December 3, 2020

Look Who's Watching (Schrems) Too – Updated Guidelines on European Essential Guarantees for Surveillance Measures Adopted

Attorneys
Robert Lister

Since the Court of Justice of the European Union's (CJEU) "Schrems II" judgment on 16th July 2020, data controllers subject to the GDPR have been scrambling to determine if and how they can continue to lawfully transfer personal data outside the European Economic Area (EEA) using Standard Contractual Clauses (SCCs). For many, a particular part of this determination has involved trying as best they can to assess whether the laws of recipient third countries ensure a level of protection that is "essentially equivalent" to that guaranteed by EU law. Cue the European Data Protection Board (EDPB), which almost four months later on 10th November, adopted its Recommendations on the European Essential Guarantees for surveillance measures (Recommendations), in order to assist with the evaluation of third-country surveillance laws.

Background

The Schrems II judgment resulted in the invalidation of the EU-US Privacy Shield, meaning that transfers of personal data to Privacy Shield-certified businesses in the US, in the absence of other approved safeguards or specific GDPR derogations, were no longer lawful under the GDPR. The CJEU found that the US government's surveillance laws, in particular, do not sufficiently guarantee the rights of individuals in the EU whose personal data is transferred to the US and such individuals do not have actionable rights against the US authorities.

Although the CJEU upheld the validity of the SCCs in Schrems II, it also raised serious concerns about their legality when transferring personal data to certain jurisdictions (and specifically the US). In particular, this was due to perceived shortfalls in the SCCs, such as a lack of individual redress against foreign governments conducting surveillance. This was somewhat confusing, especially because the whole point of the SCCs was to provide essentially equivalent protection precisely when the laws applicable to third-country data importers did not otherwise do so.

The CJEU made it clear that controllers relying on the SCCs are required to undertake a case-by-case assessment of the laws of the third countries to which they transfer personal data, to determine whether those countries provide equivalent (but not necessarily identical) protections for personal data to those guaranteed under EU law. To assist with this, the EDPB has adopted the Recommendations to provide data exporters with "elements" to determine whether third country legal frameworks governing public authorities' access to data for surveillance are a "justifiable interference" with individuals' privacy rights, and thereby permit the lawful use of the SCCs in such circumstances.

The CJEU also acknowledged that supplementary measures could be adopted, such as clauses additional to the SCCs, or obligations around technical or organizational measures, where the safeguards in the SCCs were not otherwise sufficient to address deficiencies in third-country legal regimes. Somewhat unhelpfully, however, the CJEU did not specify what those supplementary measures should be in practice. The EDPD is considering this point and has published for public consultation its separate Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data. This consultation ends on 21st December 2020, meaning that we might not see definitive clarification of this issue until early 2021.

Recommendations

In the Recommendations, the EDPB draws on and updates the working document issued by the Article 29 Working Party (WP29), (the EDPB's predecessor) in April 2016. In particular, the EDPB maintains the WP29's position that, by

looking at cases of the CJEU and the European Court of Human Rights regarding surveillance in Member States and other parties to the European Convention on Human Rights, four "European Essential Guarantees" (Guarantees) emerge.

The EDPB highlights that the Guarantees are based on fundamental and universal rights to privacy and data protection. The idea is that controllers wishing to use the SCCs should analyse the relevant laws of the third countries to which they are transferring personal data, in so far as they relate to access to data by public authorities and government agencies for the purpose of surveillance, against those Guarantees. If the local laws fall short of the Guarantees (i.e. "go beyond what is necessary and proportionate in a democratic society"), there will be deemed to be unjustified interference with fundamental rights either requiring supplementary measures to be put in place or, if this is not possible, preventing the use of the SCCs (and potentially the transfer of personal data entirely).

The four Guarantees are that:

(i) Processing should be based on clear, precise and accessible rules:

For surveillance to justifiably interfere with individuals' rights, it must be conducted in accordance with the law. Accordingly, there should be an accessible (i.e. public) legal basis setting out clear and precise rules governing the scope of the surveillance (including defined categories of surveillance targets, duration limits and restrictions on data use), as well as imposing minimum safeguards.

Individuals must also be able to invoke and rely on the relevant third country law before a court – if individuals do not have enforceable rights against public authorities in this regard, then the level of protection cannot be considered to be essentially equivalent.

Finally, the interference must be "foreseeable", so individuals can adjust their behaviour accordingly if desired. This means covert surveillance or interception of communications are unlikely to be justifiable, unless the law gives individuals an "adequate indication" as to when and how such surveillance or interception is permitted.

