# Public Security Exception in the Area of non-personal Data in the European Union

*Briefing Requested by the IMCO committee*

Irion, K.

**Publication date**
2018

**Document Version**
Final published version

BRIEFING

Requested by the IMCO committee

European Parliament

# Public Security Exception in the Area of non-personal Data in the European Union

KEY FINDINGS

- In order to avoid conflict with the freedom to conduct a business and the freedom of contract the wording of article 4(1) should be amended and be addressed to the Member States;
- The proposal underplays that information security has a legal dimension to it, notoriously so because member states' national security activities operate outside the scope of EU law;
- The principle aversion against locality that emanates from the proposal may not be fully aligned with state-of-the-art technology where multiple data mirrors geographically distribute a dataset. For example, one local mirror is advisable for business continuity in the event of a disruption of transmission infrastructure;
- Not all non-personal data is created equal; from the stream of non-personal data that is for example generated in the Internet of Things (IoT) data necessary to control real world devises should in addition be locally accessible;
- Whithout contradicting the philosophy behind the free flow of non-personal data proposal this briefing presents examples for interventions that should be justifyable on grounds of public policy or the protection of health and life of humans, animals or plants.

## The Legal Systematic of the free flow of non-personal data proposal

Mid-September last year the European Commission presented a proposal for a new regulation on the free flow of non-personal data in the European Union[1]. This initiative forms part of the "Building a European Data Economy" policy efforts which is a sub-set of the Digital Single Market Strategy (DSM Strategy)[2].

New digital technologies, such as cloud computing, big data, artificial intelligence and the Internet of Things (IoT) are designed 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[3].

The free movement of data in the digital single market has been called the fifth freedom complementing the existing freedoms on movement of goods, services, capital and people. The proposed regulation seeks to remove unjustified data localisation measures that fall in the scope of EU law. Often this will amount to cutting bureaucratic red tape in the private sector, such as for example removing a domestic obligation to maintain a full copy of bookkeeping on premise of an organisation in a given Member State.

Policy Department for Economic, Scientific and Quality of Life Policies
Author: Dr. Kristina Irion, Institute for Information Law, University of Amsterdam
Directorate-General for Internal Policies
PE 618.986 - April 2018

EN

In the following we will trace the contours of the legislative proposal and clarify the scope of the proposed instrument and certain key concepts. Against of this backdrop we can start analysing the foreseen public security exception. We will have to critically reflect on the proposal's two underlying assumption.

First, that all non-personal data is created equal and, second, that data residency does no longer matter to public policy or the protection of health and life of humans, animals or plants, which are other recognised grounds for member states to justify interferences with the free movement of goods and services.

## In the scope of Union law

The proposed Regulation shall not apply to an activity which falls outside the scope of Union law (art. 2(2)). The provision reiterates a recognised principle of EU primary law (art. 4(2) TEU). Member states' national security is the classical activity that falls outside the scope of Union law. There is no unified definition of national security but activities to counter a threat to the state's independence, sovereignty, territorial integrity, constitutional order, of that magnitude, are recognized. This standard limitation of scope poses two issues for the free flow of data in the Union.

First, in the field of state records strictly classified information, such as military and defense, state of emergency plans, etc. would not fall inside the scope. After all "no Member State shall be obliged to supply information the disclosure of which it considers contrary to the essential interests of its security" (art. 346(a) TFEU). Since it is in the executive's power to classify or declassify information, in addition to the residual legal uncertainty inherent to the very term 'national security'[4], Member States' through their national system of classifying information can retain some scope of maneuver in the field of state records.

Second, Member States' national intelligence fall as prototypes of national security activities outside the scope of Union law. However, foreign electronic surveillance and cyber espionage remain the biggest cause for mistrust in the internal market and beyond[5]. When electronic data resides in a third country there is a valid legal concern that local national security powers can override contractual relationships (SLA) with service providers[6]. I have concluded elsewhere that a third country's national security powers can inhibit the use of foreign cloud services (see also case study of Estonian data embassy below)[7].

## Substantive scope

The proposal for a regulation on the free flow of non-personal data in the European Union aims to remove obstacles to the free movement of data other than person data in the internal digital market. From all supporting documentation the instrument primarily aims to outlaw member states' data localisation requirements as incompatible with the internal market. The term 'data localisation requirement' is defined in art. 3(5) and many obligations are addressed to the member states, in particular art 4(2) to (5).

