The Deep Blue Sea of Global Data Flows. Implications of the Convergence of Privacy Regimes for Overseas Transfer of Personal Data

Francesco Molinari*, Dragan Čišić**, Božidar Kovačić***
University of Rijeka, Department of Informatics, Rijeka, Croatia
*Corresponding author: mail@francescomolinari.it
**dragan.cisic@uniri.hr ***bkovacic@inf.uniri.hr

Abstract - After the General Data Protection Regulation (GDPR) entered into force, the topic of overseas transfer of personal data for purposes of storage and processing has gained visibility and prominence in both the privacy impact assessments and the informed consent forms issued by EEA based organisations. Related compliance issues have been exacerbated by a 2020 ruling of the European Court of Justice, which upheld the adoption by US based providers of Standard Contract Clauses to safeguard the data subjects’ rights of EEA citizens whose personal data is stored or processed on their platforms. A little explored set of privacy issues materializes when data flows take the opposite direction: i.e. gathered/stored outside and shared/processed inside the EEA space. This paper takes such perspective to examine, in a comparative fashion, the similarities and distinctions between the GDPR provisions and the privacy regimes of China, US and UK (after Brexit), each of them undertaking a process of transformation, and convergence towards GDPR, although with different approaches and pathways. The topic can be of interest for research or service teams engaged in multi-country data gathering, a trend one may expect to grow in the future.

Keywords – GDPR, China, EU/US Privacy Shield, UK Brexit

I. INTRODUCTION

With the entry into force of the EU General Data Protection Regulation (henceforth: GDPR) in May 2018 [1], which introduced significant changes to the previous Data Protection Directive 95/46/EC, the level of protection of citizens in relation to the processing of personal data by organisations established in the European Economic Area (henceforth: EEA) has been enhanced considerably. Perhaps the most important provision of all is that to comply with GDPR, some internal policies must be adopted as well as specific technical and organisational measures implemented, to shape data processing activities according to the twin principles of “Data Protection by Design” and “Data Protection by Default”. Examples of such policies and measures are provided in Art. 25 of the GDPR and include, for instance, data anonymization, the use of pseudonyms to dissipate the real identity of data owners, and data minimisation, or the appropriation of only a subset of personal data which is strictly necessary for a specific purpose. Over the past few years, a plethora of ex-ante privacy impact assessments and informed data subject consent forms have been issued or revised by data controllers and processors, to document their compliance with GDPR provisions. Quite interestingly, this positive trend has not only involved EEA based organisations, but also other entities – acting as service providers – located outside the EEA space. As a result, the topic of overseas transfer of personal data for purposes of storage and processing has gained visibility and prominence in the perspective of data subjects in an unprecedented manner.

However, compliance with GDPR provisions of non-EEA based service providers is only a first step, albeit crucial, for safeguarding the data subjects’ rights of EEA citizens and businesses. What needs to be considered in addition is the alignment to GDPR of national rules and regulations in the country of destination – either temporary or permanent – of their personal data flows. Such concern was put to the forefront by the 16 July 2020 ruling of the European Court of Justice (henceforth: ECJ) [2], which upheld the adoption by US based service providers of Standard Contractual Clauses (henceforth: SCCs) to safeguard the data subjects’ rights of EEA citizens whose personal data is stored or processed on their platforms.

The case is known: an Austrian privacy advocate, Max Schrems, filed a complaint against Facebook with the Irish Data Protection Commissioner, requesting that the transfer of personal data from Ireland to the US using SCCs would be suspended, with the motivation that the SCCs provided inadequate safeguards compared with the GDPR. Already in 2015, under the previous privacy regime, Mr. Schrems won another case before the ECJ, to nullify the validity of the Safe Harbor Decision taken in the year 2000 by the EC, stating that US based organisations adopting certain policies and measures could be the recipients of personal data flows coming from the EEA space. After the October 2015 ruling of the ECJ, the so-called Privacy Shield was established on 2 February 2016 by an EC decision [3], including a deep revision of the conditions for transfer of personal data from the EEA to the US and introduced better oversight mechanisms on the US government side, somehow anticipating the main lines of thought of the GDPR, which was enacted a few months later.

