contractual freedom.

Among the **Member States** who contributed position papers to **the public consultation**, the **UK** held that the EC should be careful not to promote portability through over-prescriptive common standards, or to create unnecessary cost/burden on businesses. The **Danish** government supports the development of standards which aims to promote interoperability and portability. They also view interoperability as an essential prerequisite for a competitive well-functioning digital economy.

6.3.4.4 Security of data processing

With reference to section 6.2.4.4., we may conclude that specialised stakeholders argued that security of data processing would benefit from increased data mobility. During the evidence gathering process, this insight was frequently confirmed by other stakeholders, with no opposite views voiced. Therefore, stakeholders' judgment would be that Option 1 is suboptimal but slightly better, as it would imply a strengthened enforcement of existing legal instruments to counter unjustified data localisation restrictions.

However, as a free flow of data principle would be still absent, cyber security service providers would still have to be engaged in costly processes of compliance research. This would still result in a lack of legal certainty.

6.4 Option 2: Principles-based legislative initiative and cooperation framework to ensure trustworthy free flow of data across borders and facilitate switching and porting data between providers and IT systems

6.4.1 Economic impacts

6.4.1.1 Free flow of data across borders

Option 2 includes the establishment of a legal principle of free flow of data within the EU (as described in section 5 and in the context described in section 2). It requires Member States to notify any new data localisation restrictions they deem justified and intend to put in place by means of notification schemes of existing EU legal instruments. During a transitional period, Member States would be obliged to carry out a review of existing data localisation restrictions. Additionally, the policy option proposes awareness raising campaigns around the free flow of data principle.

Hence, this option would **ensure the effective removal of existing unjustified localisation restrictions, and the avoidance of future ones**.[92] As more than two-thirds of the sample of 45 analysed data localisation restrictions is unjustified, this would mean the removal of most existing data localisation restrictions. The remaining restrictions are not likely to affect businesses, e.g. in

[92] Under this Option, in principle all data localisation restrictions for reasons other than protecting public security would be considered unjustified or disproportionate restrictions. The precise application of this practical rule can be debated by the expert group which is to be established under this option.

the form of restrictions on accounting data, because such restrictions would not likely be justified on grounds of public security. Additionally, the at least equally important problem of market dynamics originating from a lack of knowledge by operators of the correct legal situation concerning data localisation restrictions or on implicit localisation restrictions would be addressed by the awareness raising action foreseen, effectively mitigating legal uncertainty and lack of trust. The remainder of this section will assess the economic impacts of the removal of data localisation restrictions.

Macro-economic impacts

It is, to a certain degree, possible to estimate the macro-economic impacts following the general adoption of data-driven innovation and data technologies in the EU, as in the analysis carried out by the support study for this Impact Assessment[93]. This study concludes that a free flow of data legislative proposal taking away data localisation would be the most important factor in driving the European data economy towards the high growth scenario of 4% GDP by 2020.

However, there are also challenges in calculating the exact macroeconomic impact generated from removing data localisation restrictions in quantitative terms. The link between the different levels of regulation proposed to address the problems identified in section 2 and aggregate economic elements such as GDP, employment level or competitiveness of the sector does not allow quantifying in a high level of granularity.

Certainty for the future: creating an investment climate for a true European data economy

The most notable economic effects of this Option will be achieved through creating legal certainty and raising trust levels regarding data storage and processing. This should create an optimal investment climate, directed at the EU's future. The data economy is developing rapidly at the moment. Therefore, the proposal underlying this IA deviates from the classical situation in the sense that it is not only directed at present problems but also at preventing future ones and creating the right environment for the EU to fully grasp the benefits of the data economy.

Impact on cloud service providers

The support study by Spark, Time.Lex and Tech4i2[94] has provided some evidence on stark difference across costs in setting up and operating data centres in Europe, but relativizes the link between these costs and the existence of restrictions. The study finds that data localisation has an impact predominantly on the data centres that cloud providers build in addition to their first facilities: "It is possible to assert that having built a first round of data centres primarily in locations to meet user needs, later choices for additional data centres (being built now or in the future) might be driven more by concerns of cloud service providers about cross-border data regulations - thus they might be located in sub-optimal locations"[95].

The study asserts that data localisation restrictions could lead to the provision of more cloud data centres than cloud service providers would ideally like to deploy if they wish to provide services in Member States with more onerous cross-border data transfer compliance obligations. With each cloud data centre costing €276.9 million on average in EU Member States, overprovision of centres is costly[96].

---

[93] See IDC, "European Data Market. Data ownership and Access to Data - Key Emerging Issues", 2016 (SMART 2013/0063).

[94] Time.lex, Spark and Tech4i, "Cross-border Data Flow in the Digital Single Market: Study on Data Location Restrictions", D5. Final Report (SMART 2015/0054).

[95] Interviews with cloud providers have confirmed that ten years ago cloud servers were built to meet the needs of cloud service providers. In recent years the situation has been reversed and now server locations are designed to best meet user needs and cross-border data compliance requirements. However, these location decisions could also include user concerns such as lower latency and/or cost factors.

[96] Moreover, the cost does not need to be reflected necessarily into pricing. Discussions with cloud providers also revealed that the price/subscription charged to users in the short-term can be independent of the cost of provision; as

Impacts on businesses

The study conducted by Deloitte[97] for the European Commission shows how important the removal of data localisation restrictions is for downstream business users. Although there is an overall net benefit, the removal could be detrimental to providers using data location as a specific competitive advantage. Deloitte compares a baseline scenario of no intervention with one where data localisation restrictions are removed. The results are illustrated by below, showing that **EUR 11.6 billion can be leveraged in terms of net present value (NPV) of revenues for cloud users**, providers and society as whole by the removal of data localisation restrictions. Being based on cloud services only, this is just a conservative proxy of what could happen in the entire data universe.

Figure 7 – Changes in NPV across stakeholders after the removal of data localisation restrictions

Stakeholders	Discounted NPVs 2015-2020	% change compared with baseline scenario
Cloud users	EUR 542.2 billion	1.36%
Cloud providers	EUR 19.5 billion	21.53%
Society	EUR 57.6 billion	1.49%
Total NPV added	**EUR 11.6 billion**	**1.90%**

(Source: Deloitte 2016))

In terms of different sectors of activity, the same study calculated that the largest benefits in relative terms would accrue to the manufacturing sector (+2.23%), followed by distribution retail and hotels (+2.12%).

ECIPE[98] estimated an overall EU-wide weighted impact on GDP is up to EUR 8 billion yearly, representing 0.06% of the current EU GDP. The true cost of today's restrictions is however likely to be underestimated given that this scenario does not take into account the regulations that are implicitly or indirectly localising.

The same report acknowledges that the impact of these price adjustments would not lead to a large-scale outsourcing of data hosting and processing services to other EU Member States. Imports of communication services by German customers from other EU Member States would increase within a range of 2-8% above the current levels. The ranges are similar or slightly higher for France. In all other cases, the import increase on communication services are limited to between zero and 3% according to ECIPE.

These results are corroborated by the results of **the public consultation**, which show how stakeholders are aware of these potential savings that could accrue in case of clear limits to data restrictions[99].

providers pursue goals such as maximizing market share. Over the long term, cloud service providers will need to obtain a return on their investment, but in the short-term, costs to users (in subscriptions and/or fees) may not reflect costs incurred by cloud service providers.

[97] Deloitte, "Measuring the economic impact of cloud computing in Europe", 2016 (SMART 2014/0031).

[98] ECIPE, Policy Brief "Unleashing Internal Data Flows in the EU: An Economic Assessment of Data Localisation Measures in the EU Member States", December 2016, http://ecipe.org/app/uploads/2016/12/Unleashing-Internal-Data-Flows-in-the-EU.pdf .

