EUROPEAN LAWYERS
EUROPEAN BARS
CCBE
BARREAUX EUROPÉENS
AVOCATS EUROPÉENS

Council of Bars and Law Societies of Europe
The voice of the European legal profession

Rue Joseph II, 40/8 - B-1000 Brussels
T.: +32 (0)2 234 65 10 - ccbe@ccbe.eu - www.ccbe.eu

CCBE comments on the Report from the Commission to the European Parliament and the Council on the first annual review of the functioning of the EU-U.S. Privacy Shield

The Council of Bars and Law Societies of Europe (CCBE) represents the bars and law societies of 32 member countries and 13 further associate and observer countries, and through them more than 1 million European lawyers. The CCBE responds regularly on behalf of its members on policy issues which affect European citizens and lawyers.

The CCBE has taken note of the "Report from the Commission to the European Parliament and the Council on the first annual review of the functioning of the EU-U.S. Privacy Shield" (including the "Commission Staff Working Document") dated 18.10.2017 (COM(2017) 611 final / SWD(2017) 344 final) (the "**Report**").

In its document "CCBE Comments on the Review of the EU-U.S. Privacy Shield Agreement" dated 25.09.2017 (the "**CCBE Comments**") the CCBE had urged the European Commission to suspend its Implementing Decision 2016/1250 on the adequacy of the protection provided by the EU-U.S. Privacy Shield on the basis that the U.S. does not ensure a level of protection of personal data that is essentially equivalent to the one guaranteed by the EU. The main reasons for this view were the following:

- Lack of binding legislative control;
- Lack of judicial and independent oversight mechanisms;
- Lack of effective legal remedies.

The CCBE has analysed the Report and come to the conclusion that, despite the length of the Report, none of these crucial issues are sufficiently addressed in the Report:

1. Lack of binding legislative control

a) The CCBE Comments stated: All surveillance activities need to be regulated with adequate specificity and transparency in order to avoid the risk of arbitrary disregard for human rights. In this regard, the Privacy Shield only refers to e.g. “Guidelines and Policies of the Department of Justice” or “transparent policies of the Department of Justice”. As a legal basis of clear, precise and accessible rules, these policies and guidelines cannot be deemed as a form of binding legislative control.

The Report states: Nothing. The issue is not even mentioned in the Report.

b) The CCBE Comments stated: The term ‘national security’ in the Privacy Shield is not circumscribed with adequate specificity so as to ensure that data protection infringements can

be effectively reviewed in courts to ensure compliance with a strict test of what is necessary and proportionate.

The Report states: Nothing. The Report mentions the term "national security" many times and acknowledges that the concept of national security is being used to limit rights of individuals, e.g. when it comes to the notification of the concerned individual ("As surveillance for national security purposes is conducted for threat prevention, often in the long term, rather than to investigate and punish past offences, notification of the individual is understandably subject to stricter conditions than in the area of law enforcement."). Despite recognising the importance of the term "national security", the Report does not in any way address the issue that this crucial term is not clearly defined in the Privacy Shield.

2. Lack of judicial and independent oversight mechanisms

a) The CCBE Comments stated: Any interference with the fundamental rights to privacy and data protection should be supervised by a judicial body, which is financially and politically independent from the executive and should be irremovable, because only a judge can offer the necessary guarantees of independence. The legal framework of oversight mechanism in the Privacy Shield is multi-layered and consists of two major parts: internal and external oversight. Apparently, none of the internal oversight bodies can be financially and politically independent from the executive branch because they are basically part of it, therefore internal oversight will not fulfil the requirement of supervisory control as set out above. External oversight is provided by what is said to be judicial bodies, including the intelligence committees of the Congress and the Privacy and Civil Liberties Oversight Board. The latter two are not judicial bodies, so the requirement of supervisory control can only be fulfilled by FISA Court. However, the procedure before this court is ex parte, meaning that the individuals concerned might not be heard, or they even might not be aware of the case.

   The Report states: Nothing. While extensively discussing the oversight mechanisms in place, the Report fails to even mention these structural deficits in any way.

b) The CCBE Comments stated: The surveillance activities conducted on the basis of Executive Order 12333 are not subject to any judicial review, neither a priori, nor a posteriori.

