ELB Blogpost 49/2022, 14 November 2022
Tags: Data Protection Law, Schrems, Data Transfers, US executive order
Topics: Data protection and digital governance

Nothing new in the west? The executive order on US surveillance activities and the GDPR

By Hannah Ruschemeier

All involved in data protection law are well acquainted with the constant anxiety arising in the context of international data transfers since the *Schrems* decisions of the ECJ. Long story short: According to Art. 44-49 GDPR there has to be a legal basis for transferring personal data from the European Union to third countries. The ambitious goal is to ensure compliance with the protection standards of the GDPR in the global world of data transfers even outside the Union. A very important line of data transfer is the one from the EU towards the US and the provisions are necessary to protect the right to data protection of European citizens in a globalized data-driven world. The GDPR requires the third country transfers either to occur on the basis of an adequacy decision by the Commission (Art. 45) or the transfer to be subject of appropriate safeguards (Art. 46). Additionally, Art. 49 GDPR states subsequent derogations for specific situations. Adequacy decisions refer to an assessment of the legal system of the third country while the appropriate safeguards rely on the individual protections the transferring party implements.

I will briefly summarise the main emphasis of the executive order by President Biden on enhancing safeguards for US signals intelligence activities and explain possible implications on transnational data transfers and the GDPR, followed by an analysis of the intersection of legal and political arguments and a short outlook.

The Schrems Saga

After two attempts by the Commission to establish legal certainty via adequacy decisions concerning data transfers to the US (the Safe Harbor agreement, and subsequently the Privacy Shield agreement), the legal situation is more unclear than ever since the latest ruling of the ECJ. Initiated by the personification of data protection litigation, Max Schrems, the ECJ declared the Safe Harbor agreement void (Schrems I) followed by another ruling which declared the successor Privacy Shield (Schrems II) as insufficient to comply with European data protection standards. Crucial findings by the ECJ have been the limitations on the collection of personal data from European citizens for security and intelligence purposes and the availability of effective redress for European data subjects against data protection violations, which were held not to have been met by the legal provisions and administrative practice in the US.

Uncertainties in Law and Politics

There have been numerous analyses of the decisions, see for example here, here and here. Since *Schrems II* there have been the tremendous practical problems for all kind of data users of how to comply with the GDPR while using services that transfer data to the US (e.g. Zoom!). Data users have been forced to fall back on standard contractual clauses (SSCs), which have been an emergency solution at best. The SCCs are private contractual agreements which by their very nature are not able to bind third state authorities. As a consequence, data users have been required to provide additional safeguards for the protection of data to ensure an adequate level of data protection. In fact, the SSCs were never able to solve the most striking problem of data transfers to the US: the bulk surveillance of European citizens by the US intelligence services and the lack of legal protection mechanisms. In the *Schrems II* decision, the ECJ required an impact assessment regarding the adequacy of the level of protection, including any access by the public authorities of the third country. Given what is known about the (secret!) surveillance techniques used by US authorities, these requirements are probably impossible to meet in practice. Hence, the EU and the US agreed to negotiate a new transatlantic data privacy framework.

Now there seems to be some progress in the longstanding matter. President Biden signed an executive order (EO) following the lengthy negotiations between the US and the European Union and even though an executive order is an internal directive within the federal government and not a law statue, the format and content of the decision are informative and revealing. Despite the justified criticism, the US has taken a big step towards the European Union from a political point of view; unfortunately, legal problems remain. Two major points of the EO stand out; first that the intelligence agencies will only engage in surveillance of non-US citizens when it is necessary and proportionate, and second the establishing of legal redress mechanisms.

Structure of the EO

The central provisions are laid down in sections 2 and 3 of the EO. Section 2 starts with principles: Intelligence activities should be subject to appropriate measures for safeguards; the activities shall be necessary to advance a validated intelligence activity and only conducted in a manner that is proportionate to the intelligence activity itself. The EO then lists legitimate objectives for intelligence activities such as the protection of national security, against transnational threats, terrorism, espionage and cybersecurity threats and other objectives. Prohibited objectives are also named, like the suppression of civil rights, privacy interests or disadvantaging persons based on ethnicity, race, gender and other personal characteristics.

The list of objectives is rather broad, e.g. the threats to the personnel of the US or its allies or partners will potentially cover a huge number of persons and these threats are not directly linked to national security. Additionally, the president is able to authorise updates to the list of objectives which have to be made public. However, this transparency requirement regarding the public only applies when the when the president does not determine that it would pose a risk to the national security of the US. The past has shown that the condition of national security does not mean any actual restriction, so that there is in fact no transparency with regard to new objectives.

The section on 'privacy and civil liberty safeguards' is strongly characterised by references to the principle of proportionality. The collection of intelligence has to be determined

necessary, but must not constitute the sole means available for validating intelligence priority; less intrusive measures have to be considered. Furthermore, intelligence activities must not disproportionately impact privacy and other liberties, which can include the duration, the 'suitability', meaning the contribution to the objective which is pursued, the affectedness of third parties, the nature of the collected data and the safeguards to the collected information. All of this strongly echoes the wording of European jurisprudence on data protection and surveillance, particularly by the German Federal Constitutional Court, the ECJ and the ECtHR. There are good reasons to be sceptical whether the wordings have the same meaning in effect.

