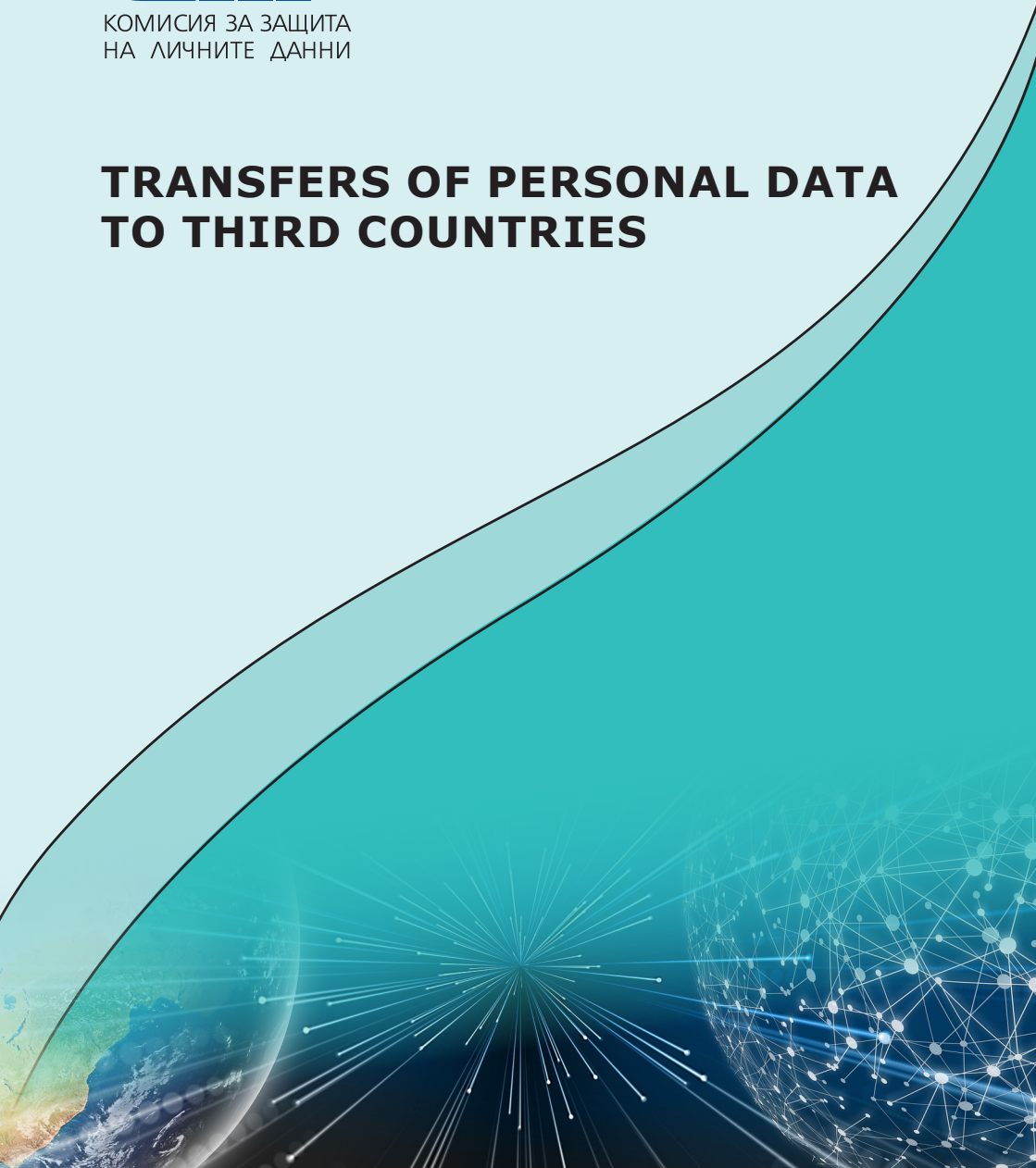
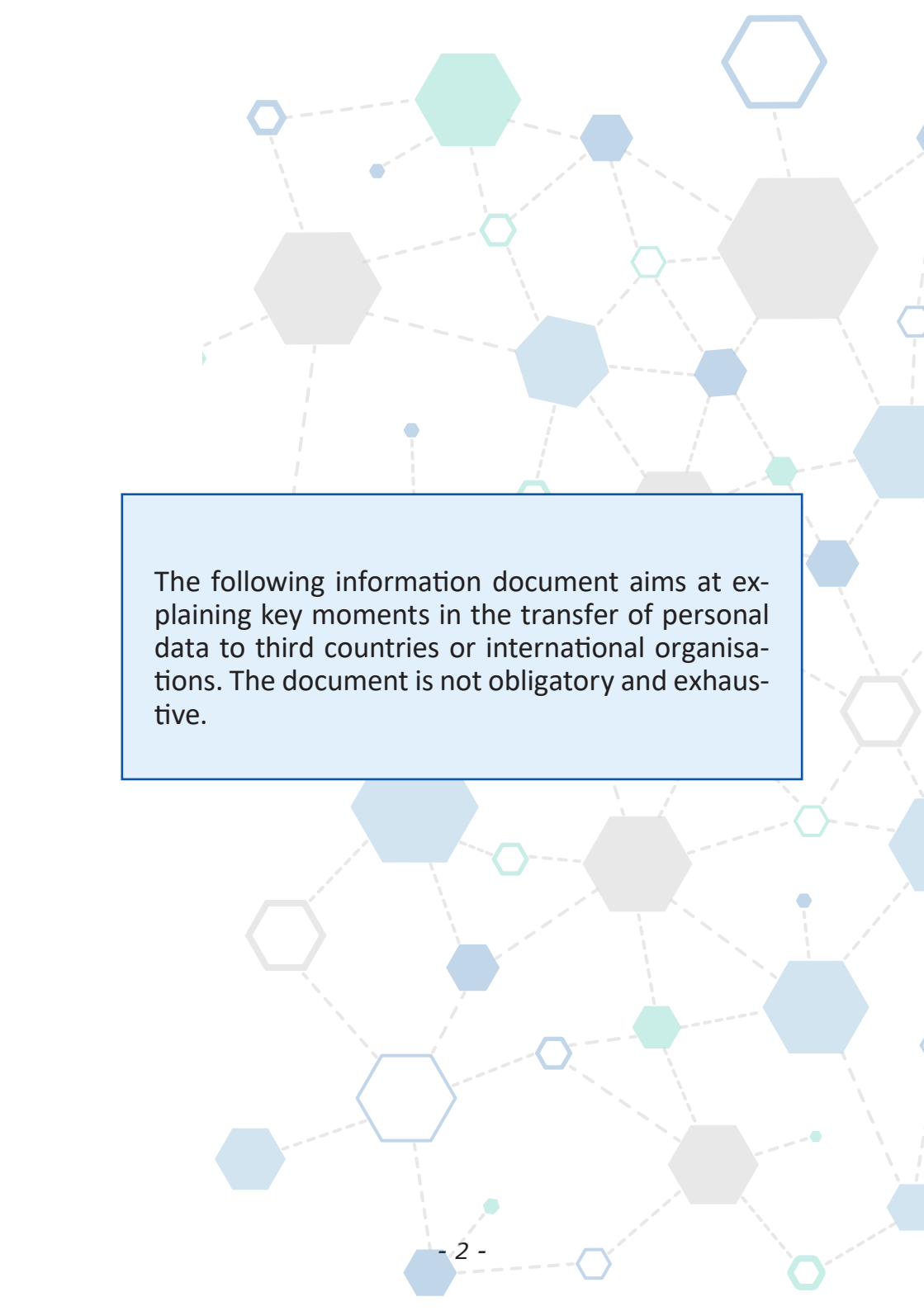