There is however an issue with legal certainty of the proposal's core provision in art. 4(1) which is formulated significantly broader.

Location of data for [storage or other] processing within the Union shall not be restricted to the territory of a specific Member State, and [storage or other] processing in any other Member State shall not be prohibited or restricted…
Art. 4(1) is neither addressed to the member states nor does it incorporate the defined term 'data localisation requirements'. Its language in an EU regulation, once becoming directly applicable law in the Member States, may actually interfere – deliberately or not - with contractual freedoms between a user and a provider but moreover with a patron's right to decide to process electronic data on premise. This would be as if the free movement of goods in the single market mandates everyone to drink Cassis de Dijon.[8]
This really needs to be better crafted to achieve unequivocal and unambiguous law.

This briefing proceeds with the assumption that the instrument means to address member states' data localisation requirements as defined in art. 3(5):

"'data localisation requirement' means any obligation, prohibition, condition, limit or other requirement provided for in the laws, regulations or administrative provisions of the Member States, which imposes the location of data storage or other processing in the territory of a specific Member State or hinders storage or other processing of data in any other Member State (emphasize added)'".

Moreover, I concur with the Council that the EU legislation should not override the internal organisation of member states on electronic data processing and the issue whether to outsource or not in the first place.[9]

## Limited exception

Following next the proposed regulation aims at removing Member State's data localisation requirements "unless it is justified on grounds of public security" (art. 4(1)). At the stage of justification, it provides for a limited exemption for cases justified on grounds of public security. If adopted the regulation would thus limit the grounds which member states could rely on to justify otherwise proportionate limitations of the free movement of non-personal data in the Union. The freedom to movement of goods and, by reference, services in contrast knows far more exceptions:

Art. 36 TFEU

The provisions of Articles 34 and 35 shall not preclude prohibitions or restrictions on imports, exports or goods in transit justified on grounds of public morality, public policy or public security; the protection of health and life of humans, animals or plants; the protection of national treasures possessing artistic, historic or archaeological value; or the protection of industrial and commercial property. Such prohibitions or restrictions shall not, however, constitute a means of arbitrary discrimination or a disguised restriction on trade between Member States.

In the following we will explore the contours of the public security exception in EU law and seek to understand what it covers and what not.

## 2. The public security exception in EU law

Member states can justify an activity that contravenes EU law on grounds of public security.

Of all the grounds for exceptions from free movement, public security is most closely associated with what is traditionally understood as the core of national sovereignty, that is, the sphere of activity within which the State has primary responsibility to protect its territory and citizens.[10]

Public security is a term open to interpretation by the CJEU and it has been applied in a highly contextualized manner. The Council correctly summarises:

'The concept of 'public security', within the meaning of Article 52 of the TFEU and as interpreted by the Court of Justice, covers both the internal and external security of a Member State, as well as issues of public safety, in particular to allow for the investigation, detection and prosecution of criminal offences. It presupposes the existence of a genuine and sufficiently serious threat affecting one of the fundamental interests of society, such as a threat to the functioning of institutions and essential public services and the survival of the population, as well as by the risk of a serious disturbance to foreign relations or the peaceful coexistence of nations, or a risk to military interests.[11]'

The CJEU judgement in Campus Oil (case 72/83) has been the leading precedent formulating the legal requirements of the public security exception.

This case concerned a national quota of refined oil provisioning in Ireland. The judges held that such measure was justifiable under the public security exception as refined oil was considered:

"of fundamental importance for a country's existence since not only its services but above all its institutions, its essential public services and even the survival of its inhabitants depend upon them.[12]"

The Court would in addition consider whether the member states' interest is already adequately protected in EU law. As Koutrakos in his concise chapter put it:

"Where a Member State seeks to deviate from free movement on the basis of a ground of justification recognised under EU law, one of the parameters which the Court examines as a matter of course is the existence of secondary EU legislation and the extent to which this protects the interest which a Member State seeks to protect: if the answer to this question is affirmative, then an exception from EU law is normally not justified as, by purporting to protect an interest already protected at EU level, such a deviation is no longer necessary.[13]"

