BDI

POSITIONS | EUROPEAN POLICY | BREXIT

Data and ICT

Challenges caused by Brexit

20 March 2018

Core Recommendations

- Data flows between the UK and the EU must be guaranteed from day one.
- The United Kingdom should implement the GDPR into UK law in order to have an adequate level of data protection, comparable to EU law.
- We urge the European Commission to start and speed up the process of an adequacy decision in order to reach a swift agreement on cross-border data flows.
- Transitional rules need to be put in place for UK-EU data flows until the adequacy decision comes into force.
- The UK should remain a member of the Working Party 29 or at least be granted observer status.
- The UK should continue to be part of the European cybersecurity exchange network despite its withdrawal from the European Union.
- Aspects of market access for cybersecurity products and services should be regulated in the EU's contractual arrangements with the UK.
- EU-NATO cooperation on cybersecurity should be continued systematically and intensified together with the UK.
- The best scenario for roaming charges would be for the UK to become an EEA member state, as EU rules would then continue to apply.
- The UK economy and the related 5G spectrum is inseparably connected to Europe. The 5G spectrum is not expected to be impacted significantly by Brexit from a purely economic perspective.

Stefanie Ellen Stündel | Digitalisation and Innovation | T: +32 2 792-1015 | s.stuendel@bdi.eu | www.bdi.eu

BDI Task Force Brexit

The BDI is committed to supporting the Brexit negotiation teams with in-depth expertise in a number of areas of economic policy. In summer 2017, the BDI set up a Brexit task force together with its member organisations, company representatives and partners including the Association of German Banks (BdB), the German Insurance Association (GDV), the Federation of German Wholesale, Foreign Trade and Services (BGA), the Confederation of German Employers' Associations (BDA) and the Association of German Chambers of Commerce and Industry (DIHK).

The BDI Task Force Brexit has established ten project teams to address specific policy areas: (1) Trade in Goods, (2) Transportation and Logistics, (3) Data and ICT, (4) Taxation, (5) Legal consequences of Brexit in core areas of business law, (6) Energy and Climate Policy, (7) Market Access, (8) Workforce Mobility, (9) Banking, Finance and Insurance, (10) Negotiation Process (including Northern Ireland, Research and Development, Defence, Financial Commitments).

The objective of the project teams is to identify the potential risks posed by the exit of the UK from the EU and to propose constructive approaches to countering these risks. The project teams are looking at the regulatory issues in the individual policy areas on the European and the national level. The BDI is also a member of a similar task force at Business Europe, the umbrella organisation for European business. The work of the BDI Task Force Brexit will progress in line with the official negotiations.

This position paper is based on the background information developed by the BDI Brexit Task Force. The views expressed in this position paper are those of the BDI and do not necessarily reflect those of the other members of the Task Force.

Contents

Data and ICT: Challenges caused by Brexit

The digital economy is highly interconnected, both on a European and on a global level. The British and European economies, too, are interlinked. The partnership between the UK and the EU should remain close after Brexit in order to avoid harming European and UK businesses. Maintaining unhindered data flows between the two sides of the Channel will be a major challenge for businesses and the Brexit negotiators. The transfer of personal data will be affected from day one after the UK leaves the EU. A swift adequacy decision by the European Commission is required and feasible as long as the United Kingdom continues to commit to the General Data Protection Regulation. Meanwhile, we need rules to guarantee the transfer of personal data during the transitional period. Another major issue is data and ICT security. The UK and the EU should continue to work together in the European cybersecurity exchange networks to combat cybercrime and cybersecurity threats. This partnership is very important to maintain trust between our countries — and cybersecurity is, after all, primarily a matter of trust. With regard to cybersecurity standards, European and international standards must be jointly introduced and promoted. The roll-out of 5G is not likely to be affected by Brexit as the UK has made great progress within the EU 5G framework and is internationally well-connected. In order to maintain the same European mobile roaming charges, the easiest solution would be for the UK to become an EEA member state. Failing this, maintaining low roaming charges will largely be a business decision made by telecom operators.

