

Brussels, 18th June 2001

Standard contractual clauses for the transfer of personal data to third countries - frequently asked questions

Directive 95/46/EC on *the protection of individuals with regard to the processing of personal data and on the free movement of such data*, requires Member States to permit transfers of personal data to countries outside the European Union only where there is adequate protection for such data, unless one of a limited number of specific exemptions applies. Where this is not the case, the transfer must not be allowed.

Without such rules, the high standards of data protection established by the Directive would quickly be undermined, given the ease with which data can be moved around on international networks.

Article 26 (4) of the Directive allows the Commission, with the support of a Management Committee composed of Member States representatives, to issue standard contractual clauses for the purpose of fulfilling the requirements set down by the Directive when transferring data to non-EU countries.

The present FAQs summarise the main issues of the Decision just adopted by the European Commission on standard contractual clauses (see IP/01/851) and provide information to individuals and companies on how to best make use of the standard contractual clauses.

Are the standard contractual clauses compulsory for companies interested in transferring data outside the EU?

No. The standard contractual clauses are neither compulsory for businesses nor are they the only way of lawfully transferring data to countries outside the EU.

First of all, organisations do not need contractual clauses if they want to transfer personal data to recipients in countries which have been recognised by the Commission as providing adequate protection of data. This is the case of transfers to Switzerland, Hungary or US based companies adhering to the Safe Harbor Privacy Principles issued by the US Department of Commerce (see IP/00/865).

Secondly, even if the country of destination does not offer an adequate level of protection, data may be transferred in specific circumstances. These are listed in Article 26 (1) and include cases where:

1. the data subject has given his consent unambiguously to the proposed transfer; or
2. the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken in response to the data subject's request; or
3. the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or
4. the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims; or
5. the transfer is necessary in order to protect the vital interests of the data subject; or
6. the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case.

Finally, under Article 26 (2) national authorities may authorise on a case by case basis specific transfers to a country not classified as offering an adequate protection where the exporter in the EU cites adequate safeguards with respect to the protection of privacy by fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights. This could be done for example by contractual arrangements between the exporter and the importer of data, subject to the prior approval of national authorities.

Can companies still rely on different contracts approved at national level?

Yes. The standard contractual clauses do not prejudice past or future contractual arrangements authorised by national Data Protection Authorities pursuant to national legislation.

Can Member States block or suspend data transfers using the standard contractual clauses?

Yes, but only in the exceptional circumstances referred to in Article 3 of the Commission Decision. These include cases where:

- (a) it is established that the law to which the Data Importer is subject obliges him to derogate from the relevant data protection rules beyond the restrictions necessary in a democratic society as provided for in Article 13 of Directive 95/46/EC where those derogations are likely to have a substantial adverse effect on the guarantees provided by the standard contractual clauses, or
- (b) a competent authority has established that the Data Importer has not respected the contractual clauses, or
- (c) there is a substantial likelihood that the standard contractual clauses in the annex are not being or will not be complied with and the continuing transfer would create an imminent risk of grave harm to the Data Subjects.

It is expected that this safeguard clause will be very rarely used as it caters for exceptional cases only. As provided for in Article 3 (3) of the Decision, the European Commission will be informed of any use made by the Member States of this safeguard clause and will forward the information received to other Member States. The Commission may take appropriate measures in accordance with the procedure laid down in Article 31 (2) of Directive 95/46/EC.

Can companies implement the standard contractual clauses in a wider contract and add specific clauses?

Yes. Parties are free to agree to add other clauses as long as they do not contradict, directly or indirectly, the standard contractual clauses approved by the Commission or prejudice fundamental rights or freedoms of the data subjects. It is possible, for example, to include additional guarantees or procedural safeguards for the individuals (e.g. on-line procedures or relevant provisions contained in a privacy policy, etc.). All these other clauses that parties may decide to add would not be covered by the third party beneficiary rights and would benefit from confidentiality rights where appropriate.

