Transfers of Personal Data to Third Countries or International Organisations

An Coimisiún um Chosaint Sonraí
Data Protection Commission

Flows of personal data to and from the European Union (the "EU") are necessary for international trade and international co-operation. However, the transfer of such personal data from the EU to controllers and processors located outside the EU in third countries should not undermine the level of protection of the individuals concerned, with a third country being any country outside the European Economic Area (the "EEA"). Therefore, transfers to third countries or international organisations should be done in full compliance with Chapter V of the General Data Protection Regulation, the "GDPR".

This note provides summary guidance on the provisions in Chapter V of the GDPR, as well as links to more detailed information and guidance.

Article 45 – Transfers on the Basis of an Adequacy Decision

The first thing to consider when transferring personal data to a third country is if there is an "adequacy decision". An adequacy decision means that the European Commission has decided that a third country or an international organisation ensures an adequate level of data protection.

When assessing the adequacy of the level of protection, the European Commission takes into account elements such as the laws, respect for human rights and freedoms, national security, data protection rules, the existence of a data protection authority and binding commitments entered into by the country in respect of data protection.

The adoption of an adequacy decision involves:

- ✓ a proposal from the European Commission
- ✓ an opinion of the European Data Protection Board ("EDPB")
- ✓ an approval from representatives of EU countries
- ✓ the adoption of the decision by the European Commissioners

The effect of such a decision is that personal data can flow from the EEA to that third country without any further safeguard being necessary. In other words, the transfer is the same as if was carried out within the EU.

A list of countries with an adequacy decision can be found here.

Article 46 – Transfers Subject to Appropriate Safeguards

In the absence of an adequacy decision, the GDPR does allow a transfer if the controller or processor has provided "appropriate safeguards". These safeguards may include:

- ✓ **Standard data protection clauses**: For the majority of organisations, the most relevant alternative legal basis to an adequacy decision would be these clauses. They are model data protection clauses that have been approved by the European Commission and enable the free flow of personal data when embedded in a contract. The clauses contain contractual obligations on the Data Exporter and the Data Importer, and rights for the individuals whose personal data is transferred. Individuals can directly enforce those rights against the Data Importer and the Data Exporter. These are known as the '**standard contractual clauses**'. There are two sets of standard contractual clauses for restricted transfers between a controller and controller, and one set between a controller and processor (linked here). The European Commission has advised the EDPB that it plans to update the existing standard contractual clauses for the GDPR. Until then, EU-based data controllers can still enter into contracts that include the standard contractual clauses based on the EU Directive 95/46/EC, which pre-dated the GDPR.

- ✓ **Binding corporate rules "BCRs":** BCRs form a legally binding internal code of conduct operating within a multinational group, which applies to transfers of personal data from the group's EEA entities to the group's non-EEA entities. This group may be a corporate group or a group of undertakings engaged in a joint economic activity, such as franchises or joint ventures. BCRs are legally binding data protection rules with enforceable data subject rights contained in them, which are approved by the competent Data Protection Authority. There are two types of BCRs which can be approved - BCR for Controllers which are used by the group entity to transfer data that they have responsibility for such as employee or supplier data; and BCR for Processors which are used by entities acting as processors for other controllers and are normally added as an addendum to the Service Level Agreement or Processor contract. Further provisions on the use of BCRs as an appropriate safeguard for personal data transfers are set out in GDPR Article 47.

- ✓ **Approved Codes of Conduct:** The use of Codes of Conduct as a transfer tool, under specific circumstances, has been introduced by the GDPR in Article 40 (3). Codes are voluntary and set out specific data protection rules for categories of controllers and processors. They can be a useful and effective accountability tool, providing a detailed description of what is the most appropriate, legal and ethical behaviour within a sector. From a data protection viewpoint, codes can therefore operate as a rulebook for controllers and processors who design and implement GDPR-compliant data processing activities that give operational meaning to the principles of data protection set out in European and national law. Codes of Conduct that relate to personal data processing activities by controllers and processors in more than one EU Member State, and for which the EU Commission has adopted an implementing act, together with binding and enforceable commitments of the controller or processor in the third country, could be used as a transfer tool in the future. The EDPB is planning to issue

separate specific guidance, in relation to the use of Codes of Conduct as a transfer tool, at a later date.

- ✓ **Approved certification mechanisms:** Certification is defined by the ISO *as "the provision by an independent body of written assurance (a certificate) that the product, service or system in question meets specific requirements".* Therefore, as introduced in the GDPR in Article 42 (2), certification mechanisms may be developed to demonstrate the existence of appropriate safeguards provided by controllers and processors in third countries. These controllers and processors would also make binding and enforceable commitments to apply the safeguards including provisions for data subject rights. The EDPB is also planning to issue separate specific guidance on the use of certification mechanisms as a transfer tool.

- ✓ **A legally binding and enforceable instrument between public authorities or bodies**: An organisation can make a restricted transfer if it is a public authority or body and is transferring to another public authority or body, and with both public authorities having signed a contract or another instrument that is legally binding and enforceable (Article 46 (2)(a) GDPR). This contract or instrument must include enforceable rights and effective remedies for individuals whose personal data is transferred. This is not an appropriate safeguard if either the transferring organisation or the receiver is a private body or an individual. If a public authority or body does not have the power to enter into legally binding and enforceable arrangements, it may consider an **administrative arrangement** that includes enforceable and effective individual rights instead (Article 46 (3)(b) GDPR). The EDPB is currently working on updated guidance in relation to these transfer tools.

Article 49 – Derogations for Specific Situations

Derogations under Article 49 are exemptions from the general principle that personal data may only be transferred to a third country if an adequate level of protection is provided for in that third country. A Data Exporter should first endeavour to frame transfers with one of the mechanisms guaranteeing adequate safeguards listed above, and only in their absence use the derogations provided in Article 49 (1). These derogations or exceptions allow transfers in specific situations, such as based on consent, for the performance or conclusion of a contract, for the exercise of legal claims, to protect the vital interests of the data subject where they cannot give consent or for important reasons of public interest. The EDPB guidance document on these derogations should always be consulted to ensure that they could be relied upon for the specific scenarios that organisations are dealing with.