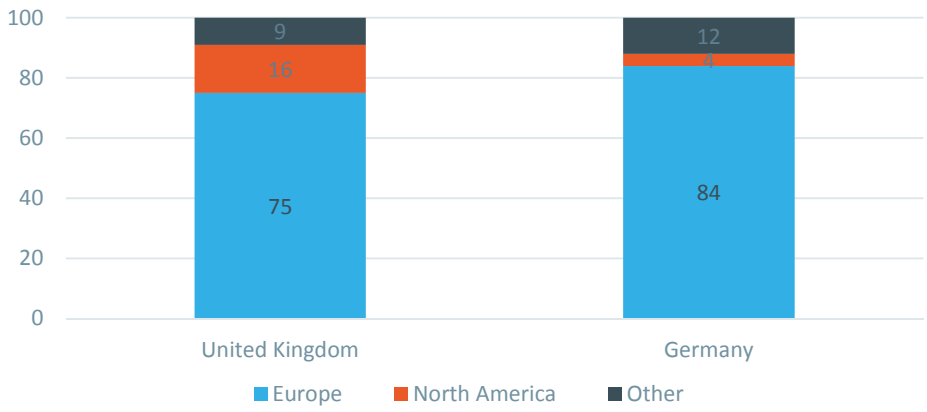
Identified Issues: Assumptions and Measures

Data Flows

Assumptions

Data flows between the United Kingdom and the European Union will be directly affected when the UK officially leaves the European Union. Currently, 75 percent of UK cross-border data flows are with EU partner countries,[1] demonstrating the interconnected nature of modern value chains. The figure below shows data flows between UK and EU households, consumers and businesses.

Distribution of international bandwidth by country and partner region (2015-2016)



Source: Frontier analysis of TeleGeography data

BDI

Data protection legislation, which is designed to safeguard personal data, does not include a free flow of data on an international level. The moment the UK becomes a third country, the transfer of personal data will only be possible with additional efforts to comply with data protection regulations. The EU rules for the transfer of personal data to third countries will apply. The transfer of personal data to a third country is only allowed under certain circumstances (Art. 25 Data Protection Directive (DPD; 95/46/EC) and Art. 44 – Art. 50 General Data Protection Regulation (GDPR)). A data transfer to a non-EU country is only possible if the processor or controller provides appropriate safeguards. The following instruments can be used directly by businesses once the United Kingdom has left the European Union:[2]

- Consent via derogations
- Binding corporate rules (Art. 46 II b, Art. 47 GDPR)
- EU-standard contractual clauses (Art. 46 GDPR)
- Approved codes of conduct (Art 40 GDPR)
- Approved certification mechanisms (Art 42 GDPR).

[1] The UK Digital Sectors after Brexit, Frontier Economics by techUK, 14.01.2018, p. 37
[2] Stakeholder Notice from the European Commission on the withdrawal of the United Kingdom and EU rules in the field of data protection, 9.1.2018: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=611943

A further option is an adequacy decision by the European Commission (Art. 45 GDPR and Art. 25 95/46/EC) declaring that the UK ensures an adequate level of protection of personal data. An adequacy decision may be the easiest way for the business community to transfer data to the UK after Brexit. The threshold for achieving adequacy is high. So far, only a few countries have been granted approval (for example Switzerland, Uruguay, Argentina and Israel).

How will Brexit affect the applicability of the GDPR?

When the GDPR comes into effect in May 2018, the UK will still be a member of the EU as the formal withdrawal of the UK is not likely to occur before the end of March 2019. The UK has confirmed that the GDPR will be applicable in the UK until Brexit. As an EU regulation, the GDPR is directly applicable in all EU member states. The UK will therefore not need to implement the GDPR into national law. However, from the moment of exit, the GDPR will no longer be directly applicable in the UK as the country will no longer be an EU member state. The status of the UK will thus change to “third country” in all aspects of the GDPR and this will influence all transfers of personal data. The transfer of personal data between an EU-based business and a third country will then only be possible if the third country provides for an adequate level of protection or other measures are taken to ensure that the level of data protection is not undermined.

Options open to the UK to ensure unhindered data flows

The UK must therefore find a way to ensure adequacy in order to maintain data flows into the country. Various options are open to the UK to achieve this status. An assessment of the various options will serve to evaluate whether the UK will maintain the GDPR after Brexit.