Next, in order to be justifiable, such measure has to pass a strict proportionality test. By today's standards the measure must:

1) Be suitable to promote the objective of public security;

2) Be adequate in a sense that there is no other measure less restrictive from the point of view of free movement that is capable of achieving the same objective; and, in addition;

3) The positive effect of this measure on public security has to be balanced with the negative effect on the international market.[14]

Ultimately, if a Member State wants to invoke the public security exception is has the burden of proof. It means the Member State has to provide concrete evidence of the substantive argument made for a deviation from EU law. National measures were not excluded from the application of EU law merely because they aimed at the protection of public security or national defence. In Commission v Italy (case C-337/05) the CJEU denied deviation from procurement rule for helicopters because "'the use of which for military purposes is hardly certain…"

Absent of a precedent interpreting public security in the context of IT outsourcing or data processing the following section attempts to apply this concept to a range of relevant circumstances in order to shed light on the consequences of the draft regulation.

## 3. Case studies

The case studies explore (1) the Estonian data embassy, (2) the freedom to contract, and (3) cybersecurity in relation to the free flow of non-personal data in the digital single market. The case-studies have been chosen for providing a representative account of the possible collisions between the free flow of non-personal data and other considerations of general interest. They correspond with the current landscape of online data hosting and processing services.

### Estonian data embassy

Since 2017 Estonia has been pioneering and piloting the so-called data embassy which offers a representative scenario of how a member state would protect the confidentiality, integrity, and availability (ie. the information security triad) of important government information and services.

That information security has a jurisdictional or legal dimension to it I have sketched out earlier.

When "information is the foundation of all governing" then the modern treasury of public institutions is where the wealth of public information is stored and processed. Government in most countries is under very strict obligations to ensure that public information technology (IT) systems and information are secure. Cloud services, however, are challenging in this regard because direct means of control over virtual assets are greatly diminished. … Furthermore, national perspectives on how government data should be handled clash in many ways with the cloud's global philosophy as a service that transcends geographical and political boundaries. Thus, cloud services that are virtual and dynamic take information governance to "a new level of abstraction". Against this backdrop, many governments have raised concerns about national data sovereignty when government information is moved to the cloud.[15]

Against this background the data embassy as is conceived by the Estonian government is a brilliant solution to the issue of technical and legal information security:

"The Data Embassy is an extension of the Estonian government in the cloud, which means the state owns server resources outside its territorial boundaries. This is an innovative concept for handling state information, as states usually store their information within their physical boundaries. Those resources are under Estonian state control and must be capable not only of providing data backups, but also of operating the most critical services. This new approach makes it possible for the Estonian state to continue operating under conditions where its local data centres have been stopped or disturbed due to a natural disaster, large-scale cyber attack, power failure or other crisis situation.[16] "

The concept of a data embassy centrally rests on a data localization requirement, in this case that data and services are located in Estonian government owned facilities in Luxemburg on which diplomatic privileges are bestowed. [17] Siim Sikkut, the government's ICT policy adviser, explained the motivation as follows:

The cloud technology provides a good opportunity, but the state also wants to maintain the full control and jurisdiction of their data and systems. For this reason the private cloud services are not exactly suitable for us (emphasize added).[18]

It should be noted that Estonia is not only one of the global champions of e-government solutions. During its presidency of the Council of the European Union in the second half of 2017, Estonia was also promoting the free movement of non-personal data proposal as fifth freedom of the European Union:

'Data localisation is the measure for the 20th century, not in the 21st century.[19]'

These two positions can only be reconciled if the Estonian data embassy can be fully justified under the public security exception. It is very likely that a judicial review would find in favour of a situation as prescribed in the CJEU ruling Campus Oil (case 72/83). Namely that the Estonian data embassy is of fundamental importance for its existence both in terms of its services and its institutions and essential public services. This is precisely the rationale conceptually underpinning the data embassy which via diplomatic privileges creates a legal and political roadblock against a third government's search and seizure or disclosure authority.

At this stage our explanation goes full cycle with the known limitation of the scope of EU law, ie. Member State's national security. It is an inconvenient truth that EU law does not afford protection against another Member State's national security measures which is inhibiting outsourcing to cloud services abroad.