[99] The impact that was most frequently mentioned across all participants is costs (130 times). The second most frequent answer is that of launching a new product or service (118 times). Subsequently follow entering a new market (95 times)

Also, the consultation showed the high impact (more than 70% of respondents) for the effects of data localisation restrictions on **launching a new product or service or entering a new market.**

Additional results of the public consultation are explored in more detail in **Annex 2.**

Costs of setting up a new business in the EU

Taking away data localisation restrictions and enshrining a legal principle on the free flow of data in European law would **reduce the cost of setting up a business in the EU** through the provision of cheaper and more competitive cloud services at a one-time cost for applicability in the whole EU. The cost of setting up a business in the EU is currently at EUR 300 and 3 days per Member State. In line with the Commission's Start-up and Scale-up initiative's findings, bringing this cost down would increase EU innovation and competitiveness, strengthening the economy.[100]

Quantitative impacts

It is possible to extrapolate some of the economic impacts in more quantitative terms to give an idea of the potential benefits from the free flow of data principle.

The very nature of data localisation restrictions implies that the offer of data services is reduced, at least in the short term, leading, potentially, to higher prices of such services in the markets concerned. This has an impact of **market structure** as pent-up demand in "expensive" Member States is not met and providers in "cheaper" Member States do not manage to attract all the potential clients. Also, the choice will be more limited in smaller Member States. In several countries, only data centre services that offer the lowest added value are available (e.g., Infrastructure-as-a-Service (IaaS)), while more value-adding services like Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS) are not available there. This limits the options of some companies to less efficient data centre solutions. For example, the price of storage per gigabyte in case of a Hungarian cloud service provider is more ***than 25 times higher than*** the price per gigabyte per month in a larger PaaS service.

Figure 8 – Diverging data storage prices

Public cloud provider location	Price(per GB of data stored)
Azure Germany Northeast (PaaS)	€0.0224
Azure North Europe (PaaS)	€0.0202
Telekom Hungary (IaaS)	€0.5371[101]

This can have an impact on the **competitiveness of European SMEs**. If we extend as an example, the price differential of 51.69 Euro cents and we assume that SMEs store 50 TB on average using private cloud services, this would entail a saving or around EUR 26,000 per SME.

In 2015 there were around 23 million SMEs in the EU[102]. The following example assumes that only 8% of them use private cloud computing services[103]. Assuming theoretically that 50% of the SMEs

---

and providing services to private entities (81 times). Other impacts, such as on providing services to public entities or conducting research, received lower scores. Only 2,6% (16 respondents) see no impact of data localisation restrictions.

[100] COM(2016) 733 final, "Communication of the European Commission to the European Parliament and 'Europe's next leaders: The Start-up and Scale-up Initiative".

[101] Source: https://azure.microsoft.com/en-us/pricing/details/storage/blobs/ http://www.telekom.hu/uzleti/szolgaltatasok/informatika/szerverek-adatparki szolgaltatasok/szerverberles/virtualis-szerverek

[102] Annual report on EU SMEs 2015/2016

[103] Eurostat, http://ec.europa.eu/eurostat/statistics-explained/index.php/Cloud_computing_-_statistics_on_the_use_by_enterprises#Main_statistical_findings

can use a 'cheap' provider and the other 50% an 'expensive' one, then the potential savings from migration of half of them from the cheap to the extensive provider would be in the area of 23.9 million euro per month. That would amount to around 276 million euro per year. This is an estimation which has little scientific value, but can give an idea of the magnitude of lifting data restrictions that may hinder this migration in fact or in perception.

6.4.1.2 Data availability for regulatory control by Member State authorities

Option 2 foresees the establishment of the principle that the holder of data shall not deny access to data to a public authority for its regulatory control purposes. As for the previous two options discussed, the impacts on the business sector are likely to be indirect.

However, the fact that the obligations on private parties are clearly established and reinforced and a cooperation framework is established to promote the effective application of the principle of availability in cross-border data storage will **reduce the level of uncertainty** for those business users who would like to move to cheaper providers in another Member State. This has a short-term positive impact on the **operational efficiency** of the **downstream sector** (business end-users).

The impacts on the **cloud service providers** are likely to be more significant in the medium term. Under a provision and a cooperation mechanism on data availability foreseen by this option, they could compete widely across borders, which would improve the **efficiency of the data service providers' sector** and contribute to bring down the costs for its clients.

The only limited negative impact on the upstream sector from Option 2 would be linked to the costs associated with the set up and enforcement of the standard contractual clauses.

6.4.1.3 Switching and porting data between providers and IT systems

The economic impacts of this option stem from establishing the principle that cloud service providers should offer data portability to facilitate the switching of providers or porting of data back to users' own IT systems. Under this option, the role of industry will be flanked by enforceable legal principles. A possible result could be more direct compliance costs, however at the same time the option would tackle vendor lock-in issues more convincingly. As these have higher and more serious impacts on stakeholders and the economy in general, they will therefore offset any increased compliance costs through the creation of a more open and competitive market.

More transparency will remove legal uncertainty, especially regarding hidden costs which are not mentioned in the contract. However, transparency and voluntary agreements on some contractual arrangements fall short of addressing the cost problem. This has to do with the **magnitude** of the costs and its **apportioning** between the "sending" and "receiving" side. The more granular the analysis of the cost apportioning gets, the more difficult (and costly) it is to extricate the cost components, especially for data which are complex in format and not raw.

Option 2 could indirectly foster, through making switching easier, the growth **and the take-up rate of cloud services** in Europe. A forecast of the growth in the uptake of public cloud has been made in the study on Switching Cloud Providers[104], using a **Mandatory Regulation Scenario**[105]. A mandatory regulation will lead to a faster take-up of public cloud services. SMEs and start-ups are expected to be most positively impacted in this scenario. The demand for public cloud is forecast to grow by 20.5 % Compound Annual Growth Rate between 2018 and 2025, reaching €71.9 billion in 2025.

Furthermore, as reported in one of the workshops with business stakeholders organised by the support study team[106], "*Standards are used in the market in an ineffective and inconsistent manner,*

[104] IDC and Arthur's Legal, "Switching between Cloud Service Providers", 2017 (SMART 2016/0032).
[105] This scenario assumes the introduction of a mandatory data and application portability right, which is somewhat broader than the scenario presented in this section. However the growth forecast is still expected to be relevant.
[106] Workshop held on 18 May 2017 in Brussels.

thus, hampering the export of data from one cloud service provider and their import to another cloud service provider". High level EU principles could **encourage industry-wide initiatives**.

Although it is currently impossible to obtain a macro-economic estimate of what this option would entail at European level in terms of costs' savings, it is possible to get some insights at the **micro-level** thanks to a study by Kolb, Lenhard and Wirtz[107] who carried out and evaluated the migration process for a real-world application among seven cloud platforms. Their study shows that there are many costly and time-consuming issues to grapple with for cloud service providers when customers migrate from platform to platform. The effort put into this by cloud service providers differs considerably from vendor to vendor. Introducing a principle of data portability to enable switching would steer the efforts made by market players in the same direction, and force more cooperation and a more streamlined approach to portability solutions (both on a technical and contractual level).

At the same time, however, evidence suggests that legislative action in this intervention area **should not be too detailed**, as this could have counterproductive effects. Analysis of the written inputs to **the public consultation** indicates that some stakeholders are concerned about the introduction of a right to data portability for any kind of data held by a company. Likewise, they flag the risk of negative impacts on innovation.

The increase of switching requirements is likely to lead to a **regulatory burden and compliance costs** on the service provider. Here it could be argued that since service providers will anyway have to give effect to the portability right under the GDPR, these negative effects will be limited. Since many of the cost factors are present but quantitatively unknown, this option aims to strike the balance in regulatory intervention.

At the same time, the level of information supplied by the evidence-gathering process (e.g. the dedicated support study 'Switching Cloud Providers') is of such a modest volume, that instituting a legal right to portability and an obligation to CSPs could yield negative externalities that are not yet assessed. In this respect, the Commission should be cautious about instituting such a right.

Sub-option 2a

Sub-option 2a would rely on self-regulation by industry through the development of codes of conduct for facilitating switching between providers. Accordingly, Sub-option 2a may lead to less directly positive economic result than Option 2, because of a more modest approach to mitigating market dynamics leading to 'self-imposed localisation'. This is because it is much more effective to raise awareness around a clear legal principle than around a decentralised effort of industry to develop codes of conduct that is foreseen under Option 2a.

Option 2a would however still induce the largest amount of the positive economic effects assessed for Option 2 above, because it would provide for action by the industry to develop codes of conduct on switching and standards of information provision to users regarding the conditions under which data can be ported out of their IT environments. This would provide for better functioning of market forces to yield easier switching and porting data for customers.