The EEA Model

The first option would be to follow the example of Norway, Liechtenstein and Iceland and become a non-EU member of the European Economic Area (EEA) by signing the EEA Agreement. The EEA Agreement makes all EU legislation that is part of the single market binding for the contracting parties through a number of annexes to the agreement. Annex 11 covers data protection. The GDPR would then be automatically binding in the UK as well. However, this scenario seems unlikely at this stage as the UK’s decision to leave the EU is based on the population’s rejection of several EU principles, especially the free movement of people and a certain loss of sovereignty. As the UK would again be bound by these principles if it signed the EEA Agreement, this move would make Brexit even less popular with citizens.

The Swiss Model

The second option open to the leaving member is a solution along the lines of the Swiss example. Switzerland is neither party to the EEA nor a member of the EU but has implemented data protection regulations that follow the EU Data Protection Directive and has consequently achieved adequacy status to ensure the free movement of data. Furthermore, Switzerland has already announced that it intends to update current Swiss legislation to comply with the GDPR rules to maintain adequacy after the GDPR comes into force. However, the Swiss model would also require the UK to comply with EU legislation on data protection and the GDPR or mirror most of the rules in its national legislation. As it will no longer be a member state, the UK would thus effectively have to comply with EU rules without being able to participate in future deliberations on new legislation.

The independent adequacy ruling

This leads us to the third and most likely option for the UK: an adequacy decision by the European Commission for the UK’s own, independently created legislation. Article 45(1) of the GDPR allows for data transfers based on such decisions. If the UK went for this option, it could, in principle, implement data protection regulations that differ from or are less stringent than the GDPR rules. However, as a

dilution of the core principles would jeopardise the adequacy status, the UK could damage business with companies in the EU that is dependent on data transmission. Another complication with this option is that reaching an adequacy decision usually takes the European Commission a minimum of several months or even years, leaving the UK without a suitable legal basis for the transfer of data. Whether the European Commission issues an adequacy decision and grants the desired status depends on various factors laid down by the European legislator to ensure that third countries guarantee the same level of protection.

Recital 104 and Article 45(2) of the GDPR state that adequacy depends on the third country ensuring an adequate level of protection. Recital 104 of the GDPR goes even further by requiring the protection to be "essentially equivalent to that ensured within the Union". The listed factors go far beyond that and include not only transfer rules for transferring the data onward to another third-party country, but also the "existence and effective functioning of one or more independent supervisory authorities with responsibility for ensuring and enforcing compliance with the data protection rules" and "legislation concerning public security, defence and national security". Furthermore, the extensive list in Article 45 of the GDPR leaves it open to the European Commission to take account of other factors not listed in the enumeration.

In view of the myriad of different factors that could contribute to the European Commission´s decision, it is difficult as things stand to assess whether the level of data protection provided in the UK will be judged as adequate. Certain factors are, however, very likely to play an important role in the decision.

One argument in favour of the level of data protection in the UK could be the ratification of Convention 108 and the ECHR. Furthermore, the UK will continue to be subject to the European Court of Human Rights as this court was installed by virtue of the Council of Europe to which the UK is still a party. However, there are also factors that speak against an adequacy decision, for example the implications of the Schrems ruling of the CJEU. In that decision, the CJEU declared the "safe harbour" agreement that facilitated data transfer from the EU to companies in the US as no longer valid. Although the decision concerned data transfer to the US, the reasons that led the CJEU to this decision may be significant for the UK as well.

It remains to be seen how much weight the European Commission will give to these circumstances and whether the UK will be granted adequacy status. The UK would do well to implement a data protection regime that is similar and essentially equal to the GDPR in its efforts to achieve adequacy. This would be an important step to ensuring unhindered and uninterrupted data flows between the EU and the UK after Brexit.

Conclusion

In the likely case that the United Kingdom implements the new European GDPR and maintains it after Brexit, it is also very likely that the European Commission will decide that the UK provides for an adequate level of protection of personal data. The UK has expressed its intentions to maintain a free flow of data between UK and EU in future.[3] However, even if the UK intends to incorporate the GDPR into its national legislation, this may still change in the medium term thus creating divergence in data protection. Furthermore, UK law and UK jurisdiction, such as the UK Investigatory Powers Act could stand in the way of a swift adequacy decision. The British Royal Courts of Justice ruled on 30 January

3 Digital Minister Matt Hancock on the introduction of a children's code of practice protecting children under 16 in the UK Data Protection Bill on 11.12.2017

2018 that parts of the Investigatory Powers Act of 2014 are unlawful,[4] confirming an earlier judgment by the European Court of Justice.[5]

With regard to EU-US data flows, the Privacy Shield currently covers data transfer from the UK to the US as part of the EU. After Brexit, the Privacy Shield will no longer protect data flowing from the UK to the US and, consequently, personal data from the UK may be less protected in the US than that coming from the EU. The UK will therefore need to find other bilateral solutions for the transfer of personal data to the US and any other country.