(ii) The legitimate objectives pursued must be demonstrably necessary and proportionate:

When assessing whether limitations to privacy and data protection rights are justified, it is necessary to assess both the seriousness of the interference and whether the importance of the public interest objective is proportionate to that seriousness. Derogations from and limitations on personal data protections must be strictly necessary – meaning that minimum safeguards need to be in place to ensure individuals have sufficient guarantees that their personal data will be protected against abuse risks. As a result, if third country laws do not indicate any limitations on surveillance powers, this Guarantee cannot be satisfied.

Indiscriminate mass surveillance will not satisfy the principle of necessity. This means, according to the EDPB, that laws permitting public authorities to have general access to the content of electronic communications (i.e. without any limitation or exceptions to the aims pursued and without objective criteria determining access and use limits), will similarly fall short of this Guarantee.

(iii) There must be an independent oversight mechanism:

Interference with privacy and data protection rights must be subject to "an effective, independent and impartial oversight system", either by judges or other independent bodies.

While prior judicial authorization of surveillance measures is important, checks and balances on the exercise of surveillance powers (and on abuse of those powers) should not be ignored. In addition, the EDPB highlights that surveillance measures should be subject to reviews by a court or independent administrative authorities whose decisions are binding, except where warranted through "duly justified urgency" (though after-the-event review should still occur shortly thereafter).

If the courts are not responsible for oversight mechanisms, then other responsible bodies will not be "independent" unless they are sufficiently separate from both the executive and those conducting the surveillance, and have "sufficient powers to exercise an effective and continuous control". Other relevant factors include how members of the supervisory body are appointed and their legal status (meaning that, for example, the appointment of a government minister would not be appropriate), the supervisory body's access to all materials and whether the supervisory body is open to public scrutiny.

(iv) Individuals must have recourse to effective remedies:

If individuals believe their rights have not been respected, then they must have redress to effective remedies. As a result, third-country surveillance laws that do not allow affected individuals to pursue legal remedies (e.g. to access their personal data or to have it corrected or erased), either before an independent and impartial court or other qualifying body (with the power to adopt decisions which bind intelligence services), are unlikely to satisfy this Guarantee.

The EDPB also identifies that, unless and until notifying individuals about the collection and processing of their personal data would jeopardise lawful surveillance activities, individuals should be notified of the surveillance, and in particular, when the surveillance is completed. This is because if individuals do not know that their personal data is being collected or that certain surveillance has been carried out in respect of them, they would have no effective recourse because they would not be aware of the surveillance.

Comment

While the Recommendations help in assisting data exporters to understand the types of surveillance issues they need to consider when using SCCs, certain practical issues remain.

Firstly, the EDPB acknowledges that the Recommendations and Guarantees are not exhaustive – they are only "elements" or minimum levels to consider when determining whether the surveillance laws of third countries prevent essentially equivalent protections for personal data to those provided in the EU. The Guarantees require interpretation by controllers (which may result in subjective differences of opinion and inconsistent approaches) and it is somewhat frustrating that the EDPB has failed to provide a definitive list of factors which must be satisfied for continued use of the SCCs to be valid (although this failure may reflect the difficulty in making such assessments in practice).

Secondly, the Recommendations appear to far exceed what most businesses could diligence regularly and consistently in the usual course, and it seems unrealistic to expect most businesses to be able to form watertight analyses regarding third-country surveillance laws. These are complex and difficult issues, particularly for SMEs, which raises the question of why such a heavy burden is being imposed on controllers when the invalidation of the Privacy Shield adequacy decision suggests that the European Commission itself has struggled with this issue. The European Commission is responsible for establishing through adequacy decisions a white list of third countries with essentially equivalent regimes for protecting personal data and associated rights, so it is difficult to see why the Commission should not also be responsible for determining and maintaining an additional list of countries which categorically do not provide essentially equivalent protections in so far as surveillance measures are concerned.

It is also important to keep in mind that the issues raised in Schrems II apply equally to other safeguards under the GDPR, including Binding Corporate Rules. Given that the derogations contained in the GDPR are rarely workable in a commercial context, controllers may find themselves in a position where they lack certainty as to whether they are compliant with the GDPR's international transfer restrictions. The issues here may, to some extent, be resolved by the EDPB's recommendations on supplementary measures, once formally adopted – though if they do not adequately address how the most frequent international business transfers are conducted (such as transfers to SaaS and cloud service providers in the US or intra-group transfers to US parent companies), then we may be heading (perhaps unwittingly) towards EU data localisation.