КОМИСИЯ ЗА ЗАЩИТА
НА ЛИЧНИТЕ ДАННИ

TRANSFERS OF PERSONAL DATA TO THIRD COUNTRIES





The following information document aims at explaining key moments in the transfer of personal data to third countries or international organisations. The document is not obligatory and exhaustive.

What is the transfer of personal data?

The transfer of personal data occurs when the data of member states citizens or persons, staying on EU territory are processed or are intended for processing after being provided to third countries or international organisations.

The transfer of personal data to third countries or international organisations is performed only after complying with the requirements, foreseen in Chapter V of the Regulation (EU) 2016/679, General Data Protection Regulation (GDPR).

The transfer of personal data transfer for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties within the scope of Directive (EU) 2016/680 is performed under the conditions, set in Chapter VIII of the Personal Data Protection Act (PDPA).

What does "third country" means?

This is every country outside the European Union or the European Economic Area. The General Data Protection Regulation requires the application of measures for permanent protection of personal data, transferred to "third countries/parties", i.e. countries outside of EU/EEA.

GDPR and transfers of personal data to third country

The GDPR identifies three complementary criteria, defining the processing activities as international transfer:

- Personal data controller or processor, which specific processing activity falls within the GDPR scope;
- Personal data controller or processor ("exporter") discloses via transfer or submits by other means personal data to other controller, joint controller or processor ("importer").
- The importer is established in a third country or is an international organisation with regard to the specific processing.

Rules on transfer of personal data

In cases of the transfer of personal data from Bulgaria (or other EU member state) to third countries and/or international organisations, it could be performed only if the data controller or processor fulfil the conditions or comply with the personal data transfer rules, defined in Chapter V of the GDPR, namely:

- on the ground of European Commission's decision on the adequacy level of protection under the GDPR;
- if "appropriate safeguards" are provided via other tools for the transfer of personal data to third countries (Binding Corporate Rules, Standard Contractual Clauses, Codes of Conduct, Certification mechanisms, seals or personal data markings);
- when some of the above requirements are missing via "derogations for specific situations", when the transfer is performed as exception.

Transfer of personal data based on an adequacy decision

Under Article 45 of the GDPR, the European Commission has the power to determine, whether a transfer of personal data to third country can be performed if this country offers an adequate level of data protection. After the adoption of the relevant third country Adequacy decision transfers can be carried out (on its territory, in particular sectors) and with this decision is guaranteed the adequate level of protection. In such situation no alternative data transfer tool under Art. 46 of the GDPR is needed.

