



## **Transfer of Data to Third Countries**

Transfer of data to third countries is a politically sensitive subject. The Regulation is trying to serve two goals that appear to be in conflict: protecting data and facilitating the flow of data, including to third countries outside the EU that do not provide for adequate protection of personal data.

### **General principle (Article 40)**

EDRi is concerned with a significant shift in the data protection framework from a general prohibition of transferring data to third countries (notwithstanding derogations) as contained in the Directive to the principle that transfers can only take place if enumerated conditions are met, which has been formulated in the draft Regulation. As a result, more legal grounds permitting the transfer of data to outside the European Union would exist under the Regulation than exist under the Directive. EDRi would welcome a reverse trend and reintroduction of the principle that international transfers of data are, in principle, prohibited, with this prohibition being lifted when essential criteria are respected.

The draft Regulation attempts to clarify the grounds for the responsibility of data controllers and data processors as well as the legal basis allowing international transfers of data including onward transfers. The main problem, however, is that essential safeguards to protect personal data in this context are not sufficiently specific. This creates a serious risk of their misinterpretation, circumvention or other abuses.

### **Adequacy rule**

The adequacy rule is a delicate issue. While EDRi agrees that adequacy does not mean having the exact same rules but rather following the same (adequately enforced) principles, it seems that the Commission's proposal does not take into account the stage of practical implementation of the Regulation. The authority of the European Commission to issue adequacy decisions should be revised thoroughly. In our opinion, the possibility of issuing an adequacy decision should be limited to situations in which the unilateral decision made by the Commission will not be able to affect the level of data protection as guaranteed in the draft Regulation.

The adequacy rule has become bureaucratic and the examination procedure seems to be about looking only at the legislation and not at the way it is implemented – either at the time of approval or on an ongoing basis. Ongoing review must become part of the adequacy procedure. The wording of this provision should be more detailed and rigorous. In many cases, these issues are so important and so closely associated with the protection of fundamental rights that they cannot be regulated solely by a judgement made by the European Commission. The problem is that the Commission is both judge and jury. It would be valuable, also for the credibility of the process, to include additional checks and balances, such as review or appeal possibilities being given to the Data Protection Board and/or national Data Protection Authorities. Giving at least the right to veto on the adequacy decision to the Data Protection Board would eliminate the criticism that there is no counter-balance to the Commission's decisions. Another issue that calls for a more detailed approach is the examination procedure. Experience shows that the formal "examination procedure" implemented by the European Parliament is not, on its own, an adequate safeguard.

## **Transfers by way of appropriate safeguards**

Experience shows that standard clauses do not provide sufficient protection of personal data. Adequate safeguards are necessary; article 42 needs to be more specific and prescriptive. An approach requiring a prior approval from Data Protection Authorities (such as the one foreseen in Article 42(5)) would therefore be preferred for all transfers based on contractual clauses and not only for transfers that take place without a legally binding instrument in place.

## **Existing safeguards**

The Regulation leaves existing adequacy decisions as well as the Safe Harbor framework intact. This is a missed opportunity to reform existing agreements, most particularly the Safe Harbor framework, which has been an unequivocal failure, offering little or no meaningful protection of European data subjects' data.

Standard protection clauses are not sufficient, and more adequate safeguards are necessary.

## **Binding corporate rules**

Binding corporate rules (BCRs) open the way for private arrangements for the protection of exported data and made-to-measure solutions for groups of undertakings. Rules adopted by means of BCRs are not clear to data subjects and thus raise significant transparency issues. The safeguards provided by BCRs are frequently weak and ultimately promise something that cannot be delivered – control by the data controller over data that they have limited practical control over. EDRi believes that rules on BCRs should be revised and strengthened significantly in order to prevent them from being used as a way to legally circumvent obligations without offering appropriate guarantees.

In addition, Paragraph 43(2)d should be amended to include data minimisation, storage periods and purpose limitation.

## **Derogations**

Article 44 contains a number of derogations that are too vague. There is a clear risk that the protection against real risks associated with transfer of personal data to third countries will be weakened by these broad derogations. Moreover, it should be expected that data controllers will be tempted to rely on derogations instead of providing for appropriate safeguards before deciding to transfer personal data.

The wording of Article 44(1)(d), for example, should be more specific. “Public interest” is too broad, while recital 87 seems to extend the scope of this derogation even more. The range of grounds that may come under a vague label of public interest is therefore clearly too broad, thus creating legal uncertainty for data subjects.

Article 44(1)(h) is specifically of a great concern because it creates endless possibilities for transfers of personal data to third countries. The meaning of “legitimate interest”, as a legal ground for processing, has proven to be extremely broad, thus undermining the protection of data subjects. The draft Regulation should prevent the transfer of personal data from taking place on this vague basis. This problem could be made even worse by the lack of consistency between Data Protection Authorities while applying this general clause in practice. EDRi therefore proposes

the deletion this paragraph.

If the derogations are not carefully re-drafted, they will also allow for transfers of data from private companies to law enforcement authorities without any, or with inadequate, safeguards, undermining the quality and predictability of the protection of the personal data of European data subjects.

When transfers of data are based on derogations, the legal ground claimed should be subject to prior approval and publicly registered. The Commission's proposed text makes it difficult, if not impossible, to guess how Data Protection Authorities will regulate the proposed derogations.

### **International cooperation**

EDRi is concerned about the international cooperation provided for in Article 45. The example of the Safe Harbour with the United States of America is a cautionary one. The FTC (Federal Trade Commission) appears to see its role as a purely bureaucratic one, only acting ex post and in cases of the largest of the breaches of the agreement. The agreement seems more symbolic than practical, doing little or nothing to protect the data subjects in the vast majority of cases. Therefore EDRi would like to express its conviction that the Safe Harbor agreement is wholly inadequate for the protection of the fundamental rights of European data subjects. The entire current EU approach to international data transfers undertaken outside the scope of adequacy findings needs to be carefully redesigned.

### **Disclosure to third countries by virtue of extra-territorial laws, regulations and other legislative instruments**

The draft Regulation in its current version does not address the challenge of data transfers to third countries by virtue of extra-territorial laws, regulations and other legislative instruments, including for the purpose of law enforcement. It should be noted that existing practice in this area is very disquieting. Specific risks are related to the processing of data in cloud computing, when the providers of such services are legally established outside the EU. For example, under the U.S. Foreign Intelligence Surveillance Act of 2008 Act (Article 1881), the U.S. government is entitled to carry out surveillance of European data subjects on the basis of their data being processed by U.S. companies. The draft Regulation does not provide for any specific guarantees in this regard while, at the same time, aims at facilitating the transfer of personal data to third countries.

In the inter-service version of the Regulation (Article 42) it was stated that in the cases of disclosure of data to third countries by virtue of extra-territorial laws, regulations and other legislative instruments prior approval/authorisation of the Data Protection Authorities is required. EDRi regrets that this important safeguard was removed in the course of the latter stages of the inter-service consultation process and urges the European Parliament and Council to re-introduce this measure. Reintroduction of this provision would provide legal certainty for both data subjects and businesses. Having this principle in a recital does not provide a sufficient safeguard for the protection of personal data. It is at best inappropriate and, at worst, a breach of the Charter on Fundamental Rights, for this issue not to be clearly and thoroughly addressed by the new Regulation.