Apart from general information security aspects, there are concerns relating to potential enforced access to information stored in a cloud by a public entity. As long as the enforcement agency comes from the same country as the public entity using the cloud, there should not be any particular concern.

The situation differs when a foreign agency may enforce access to information stored in a cloud by a public sector entity of another country.[20]

Secondary EU law certainly governs many aspects of information security but can hardly substitute for a data mirror of the Estonian government. What would be, in the event of a judicial review, more speculative is whether the Estonian data embassy in its entirety meets all tenets of the proportionality test. This would depend on a detailed assessment of every type of data backups and the relative criticality of the government data and services. Henceforth, also the concept of a data embassy, if appraised under the public security exception, is not without boundaries imposed by EU law.

If, however, member states can have considerations other than technical security that justify data localization there may also be a pendant in the private sector.

## Freedom of contract

Also private organisation have own considerations about data storage and processing, in particular whether to outsource data processing. Whereas cloud computing is a very good preposition for business models that require scalable computing resources, not every business is virtual and scales. Some organisations are more risk averse than others and certain mission-critical data may not be outsourced at all. Only think in this context about the underlying concerns in the data ownership discussion at EU level mirroring German manufacturers concerns about data generated by their equipment or cars. [21] But also consider the new EU Trade Secrets Directive requiring that

"the information is secret in the sense that it is not generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question and it has been subject to reasonable steps … to keep it secret.[22]"

Next, if an organisations decides to outsource some of its data processing it will also consider the whereabouts of data assets and the provenience of the service provider. Depending on the circumstances, certain enterprises have a demand for a data residency clause being inscribed in the service level agreement with the provider. This is often the first step for organisations to outsource data hosting and it can help reduce legal complexity.[23] To my knowledge this is not just a general misconception among administrations and businesses that there is a legal obligation to store data within national borders. [24] If multi-homing, i.e. the storage of data at different geographical locations is the future, a local mirror would also not seem disproportionate.

The European Commission, in its accompanying staff working document, tends to underplay the legal dimension of information security when it states:

"In most cases, the level of security of data in electronic format does not depend on its storage location, but rather on the security of the IT infrastructure and strength of the encryption techniques used.[25]"

Bu contrast, that legal aspects can co-determine information security has been visible in the Islandic government's strategy to become the Switzerland for data, [26] in the rising demand for cloud services made in Europe and the substantial investments in cloud infrastructure in the Union recently.[27] Also the much quoted cloud data trustee arrangement between Microsoft and Deutsche Telekom is a direct outflow of a legal risk of - in this case - US-government disclosure authority:

"As data trustee, T-Systems controls access to customer data. Microsoft cannot access the data without the consent of the data trustee or the customer in question. Where the data trustee gives its consent, Microsoft receives only time-limited access to the data and only under the trustee's supervision.[28]"

The freedom to conduct a business protects the self-organisation of private organisation, including whether they wish to process data on premise or outsource it to a service provider (art. 16 CFR). In textbook economics, transaction cost theory determines if economic tasks are performed by firms, and when they would be traded through contracts.[29] In the online environment trust in the security of the transmission and cloud services is certainly an ingredient in the decision-making over whether to enter into a contract or not. Next, freedom of contract is yet another fundamental principle of European private law. It recognises that private parties enjoy the freedom to determine inter partes the conditions of a transaction.

Turning to art. 2(1) and 4(1) of the proposed regulation on a framework for the free flow of non-personal data in the European Union there are some – I suspect - unintended consequences for both, the freedom to conduct a business and for the freedom of contract. It is important to note that the proposed regulation would apply to users of in-house solutions, e.g. own hardware on premise, and to the out-sourcing to a provider of data storage and processing services (art. 2(1) in connection with art. 3(7), (8)). In other words, the scope of the regulation is broader than what is commonly understood as cloud computing which presupposes an outsourcing arrangement of some sort. Second, as was noted earlier, the core provision on the free movement of data is not addressed to the member states and does not incorporate the defined term 'data localisation requirements' (art. 4(1)).

If the EU legislator would pass this text without amendment they would strip private organisations over their autonomy to decide about their data practices and prohibit private actors from entering into a data residency clause. This cannot be intended, given the accompanying documentation that exclusively focuses on removing member states' unjustified data localisation requirements. Likewise there is no compelling argument why the fifth freedom should override the freedom to conduct a business and the freedom of contract.