In its judgement the ECJ examined, but not repealed, the validity of the EC adequacy decision 2010/87 on SCCs [4]. Indeed, the validity of that decision is not called into question by the mere reason that, being contractual in nature, SCCs do not bind the competent authorities of the
country where data is transferred, the US in our case. Regrettably for the US-EEA relationship, the ECJ stated that pertinent regulations (i.e., Section 702 of the Foreign Intelligence Surveillance Act and the Executive Order No. 12333) fail to ensure an essentially equivalent level of protection to the GDPR. Therefore, the personal data transfers done from the EEA to the US on the basis of the Privacy Shield alone have become illegal. This is also the opinion expressed by the European Data Protection Board, in a FAQ document issued right after the ECJ judgement of July 2020 [5].

Six months after that ruling, another challenge to the current privacy regime was posed by Brexit, that is, the withdrawal of the UK from the EU and European Atomic Energy Community (EAEC or Euratom) occurred as of 1st January 2021. This brought about potentially significant consequences on the legal handling of data flows from the EEA to the UK, for two main reasons: first, the number of companies that offer data storage and processing services from the UK to the EEA is not negligible, although less pronounced than in the US case. Second, following Brexit, EU law and the ECJ rulings no longer have supremacy over British laws or UK Supreme Court judgements, and this may turn the UK into a similar case to the US.

Despite all the above, the concrete impacts of the July 2020 ECJ verdict have materialized to a far lesser extent than one may have expected. Most US service providers have simply updated once more their privacy notices and informed consent forms – renewing their commitments not to make an improper use of personal data conferred to them, either directly or indirectly, by EEA based subjects. The UK privacy legislation has not moved away from the GDPR principles (as will be shown later in this paper), although the 2018 Withdrawal Agreement [6] enabled the UK Parliament to amend or repeal any EU law as it was a domestic one. The ECJ concerns about SCCs not offering sufficient safeguards for personal data transfers from the EEA to those non-EEA countries have factually never translated into a real hamper to the business previously in operation.

In fact, Art. 49(1) of the GDPR allows EEA based organisations unlimited transfer of personal data to any third country (like the US after the nullification of the Privacy Shield, or the UK after Brexit) where neither an adequacy decision from the EC pursuant to Art. 45(3), nor appropriate safeguards pursuant to Art. 46 are operational, provided that at least one specific condition occurs among those listed in the remainder of the same Art. 49(1). Such conditions include that the data subject has given explicit consent to the proposed transfer prior to it and after having been informed of the possible risks due to the absence of an adequacy decision and appropriate safeguards, and/or that the data transfer is necessary for the performance of a contract between the data subject and the controller.

The problem with this approach lies in the fact that – as stressed in the 2018 Guidelines of the European Data Protection Board [7] – the cross-border data transfers invoking derogations under Art. 49 of the GDPR should be occasional and not repetitive, concern only a limited number of data subjects, be necessary for pursuing compelling legitimate interests by the controller which are not overridden by the interests or rights and freedoms of data subjects, and follow an assessment by the controller of all circumstances surrounding data transfer which provided suitable safeguards with regard to the protection of personal data. The term “occasional” is used in recital 111 while the terms “not repetitive”, “limited number of data subjects”, “compelling legitimate interests” and “assessment” are used in Art. 49(1) par. 2 of the GDPR. The above terms indicate that such transfers may well happen more than once, but not regularly, as would be the case when a stable contractual relationship exists between the EEA based data exporter and the non-EEA based data importer and/or when the data importer is granted direct access to a database (e.g. via an interface to an IT-application) on a general basis.

With the new US administration fully functional and after the global Covid-19 emergency is finally overcome, we can probably expect new bilateral agreements with the EC to emerge, which will lead to increase the safeguards for EEA-resident citizens and businesses in terms of privacy protection in all the cases of international data outflows where derogations ex Art. 49 are insufficiently justified.

Against this background, the present paper deals with another, very related but little explored topic: privacy protection when international data flows take the contrary direction to that examined so far, i.e. they are gathered/stored outside and shared/processed inside the EEA space. This topic can seem trivial, if not specious: in fact, EEA based organisations must adopt the GDPR principles and rules of conduct universally, not limited only to data subjects being EEA residents. With the fast-paced globalization of empirical research – not just marketing or CRM – activities, it becomes more and more frequent that EEA based universities or research companies are contractually bound to store and process personal data not originated inside the EEA space. The question in that case is: what are the legal requirements and rules of behaviour that ensure, to the best possible extent, that no national privacy protection law is infringed in the place of personal data collection and/or while acting as processors for non-EEA citizen or business data?