What is more, the sub-option would probably result in lower compliance costs for cloud service providers than under Option 2, because self-regulation would present the cloud service industry with the opportunity and responsibility to self-regulate while minimising compliance costs.

6.4.1.4 Security of data processing

This option would facilitate the identification and development of reliable common standards and/or certification schemes for the security of storage and/or processing of data. Concretely, a specific

[107] Stefan Kolb, Jorg Lenhard and Guido Wirtz, "Application Migration Effort in the Cloud – The Case of Cloud Platforms" (2015), available at: https://www.researchgate.net/publication/303750569_Application_Migration_Effort_in_the_Cloud

cloud service providers' certification scheme could be developed through cooperation on standards by the Member States.

There will be an impact on the providers of cloud services which will be involved in the making of the **codes of conduct and standard-setting**. This is likely to entail only moderate **costs,** as participation would be voluntary and possibly devoted to trade associations and bodies. The cloud services providers may be more extensively affected by the specification of EU standards, to the extent that they would implement new standards (one-off cost and lower running cost ensuring updates).

The **benefits from standards** would be expected to outweigh the costs if an EU-wide certification and labelling scheme for the Cloud sector is established. This would enhance the **efficiency of companies** operating cross-border as industry could certify their products and services only once and against a scheme that is recognised in the whole of the EU. The existence of standards in areas such as security is likely to increase trust and hence attract more business end users of cloud services, thus fostering **growth and competitiveness** across the borders

At the same time a minimal level of common requirements would reduce uncertainty and lack of trust stemming from different levels of data security among the Member States[108] which is currently contributing to alter the market structure and the client choice[109], as has been proven by stakeholders consulted and by the support studies.

The importance of certification and standards has been quantified by Deloitte[110] calculating that cloud users are expected to experience an additional NPV creation of 0.64% (which corresponds to around EUR 3.5 billion) from the additional user uptake generated by these certifications and standards and the reassurance they provide that these cloud services can be considered safe and reliable.

Sub-option 2a

Instead of catering the possibility for a new cooperation mechanism on security standards or certification schemes, Sub-option 2a would enhance legal certainty on the already applicable security requirements. It would recall that any existing security requirements for companies will continue to apply to them, regardless the location in the EU where their data is stored or processed and also when this is subject to outsourcing to a cloud service provider.

The economic impact of security elements of the sub-option would be more positive than under Option 2, as it would lead to a higher degree of legal certainty in the market. This positive effect is attained by explicitly avoiding any overlap with existing requirements, while at the same time providing reassurance to businesses about the continued applicability, also across borders in the EU and under outsourcing arrangements, of the security provisions under which they already operate.

The actual security levels of data storage and processing in the EU would be maintained or even improved compared to Option 2, because the same EU actions on security of data storage and processing would still be provided for under Sub-option 2a, only on a different legal basis, making use of other cyber security initiatives and the NIS Directive.

[108] The Study by London Economics Europe et al., "Facilitating cross border data flow in the Digital Single Market", 2016 (SMART 2015/0016) provides clear insights and figures about how business and individuals tend to perceive or assume real **differences in the level of data security across European countries;** and use data **location as a proxy for security** (with one's own country often, though not always, seen as more secure).

[109] For example, the LE Europe study (SMART 2015/0016) notes that "For the UK, a recent study by Vanson Bourne found that 86% of enterprise customers believe it is important for business-critical data to be stored by a UK-based cloud service provider to ensure "data sovereignty"".

[110] Deloitte, "Measuring the economic impact of cloud computing in Europe", 2016 (SMART 2014/0031).

6.4.2 Environmental and social impacts

6.4.2.1 Free flow of data across borders

Option 2 would have a positive impact on the environment, since data service providers and organisations using in-house data storage or processing IT systems would receive concrete benefits. Firstly, they would be free to deploy data storage or processing infrastructures in those locations which are characterised by low average temperatures and/or abundance of renewable sources of energy, thereby achieving small environmental footprints of their activities. Secondly they would be able to adopt innovative approaches to the use of energy in data centres, e.g. maximising the use of renewables by shifting the data processing load to a data centre where renewable energy is available at a particular moment.

In **direct terms**, Option 2 would have a positive impact on social issues in terms of employment. An interview with a large European cloud service provider on the specific conditions for investment in data centre locations led to the conclusion that a moderate number of new jobs might well be created thanks to relocation of data centres to Member States with better conditions in terms of climate, energy prices or land prices. In line with EU-regional policy objectives to diversify economic activities in rural areas, this is likely to more evenly spread data centre jobs over geographical locations in the European Union. At the same time, this would not lead to loss of jobs in the locations were data centres are located before relocation, because they can be operated remotely, so current personnel would not have to be necessarily relocated. Data centres can easily service clients over larger distances, for instance 2000 kilometres between a data centre and its clients is feasible.[111] This allows for an optimal distribution of resources of cloud service providers over the EU because of the more transparent, predictable and open regulatory environment for data storage and processing activities. [112]

More generally, as illustrated in the high growth scenario by the European Data Market Study, by 2020 the overall number of data jobs is estimated to amount to 10.4 million, subject to a set of very favourable framework conditions triggering a faster take-up of data services and technologies. Apart from other factors such as the adoption and diffusion of all digital technologies, as well as the awareness and willingness to deploy them, the removal of regulatory barriers such as restrictions to the free flow of data, is critical to a favourable framework.[113] Therefore, Option 2 would have a positive impact on the overall creation of data jobs by 2020.

In **indirect terms,** however, Option 2 would have a positive impact on employment because of the added growth and innovation potential, caused by the lower costs for (i) setting up a business in the EU, (ii) entering a new market, (iii) launching a new product or service to the market and (iv) the ability to serve public and private customers, as indicated in section 6.4.1.

In **social terms**, Option 2 would reduce the number and range of limitations constraining (i) business choices regarding the location of data storage or processing infrastructures and (ii) the opportunities for data service providers to serve customers in other Member States. It would, therefore, have a positive impact on the freedom to conduct a business provided for by Article 16 of the European Charter of Fundamental Rights.

6.4.2.2 Data availability for regulatory control by Member State authorities

Policy action on improving data availability to Member State authorities for regulatory control purposes would increase cross-border data mobility because of raised levels of trust both with

[111] Latency requirements persist only for a very small number of applications, such as high-frequency trading.
[112] Discussions with a large cloud service provider, headquartered in France.
[113] See further pp.190 & 195, European Data Market, 2017 [IDC Study (SMART 2013/0063)].

market participants and with Member States authorities. Therefore, there would be significant positive environmental impacts flowing from this intervention area under Option 2.

6.4.2.3 Switching and porting data between providers and IT systems

The introduction of a legal principle of data portability to facilitate cloud switching, especially when accompanied by guidance and recommendations on the levels of interoperability needed, would force companies to improve the interoperability of their systems. With a minimum level of interoperability ensured, migration processes would need less processing power and thus have less of an environmental imprint.

As for the social impacts of this option, the assessment is the same as for the preceding options.

Sub-option 2a

Sub-option 2a does not include a legal principle of data portability. For that reason, it might lead to less directly positive environmental and social effects in terms of the decrease of processing power used for migrating data from one server (of a service provider) to another server. However, this difference in impact would be negligible as Sub-option 2a would provide for self-regulation through the development of codes of conduct, which will also lead to improved interoperability of systems.

6.4.2.4 Security of data processing

Option 2 foresees in the development of a specific cloud service providers' certification scheme. This would mean a considerable improvement in terms of cyber security, compared with Option 1. Therefore, potentially negative environmental and social impacts of cyber-attacks, as described in 6.2.2.4 would diminish under Option 2.

Sub-option 2a

Sub-option 2a would not provide for any additional actions on cyber security. However, the issue will be addressed by of other/existing EU instruments, such as the NIS Directive. As for potential environmental/social impacts of cyber security it is not important at all which instrument is used, Sub-option 2a would not lead to impacts different from Option 2.

6.4.3 Impact on Member States' public authorities

6.4.3.1 Free flow of data across borders

Option 2 would lead to moderate administrative burden for Member States' public authorities, caused by the allocation of Member States' human resources necessary for structured cooperation between Member States and the Commission by means of a 'single points of contact' expert group in the Member States. The single points of contact would be represented by civil servants who are already employed by Member States' public services, but whose responsibilities would be expanded or further coordinated.