From the outset, the subjective perceptions that show a preferences for on premise data processing or someone's own country are likely rooted in human psychology. In the psychology of ownership this is commonly discussed as endowment effect which appears to extent to information and data assets. According to the hypothesis people (and organisations are composed of people too) ascribe more value to something they have already and are relatively reluctant to part from what is perceived theirs. By contrast, start-ups and companies that really need to scale computing power will quickly arrive at the conclusion that the only way to be competitive is to outsource and use cloud services where they are cheapest.

## Cybersecurity

The EU strategy to promote an European data economy and to remove unjustified obstacles for the free flow of non-personal data in the digital single market is certainly relevant and important. The sheer amount of sensor data that will be produced by connect devices is mind-boggling. Such a data stream– provided there is adequate security – can flow as non-personal data freely in the digital single market. This, I conclude, is the vision of the European Commission when it drafted the proposed regulation that prohibits member states' data localisation requirements en gros.

Being asked for a critical assessment of the scope of the public security exception, I content that the impact assessment and the drafting history is rather short-sighted on the issue of IoT devise security. Note that my caveat is not about the security of the data its sensors generate but whenever such a device can make an impact in the physical world.

In this section we will explore cybersecurity in the Internet of Things (IoT) as a potential rational for introducing additional exception besides public security. As an example we will draw the parallel between fire safety regulation, on the one hand, and smart devices and buildings, on the other hand, and argue that local security controls should be justifiable on grounds of public policy or the protection of health and life of humans, animals or plants.

Let's recapitulate that the existence of EU secondary law addressing a particular Member State's concern can reduce its ability to invoke the public security exception as a justification. It is granted that EU secondary law provides for measures to ensure the integrity and resilience of critical information infrastructure.

In particular, the Network and Information Security Directive (NIS Directive No. 2016/114841)[30] provides for legal measures to enhance the overall level of cybersecurity in the Union. The NIS Directive has two tiers: essential network and information systems and other digital services. Member states are in charge to identify which services belong in the first tier because they are essential for the maintenance of critical societal and/or economic activities. The corresponding annex covers the following sectors: energy, transport, banking and financial market infrastructure, health sector and digital infrastructure. This list would largely correspond with what is deemed public security. Digital services, such as cloud computing, search engines and electronic market-places are in a different, somewhat lower tier of the Directive.

Outside sectors and services that are recognized in the NIS Directive the security of IoT devices and smart buildings are not particularly addressed in EU secondary law and incident levels may be below the arguably strict threshold for the public security exception to apply. In its Communication on Building a European Data Economy the European Commission in addition pays attention to EU product liability in the IoT environment:

"Autonomous systems and advanced robots may act in a way which was not foreseeable at the time when the system was produced or put into operation. Such autonomous actions may cause harm to humans or damage to other objects. … The issue of how to provide certainty to both users and manufacturers of such devices in relation to their potential liability is therefore of central importance to the emergence of a data economy.[31]"

Obviously, prevention should take priority before liability arises. Just take as an example that fire safety regulations would require automatic doors to open manually from the inside. This is a precaution against people being trapped in a building in a dangerous situation. Another example is an emergency button at an automatic door that can be pushed in the event a person has become trapped. The same way it must be possible to deactivate a malfunctioning IoT device or smart building through local intervention. And this may need some local data mirror or control center, possible in addition to smart building control room elsewhere in Europe or the world.

This may be a good moment to recall that with IoT there are at least two possible points of failure, i.e. electricity supply and Internet connection. If either is at a given moment not available a connected device may no longer react to remote controlled signals and public prevention on grounds of public policy or the protection of health and life of humans, animals or plants may require firefighters, police officers or any other person to be able to override remote controls and for example deactivate a device at the spot. For this reason a physical place in the world will continue to matter since a connected device is real and can cause real harm. Such will require a control interface at the connected device and local access to data necessary to take over control over the device.

## 4. Conclusion

Overall, I conclude that the fifth freedom would have a moderate impact for the European data economy. The alarming 100 percent increase in data localization requirements in the member states in the last 10 years appears much more relative if we consider the actual numbers:

From around 13 restrictions in 2006 to around 26 restrictions in 2016. [32]

The European Commission's impact assessment, for example, lists 45 data localization requirements in member states' domestic laws; some also concern personal data, others will remain excepted even with this draft regulation being adopted.