In partial reply to that question, the next Section of this paper examines, in a comparative fashion, the similarities and distinctions between the GDPR provisions and the privacy regimes of China, US and UK (after Brexit), each of them for various reasons now undertaking a process of transformation, and convergence towards GDPR, although according to different approaches and pathways. Some practical recommendations are presented in the following Section III, which precedes the Conclusion where the evidence and take-aways from the previous discussions are summarized.

II. LOOKING OUTSIDE THE EEA SPACE

This section addresses the two topics of personal data gathering in a non-EEA country by agencies or branches of EEA based organisations and transfer of collected data to an EEA country for storage and processing purposes. In the following subsections, the privacy regimes of China, US and UK are examined in turn.

MIPRO 2021/ICTLAW
A. China

There is a diffused consensus \[8\] on the fact that the People’s Republic of China, particularly since 2016-2017, has set up a privacy regime that closely resembles the GDPR, although it does not yet provide a comparable protection for individuals, due to a limited or partial application in the concrete cases submitted for judgement to the Chinese courts.

This regime is built on two distinct, yet convergent elements, which have both experienced considerable revisions in 2020, with the aim of further strengthening the protection level of individual rights to privacy and personal information:

- A collection of laws that look at the personal right to privacy from different angles, including the Cyber Security Law (passed on 6 November 2016, effective as of 1st June 2017), the Consumer Protection Law (promulgated on 31 October 1993, amended on 27 August 2009 and on 25 October 2013, effective as of 15 March 2014), and the Criminal Law (first adopted on 1st July 1979 and amended on 14 March 1997). More recently, on 28 May 2020 a new Civil Code was adopted, which entered into force on 1st January 2021. This is the most comprehensive law ever passed in China, with more than 1200 articles, and dedicates an entire Book (IV) to personal rights, including privacy and data protection;

- Accompanying national standards, which are meant to explain and reinforce the aforementioned legislation, as non-binding recommendations for the China based actors who professionally collect and handle personal data.

Two (groups of) such standards are relevant to our discourse:

- The GB/T 35273-2017 Personal Data Security Specification, superseded as of 1st October 2020 by the GB/T 35273-2020 Information Security Technology – Personal Information Security Specification; and


On the specific topic of cross-border data transfer, it is also worth mentioning the existence of two draft regulations:

- the Measures for Security Assessment for Cross-border Transfer of Personal Information (Draft for Comment) issued on 13 June 2019 by the Cyberspace Administration of China, which in turn make significant adjustments to the Measures for Security Assessment for Cross-border Transfer of Personal Information and Important Data (Draft for Comment) released on 11 April 2017; and

- the Data Security Management Measures (Draft for Comment) issued on 28 May 2019, again by the Cyberspace Administration of China, which supersede the draft Regulation on the Cybersecurity Multi-level Protection Scheme, issued on 27 June 2018 by the Chinese Ministry of Public Security, containing the first version (1.0) of the Multi-Level Protection Scheme for Data Security.

Neither regulation has been formally adopted as of today, but we can consider their provisions as a useful complement, and in the latter case also a summary, of the corresponding rules, principles and standards, particularly on the topic of data security, which clarify under which specific conditions personal data transfer from China to overseas is legitimate and creates no harm for the data subjects. First and foremost, personal information should never be publicly disclosed, unless the data controllers have conducted the necessary security impact assessments in advance, have informed the subjects of their intent, received the subjects’ explicit consent, and kept a detailed record of the public disclosure. Moreover, there is no possibility of publicly disclosing personal biometric data, or the results of analysing sensitive data, such as race, ethnicity, political views, and religious beliefs. Finally, controllers must develop specific and detailed protocols for handling and reporting any data security incidents, including regular trainings for their employees who handle personal information. Data subjects must be notified immediately if their personal information has been leaked or breached in any way.