As indicated in the description of Option 2 in section 5.4, these single points of contact would be tasked with cooperation regarding free flow of data categories (in particular in the context of the expert group) and organising awareness raising campaigns around the free flow of data principle.

The expert group would meet regularly. Accumulating the tasks mentioned above, it can be estimated that 0.5 FTE would be sufficient to fulfil these duties, because the expert group would not meet frequently. Moreover, any implementing acts could be taken by making use of the comitology procedure of an existing Committee. According to the 'institutional cost estimation' tool used for the

European Electronic Communications Code, this would result in an annual cost of EUR 33.384 for Member States. [114]

Option 2 would also put in place the notification/review procedures to verify the compatibility with the EU law of Member States' planned and existing derogatory measures as well as the transparency mechanism and could, therefore, result in administrative burden on Member States' public authorities. However, all options would include notification and review process, including the baseline option. Therefore, there are no further added costs in this respect in the higher intervention range options. As demonstrated in the section describing drivers of the problem above, the number of measures to be notified and reviewed is not expected to be very high. Assuming that a Member State would have to provide between 1 and 5 notifications per year and that an average administrative cost is around €385 per notification[115], the annual administrative burden per Member State would range between approximately €385 and €1925.

6.4.3.2 Data availability for regulatory control by Member State authorities

Although this option would slightly increase the coordination costs for the Member States' administrations as compared to the previous two options, this cost would be fixed and the effort to establish the system would be a one-off. On the other hand, the benefits of common approaches and guidelines, as well as increased cooperation on data availability in electronic format are going to be increasingly large as the volume of cross-border data availability requests increases.

As Option 2 would place any actions on this intervention area under the cooperation framework of single points of contact mentioned in section 6.4.2.1, the financial burden for this intervention area will be shared with the free flow of data area and will not generate extra costs.

6.4.3.3 Switching and porting data between providers and IT systems

Under Option 2, market participants would be required to give insights in the processes, technical requirements, timeframes and charges that apply in the situation of switching providers. So, although Option 2 would institute a legal principle on porting for switching provider, any burdens would be placed on the private sector, not the public authorities of Member States.

Sub-option 2a

This option would rely on self-regulation, to be monitored by the European Commission. Therefore, there would be no conceivable additional impact on Member States.

6.4.3.4 Security of data processing

There would be no administrative burden for Member States in the intervention area of security under this option. It envisages the development of common standards, but this could also be done by industry.

Members of the cooperation group of single points of contacts would be expected to have regular but non-frequent meetings with the data protection authorities and cyber security authorities of Member States, but because this will constitute a maximum number of two meetings annually, no extra burden in terms of HR or finance is to be expected.

Sub-option 2a

[114] The "Institutional Cost Estimation tool", used to calculate Full Time Equivalent cost parameters, was developed in the context of the support study for the Impact assessment of the European Electronic Communications Code (SMART 2015/0005).

[115] Based on the data presented in the Impact Assessment accompanying the proposal for a Directive on the enforcement of Directive 2006/123/EC of 12 December 2006 on services in the internal market, laying down a notification procedure for authorisation schemes and requirements related to services, the average time spent to comply with the notification procedure analysed in the IA is 12 working hours per notification. Taking the EU average of hourly earnings of civil servants with university education of €32.10, this results in an average administrative cost of €385.20 per notification.

This option would rely completely on existing legislative instruments for security. Therefore, there would be no conceivable additional impact on Member States.

6.4.4 Stakeholder views

6.4.4.1 Free flow of data across borders

The majority of stakeholders who responded favour Option 2 for this intervention area, because it concerns a legislative approach, combined with certain non-legislative elements such as cooperation and awareness raising.

The public consultation consulted stakeholders on the type of EU-level action they consider appropriate to address data localisation restrictions. 55.3% of respondents advocate legislative action[116]. Cross-checking the multiple-choice answers to this question with the written contributions to the same question leads to the conclusion that most respondents see a combination of a legislative instrument and increasing the transparency of justified restrictions as the most appropriate option. As Option 2 foresees precisely this, it may be inferred that the majority of public consultation respondents would have chosen Option 2.The respondents' argument behind the call for a legislative instrument is that this provides clarity and legal certainty by establishing a general principle of the free movement of data.

Exemplifying this argument, in one of its responses to the public online consultation, a cloud service provider stated: "*In the cloud computing business, the most common data localisation restrictions we see target financial, health, telecom and public sector data. However, these measures are less often found in black and white legislation, but rather in sectorial guidelines by national regulators or government agencies*". As the respondent also stated, it is increasingly difficult for data storage and processing (cloud) service providers to be aware of all data localisation restrictions that are in place at a given time, because of the multitude of regulators and agencies and of their varying approaches to technology and data transfers.

Therefore, only a legislative instrument would be appropriate to solve the problems, as non-legislative initiatives would not replace the current patchwork of applicable legislation and therefore retain legal uncertainty. As was demonstrated in the previous sections, perceived localisation by the market is an important obstacle to data mobility. As the policy objective is to take these obstacles away, Options 1 and 2 would be disqualified.

According to certain stakeholders, awareness-raising around a legal principle on the free flow of data is important. The government of the United Kingdom phrased it accordingly while discussing its favoured policy option in a position paper submitted as answer to **the public online consultation**: "*The European Commission proposes a new consolidating regulation which provides clarity and legal certainty […]. To be effective, this should be accompanied by awareness raising in Member States […]*" Option 2 foresees in such **awareness raising** around the Free Flow of Data principle (awarding this task to the single points of contact group). Therefore, Option 2 would be in line with these stakeholders' views.

6.4.4.2 Data availability for regulatory control by Member State authorities

During the **structured dialogues with the Member States** the availability of data for regulatory control emerged as a key concern. During the first dialogue the fact that cross-border storage could in some cases mean that data would be unavailable for inspection, was flagged by Member States as a 'key challenge or threat' of a future free flow of data right. In the second dialogue this was reversed to a positive 'functional requirement' to flank a potential free flow of data right: Member States indicated to be willing to remove certain data localisation restrictions if availability of certain data would be guaranteed by another provision of the legal act. At the end of the dialogue process,

[116] 289 respondents participated in this particular multiple choice question, of which the outcome is that 'a legislative instrument' is the most favoured option. However, respondents could indicate multiple options.

during the third meeting, the majority of Member States agreed that data availability should be a building block of a forthcoming free flow of data proposal.

22.3% of stakeholders responding to **the public online consultation** identified the immediate availability of data for supervisory authorities as an important enough issue to keep (some form of) data localisation restrictions to safeguard it, while at the same time a majority of respondents voted for taking away data localisation restrictions in general. This clearly shows that stakeholders feel that data availability for regulatory control is an important issue that needs to be tackled.

Option 2 will address these legitimate concerns by providing certainty on private undertakings' responsibility to provide data and strengthening Member State cooperation. Appointing single points of contact in the Member States and putting in place a cooperation framework on data issues should further promote the effectiveness of the principle of data availability for regulatory control and its development via model clauses and practices. Therefore, Option 2 would correspond to the views of the majority of stakeholders.

6.4.4.3 Switching and porting data between providers and IT systems

Of the stakeholders that participated in the **public consultation**, most argued for non-legislative forms of EU intervention, such as setting standards or addressing the issue through developing model-contracts for cloud service providers.

In written contributions to the public consultation, a small majority reacted positively when asked about their attitudes towards a more general portability right for non-personal data. Although they were not specifically consulted about the introduction of data portability rights for cloud switching, many of the respondents to the public consultation were also cautiously positive towards the possible EC introduction of such rights.[117] When it comes to cloud-specific portability rights, several positive effects were cited by the respondents, such as reduced vendor lock-in, increased competition, new business opportunities, more data-driven innovation and research and better convenience for the customers. Among the negative effects cited by the respondents were increased financial and technical burdens on providers and the possible disclosure of IPR and trade secrets.