The proposed framework on the free flow of non-personal data in the European Union appears more politically motivated than an economically significant imperative. If anything, the Commission and supporting documents discovered a fair number of data localization requirements in member states' law, such as public registries, that would interfere with the free flow of personal data as foreseen under the General Data Protection Regulation (GDPR).[33]

In this briefing I challenged two assumption underpinning the Commission's proposal for a regulation on a framework for the free flow of non-personal data in the European Union: First, that all non-personal data is created equal and, second, that that data residency does no longer matter for measures on grounds of public policy or the protection of health and life of humans, animals or plants.

Not all electronic data is created the same, some is more critical than others, yet below the threshold of the public security exception. Electronic data controlling smart devices and buildings for example are different from other sensor and performance data. From the stream of non-personal data that is for example generated in the Internet of Things (IoT) data necessary to control real world devises should in addition be locally accessible as required to deactivate a malfunctioning IoT device or smart building through local intervention.

Next, the proposal underplays that information security has a legal dimension to it, notoriously so because member states' national security activities operate outside the scope of EU law. The principle aversion against locality that emanates from the proposal may not be fully aligned with state-of-the-art technology where multiple data mirrors geographically distribute a dataset. For example, one local mirror is advisable for business continuity in the event of a disruption of transmission infrastructure. In any event, the free flow of non-personal data initiative should not interfere with the freedom to conduct a business and the freedom of contract.

For these reasons, I argue that the public security exception is too narrow because it precludes member states to take measures that can be justified on grounds of public policy or the protection of health and life of humans, animals or plants. Drawing on the analogy with fire safety regulations in the member states it would be too early to preclude that in the future we will need local mirrors and handles. Locality continues to matter in the IoT environment because as individuals we live in a physical place.