List of the countries with adequate level of protection can be found on [here](#)

However, the existence of decision on the adequate level of protection is not a basis to restrict the data subjects' right to file complaint. It does not restrict the supervisory authorities to investigate or refer to a national court when doubts about the decision's validity exist, which is established by the Court of the EU.

Important: The personal data controller or processor should periodically monitor the current status of the decision on the adequacy level of protection (under Regulation (EU) 2016/679 or Directive (EU) 2016/680) based on which the personal data will be transferred in order to guarantee the equivalent level of protection in the specific third country in accordance with the EU law.

Transfer of personal data based on appropriate safeguards

By regular or repetitive data transfer lacking decision on the adequate level of protection, it should be relied on some of the transfer tools, referred to in Art. 46 of the GDPR. The personal data controller should provide “adequate safety measures/appropriate safeguards”, as well as, guarantee the “aplicable rights” of the data subjects and the effective legal safeguards. These measures can include:

- *Binding corporate rules (BCR)* are internal personal data protection rules, defining the personal data protection policy in multinational group of entities/companies, established in EEA, to companies outside EEA. BCR is a whole system for compliance, including observance of policies and procedures, audits, complaints handling and training within the organization. Every company from the group of entities, in its capacity as personal data controller should comply or be able to provide compliance with the BCR. [More...](#)

- *Standard Contractual Clauses (SCC)* are contractual clauses used as a tool for third country data transfer in accordance with the GDPR. They contain contractual obligations for the data exporter and importer with regard to the protection of the rights of the individuals, whose personal data is transferred. They also represent appropriate safeguards in case of third countries transfers. The SCC are approved and adopted by the European Commission. [More...](#)

- *The Codes of Conduct* are voluntary audit tool for the personal data controllers and processors implementing

specific and appropriate safeguards/data protection rules in specific field or in connection with particular processing operations. The Codes can help the organisations (for example: micro, small and medium-sized enterprises) to guarantee the compliance with the best practices and rules and thus to ensure effective application of the GDPR, as well as, to serve for third countries data transfer basis. [More...](#)

Important: The organisations responsible for the application of the supranational codes should submit for review the draft Code of Conduct to the data protection supervisory authority. After its review, the Code is sent for approval to all concerned supervisory authorities and to EDPB for complete content evaluation in accordance with Articles 40 and 41 of the GDPR.

- Certification mechanisms, seals and data protection markings, which are voluntary tool, used to prove the application of the appropriate data protection safeguards in accordance with GDPR. They allow the data subjects to quickly assess the data protection level of specific products and services. [More...](#)

Important: The personal data controller/processor should evaluate the legislation of the third country to which the personal data will be transferred. The necessity of implementing "supplementary measures" in order to guarantee the essentially equivalent level of protection in the specific third country, as required by the EU law, can arise irrespective of the used transfer tool.

Third countries data transfer tools after "Schrems II"

The Court of EU decision refers to all appropriate safeguards under Art. 46 of Regulation (EU) 2016/679, which are applied for data transfer from the European Economic Area (EEA) to any third country. The US legal regulations specified by the Court (Art. 702 of the Foreign Intelligence Surveillance Act (FISA) and Executive order 12 333) apply to any transfer to the U.S. via electronic means that falls under the scope of this legislation, regardless of the transfer tool used for the transfer.

In order for the personal data controller to continue the third countries data transfer after the Court decision, it should analyse individually the third country protection level, which should be essentially equivalent to that guaranteed within the EU. This way it could be determined, whether the SCC or the BCR can be applied in practice and whether it is necessary to implement supplementary measures, as well as, whether the third country law does not contradict the foreseen supplementary measures, which could influence their effectiveness. [More...](#)

Third countries personal data transfer tools based on derogations

By incidental and non-repetitive data transfer you can refer to any of the derogations foreseen in Art. 49 of the GDPR. For example on the basis of consent by the data subject; for performance or conclusion of contracts; for protection of data subject's vital interests, where the individual is incapable of giving his/her consent. [More...](#)

Seven practical steps for the transfer of personal data to third countries, which the exporter should perform:

Step 1: To be aware of the place, where the subjects data will be transferred to in order to guarantee the essentially equivalent level of protection.

Step 2: To check whether the country has a decision on adequacy, adopted by the European Commission.

Step 3: To check which personal data transfer tool, defined in Chapter V of the GDPR is appropriate in the specific case.

Step 4: To assess whether the third country legislation or practice could impact the used transfer tools with regard to the specific transfer.

Step 5: To identify and adopt supplementary measures in order to ensure the level of data protection is in compliance with the GDPR, i.e. with the EU equivalent standard.

Step 6: To undertake formal procedural steps after defining effective supplementary measures. These are measures, complementing the third countries personal data transfer tools under Art. 46 of the GDPR.

Step 7: To periodically evaluate the level of protection and to monitor for changes, which could have relation to the data transfer in specific third country.



Commission for Personal Data Protection

Address: 2 Prof. Tsvetan Lazarov Blvd.

Sofia 1592

E-mail: kzld@cpdp.bg

Web-site: www.cpdp.bg