Measures

It is important that the United Kingdom implements the GDPR into domestic law in order to have an adequate level of data protection that is comparable to EU law. This is a crucial step towards facilitating a positive and swift adequacy decision by the European Commission. Furthermore, a transitional arrangement needs to be put in place for UK-EU data flows until the adequacy decision comes into force. The UK should stay in close cooperation with the EU. As the European Data Protection Board plays a crucial role in shaping the future data framework in a harmonised manner across the EU, the UK should remain a member of the Working Party 29 or at least receive observer status, like Norway, Lichtenstein and Iceland.

4 UK Royal Courts of Justice from 30.01.2018, Case No: C1/2015/2612 & 2613
5 ECJ judgement from 21.12.2016, C-203/15

Cybersecurity

Assumptions

In a digital economy, where everything is increasingly interconnected, cooperation in the field of cybersecurity is more important than ever. The exchange of information in early alert systems and the sharing of best practices is not only a matter of security – it is primarily a matter of trust. After leaving the European Union, the United Kingdom will continue to face the same challenges with regard to cyber threats. It will thus be important for the country to maintain strong ties with European cybersecurity agencies in the future.

European information exchange networks on cyberattacks

The first EU-wide legal framework for cybersecurity is the Network and Information Security Directive (NIS). The NIS Directive will be implemented into UK law on 9 May 2018. Its National Cybersecurity Strategy will give the United Kingdom a comprehensive cybersecurity framework for its critical infrastructure. Critical infrastructure encompasses the energy, transport, water and banking sectors, the financial market infrastructure, and the healthcare and digital infrastructure (e.g. cloud service providers). Operators of these essential services will have to take appropriate security measures and notify serious incidents to the relevant national authority. Under the NIS Directive, EU member states will also set up Computer Security Incident Response Teams (CSIRTs). This EU CSIRT network will facilitate swift and effective operational cooperation on specific cybersecurity incidents and the sharing of information on risks across the EU.

Three communication channels will be needed in the future to share information on cyberattacks and incidents.

- An exchange network between public authorities and the Computer Emergency Response Team (CERT) of the EU and the CERTs of the member states in case of cyberattacks against a public authority on EU or member state level..
- An exchange network between public authorities and the national CSIRT in the event of an incident involving critical infrastructure.
- An exchange network between big high-tech companies. In Germany, the DAX-30 have been operating this kind of communication channel for a few years now.

The reason for this differentiation is that the profile of the attackers with regard to their budget, motives and expertise also differs depending on their target. Furthermore, disclosure obligations also differ depending on who is affected. As an additional measure, a rapid reaction force (RRF) should be installed on an EU level. All EU member states and the United Kingdom can only stand to benefit from participating in this kind of RRF and information exchange. Furthermore, it is crucial that cooperation between the UK and the EU in the fight against cybercrime continues. The main obstacle preventing companies from filing a criminal complaint in the event of a cybersecurity incident is still the low chance of winning the case. This makes it important to have many partners in the fight against cybercrime.

European network of national cybersecurity competence centres

Cooperation with the United Kingdom can only be beneficial for cybersecurity labs as well. The European Commission is currently working on cross-linking and mapping the existing national cybersecurity competence centres. The network will bring together research expertise in cybersecurity from across the European Union, from university labs as well as public and private non-profit research centres. The aim is to create synergies and scale up existing competences and research in order to come up with marketable solutions to improve cybersecurity in the EU. For this purpose, the European Commission launched a call for proposals on 1 February 2018 and has earmarked 50 million euros for

this pilot project.[6] A further call for proposals is scheduled for spring 2018 to further develop cooperation between the EU cybersecurity centres and cybersecurity laboratories in the individual member states. The United Kingdom should be able to tap into the expertise and synergies of these networks. It would otherwise have to build up its own competences.