1 European Commission, 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), Brussels, 13 September 2017.
2 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the Mid-Term Review on the implementation of the Digital Single Market Strategy A Connected Digital Single Market for All (COM(2017) 228 final), Brussels, 10 May 2017; Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions "Building a European Data Economy" (COM(2017) 9 final), Brussels, 10 January 2017.
3 European Commission (fn. 1).
4 Didier Bigo et al, "National security and secret evidence in legislation and before the courts: Exploring the challenges", Study for the LIBE Committee September 2014, Brussels, http://www.europarl.europa.eu/RegData/etudes/STUD/2014/509991/IPOL_STU(2014)509991_EN.pdf
5 Concrete evidence is hard to find but the concern is notorious, e.g. Dutch Cybersecurity Center, Cyber Security Assessment Netherlands 2016, https://www.ncsc.nl/binaries/content/documents/ncsc-en/current-topics/cyber-security-assessment-netherlands/cyber-security-assessment-netherlands-2016/1/CSAN2016.pdf ; see also Gilliam de Valck, "Mind the gap: economic espionage within the EU," Leiden Safety and Security Blog, 20 November 2017 http://www.leidensafetyandsecurityblog.nl/articles/mind-the-gap-economic-espionage-within-the-eu .
6 E.g. Bird&Bird, Cloud Computing for the Public Sector in Central Europe, Warsaw 2014, https://www.twobirds.com/~/media/pdfs/brochures/information-technology/bird--bird--cloud-computing-in-central-europe-public-sector.pdf?la=en
7 Kristina Irion, "Government Cloud Computing and National Data Sovereignty," *Policy & Internet*, Vol. 4, No. 3-4, 2012.
8 After the famous CJEU ruling *Cassis de Dijon* (case 120/78), judgment of 20 February 1979.
9 Council of the European Union, Interinstitutional File: 2017/0228 (COD), http://www.consilium.europa.eu/media/32307/st15724-re01en17.pdf
10 Panos Koutratkos, «Public Security Exceptions and EU Free Movement Law", in: P. Koutrakos, N. Nic Shuibhne and P. Sypris (Eds.), *Exceptions from EU Free Movement Law* (2016 Hart Publishing Limited), pp. 190-217.
11 Council of the European Union (fn. 8), Recital (12a)
12 CJEU, Campus Oil (case 72/83), judgment of 10 July 1984.
13 Koutrakos (fn. 9).
14 See AG van Gerven, SPUC v. Grogan (case C-159/90), opinion of 11 June 1991.
15 Irion (fn. 7), p. 41.
16 From https://e-estonia.com/ . See for a case study OECD, *Innovative Government*, "The world's first data embassy – Estonia", p. 42. http://www.oecd.org/gov/innovative-government/Estonia-case-study-UAE-report-2018.pdf .
17 Via a bilateral agreement between Estonia and Luxemburg pursuant to the Vienna Convention on Diplomatic Relations Vienna, 18 April 1961.
18 See e-Estonia, "Estonia to open the world's first data embassy in Luxembourg," https://e-estonia.com/estonia-toopen-the-worlds-first-data-embassy-in-luxembourg/
19 Estonian Vision Paper on the Free Movement of Data - the Fifth Freedom of the European Union, p. 10. https://www.eu2017.ee/sites/default/files/inline-files/EU2017_FMD_visionpaper.pdf
20 Maciej Gawroński (Bird & Bird), "Cloud Computing for the Public Sector in Central Europe – the Legal Landscape," Warsaw, December 2014, https://www.twobirds.com/~/media/pdfs/brochures/information-technology/bird--bird--cloud-computing-in-central-europe-public-sector.pdf?la=en .
21 Günther Oettinger, 'Wem gehören die Daten?', *Frankfurter Allgemeine Zeitung*, 14 October 2016.
22 Art. 2(1) of the Directive (EU) 2016/943 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure, Official Journal L 157, 15.6.2016, p. 1–18
23 Michael McLaughlin, "Separation Anxiety: How to Cope with Data Residency in Cloud," CapGemini 14 April 2014 https://www.capgemini.com/2014/04/separation-anxiety-how-to-cope-with-data-residency-in-cloud/#
24 See European Commission Staff Working Document on the free flow of data and emerging issues of the European data economy. Accompanying the document Communication Building a European data economy COM(2017) 9 final, Brussels, 10 January 2017, p. referring to London Economics, "Facilitating cross border data flow in the Digital Single Market", 2016.
25 Ibid., p. 7.
26 International Modern Media Institute (IMMI), Islands of Resilience, Comparative Model for Energy, Connectivity and Jurisdiction, Realizing European ICT possibilities through a case study of Iceland, Brussels 2012 https://www.greens-efa.eu/files/doc/docs/afb325f24f941eb3c5b2b5307d149ba2.pdf
27 Kristina Irion, "Cloud services made in Europe after Snowden and Schrems," Internet Policy Review, 23 October 2015 https://policyreview.info/articles/news/cloud-services-made-europe-after-snowden-and-schrems/377
28 Deutsche Telekom, „Sales of Microsoft Cloud Deutschland launch at Deutsche Telekom," press release 13 March 2017 https://www.telekom.com/en/media/media-information/archive/sales-of-microsoft-cloud-deutschland-launch-at-deutsche-telekom-487998
29 Deutsche Telekom, „Sales of Microsoft Cloud Deutschland launch at Deutsche Telekom," press release 13 March 2017 https://www.telekom.com/en/media/media-information/archive/sales-of-microsoft-cloud-deutschland-launch-at-deutsche-telekom-487998
30 Deutsche Telekom, „Sales of Microsoft Cloud Deutschland launch at Deutsche Telekom," press release 13 March 2017 https://www.telekom.com/en/media/media-information/archive/sales-of-microsoft-cloud-deutschland-launch-at-deutsche-telekom-487998
31 European Commission, "Building a European Data Economy" (fn. 2), p. 13f.
32 European Commission Staff Working Document on the free flow of data and emerging issues of the European data economy (fn. 26), p. 6 in fn. 6.
33 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Official Journal L 119, 4.5.2016, p. 1–88.

Contact: Poldep-Economy-Science@ep.europa.eu

This document is available on the internet at: www.europarl.europa.eu/supporting-analyses

IP/A/IMCO/2018-08

Print ISBN 978-92-846-2823-0 | doi: 10.2861/37814 | QA-01-18-393-EN-C

PDF ISBN 978-92-846-2824-7 | doi: 10.2861/44889 | QA-01-18-393-EN-N