Contrary to what is commonly believed, personal information collected and generated in China can be transferred overseas. Severe legal restrictions only apply to what the 2017 Cybersecurity Law names “important data”, as distinct from personal or sensitive data. What this term exactly means has been clarified only two years later, in Art. 38(5) of the 2019 Draft Regulation on Data Security Management Measures: “Important data refers to data that, if divulged, may directly affect national security, economic security, social stability, or public health and safety, such as undisclosed government information or large-scale data on the population, genetic health, geography, mineral resources, etc. Important data generally does not include enterprises’ production, operations, and internal management information, personal information, etc.” For that kind of data, which may involve national security, social order or public interest on a general level, transferability outside China is possible only if “truly necessary for the requirements of the business”, a concept introduced by Art. 37 of the Cybersecurity Law but still missing a precise definition in the legislation.
In practical terms, whoever aims to transfer important data stored in infrastructure located within the Chinese borders must ask the authorization of local Public Security Bureaus. For all other kinds of data, and particularly personal information, transfer abroad is indeed possible, but Chinese based actors (including foreign operators) must comply with all the relevant national regulations and standards. Among these, the already mentioned draft regulations entitled Measures for Security Assessment for Cross-border Transfer of Personal Information and Data Security Management Measures, which summarize the Multi-Level Protection Scheme for Data Security 2.0 package of standards referenced to above.

The 2019 Measures for Security Assessment, which did not become effective after the end of the consultation period, exactly like those issued in 2017 that they were supposed to improve – which created a lot of confusion among the practitioners – have introduced the obligation to conduct a security assessment in case of transfer of personal data outside of China. This obligation is also part of the GB/T 35273-2020 Specification, which concerns any case of sharing and transfer of personal data, even within the national borders. We can then consider this a precise requirement for any organisation located in China, including the foreign network operators (such as Amazon, Google, etc.) providing cloud services in the country.

In turn, the 2019 Multi-Level Protection Scheme for Data Security 2.0 package made the crucial distinction between “Level 1” and “higher level” operators (from 2 to 5): the first group includes any organisation running a network or online business, the damage of which may cause harm to the legitimate rights and interests of Chinese citizens, legal persons and other organisations, but not to national security, social order or public interest on a general level, as it would be the case of the other four groups. Therefore, only for the operators in the first group (indeed, the majority of Chinese and foreign businesses) the requirements of the Cybersecurity Law are softened, in terms of e.g. no need to hire a qualified external expert to assess the security risks of the current infrastructure.

If the data transmission may affect or result in damage to national security or the public interest, or it may make it harder to protect the security of personal data during the data transfer, such data may not be transferred beyond China. However, it may be supposed that if a data transfer is liable to affect or damage the national security or the public interest, then that data may be considered “important” according to the definition in the Cybersecurity Law, and therefore restricted to sharing and transfer overseas, unless compliance with the “needs of the business” is certified and a prior authorization from the local Public Security Bureau is obtained.

We can therefore conclude this analysis that although the aforementioned draft regulations on cross-border data transfer never went into effect and the Multi-Level Protection Scheme package is only a standard, therefore has an “advisory” role not carrying the force of law, foreign companies operating in China should develop, through their onsite data processors, a security impact assessment, to evaluate the implications of adopted personal information security standards on the legal rights and interests of the data subjects, before carrying out any cross-border transfer of personal data. This assessment can be done internally, under the condition that the organisation in question belongs to the “Level 1” group of operators.

Based on the overview of legislation and standards presented above, there seems to be no significant difference between the GDPR and the Chinese privacy regime as far as the principles and prescriptions concerning privacy and personal data protection are concerned. In particular, a security impact assessment is required prior to sharing and transferring personal data within and beyond the Chinese borders. However, it is important to bear in mind that the above prescriptions concern only the transfer of (recognizable) personal information, and not aggregated or anonymised data.

We summarise this overview by saying that the whole privacy regime in the People’s Republic of China is in rapid transformation, and most of the recent changes are becoming effective right in these months. As we will discuss in the next two subsections, the situation is pretty much the same as (and perhaps a bit clearer than) with the US and UK regimes in relation to the GDPR.

B. United States

As a matter of principle, the US legislation imposes very few, if any, restrictions on transferring personal data outside the country due to the normal course of business or research operations. Likewise, the US does not protect the personal data of its citizens outside of country borders. To mitigate such risks, “savvy” corporate lawyers do often prohibit the transfer of key data overseas, impose viewpoint access, or limit the disclosure of sensitive data, particularly to organisations not residing in the EEA space and therefore not subject to the GDPR. However, this sort of “piecemeal approach” does not provide comprehensive protection while the Congress is not putting the issue high on the political agenda.

From the perspective of full GDPR compliance, the issues and concerns mentioned in the Introduction – particularly the references made by the ECJ ruling of July 2020 to the provisions of Section 702 of the Foreign Intelligence Surveillance Act and of the Executive Order No. 12333 – do not seem to apply to the international transfer of data originally sourced from people residing in the US.