   The Report states: Nothing. While mentioning the concerns of NGO's, the Report fails to mention the lack of any judicial review of surveillance activities conducted on the basis of Executive Order 12333. Instead it appears that the Report comes to the conclusion that the self-assessment of the NSA and compliance programs run within the NSA are sufficient safeguards – which they are clearly not. Against the background of lacking judicial review, it is all the more worrying that it is unclear whether “tailored as feasible” in PPD-28 is equivalent to the European standard of strict necessity and proportionality. The report of the art. 29 Working Party criticizes as well that it is uncertain and unforeseeable how Executive Order 12333 is made use of.

c) The CCBE Comments stated: In order to fulfil its mandate, the oversight body must be given proportionate, adequate, and binding powers by law. These competences must enable the body to make fully informed and enforceable decisions. However, the Privacy Shield only specifies the rather limited competence of the Ombudsperson, and even if one considers the Ombudsperson as an oversight body (which is not made clear in the Privacy Shield), it is evident that the Ombudsperson lacks any effective powers since it can only request further action by the appropriate United States Government body or request information from other governmental entities. It cannot order the authorities to cease and discontinue unlawful surveillance, or order the permanent destruction of information obtained through direct and indirect surveillance.

The Report states: Nothing. While praising the Ombudsperson mechanism as being unique at international level and calling on the U.S. administration to confirm its political commitment to the Ombudsperson mechanism by filling the position of the Ombudsperson with a permanent appointee as soon as possible, the Report fails to even mention the lack of effective powers of the Ombudsperson. Instead it appears that the Report finds it sufficient that the Ombudsperson may report any findings to the Secretary of State, even though the Secretary of State is part of the U.S. Government which is responsible for the threats from which the Privacy Shield seeks protections. Likewise, the report of the art. 29 Working Party doubts the powers of the Ombudsman are sufficient vis-à-vis the intelligence authorities.

d) The Report states that "the DoC has not made use of the possibility provided in the Privacy Shield to request copies of the contractual terms used by certified companies in their contracts with third parties to ensure compliance". In other words, so far there is no effective control whether certified companies actually comply with the provisions of the Privacy Shield.

The CCBE is very worried by this observation and fails to understand why the Commission obviously does not see the need to draw consequences from this observation. Furthermore, as correctly assessed by the Art. 29 Working Party report, the DoC fails so far to conduct *ex officio* compliance reviews, but simply intervenes if there is a suspicion of breach. We doubt that such a practice leads to an effective oversight and urges the Commission to insist on sample inspections.

3. Lack of effective legal remedies

a) The CCBE Comments stated: In order to provide effective legal protection against unlawful surveillance, it is necessary that legal remedies are made available to lawyers and their clients who have been the subject of unlawful surveillance. The U.S. government does not regard the protections of the U.S. Constitution, which prohibits “unreasonable” searches and seizures and imposes a warrant requirement to prevent such actions, as extending to non-U.S. persons who are outside the United States. Therefore, in the intelligence surveillance context, people in the EU who are not U.S. persons will not benefit from these constitutional protections (whereas in the EU anyone can go to court if they have a legitimate reason to suspect an interference of their fundamental rights, regardless of their citizenship).

The Report states: Nothing. While the Report mentions several alternative options for legal redress – FISA (50 U.S.C. §§ 1806, 1810), the Electronic Communications Privacy Act (ECPA, 18 U.S.C. 2701-2712), the Computer Fraud and Abuse Act (18 U.S.C. § 1030), the Right to Financial Privacy Act (12 U.S.C. § 3417), the Administrative Procedure Act (APA) (for any person suffering "legal wrong", or adversely affected/aggrieved by agency action), and the Freedom of Information Act (FOIA) (for access to documents) –, it concedes that there is a problem with the issue of "standing" (a prerequisite for a claim being admissible to the court) and concludes as follows:

"U.S. jurisprudence on the issue of standing in the case of government surveillance is still evolving. In this respect, the U.S. authorities have pointed the Commission to the proceedings in Jewel v. National Security Agency and Wikimedia v. National Security Agency. While these cases are not yet finally decided, they nevertheless suggest that, depending on the circumstances, applicants can succeed at the admissibility stage. In addition, the U.S. authorities have pointed to the requirement for notification that exists with respect to certain surveillance laws (e.g. the Wiretap Act) and which facilitates a showing of standing."

