Personal data protection

1990/0287(COD) - 23/10/2019 - Follow-up document

The Commission presents its report on the third annual review of the functioning of the EU-U.S. Privacy Shield.

In its third year of operation, the Privacy Shield, which at the time of the annual review meeting had more than 5000 participating companies, has moved from the inception phase to a more operational phase. Covering both commercial aspects and issues relating to government access to personal data, the third annual review focused on the experience and lessons learnt from the practical application of the framework.

Main findings

Commercial aspects

In light of the findings of last year's annual review, the Commission's assessment of the commercial aspects focused notably on the progress made by the Department of Commerce on:

- Re-certification process

With respect to the re-certification process, it emerged at the third annual review that as a regular practice, at the expiration of the (re)certification period, if a company has not yet completed the re-certification process, the Department of Commerce, following an internal procedure, grants to the company a "grace period" of a significant length. During this period (for approximately 3.5 months, or, in some instances and depending on when the Department of Commerce detects that the re-certification process was not completed, even a longer period of time), the company remains on the Privacy Shield "active" list. For as long as a company is listed as participating in the Privacy Shield, the obligations under the framework remain binding and fully enforceable. However such a long period in which a company's recertification due date has lapsed while the company continues to be listed as active Privacy Shield participant reduces the transparency and readability of the Privacy Shield list for both businesses and individuals in the EU. It also does not incentivise participating companies to rigorously comply with the annual re-certification requirement.

- Effectiveness of the "spot-checks"

With respect to proactive checks of companies' compliance with the Privacy Shield requirements, the Department of Commerce introduced in April 2019 a system in which it checks 30 companies each month. The Commission welcomes that the Department of Commerce is carrying out proactive compliance spot-checks on a regular basis and in a systematic manner. However, it notes that these spot-checks tend to be limited to formal requirements such as the lack of response from designated points of contact or the inaccessibility of a company's privacy policy online. Compliance with these spot-checks are crucial for the continuity of the Privacy Shield and should be subject to strict monitoring and enforcement by the U.S. authorities.

- Tools to detect false claims

The Department of Commerce had continued to conduct searches on a quarterly basis, which has led to the detection of a significant number of cases of false claims, which in some instances were also referred to the Federal Trade Commission. However, these searches have so far only been aimed at companies that

had in some way already been certified or applied for certification under the Privacy Shield (but, for example, were not re-certified). It is important that they also target companies that have never applied for certification under the Privacy Shield. From all kinds of false claims, the false claims from companies that never applied for certification are potentially the most harmful.

- Progress and outcome of Federal Trade Commission enforcement actions regarding violations of the Privacy Shield

The Commission noted that since last year, the Federal Trade Commission concluded seven enforcement actions related to Privacy Shield violations, including as a result of the announced ex officio sweeps. All seven cases concerned false claims of participation in the framework. The Commission welcomes the enforcement action taken by the Federal Trade Commission in the third year of operation of the Privacy Shield. However, the Commission would have expected a more vigorous approach regarding enforcement action on substantive violations of the Privacy Shield Principles.

Access and use of personal data by U.S. public authorities

The third annual review was, first of all, aimed at confirming that all the limitations and safeguards that the adequacy decision relies on remain in place. In addition, the third annual review provided an opportunity to look at new developments and to further clarify certain aspects of the legal framework, as well as the different oversight mechanisms and the possibilities for redress, in particular with respect to the handling and resolution of complaints by the Ombudsperson.

Conclusion

The information gathered in the context of the third annual review confirms the Commission's findings in the adequacy decision, both with regard to the commercial aspects of the framework and with regard to aspects relating to access to personal data transferred under the Privacy Shield by public authorities. In this respect, the Commission noted a number of improvements in the functioning of the framework as well as appointments to key oversight bodies.

However, in light of some issues that emerged from the day-to-day experience or became more relevant in the context of the practical implementation of the framework, the Commission concludes that a number of concrete steps need to be taken to better ensure the effective functioning of the Privacy Shield in practice:

- The Department of Commerce should shorten the different time periods that are granted to companies for completing the re-certification process. A period of maximum 30 days in total would seem reasonable to allow companies sufficient time for re-certification, including for rectifying any issue identified in the re-certification process, while at the same time ensuring the effectiveness of this process. If at the end of this period the re-certification is not completed, the Department of Commerce should send out the warning letter without further delay.

- In the context of its spot-check procedure, the Department of Commerce should assess companies' compliance with the Accountability for Onward Transfers Principle, including by making use of the possibility provided by the Privacy Shield to request a summary or a representative copy of the privacy provisions of a contract concluded by a Privacy Shield-certified company for the purposes of onward transfer.

- As a matter of priority, the Department of Commerce should develop tools for detecting false claims of participation in the Privacy Shield from companies that have never applied for certification, and use these tools in a regular and systematic manner.

- The Federal Trade Commission should, as a matter of priority, find ways to share meaningful information on ongoing investigations with the Commission, as well as with EU Data Protection Authorities that also have enforcement responsibilities under the Privacy Shield.

- The EU Data Protection Authorities, the Department of Commerce and the Federal Trade Commission should develop common guidance on the definition and treatment of human resources data in the coming months.

Lastly, the Commission will continue to follow closely the ongoing debate about federal privacy legislation in the U.S. A comprehensive approach to privacy and data protection would increase the convergence between the EU and the U.S. systems and this would strengthen the foundations on which the Privacy Shield framework has been developed.