In fact, Section 702 of the Foreign Intelligence Surveillance Act permits the Attorney General and the Director of National Intelligence to jointly authorize the targeting of persons reasonably believed to be located outside the US, rather than inside it, and is limited to targeting non-US citizens.

As far as the Executive Order No. 12333 is concerned, which was originally signed by President Ronald Reagan on 4 December 1981 and later modified in 2004 and 2008 by President George W. Bush, it had the main purpose of coordinating the intelligence activities of CIA and other federal agencies, but has been employed by the National Security Agency (NSA) as legal authorization for their appropriation of data and generic unencrypted information.
from US big players such as Google and Yahoo!, with the aim of preventing or fighting against the insurmountability of criminal activities on the US soil.

It remains therefore indetermined whether the personal data gathered by non-US based organisations on the US soil and through local data processors are subject to any prescriptions, and if so which – e.g. a security impact assessment, like in the China example. It is also unclear if the coverage of the NSA foreign surveillance programmes – within the scope of both Section 702 and Executive Order No. 12333 – can legitimately extend to EEA based data controllers, and if so, if any limitation is posed by this circumstance to the general principle of free and uncontrolled overseas transfer of the personal data of US citizens.

C. United Kingdom

Art. 7(1) of the Withdrawal Agreement specifically mentions that the EU law – thus, the GDPR – continues to apply in the UK in respect of the processing of personal data of data subjects outside the UK, provided that the personal data: (a) was processed under the EU law in the UK before the end of the transition period, i.e. until December 31\textsuperscript{st}, 2020; or (b) is processed in UK after the end of the transition period on the basis of the Withdrawal Agreement itself. This subsection aims to clarify, at least to some extent, what the condition under point (b) means.

Paragraph 2 mentions in fact an adequacy decision to be taken by the EC in compliance with Art. 45(3) of the GDPR – or Art. 36(3) of Directive (EU) 2016/680 on data protection in the police and criminal justice sectors. Paragraph 3 specifies that “to the extent that a decision referred to in paragraph 2 has ceased to be applicable, the United Kingdom shall ensure a level of protection of personal data essentially equivalent to that under Union law”.

Globally, the situation in the UK is not unfavorable after Brexit [9]. In fact, according to the Information Commissioner’s Office (ICO), as of 1\textsuperscript{st} January 2021 data transfers from the UK to other countries, including to the EEA, are now subject to the rules of the UK regime, but these broadly mirror the GDPR provisions, although the UK “has the independence to keep the framework under review” [10]. Currently, the new UK privacy regime [11], starting to be known as the UK GDPR, bears very few differences from the EU GDPR. Therefore, UK based organisations that transfer to the EEA any personal data gathered locally or pre-processed to some extent, do not need to take any other initiative than continuing to comply with the GDPR provisions as they stood until the end of the transition period. This includes frequently revising privacy notices and impact assessments, as well as the data subjects’ prior consent forms. The UK GDPR currently doesn't require any safeguards for data transfers to the EEA, although the situation is prone to change according to the regained amending power of the British Parliament.

What can be reasonably expected for the near future is a dedicated adequacy decision taken from the EC pursuant to Art. 45(3) of the GDPR – identical to that taken in 2010 for the EU/US Privacy Shield – to validate the level of compliance with GDPR provisions of all data processing activities done in the UK after the end of the transition period, based on the enforcement of SCCs and/or binding corporate rules and/or invoking the derogations pursuant to Art. 49 of the GDPR.

III. DISCUSSION AND RECOMMENDATIONS

In a globalized world, it is rather commonplace to see data flows moving from country to country, with the appropriate safeguards and protection measures, for technical rather than commercial purposes: i.e. unrelated from a purposeful act of trade, just following the rules of demand and offer and the principle of value for money in the identification of the best service provider for certain activities. These flows, although quite important also before the GDPR advent, were left rather obscure or peripheral in the consideration of the previous law regime. Currently, the concern is well addressed that when any personal data is transferred outside the EEA, it can rely on the same level of protection as it received inside it. But what about the storage and processing inside the EEA of personal data gathered outside that space? This paper has considered the rules and regulations belonging to the three privacy regimes of China, US and UK after Brexit.