One responding organisation to this open question explained its position by drawing a comparison between portability rights for individuals regarding their personal data and the data flows that businesses deal with: "*Organisations using cloud services are no different to consumers in terms of their need for the portability of the data they collect with these systems and services, it is the history of their organisations business transactions and the portability of such data is an essential element of protecting any organisations assets and capability*."[118]

Among the participants in the **workshop on cloud switching**[119] (who were all either cloud service providers or business customers of such services), about half considered there is need for a European regulation to ensure a right to port data in view of switching cloud service providers[120]. There was a preference among the participants for principles-based legislative initiative rather than more detailed legislation, as too much detail in the provision might hamper the development of flexible and innovative solutions.

Certain **Member States** have also shown interest in a legal right to data portability. The **French** Digital Council has announced its support of an EC initiative to introduce legal rights to portability

[117] Stakeholders from certain more industrial sectors, such as the transport, utilities and energy sectors, as well as the media sector, were generally more positive towards the introduction of a data portability right in order to facilitate cloud switching.

[118] Answer from Mydex CIC (United Kingdom)

[119] Workshop "Data and application portability in the cloud: current challenges & policy scenarios", Workshop organised by IDC and Arthur's Legal (SMART 2016/0032), 18 May 2017. Workshop report accessible via: https://ec.europa.eu/digital-single-market/en/news/stakeholder-dialogue-building-european-data-economy

[120] The polarisation observed between stakeholders calling for legal actions on portability and those opting for softer measures corroborates the input provided by Member States at the occasion of the 3rd structured dialogue.

of non-personal data[121], as discussed in the EC Communication on Building a European Data Economy. The **Estonian** government has also recently published a vision paper on the free movement of data in which they elaborate on the possible future framework for data access and portability[122]. Although no direct call is made for the development of new data portability rights, the Estonian government clearly sees the need to address the issue, claiming that "there are at present no obligations to guarantee even a minimum level of data portability, even for widely used online services such as cloud hosting providers", and that " The right to data portability is relevant both in the B2C and B2B contexts".

Sub-option 2a

As indicated above, many stakeholders that participated in the public consultation and the dedicated workshop on switching cloud providers, propagated a soft law, market driven approach to porting data and switching providers/IT-systems, as they believed that a portability right could potentially curb innovation in the market. This sub-option, relying on self-regulatory codes of conduct, would therefore better respond to the vision of the majority of stakeholders.

6.4.4.4 Security of data processing

Nearly all stakeholders with an IT background state that security of data processing would benefit from increased data mobility. Other stakeholders concur with this, or remain silent on the topic. Keeping this in mind, it could be inferred that their opinion would be that Option 2 is preferred, as it proposes to introduce a principle of free flow of data within the EU and the review of existing measures. This would enhance legal certainty to cyber security providers, meaning that they would be able to deliver better cyber security services to their customers, for instance by doing cyber security updates at once for all customers, regardless of their location in the EU.

Sub-option 2a

No significant stakeholders' views were received regarding this Sub-option, as it was not tested in the public online consultation. This is because Sub-option 2a relies completely on existing security requirements. Assuming that these requirements achieve the policy objectives in an efficient manner, stakeholders' judgment would be that the sub-option is equally positive as Option 2.

6.5 Option 3: Detailed legislative initiative to ensure trustworthy free flow of data across borders and facilitate switching and porting data between providers and IT systems

6.5.1 Economic impacts

6.5.1.1 Free flow of data across borders

As this option would establish pre-defined, harmonised white or black list of localisation restrictions, as well as a dedicated platform to ensure transparency around them, it would have a large impact on data localisation restrictions and would provide legal certainty. At the same time, it can be expected that the option would **only moderately reduce the number and range of data localisation restrictions and prevent the emergence of new restrictions, since the pre-defined assessments approach would incite Member States to seek listing entire sectors or types of data as areas of justified restrictions**. Also, this option and the measures included therein would entail a higher regulatory burden for the Member States' public administrations. As the benefits of

[121] CNNum, "La consécration d'un droit a la portabilité des donneés non-personnelles", New Opinion of the French Digital Council on the Free Flow of Data in the European Union. Enshrining a right to non-personal data portability. Also: https://cnnumerique.fr/wp-content/uploads/2017/05/OpinionCNNum_FFoD_ENG-1.pdf

[122] Ministry of Economic Affairs and Communications of Estonia, "Estonian Vision Paper on the Free Movement of Data: the Fifth Freedom of the European Union", available at: https://www.eu2017.ee/sites/default/files/inline-files/EU2017_FMD_visionpaper_1.pdf

these more stringent measures could not be justified, the precautionary and better regulation principles would not be well served by this intrusive option.

In terms of **impacts on the cost and choice for users,** Option 3 would relieve organisations using external data services from negative **indirect effects**. To recall, it is reasonable to assume that under the baseline scenario and in the absence of intervention the additional costs borne by the cloud service providers due to data localisation restrictions would be passed on to users (e.g. cloud providers might charge a premium for the use of cloud data centres in particular locations). In fact, prices for the same quality of services can differ up to 50% between different Member States[123].

6.5.1.2 Data availability for regulatory control by Member State authorities

Option 3 foresees to establish a detailed cooperation mechanism to enforce the possibility for public authorities to effectively obtain data subject to detailed procedures, when it is stored or processed in another Member State. This type of intervention will require competent authorities to meet deadlines for answering the enquiries by other Member States, and common request and response templates would be specified for the implementation of the policy initiative. As for the previous two options discussed, the impacts on the business sector from provision easing data availability for regulatory control by Member States authorities are likely to be indirect.

This option would probably incur a higher increase in **coordination costs** for the **Member States' administrations** as compared to Option 2 due to the number of elements in the process that will have to be harmonised (including templates and dispute resolutions mechanisms). The evidence from the structured dialogue with the member states is not clear on whether the benefits (similar to the ones from Option 2) would overcome the costs (higher than Option 2).

The impacts on the **business sector** under this option are going to be equally sizeable as under Option 2 and of the same indirect nature.

6.5.1.3 Switching and porting data between providers and IT systems

As outlined in section 5, this option would establish both the principle of switching / porting facilitation and harmonise the key technical and legal conditions (e.g. concerning types of data, usable formats / structures, timeliness). In section 2.3 the trade-off between the regulatory burden on providers and the higher operational efficiency of the business end-users was described. This trade-off would be even more radical under Option 3, which would be more prescriptive in nature. Too invasive a regulatory intervention may also **stifle innovation and undermine growth** of the cloud data services sector in Europe.

The scant quantitative evidence currently available and the results of the support study and the public consultation do not seem sufficient to argue the case for the type of strong regulatory intervention under Option 3.

This is in line with stakeholders' concerns emerging from **the public consultation** about overly prescriptive regulation. They suggest that business models and types of non-personal data are too different to allow for full regulatory intervention. Rather, a principle-based approach is advocated.

6.5.1.4 Security of data storage and processing

This option entails developing common standards, a European certification scheme for the security of storage and processing of data. Their use would be mandated. The economic impacts are qualitatively very similar to those of Option 2, but the magnitude of their economic impact on business is likely to be wider as it would become an obligation for all companies, who would have to adopt the standards irrespective of their size and cross-border activity.

[123] *Supra,* p.14

6.5.2 Environmental and social impacts

6.5.2.1 Free flow of data across borders

Option 3 would have a positive impact on the environment, since cloud service providers and organisations using in-house data storage or processing IT systems would have more opportunities to deploy data storage or processing infrastructures in those locations which are optimal from the environmental point of view and to adopt innovative approaches to the use of energy in data centres.

The social/employment impacts foreseen by Option 3 are similar to those in Option 2, so the reader is referred to section 6.4.2.

6.5.2.2 Data availability for regulatory control by Member State authorities

Policy action on improving data availability to Member State authorities for regulatory control purposes would increase cross-border data mobility because of raised levels of trust both with market participants and with Member States authorities. Therefore, there would be positive environmental impacts flowing from this intervention area under Option 3, in line with the previous section.

6.5.2.3 Switching and porting data between providers and IT systems

The assessment of environmental and social impacts for this option is the same as for Option 2.

6.5.2.4 Security of data processing

As Option 3 contains the same provisions on security as Option 2, the impact on environmental and social issues can be considered the same.

