Transfer of personal data to a foreign country

05.06.2018

These materials are being changed according the new data protection regulation.

Transfer of personal data to a foreign country with an adequate level of data protection

It is permitted to transfer personal data from a database located in Estonia to a foreign country which provides an adequate level of data protection. The prerequisite for the attainment of an adequate level of data protection is the transposition of the requirements of the Data Protection Directive 95/46/EC and the creation of the necessary organizational and legal conditions through the instrument of national law to ensure the respect and protection of privacy and other fundamental rights and freedoms in the course of data processing.

The transfer of personal data is permitted to the 28 Member States of the European Union and to the European Economic Area member countries (Norway, Iceland, Lichtenstein). The rest of the foreign countries are often referred to as "third countries". It is permitted to transfer personal data to a third country, if its level of data protection is deemed to be sufficient by the European Commission. The level of data protection is assessed in the light of all the circumstances surrounding the transfer operation or set of transfer operations. Particular consideration is given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.

Commission decisions on the adequacy of the protection of personal data in third countries can be found at the following web address:
http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm [1]

The fact that a foreign country ensures an adequate level of data protection does not signify that personal data can be transmitted to that country without any restrictions. It merely means that the transfer does not require additional guarantees for the protection of the data subject's rights and privacy. Transfers of personal data to countries with a sufficient level of data protection can only be carried out on adequate legal grounds, such as:

- the data subject has given their informed consent (Personal Data Protection Act § 12). When the data subject's personal data are intended to be transferred to a foreign country, then prior to seeking the data subject's consent for the processing of their personal data, the chief processor or authorized processor is required to notify the data subject, among other things, of the fact that their personal data will be transferred to a foreign country.

- the person to whom the data are transmitted processes personal data for the performance of duties prescribed by law (Personal Data Protection Act § 14-2-1)

- the transfer is necessary for the protection of the life, health or freedom of the data subject or another person (Personal Data Protection Act § 14-2-2)

- a third person requests information which was obtained or created upon performance of public duties provided by law or legislation issued on the basis thereof and the access to such information is not restricted (Personal Data Protection Act § 14-2-3)

Thus, the transfer of personal data to a foreign country with an adequate level of data protection can be carried out under the same conditions as are applicable to transmission within Estonia. It is crucial to take into consideration the data processor's duties of ensuring the availability of information on the transfer of personal data (when, to whom and which personal data were transmitted), guaranteeing the storing of personal data in unaltered form (Personal Data Protection Act § 25-2-5) and preventing unauthorised reading, copying, modification or deletion of personal data during their transmission by means of data communication equipment and during the transportation of data storage devices (Personal Data Protection Act § 25-2-6). It is also necessary to take into consideration the data protection legislation of a target country. Such legislation might, for instance, require notification of the data protection supervision authority.

Transfer of personal data to a foreign country without an adequate level of data protection

Under Article 26 of the Data Protection Directive 95/46/EC, the Member States may authorize a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2), where the chief processor adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights; such safeguards may in particular result from appropriate contractual clauses.

Under Paragraph 18 (3) of the Personal Data Protection Act, personal data may be transmitted to a foreign country which does not ensure an adequate level of protection only with the permission of the Data Protection Inspectorate:

1) if, in this particular case, the chief processor guarantees the protection of the data subject's rights and privacy in that country;

2) if, in this particular case of personal data transmission, the sufficient level of data protection is ensured in the country. The level of data protection should be assessed in the light of all the circumstances surrounding the transfer of data, including the content of the data, the purpose and duration of the proposed processing operation(s), the country of origin and country of final destination, and the law in force in the country in question.

In order to obtain permission, the chief processor who intends to transfer personal data to a foreign country with an insufficient level of data protection (data exporter) is required to submit the following documents and information to the Data Protection Inspectorate:

1. a request for permission to transfer personal data to the data processor established in the third country specifying the identities of the requesting party (data exporter) and the data processor established in a third country (data importer), the name of the third country, the purpose and duration of the data transfer operation for which permission is being sought.

2. a certification that the data processor in the third country will process personal data solely for the purpose and to the extent permitted by law.

3. a certification that, in this particular case, the chief processor guarantees the protection of

the data subject's rights in the third country and that, for this particular case of data transfer, this country ensures an adequate level of data protection (a copy of the contract concluded with the data processor in the third country and other instruments and documents that the data processor deems necessary to submit)

The Data Protection Inspectorate shall process the request and grant permission or refuse to grant permission without assigning any reason within 30 days of receiving the request. When necessary to additionally ascertain certain facts during the consideration of the request, the Data Protection Inspectorate may extend the time period for processing the request for up to 60 days. The requesting party shall be notified of the extension in writing.

Standard contractual clauses for the transfer of personal data to countries which do not ensure an adequate level of data protection

When third countries do not provide adequate protection for data, the chief processor is required to guarantee the protection of the data subject's rights and privacy in this country in this particular case, compensating for the lack of an adequate level of protection through specific measures. The aim of specific measures is to guarantee due protection of personal data even after their transfer to the country of destination. One of these measures are the appropriate contractual clauses pursuant to which the data recipient established in a country which does not ensure an adequate level of data protection undertakes to comply with the requirements laid down in the Data Protection Directive.