Member States may also further specify or complete the Appendix annexed to the contract.

In all cases, the standard clauses have to be fully respected if they are to deploy the legal effect of providing for an adequate safeguard for the transfer of personal data as required by the EU Directive.

Can Data Importers be exempted from the application of the mandatory principles to fulfil their obligations under national law?

Yes, as provided for in the closing paragraph of the mandatory principles they may do so as long as they are not confronted with mandatory requirements that go beyond what is necessary in a democratic society, namely because they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions; an important economic or financial interest of the State or the protection of the Data Subjects or the rights and freedoms of others.

What does joint and several liability mean?

Joint and several liability means that, when data subjects have suffered damage as a consequence of the violation of the rights conferred on them by the contract, they are entitled to obtain compensation from either the Data Exporter or the Data Importer or both.

Without joint and several liability, the data protection safeguards provided for by the standard contractual clauses would be severely diminished. Finding ways of ensuring that the rights of data subjects – who are not parties to the contracts – are adequately safeguarded – was the principal challenge of preparing this Decision.

When trying to enforce their rights under a contract between two data controllers, one inside and one outside the EU, data subjects are faced with two main difficulties. First, when a data subject becomes aware of a violation of his/her data protection rights, it is often very difficult to know exactly who is responsible for the violation. Was data unlawfully disclosed by the Data Exporter before the transfer took place or by the Data Importer after the transfer? Joint and several liability prevents this uncertainty from becoming an obstacle to the pursuit of the claim for compensation.

Secondly, even if the data subject knows that the violation has been committed by the importer, it may be very difficult in practical terms for him to enforce the contract and obtain compensation from the importer outside the EU. Submitting the importer to European jurisdiction does not completely solve the problem, because the recognition and enforcement of rulings of EU courts is not always possible in the country where the importer is established. In any case, it is much more straightforward to pursue the claim against the data exporter, who is established in the EU.

But will this not produce unfair burdens on exporters and/or importers who have done nothing wrong?

No. Several steps have been taken to ensure that this is avoided. In particular the scope and applicability of joint and several liability is strictly limited. It only applies to violations of those clauses which produce rights for data subjects (see the “third party beneficiary clause”, Clause 3) and only in cases where it is necessary to compensate individuals for damage resulting from the violation.

As a result, various scenarios which have been of concern to industry commentators during the preparation of the Decision are clearly excluded. For instance, companies outside the EU have objected that they might be held responsible and brought to court in the EU for the Data Exporter's violations of the national law (unlawful processing operations) taking place before the data transfer, but this is excluded by the limited scope of Clause 3.

Companies within the EU, on the other hand, are concerned that they may be required to compensate data subjects for damage resulting from a violation committed by the data importer. This effect is offset by the mutual indemnification clause which, in such a case, would give the exporter the right to recover from the importer any compensation it has had to pay to the data subject. The general rule is that every party to the contract is responsible for his/her acts *vis-à-vis* the data subject.

It may be argued that claiming indemnification will in itself be a burden for exporters. This is recognised, but it is considered fairer to place this burden on exporters rather than on individuals, who will often have had nothing to do with the transfer. Moreover, if the effect of seeking to avoid any such burdens is to make data exporters choose more carefully their data importers this is a wholly welcome effect.

Can US-based organisations that have joined the ‘Safe Harbor’ use the standard contractual clauses to receive data from the EU?

As a general rule, standard contractual clauses are not necessary if the data recipient is covered by a system providing adequate data protection such as the ‘Safe Harbor’. However, if the transfer concerns data that is not covered by their ‘Safe Harbor’ commitments, use of the standard contract clauses is one way of providing the necessary safeguards.

Can US-based companies that have not joined the ‘Safe Harbor’ use the relevant ‘Safe Harbor’ rules under the contract?

Yes, provided that they also apply the three mandatory data protection principles in the Annex (applicable to all countries of destination): the purpose limitation, restrictions on onward transfers and the right of access, rectification, deletion and objection.