6.5.3 Impact on Member States' public authorities

6.5.3.1 Free flow of data across borders

The administrative burden on Member States' public authorities posed by Option 3 would be significantly higher than for the other options. The reason is the proposed set-up of a new Committee under EU law. Member States' civil servants would have to travel to Brussels more frequently than in Option 2. This would result in human resources costs of 0.75 FTE, i.e. 0.25 FTE more than in Option 2 as a result of more frequent meetings and travelling by Member States' civil servants. On top of this 0.75 FTE, there would be an additional 0.5 FTE needed because of the high number of implementing acts (and the resulting comitology work) that is envisaged under this policy option. It would therefore mean a total of 1.25 FTE per Member State. Using the institutional cost estimation tool, this would mean an average annual cost of EUR 83.460 per Member State.[124]

6.5.3.2 Data availability for regulatory control by Member State authorities

As Option 3 would place any actions on this intervention area under the comitology mechanism mentioned in section 6.5.3.1, the administrative burden for this intervention area will be shared with the free flow of data area and will not generate extra burden in excess to this.

6.5.3.3 Switching and porting data between providers and IT systems

The expected impacts of Option 3 on Member States' public authorities are the same as those of Option 2 for the intervention area of switching and porting data between providers and IT systems, because this option leaves the responsibility with the private sector.

[124] The "Institutional Cost Estimation tool", used to calculate Full Time Equivalent cost parameters, was developed in the context of the support study for the Impact assessment of the European Electronic Communications Code (SMART 2015/0005).

6.5.3.4 Security of data processing

The expected impacts of Option 3 on Member States' public authorities are the same as those of Option 2 for the intervention area of security of data processing, as both options contain the same policy approach to this area.

6.5.4 Stakeholder views

6.5.4.1 Free flow of data across borders

In position papers submitted to the Commission in the framework of **the public online consultation**, several stakeholders have emphasized the importance of awareness raising around the principle of the free flow of data. In their opinions, Option 3 would be probably less convincing than Option 2 because Option 3 is a purely legislative option and makes no reference to awareness raising activities. The reason is that Option 3 foresees comitology as execution mechanism, instead of a cooperation group made up of representatives of Member States' civil services. Without awareness raising, these stakeholders could argue, it is not efficient to adopt legal principles on the free flow of data as this would insufficiently address the legal uncertainty and lack of trust problems that were identified by nearly all stakeholders.

6.5.4.2 Data availability for regulatory control by Member State authorities

As indicated above, stakeholders identified data availability for regulatory control as an important issue in their responses to the public online consultation.

Option 3 would meet stakeholders' views in this respect, as it would develop a detailed cooperation mechanism to enforce the possibility for public authorities to effectively obtain data in a timely manner, when it is processed in another Member State.

6.5.4.3 Switching and porting data between providers and IT systems

Although around 60.6% of stakeholders participating in the public consultation support the introduction of a specific right to ensure the possibility of switching between providers and IT systems, almost all stakeholders have pointed to the risk of being too specific in proposed legislation.

Stakeholders emphasize that being over-prescriptive is a risk regarding multiple elements of a switching right, but technical standards were mentioned most in this context. As one respondent put it: "*Rebuilding IT solutions entails high costs. Imposing similar demands on machine-generated data would mean enforcing technical solutions, which would hardly benefit innovation and competitiveness in Europe*."[125]

Also in the cloud switching workshop[126] many participants were positive towards the establishment of a legal principle of data portability to facilitate switching, however many explicitly noted that any such right should not be too detailed, as too many prescriptive solutions in law might prevent the industry from coming up with good solutions.

6.5.4.4 Security of data processing

As Option 2 and 3 contain the same policy approach to this area, stakeholder views for security of data processing would here be the same as for Option 2. Therefore, the reader is referred to section 6.4.4.4.

[125] IBEC Position Paper submitted to the Public Online Consultation 'European Data Economy'
[126] Workshop, "Data and application portability in the cloud: current challenges & policy scenarios", 18 May 2017, for Study SMART 2016/0032, IDC and Arthur's Legal, "Switching between Cloud Service Providers", 2017.

7 How do the options compare?

This section presents a comparison of the options in the light of the impacts identified. The options are assessed against the criteria of efficiency of reaching the policy objectives, potential impacts in terms of economy, environment, society and financial burden, as well as taking into account the support expressed by the different stakeholders. *For each of the different categories, the options*[127] *receive scores on a scale from -2 to +2, taking into account the following rules:*

-2: directly negative impacts
-1: indirect negative impacts
0: neutral
+1: indirect positive impacts
+2: direct positive impacts[128]

In the descriptions below, an explanation of the scoring will be provided. The calculated total scores per option are displayed in the last row of the table below summarising the findings.

Effectiveness

In this comparison exercise, effectiveness is defined as the ability of the options to reach the specific policy objectives of this initiative.

Option 1 would use non-legislative initiatives and a strengthened enforcement of existing legislation to promote the stated policy objectives. Such an approach could persuade Member States to remove certain existing data localisation restrictions, as was indicated by the structured dialogue with the Member States. Moreover, a strengthened enforcement approach could be an improvement on the baseline scenario. However, there would be no clear legal framework for discussions with Member States and the impact of infringement procedures would be limited and likely to take considerable time to deliver results. This leads to an overall indirect negative scoring for effectiveness **(Option 1: -1).**

Option 2 would prevent Member States from putting in place unjustified data localisation restrictions, requires the review and evaluation of all existing data localisation restrictions and foresees a notification mechanism in case Member States intend to put in place new (in their view justified) data localisation restrictions. It would also introduce the principle of switching and porting data between cloud service providers and back in-house, but it avoids prescriptive and technical legislation in the first instance. The same method applies to the area of security of data processing and storage. This option would therefore achieve all four policy objectives **(Option 2: +2)**. **Sub-option 2a** also receives a positive scoring for effectiveness, as the policy objectives of easier switching and porting of data and security of data storage and processing can also be attained by relying on existing instruments and self-regulation. More specifically, the reassurance provided by Sub-option 2a that the legal proposal would avoid any overlap with other EU security instruments, would lead to a higher level of legal certainty **(Sub-option 2a: +2).**

Effectiveness-wise, **Option 3** would be less likely than Option 2 to realise the policy objectives set out in section 4 of this Impact Assessment. By enshrining detailed provisions in law on what constitutes (un)justified data localisation restrictions, and forbidding the existence of all unjustified data localisation restrictions along these lines, it would significantly lighten up the existing situation. But it would also risk inciting Member States to list entire sectors or types of data as areas of justified restrictions and therefore only moderately reduce the number and range of data localisation restrictions and prevent the emergence of new restrictions. The positive impact in terms of reaching the policy objectives is therefore less predictable **(Option 3: +1)**.

[127] Sub-option 2a will only be described when its scoring deviates from Option 2.
[128] As 'coherence' is not a scalable issue but of a binary nature (something *is* or *is not* coherent), the following scoring method will be used for coherence: -2: 'coherence problems' / 0: 'no coherence problems'.

Economic impacts

As **Option 1** would not change the more fundamental problem of localisation by the market as a result of legal uncertainty and a lack of trust, it is not deemed to generate positive economic effects **(Option 1: 0)**.

By establishing a clear legal principle accompanied by cooperation between and with Member States as well as self/co-regulation, **Option 2** will enhance legal certainty in the short term, while staying relevant and effective in the long term. This option would have a much stronger impact in addressing the problems related to legal uncertainty and lack of trust, which is needed for a true change in market dynamics, removing 'self-imposed' localisation. Evidence gathered for this Impact Assessment shows that this would have the most significant economic effects **(Option 2: +2). Sub-option 2a** may lead to less effective mitigation of market dynamics leading to 'self-imposed localisation'. This is because, it is harder to successfully conduct awareness raising campaigns around self-regulation (e.g. on switching and porting data) than around a new legal right (e.g. the right to switch and port data). On the other hand, as indicated in section 6.4.1.3, the introduction of a portability right could lead to significant compliance costs for cloud service providers. Self-regulation, however, would present the cloud service industry with the opportunity and responsibility to self-regulate while minimising compliance costs. Also in the area of security of data storage and processing, Sub-option 2a yields positive economic effects, as it will enhance legal certainty for businesses, clarifying that any currently applicable security requirements will remain applicable to them regardless of the location of the storage or processing in the EU and also under potential outsourcing of these activities. Therefore, sub-option 2a receives a positive scoring for economic impact as well (**Sub-option 2a: +2).**

Option 3 could also lead immediately to significant burden for businesses, through very detailed technical specifications for switching between providers. Therefore, although it will likely reduce the number of data localisation restrictions to a degree, it will only get an indirectly positive score in terms of economic impacts **(Option 3: +1).**

Environmental & social impacts

Because **Option 1** envisages the use of existing legislation to eliminate unjustified data localisation restrictions at least to a certain degree under this option, it can have indirectly positive effects in terms of environment and employment **(Option 1: +1)**.