EU Cybersecurity Certification Board

The planned Cybersecurity Certification Board (Article 53 of the ENISA mandate) has not yet been established. According to the new Cybersecurity Framework, this new board with DG CONNECT, ENISA and representatives of member states will be tasked with creating cybersecurity schemes that can be adapted and used for many IoT verticals. Compliance with the new schemes will be displayed on a broad range of IoT products and goods produced and sold across the EU. The UK can only influence these schemes if it works actively on this board. The Cybersecurity Act, including the European Cybersecurity Certification Framework, which is currently in the legislative process, may become binding at the end of 2018.

Measures

Close cooperation between the UK's national cybersecurity agency and the national cybersecurity agencies of the EU member states and ENISA is of paramount importance. The UK must be a partner in the European cybersecurity exchange network as well as in the fight against cybercrime. In addition, EU-NATO cooperation on cybersecurity should be continued systematically and intensified together with the UK. With regard to cybersecurity standards, European and international standards must be introduced and jointly promoted.[7] The EU and the UK should also jointly promote the concepts of cybersecurity and trustworthiness at ISO and IEC level. Work on the EU Cybersecurity Framework, including the Cybersecurity Act, must progress despite Brexit. Technical market access for security products, systems and services to the UK must be barrier-free. The principle of mutual recognition, such as SOG-IS Mutual Recognition Agreement for Common Criteria in cases of governmental use could serve as an example here. Furthermore, aspects of market access for cybersecurity products and services should be included in the EU's contractual arrangements with the UK. Mutual recognition agreements should be encouraged in order to ensure access to the UK cybersecurity market. At the same time, an integrated European system for reporting, warnings, CERTs/CSIRTs and law enforcement should be introduced, similar to the one that already exists for the defence sector.

---

[6] https://ec.europa.eu/digital-single-market/en/news/commission-launches-call-proposals-eu50-million-pilot-support-creation-network-cybersecurity

[7] Concerning standardisation and certification, please see the BDI position of Working Group 7 on Market Access.

Roaming

Assumptions

If Brexit takes place without a free trade agreement in place comparable to an EU or EEA member state, current roaming arrangements with the EU will end. Regulation (EU) No 531/2012 on roaming will no longer apply with respect to the UK, affecting business and other travellers to and from the UK. In this case, transitional arrangements will be required. If the UK were to decide either to remain an EU member state or become an EEA member state, roaming arrangements with the EU would continue as they are today. In all other scenarios, EU roaming arrangements will cease to apply to UK mobile customers in the EU and EU citizens in the UK at the moment of Brexit. This issue will have far greater visibility in the UK than in the EU because the price increases to be expected will have a disproportionately higher impact on UK subscribers than on EU subscribers. The UK will not be able to solve this problem by itself. The UK's Great Repeal Bill could control retail prices within the UK, but it cannot dictate the wholesale charges that EU network operators levy on UK network operators for UK subscribers roaming in the EU. Current retail prices for roaming cannot be sustained if wholesale costs are allowed to run wild.

One of the most rational and realistic solutions for the UK to maintain low-cost roaming charges with the EU is an arrangement between UK and EU operators, agreeing on a contractual basis to leave the prices at their current level. Otherwise, the UK and the EU need to agree on new low wholesale roaming prices as part of the Brexit negotiations. Any agreement here should form part of a broader arrangement that has "substantial sectoral coverage" to ensure compliance with GATS/WTO rules. The EU has been reluctant to grant mobile roaming privileges to third countries under the General Agreement on Trade in Services (GATS) on account of the so-called most-favoured nation (MFN) clauses. The GATS problem: Under these MFN clauses, if multinational organisations (MNOs) of one country offer a wholesale price to MNOs of another country they are obliged to offer the same terms and conditions to all WTO members. The GATS does not foresee the need to impose reciprocity in wholesale pricing or in retail conditions. In the absence of additional safeguards, if the EU agrees to such arrangements with any third country, all other WTO members could free-ride, without being obliged to take steps to make inexpensive roaming available to EU subscribers in return. A free trade agreement that also regulates roaming fees as part of the Article 50 of the Treaty on European Union (TEU) process could avoid this problem.