In other words, the legal situation is everything but clear and it remains an open question whether effective legal remedies exist. Instead of certainty the Commission offers hope:

"In this context, the Commission hopes that the Congress will consider favourably enshrining the protections offered by Presidential Policy Directive (PPD)-28 with respect to non-US persons in FISA, with a view to ensuring the stability and continuity of these protections. Any further reforms, both in terms of substantive limitations and in terms of procedural safeguards, should be implemented in the spirit of PPD-28 and thus provide protection irrespective of nationality or country of residence."

Although the report of the Art. 29 Working Group found clear words on the unclear requirement of legal standing, we are not convinced that the pending case of ACLU v. Clapper and Wikimedia v. NSA will interpret "standing" in a way to help European citizens to satisfy this procedural requirement due to the fact that the plaintiffs are not individuals and US courts have so far never addressed the lawfulness of surveillance measures.

It is the position of the CCBE that hope for a better future cannot replace effective legal remedies. This applies in particular in view of the facts that "currently, four of the PCLOB's (Privacy and Civil Liberties Oversight Board) five seats are vacant with only one Board member (E. Collins) remaining" and "that the PCLOB currently cannot initiate new oversight projects and/or adopt reports in on-going investigations". Since the report of the Art. 29 working group seems to focus on the PCLOB vacancies, it is important to stress once more, that even if all positions in the PCLOB were filled, the PCLOB does not have any effective powers and is thus a toothless tiger that cannot protect European citizens from arbitrary interferences.

Moreover, European Citizens may be hindered from legal remedies because they do not know of surveillance measures against them. Under European law (ECtHR, Zakharov v. Russia, Application no. 47143/06, 4 December 2015), targeted individuals have to be informed of any surveillance measures at the latest after their termination so as to be in the position to seek ex-post legal remedy. Apart from criminal proceedings, subjects of surveillance measures are not notified of actions taken against them. Such surveillance measures are therefore not proportionate as required by the ECtHR.

b) The CCBE Comments stated: Although the Privacy Shield highlights in general that there are both judicial and administrative remedies available to the individuals in the U.S., this has been seriously put into question by Executive Order 13768 Enhancing Public Safety in the Interior of the United States. The Order specifically provides that the provisions of the Privacy Act will no longer apply to those "who are not United States citizens or lawful permanent residents". The guarantees and remedies of the Privacy Act would therefore no longer benefit EU citizens who are not lawful permanent residents in the United States. Consequently, this Decree appears to over-ride the guarantees granted during the discussions on the Privacy Shield.

   The Order allows the NSA to share large amounts of personal data of non-US persons with 16 other government agencies without any mandate, court decision or authorisation from Congress.

   Congress has also authorised Internet service providers to sell their subscribers' personal data, including history and other private information, without their consent.

   Given that an Executive Order has a lower status than a statute in the US legal system, it could be argued that the Order of 25 January 2017 should not be regarded as calling into question the Judicial Redress Act of 4 November 2015. However, this Order shows, at the very least (i), the intention of the American executive to reverse the guarantees previously granted to EU citizens with regard to the protection of their personal data; (ii) raises concerns that, in practice, US governmental authorities directly dependent on the executive are seeking to override the commitments made during the Obama Presidency towards the EU, and (iii) exposes EU citizens to the unauthorised use of their personal data, with no effective remedy.

The Report states: Very little. "In the Commission's view, this does not affect the Privacy Shield given that the adequacy assessment does not rely on the protections of the Privacy Act. Following a written request from the Commission, the DoJ has explicitly confirmed this analysis in writing by letter dated 22 February 2017. These developments, which were also material in the sense explained, should have been reported by the U.S. authorities to the Commission, in line with their commitment under the framework. Only upon enquiries from the Commission did the U.S. government provide clarifications and reassurances. Hence, the Commission services expect that in the future the U.S. authorities provide timely and comprehensive information about any development that could be of relevance for the Privacy Shield."

Again, the Commission hopes for improvements, which in the view of the CCBE cannot replace effective legal remedies.

On the basis of this assessment the CCBE strongly disagrees with the conclusion of the Report – "On the basis of these findings, the Commission concludes that the United States continues to ensure an adequate level of protection for personal data transferred under the Privacy Shield from the Union to organisations in the United States. At the same time, the Commission considers that the practical implementation of the Privacy Shield framework can be further improved in order to ensure that the guarantees and safeguards provided therein continue to function as intended."

Instead, the CCBE calls on the Commission to suspend the Privacy Shield and to offer its re-implementation on the condition that the necessary guarantees and safeguards, which are currently lacking, have been implemented.