Because **Option 2** is expected to achieve all four policy objectives efficiently, this will yield positive economic and social impacts, as explained in section 6.4.2. However, as these impacts will be of indirect nature (e.g. through the relocation of data centres), the scoring is kept at +1 **(Option 2: +1)**. This would be the same for Sub-option 2a **(Sub-option 2a: +1).**

As **Option 3** would also decrease the number of data localisation restrictions, there will also be positive environmental and social impacts, As in Option 2 these will be of an indirect nature **(Option 3: +1).**

Coherence with existing legislation

As **Option 1** concerns a soft-law approach, the option will however not lead to problems of coherence with existing EU-legislation **(Option 1: 0)**.

Option 2 is nearly consistent with all existing EU legislation, because its principles merely complement the provisions in existing legislation, such as the General Data Protection Regulation. Its scope explicitly does not overlap with this regulation. However, the Option would run the risk of overlapping with other EU instruments on security of data storage by providing for cloud specific certification schemes, notably with the NIS Directive **(Option 2: -2)**. **Sub-option 2a** ensures full coherence with existing EU legislative instruments, because it is consistent with the GDPR in the

same way as Option 2, but leaves any EU policy actions on security to the scope of other/existing EU instruments, such as the NIS Directive **(Sub-option 2a: 0).**

As regards coherence, **option 3** would risk overlapping with existing mechanisms, for example in the area of data availability for regulatory control, because currently there are already many sectoral cooperation mechanisms in place **(Option 3: -2)**.

Administrative burden on Member States' public authorities

Option 1 will lead to a higher administrative burden for both the Member States and the Commission, because of the strengthened enforcement of existing legislation. This, however, will be in placed in the category of indirect costs **(Option 1: -1).**

Since **Option 2** does not envisage prescriptive detailed provisions it will achieve the objectives of the initiative at a limited and reasonable cost to the public authorities and market players. It would however lead to direct costs for the Member States in terms of human resources **(Option 2: -2).** This would be the same for Sub-option 2a **(Sub-option 2a: -2).**

Option 3 will result in direct higher burdens for Member States public authorities, because of the likelihood of many implementing procedures. **(Option 3: -2)**.

Stakeholder support

Stakeholders across the spectrum have strongly advocated legislative action to ensure free flow of data in the EU. Therefore, **Option 1** receives a -2 as it relies entirely on soft measures. However, on the intervention area of switching and porting data between cloud service providers, they were less in favour of legislative action. Therefore, in this area it receives a 0. Therefore, the overall score for stakeholder support will be averaged out to -1 **(Option 1: -1).**

Option 2 combines measures that are supported by stakeholders as best ways to foster the free movement of data in the EU single market **(Option 2: +2)**. **Sub-option 2a** will also obtain a positive scoring in this category, many stakeholders that were in favour of a legal right for the free flow of data, propagated a soft law approach to porting data and switching providers/IT-systems, as they believed that a portability right could potentially curb innovation in the market **(Sub-option 2a: +2).**

For **Option 3**, stakeholders' views were of diverging nature across the different intervention areas. As indicated before, most stakeholders see legislative intervention as suitable to introduce a free flow of data principle. However, they have not advocated a *detailed* legislative initiative. This results in a score of +1 for stakeholder support in this intervention area. Regarding switching for porting data, however, the majority warned the Commission for being too prescriptive in terms of prescribing technological standards, as this could be a barrier for innovation, leading to a -2 on this intervention area. Therefore, the stakeholders support is averaged to -1 **(Option 3: -1)**

Impacts	Option 0: Baseline Option – no EU policy change	Option 1: Non-legislative initiatives to promote free flow of data	Option 2: Principles-based legislative initiative and Sub-option 2a: Combination of principles-based legislation and self-regulation	Option 3: Detailed legislative initiative
Effectiveness	**0**	**-1**	**Option 2: +2** ***Sub-option 2a:* +2**	**+1**
Economic	**0**	**0**	**Option 2: +2** ***Sub-option 2a:* +2**	**+1**
Environmental & Social	**0**	**+1**	**Option 2: +1** ***Sub-option 2a:* +1**	**+1**
Coherence with existing legislation	**0**	**0**	**Option 2: -2** ***Sub-option 2a:* 0**	**-2**
Burden on MS authorities	**0**	**-1**	**Option 2: -2** ***Sub-option 2a: -2***	**-2**
Stakeholders' support	**0**	**-2 (free flow of data)** **0 (switching & porting data)**	**Option 2: +2** ***Sub-option- 2a:* +2**	**+1 (free flow of data)** **-2 (switching & porting data)**
Total	**0**	**-2**	**Option 2: 3** ***Sub-option 2a:* 5**	**-2**

For each of the different categories of consideration, the options received scores on a scale from -2 (direct negative impacts) to +2 (direct positive impacts). The calculated total scores are displayed in the last row.

8 Preferred option

Based on the above comparison, it appears that on balance Option 2a is the option that would best achieve the objectives of the initiative, taking into account the criteria of effectiveness, economic impacts and stakeholder support.

By combining clear legal principles, transparency requirements, clarifying the applicability of current security requirements, cooperation between and with Member States through the establishment of an expert group and self-regulation, the option will enhance legal certainty and raise trust levels, deliver tangible results in the short term (especially compared with the baseline option and option 1), while leaving substantial flexibility for the framework to evolve and adapt. Option 2a also combines measures that are supported by stakeholders as best ways to foster the free movement of data in the EU single market.

Subsidiarity, proportionality and coherence of the preferred option

The preferred option complies with the principle of subsidiarity, as the EU digital single market in this field cannot be accomplished by Member States acting nationally.

In particular, Option 2a would result in an effective and coherent framework in all the four intervention areas of this initiative:

(i) The combination of a legal free movement of data principle, notification, and review and transparency requirements would give appropriate incentives to remove and prevent data localisation restrictions across the EU single market.

(ii) Strengthening the commitment of market players to provide data for regulatory control even if it is stored in another Member State (legal principle) and a complementary administrative cooperation between the Member States where needed, would reinforce the case for the free movement of data in the single market.

(iii) Self-regulation and codes of conduct would induce a market-driven progress towards free movement of data across data cloud service providers and/or in-house IT systems in the single market.

(iv) Clarification that existing security requirements remain applicable to data storage and processing in other Member States and under outsourcing agreements would foster trust and facilitate a single market for this type of services and activities.

The preferred option does not go beyond what is necessary to solve the identified problems and is proportionate to achieve its objectives. Firstly, **Option 2a will rely to a high degree on the existing EU instruments and frameworks**: the Transparency Directive for notifications of data localisation restrictions and different existing frameworks ensuring data availability for regulatory control by Member States, thereby limiting additional administrative burdens on Member States. Secondly, the approaches to the movement of data across borders and across cloud service providers / in-house IT systems would seek balance between EU regulation and the public policy interests of Member States as well as balance between EU regulation and self-regulation by the market.

As regards switching / data porting, Option 2a would also be coherent with the IPR protection mechanisms of the Database Directive and the Trade Secrets Directive - it would not require any disclosure of IPR-protected information. Secondly it would not preclude foreign operators from accessing the EU market, would not treat foreign providers differently from EU providers or other foreign providers.

9 How would actual impacts be monitored and evaluated?

The Commission will ensure that the action selected in this IA contributes to the achievement of the policy objectives defined in Section 4. The monitoring process could consist of two phases:

The first phase would concentrate on the short-term and start right after the adoption of the legislative act. During this phase the Commission would engage with Member States (e.g. groups of experts) in order to increase their awareness and understanding of the new rules and stimulate the adoption of pro-active approaches when it comes to notifying data localisation restrictions and ensuring their transparency. The Commission would also engage with the relevant stakeholders in order to increase their awareness and understanding of the new rules.