Bulk surveillance is here to stay

The handling of personal information collected through signals intelligence must follow the principle of minimization, retention, data security and access and data quality (sec. 3 iii A). Though, the biggest problem in terms of the compliance with the GDPR still remains: the bulk collection of signals intelligence. Although the EO requires that a validated intelligence priority cannot reasonably be obtained by targeted collection for limited objectives, this is only a presumed limitation since the objectives are actually broad. The legitimate objectives for bulk surveillance are only slightly narrower than those for general signal intelligence activities. Notably, surveillance on the basis of the potential threats to the personnel of the US or its allies is not factually restricted and the president is authorized to update the list without publication.

Investigation of complaints and the Data Protection Review Court

In matters of redress, the EO provides two new procedures. The first opportunity is to complain towards the independent Civil Liberties Protection Officer (CLPO) who reviews and then informs the complainant if the review did/not identify any violations, but without confirming or denying that the complainant was subject to intelligence activities. In the 'second instance', the complainant may apply for review by the Data Protection Review Court (DPRC), where they will be provided with a 'special advocate'. Within 60 days of the date of the EO, the Attorney General shall establish the DRC with appointed judges – it remains unclear how many in total, but a three-judge panel shall review the application

against the decision of the CLPO. The subject matter of the decision is limited solely to whether a violation has occurred or an appropriate remediation has been determined by the CLPO. Consequently, the binding decision of the 'court' – which remains a body within the US executive – will be made only about these questions as a kind of declaratory judgment, leaving the complainant without any corresponding subjective rights. The purpose of an appeal to the court remains unclear if the decisions of the two bodies are congruent anyway. There are good reasons to doubt whether this meets the requirements of an effective remedy and, in particular, the independence of the court, as required by Art. 47 of the Charter. At least the ECJ has not recognised executive institutions in its previous case law.

Therefore, data subject rights do not correspond to the level of protection of the GDPR since the data subjects have no judicial remedy to access, rectify or erase their personal data processed by the intelligence services. Transparency is needed to exercise these rights and it is not revealed to the data subject whether their data have been processed by the agencies in the first place. Deletion seems possible because of the principle of retention: section 3 ii A (2) (c) requires that that the intelligence community shall delete the personal information of non-US citizens that may no longer be retained in the same manner that comparable information concerning US-citizens would be deleted.

After a period of 5 years, the Secretary of Commerce has to notify the complainant whether information pertaining to the review has been declassified and may be available under applicable law.

The stated redress process will be reviewed by the PCLOB to the effect that the complaints are processed in a timely manner, whether the CLPO and the DPRC have access to necessary information and are operating consistently. Importantly, the reviews will be publicly available.

Qualifying states: those that benefit the interests of the US

Interestingly enough, the redress mechanisms do not apply to all non-US citizens. Instead, the Attorney General is authorized to designate a country or a regional economic

integration organization as a qualified state. Conditions are that the laws of the country require appropriate safeguards in the conduct of signals intelligence activities for personal information of US citizens that is transferred from the US to the third country – which reflects the requirements of the EU. Additionally, the country has to permit the transfer of personal information for commercial purposes to the US and that this would advance the national interests of the US. This passage clearly shows that the emphasis does not primarily lay on elements of fundamental rights protection, but rather commercial interests. According to the European understanding, national economic interests are not a prerequisite for protecting fundamental rights but rather a factor to be weighed in the balance of interests between conflicting goods.

Problems impossible to solve by law?

The legal-political implications create dilemmas: the Commission is under a lot of pressure from the industry to find a solution to the issue of EU-US data transfers, but the devil is in the construct itself (and the details). The GDPR establishes a challenging, sophisticated provision for data protection on paper but it clearly lacks execution. Some may call it megalomaniac that the GDPR requires third countries to follow legal standards of protection which have been enacted outside their own territories. At the end, the Brussels effect remains an effect but not a legal principle or provision. It describes the effect that the legislation of the EU leads to de facto unilateral regulatory globalisation by influencing laws of third countries via market mechanisms.

This discussion vividly shows that the law has not yet found satisfactory answers to the challenge of global digital technologies and may not find them in the present form. Nevertheless, is it still worth trying? Even though the GDPR is deserving of criticism in many respects, it has set a global example for data protection, followed by many other countries. The example of data protection and the effects produced by the legal act of the GDPR shows that it is precisely the correlation between the European protection of fundamental rights and a demanding jurisprudence of the ECJ that can provide arguments for political negotiations. Law cannot solve global problems on its own, but can undoubtedly contribute to their resolution by providing coherent jurisprudence and

arguments emphasising fundamental rights. The hopefully successful negotiations on transatlantic data protection could provide a blueprint for other problems at the interface of law and politics: the mechanism of negotiating a level of protection in the interaction between Union legislation, case law and political negotiations could also be applied to the climate crisis, even if the results of international legal agreements are less hopeful. The rule of law remains important.

What's next?

The Commission announced it will draft a new US 'adequacy decision' under Art. 45 GDPR which will be followed by a hearing of the European Data Protection Board. It is expected that this decision will be drafted within 6 months. The EO is only a baby step towards a new transatlantic privacy framework, the adequacy decision is not a done deal. Even if the Commission makes a formal adequacy decision, *Schrems III* seems to be just around the corner since the EO is far from creating clear conditions, whether the requirements of the ECJ regarding bulk surveillance and legal redress are met can be questioned. For data transfers in practice it is highly uncertain whether an adequacy decision will even be able to establish trust and acceptance in the market place after multiple invalidations of previous decisions by the ECJ.