Measures

It is important to keep a close watch on developments here. With regard to roaming charges, the best scenario would be for the UK to become an EEA member state, as EU rules would then continue to apply. Otherwise, it will be up to telecom operators to agree to leave prices at their current level. In the meantime, a transitional agreement will be required.

Spectrum Policy and 5G

Assumptions

Connectivity is key to a successful society and economy. There are many good reasons for the UK to continue the progress on 5G, which has already been achieved together with the EU, the 49 countries of the European Conference of Postal and Telecommunications Administrations (CEPT) and within the International Telecommunication Union (ITU).

The ongoing modernisation of the European Electronic Communications Code is the opportunity for Europe to make the gigabit society a reality. In addition, the European Commission launched an action plan[8] in September 2016 to boost the EU's efforts for the deployment of 5G infrastructures and services by 2020. This plan sets out a roadmap for public and private investment in 5G infrastructure in the EU. The new European Electronic Communications Code and the 5G Action Plan are closely connected. One year later, on 18 July 2017, the 28 EU representatives and Norway signed a ministerial declaration on "making 5G a success for Europe" during an informal meeting of competitiveness and telecommunications ministers in Tallinn. Despite Brexit, the EU (including the UK) and Norway furthermore agreed on a roadmap for 5G services in December 2017 to. This roadmap sets out concrete deadlines for the spectrum harmonization necessary for the rollout of 5G as agreed between member states and confirms the objective of positioning Europe as a leading market for 5G on the global level. The main goals of the roadmap are the technical harmonisation of the spectrum bands 3.4-3.8 GHz and 24.5-27.5 GHz by 2019 and 700 MHz in most member states by 2020. By 2022, the 700 MHz band will be available in most member states.

The UK also has a leading role in the 5G groups of the CEPT, a coordinating body for 49 European telecommunications and postal administrations. The CEPT group for International Mobile Telecommunication (IMT) is currently chaired by the British regulatory agency Ofcom (chair: Steve Green). This CEPT group is currently preparing the position for the 5G spectrum agenda item 1.13, also chaired by a CEPT coordinator from Ofcom. The UK is the first EU member state to have launched a national consultation to explore whether the 3.8-4.2 GHz range can be shared with mobile phones using sharing models. The UK also plays a crucial role on the international level. UK is actively involved in the International Telecommunication Union (ITU), the United Nations (UN) agency for telecommunications. The UK actively participates in the ITU-R (subgroup of the ITU for the Radiocommunication Sector) on studies regarding the coexistence of IMT-2020 (ITU-R term for 5G radio technology) in all relevant bandwidths (as defined by the World Radiocommunication Conference 2015, WRC-15).

Measures

Considering all the steps that the UK and Europe have already taken for the development of 5G technology in Europe and worldwide, we do not expect Brexit to have a significant economic impact here. The UK's economy and the related 5G spectrum is also inseparably connected to Europe from a geographical point of view. A successful and harmonised 5G implementation cannot be achieved to the required degree by one single member state or future single partner state acting alone. Unilateral action in spectrum policy and the rollout of 5G would not achieve the goal of harmonisation. It is therefore important that the UK continues to be an active member of the CEPT after a "friendly" Brexit

[8] 5G for Europe: An Action Plan - COM(2016)588: https://ec.europa.eu/digital-single-market/en/news/communication-5g-europe-action-plan-and-accompanying-staff-working-document

with the same voting and participation rights in the European regulatory framework as are enjoyed by Switzerland and Norway, for example.

Imprint

BDI – Federation of German Industries
Breite Strasse 29, 10178 Berlin
Germany
www.bdi.eu
T: +49 30 2028-0

Editor
Stefanie Ellen Stündel
T: +32 2 792 1015
s.stuendel@bdi.eu

Special thanks go to the valuable expertise of the members of Project Group 3:

Thomas Prinz (BDA), Marek Jansen (BDI), Rebekka Weiß (Bitkom), Alexander Kolodzik (BGA), Nicola von Holleben (VDA), Lukas Linke (ZVEI), Wolfgang Müller (Deutsche Telekom AG), Dr Detlef Houdeau (Infineon Technologies AG), Fabian Bahr (Giesecke+Devrient), Matthias Goebel (Robert Bosch GmbH), Wiebke Metzler (Siemens AG)