The second phase would focus on the mid-to-long-term and would address direct effects of the rules contained in the legislation. The table below presents the **operational objectives** corresponding to the identified specific policy objectives, the indicators that would be used to monitor progress towards meeting the objectives as well as the possible sources of information. The information-gathering would start immediately after the beginning of application of the legislation and then continue every year (every second year in the case of the number and use of dedicated information channels).

9.1 Monitoring of the preferred policy option

The preferred option selected above will be monitored by the indicators listed in this section. Different indictors and sources of information are listed for the different operational objectives.

Figure 9 – Operational objectives for the preferred option

Area	Operational objectives	Indicators	Sources of information
Free flow of data	Prevent the adoption of unjustified and/or disproportionate national measures, eliminate existing unjustified and/or disproportionate national measures	The prevention indicator developed to measure the ability of the procedures provided by Directive 2015/1535 (the Transparency Directive) to prevent barriers to trade[129]	Internal: Commission services Single points of contact/ expert group
	Stimulate dissemination of information on data localisation restrictions by Member States, aggregate the information at the EU level	The number of dedicated information channels (websites, applications, etc.) To the extent the relevant data is available - the effective use of the information channels	This information would be obtained from publicly available sources or directly from Member States or the Single points of contact expert group
	Foster the adoption of data storage services	Increase in the % of European companies using cloud (hosting companies	Eurostat survey Single points of contact

[129] The ratio of the sum of the comments and detailed opinions of one year, divided by the total number of notifications which is then filtered to eliminate double counting due to the fact that more than one Member State can have a detailed opinion on the same notified draft law and/or that a Member State and the Commission may file a detailed opinion on the same draft law. For further details see the Impact Assessment accompanying the Proposal for a Directive on the enforcement of the Directive 2006/123/EC of the European Parliament and of Council of 12 December 2006 on services in the internal market, laying down a notification procedure for authorisation schemes and requirements related to services and CEPS Policy Brief, Anabela Correia de Brito and Jacques Pelkmans, "Pre-empting Technical Barriers in the Single Market", No. 277, 11 July 2012.

		database or CRM)	expert group
Data availability for regulatory control by MS	Stimulate exchange of information among MS and collaboration on data request	Number of consultations among MS	EDPR Single points of contact expert group
	Provide clarity on applicable law and jurisdiction	Decrease in the % of companies (large or SMEs) worried by unclear jurisdiction / applicable law	Eurostat survey Single points of contact expert group
Switching and porting data	Lower switching barriers for users	Decrease in the % of companies (large or SMEs) worried by the difficulty to unsubscribe or change cloud service provider	Eurostat survey Single points of contact expert group
Security of data storage and processing	Improving the level of actual and perceived security linked to data storage	Decrease in the % of companies (large or SMEs) worried by the risk of security breach Decrease in the number of incidents involving data centres	Eurostat survey Single points of contact expert group Industry ENISA Annual Threat Landscape

9.2 Sources of monitoring

9.2.1 Single points of contact expert group

The legislation will require Member States to designate a single high-level contact point to coordinate and facilitate the application of the measure in their respective jurisdictions. These contact points will serve collectively as an expert group that would allow for the exchange of information and for a process of constant monitoring by the Member States and the Commission. Furthermore, the experience of the expert group will serve as a valuable source of information during the ex-post evaluation phase of the legislation, which should take place five years after its application.

9.2.2 The Eurostat survey and its indicators

Eurostat tracks indicators on enterprises' use of cloud computing services in the EU[130]. Eurostat also conducts a bi-annual survey of the companies operating in the market tracking the factors limiting the enterprises' use of cloud computing-related services. This data can be used to determine a benchmark and to monitor the impact on the business sector of the provisions adopted.

9.2.3 DESI and the European Digital Progress report

The **European Digital Progress Report** (EDPR) covers 28 Member States and provides comprehensive data and analysis of market, regulatory and consumer developments in the digital economy. It is based inter alia on DESI[131] **(Digital Economy and Society Index**) combining the quantitative evidence from the DESI with country-specific policy insights. DESI is based on data

[130] http://ec.europa.eu/eurostat/statistics-explained/index.php/Cloud_computing_-_statistics_on_the_use_by_enterprises
The survey is carried out every two years on a sample of almost 2000 firms in the EU
[131] DESI reports available here: https://ec.europa.eu/digital-single-market/en/desi

from Eurostat and various studies and surveys[132], and is structured in five dimensions: Connectivity, Human Capital, Use of Internet, Integration of Digital Technology and Digital Public Services. DESI already tracks the degree of take-up of cloud services, but more specific indicators may be designed.

Insights on national policies come directly from the in-house expertise and research of country teams and daily policy work on data policy issues and the input from Member States. The information provided will be complemented by information collected through country visits.

9.2.4 The ex-post evaluation

A comprehensive evaluation could take place 5 years after the start of application of the rules. This evaluation will be executed in close cooperation with and relying on the information provided by the single points of contact of the Member States.

Since the principle of free flow of data is a pre-condition for the emergence of innovative virtualised and/or distributed data storage and processing technologies, as well as an enabler of data-driven innovation in general[133], this evaluation will have to assess the impact that the policy initiative suggested in this IA had on the capacity of businesses and the public sector to innovate as a consequence. It may seek synergies with the evaluation of other data policies.

Taking into account that data storage and processing are features of numerous services provided by both private and public sectors, the hurdles (extra costs and administrative burden) associated with (proliferating) data localisation restrictions could lead, indirectly, to negative impacts on consumers and citizens as users of those services. For example it could lead to no service being provided where otherwise it could have been provided - such as cross-border digital public services - or less attractive terms and conditions of a service[134]). The evaluation will have to cover these aspects and assess the extent to which the option chosen had an impact on the development of the Digital Single Market. It would need to examine whether it contributed to reducing the number and range of data localisation restrictions and to enhancing legal certainty and transparency of remaining (justified and proportionate) requirements, which is the **first specific objective** pursued by this initiative. Moreover, repercussions could be on the **fourth specific objective** concerning trust in / security of (cross-border) data storage and processing, since often localisation is driven by legal uncertainty / lack of trust in the market, as emphasised by the results of the public consultation. The evaluation will also have to assess whether the policy initiative has contributed to improve the trust in free flow of data from the Member States and whether they can reasonably have access to data stored abroad for regulatory control purpose (**second specific objective**). The evaluation shall be accompanied by an ad-hoc industry survey to assess progress in the area of switching (**third specific objective**), pricing and take-up of cloud services. A special edition of Eurobarometer may be considered for this purpose.

[132] Indicators and sources are available here: http://digital-agenda-data.eu/datasets/desi/indicators

[133] E.g. data localisation restrictions make it complicated for a researcher to aggregate data from various sources and use advanced data analytics tools.

[134] Localisation tends to reduce services and increase prices for domestic consumers: http://www.albrightstonebridge.com/files/ASG%20Data%20Localization%20Report%20-%20September%202015.pdf

GLOSSARY

Acronym	Meaning
API	Application Programming Interface
CAGR	Compound Annual Growth Rate
CNNum	Conseil National du Numérique – French Digital Council
CRM	Customer Relationship Management
CSP	Cloud Service Provider
DEI	Digitisation of European Industry
DESI	Digital Economy and Society Index
DLR	Data Localisation Restriction
DSM	Digital Single Market
ECFR	European Charter of Fundamental Rights
EDPR	European Digital Progress Report
EIO	European Investigation Order
ENISA	European Network and Information Security Agency
FFD	Free Flow of Data
FTA	Free Trade Agreement
FTE	Full Time Equivalent
GDPR	General Data Protection Regulation
IA	Impact Assessment
IaaS	Infrastructure as a Service
ICT	Information and Communication Technologies
IoT	Internet of Things
NIS	Network and Information Security
NPV	Net Present Value
PaaS	Platform as a Service
QoS	Quality of Service
R&D	Research and Development
SaaS	Software as a Service
SMTD	Single Market Transparency Directive
TFEU	Treaty on the Functioning of the European Union