General requirements for such contracts derive from Commission Decision 2001/497/EC of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries under Directive 95/46/EC, Commission Decision 2004/915/EC amending Decision 2001/497/EC and Commission Decision 2002/16/EC of 27 December 2001 on standard contractual clauses for the transfer of personal data to processors established in third countries, under Directive 95/46/EC.

Commission Decision 2001/497/EC [2]

Commission Decision 2004/915/EC amending Decision 2001/497/EC [3]

Commission Decision 2002/16/EC [4]

The standard contractual clauses are only one of several possibilities under Directive 95/46/EC, together with Article 25 and Article 26(1) and (2), for lawfully transferring personal data to a third country. It will be easier for organisations to transfer personal data to third countries by incorporating the standard contractual clauses in a contract. The standard contractual clauses relate only to data protection. They can thus be combined with other contractual clauses or stand alone as a separate instrument.

Data should be processed and subsequently used or further communicated **only for specified purposes** and should not be kept longer than necessary. The data subject should be guaranteed the right to access all data relating to him and, if necessary, to rectify, erase or block certain data. The transfer should be permitted only if it is guaranteed that data subjects are given proper information and have the opportunity to object, or in certain cases to withhold their consent.

The standard contractual clauses should be enforceable not only by the organizations and persons which are parties to the contract, but also by the data subjects, in particular, where the data subjects suffer damage as a consequence of a breach of the contract. The law governing the contract should

be the law of the Member State in which the data exporter is established, enabling a third-party beneficiary to enforce a contract. Data subjects should be allowed to be represented by associations or other bodies if they so wish and if authorised by national law.

The Data Protection Inspectorate may exercise their powers under the Directive to prohibit or suspend data flows to third countries in order to protect individuals with regard to the processing of their personal data in cases where:

(a) it is established that the law to which the data importer is subject imposes upon him requirements to derogate from the applicable data protection rules where those requirements are likely to have a substantial adverse effect on the guarantees provided by the standard contractual clauses; or

(b) 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 complied with and the continuing transfer would create an imminent risk of grave harm to the data subjects.

The prohibition or suspension shall be lifted as soon as the reasons for the suspension or prohibition no longer exist.

The standard contractual clauses should provide for the technical and organisational security measures that a data processor established in a third country not providing adequate protection must apply in order to ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected. Parties should make provision in the contract for those technical and organisational measures which, having regard to applicable data protection law, the state of the art and the cost of their implementation, are necessary in order to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access or any other unlawful forms of processing.

The data importer should process the transferred personal data only on behalf of the data exporter and in accordance with his instructions and the obligations contained in the clauses. The data importer cannot disclose the personal data to a third party unless authorized to do so by the contract. The data exporter should instruct the data importer throughout the duration of the data processing service to process the data in accordance with his instructions, the applicable data protection laws and the obligations contained in the clauses. The transfer of personal data to processors established outside the Community does not prejudice the fact that the processing activities should be governed in any case by the national data protection law.

It is the duty of Estonian entrepreneurs to guarantee that:

- the processing and transfer of personal data is carried out in accordance with the requirements set out in the Personal Data Protection Act;
- in the case of sensitive data transfer, the data subject is specifically notified thereof;
- the data subject has access to the contract on the basis of which the data transfer is carried out;
- the data subject's requests pertaining to the circumstances surrounding the data transfer are processed without delay;

- the Data Protection Inspectorate is provided with the necessary information concerning the data transfer.

Derogations

Under the Data Protection Directive 95/46/EC it is forbidden to transfer personal data to third contries where an adequate level of data protection is not ensured. Derogations are allowed on condition that:

a) the data subject has given his consent unambiguously to the proposed transfer; or

b) the transfer is necessary for the performance of a contract between the data subject and the chief processor or the implementation of precontractual measures taken in response to the data subject's request; or

c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the chief processor and a third party; or

d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims; or

e) the transfer is necessary in order to protect the vital interests of the data subject; or

f) the transfer is made from a register which according to 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.

Similar derogations from the prohibition to transfer personal data to third countries which do not ensure an adequate level of data protection are set out in the Personal Data Protection Act. Under Paragraph 18 (5) of the Personal Data Protection Act, the Data Protection Inspectorate may authorise the transfer of personal data to a foreign country where an adequate level of data protection is not ensured:

1. if the data subject has given his consent pursuant to Paragraph 12 of this Act;

2. in cases provided for in Paragraph 14-2-2 ja 14-2-3 of this Act;

Source URL: https://www.aki.ee/en/guidelines/transfer-personal-data-foreign-country

Links:
[1] http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm
[2] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32001D0497:en:NOT
[3] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004D0915:EN:HTML
[4] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0016:EN:HTML