Above and beyond what has been presented in the previous Section, if it was possible to demonstrate that the data of interest was already in the public domain before or that the field activity does not lead to gather any personal data – for example, if data is collected in aggregated form or was anonymised by origin – then no particular attention to legal compliance should be paid by EEA organisations engaged in data gathering, storage and processing activities in those three countries through local agents or branches (data processors). On the other hand, if any sensitive data was involved in those activities, then some (or all) of the conclusions of the analysis carried out in this paper should be revised and subject to deeper introspection and reflection. According to the GDPR, particularly Art. 4(13-15), Art. 9 and recitals 51-56, sensitive data includes a person’s racial or ethnic origin, political opinions and activities, religious or merely philosophical beliefs, trade union memberships, genetic data, biometric data, data concerning health or sex life or sexual orientation etc. Thus, we can state that the lessons below are not immediately applicable to the scenario of sensitive data handling.

In the event of gathering fresh/raw personal data from residents in the three above countries, informed consent forms will have to be withdrawn from the data subjects, whatever the local privacy regime (including the severe provisions of the Chinese law in the case of emergent risks for security). It is also recommended that the prior information notice and/or informed consent form specify the exact country of location of the cloud server where storage and processing is foreseen, and consequently the applicable law for those operations – which can well be the law of the country where data was originally gathered if for any reason, including an immediate anonymisation and/or pseudonymisation, no raw or personal data transfer is planned to occur out of the national borders. In other words, if data gathered in (e.g.) the US is uploaded to a Google drive folder, there is no actual transfer across the
US border yet. Same goes in the case data is anonymised or pseudonymised at the time and place of first collection.

Then, an assessment of security (for the Chinese law) and privacy (for both national laws and GDPR) must be executed and its results are to be made publicly accessible. A “grey zone” not properly discussed in the previous Section pertains to the US regulations governing data gathering from national residents, due to the difficult interpretation of apparently open and free but substantially prone to surveillance and control data handling operations.

All other cases – namely the Chinese laws and standards and the UK regulations and ICO recommendations – have been assessed to be at least as conservative as the GDPR in terms of personal data protection. However, based on the ECJ sentence repealing the Privacy Shield, we can assume that adopting the provisions of the GDPR would be more than appropriate to safeguard the individual rights of US data subjects in any relevant situation. Finally, some additional security caveats, or policies and technical and organisational measures that are specific to the case of data transferred from China to the EU/EEA space, should be adopted, particularly in light of the risks of inadvertent break-up of data security provisions within the normal activities of storage and processing.

IV. Conclusion

Despite the different starting points, the three privacy regimes of China, US and UK (after Brexit), for various reasons all undertaking a process of transformation, are showing a good level of convergence towards, if not full alignment with, the GDPR provisions, across different approaches and pathways. Knowing about this can be of interest for e.g. international research consortia engaged in multi-country data gathering, a trend one may expect to grow linearly, if not exponentially, in the near future.

Overall, we can conclude that no major change should be envisaged in the contents of a well-developed privacy impact assessment, to make room for a specific distinction between personal data gathered in the EEA space and outside it. If anything, in the case of recourse to field data gathered both inside and outside that space, the GDPR requirement mentioned in the Introduction, of a full and transparent adoption of GDPR principles and rules of operation, can only be reinforced in retrospect.

Acknowledgment

This paper stems from some reflections done by the first author in the context of the H2020 project T-Factor, having its pilot sites located in EU, China, US and UK. Despite that, none of the opinions expressed herein engage any EU institution or member of the consortium. We are grateful to two anonymous referees for their constructive comments.

References


[7] European Union in Case C-311/18 - Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems. Request for a preliminary ruling — Protection of individuals with regard to the processing of personal data — Cha rter of Fundamental Rights of the European Union — Articles 7, 8 and 47 — Regulation (EU) 2016/679 — Article 2(2) — Scope — Transfers of personal data to third countries for commercial purposes — Article 45 — Commission adequacy decision — Article 46 — Transfers subject to appropriate safeguards — Article 58 — Powers of the supervisory authorities — Processing of the data transferred by the public authorities of a third country for national security purposes — Assessment of the adequacy of the level of protection in the third country — Decision 2010/87/EU — Protective standard clauses on the transfer of personal data to third countries — Suitable safeguards provided by the data controller — Validity — Implementing Decision (EU) 2016/1250 — Adequacy of the protection provided by the EU-US Privacy Shield — Validity — Complaint by a natural person whose data was transferred from the European Union to the United States. Case C-311/18. Retrieved online at: https://eur-lex.europa.eu/eli/dec_impl/2016/1250/ij


