

Hanoi, 25th May 2018

DIGI-TEXX Vietnam - Transfer and processing of personal data in third countries: Implementation of the EU General Data Protection Regulation (GDPR), in force since 25 May 2018

Dear Sir or Madam,

On May 25th, 2018, both the Federal Data Protection Act (FDPA) and the EU Data Protection Directive 95/46/EC were replaced by the so-called "EU General Data Protection Regulation" (GDPR). Compared to the Directive 95/46/EC, the GDPR contains - amongst others - the following new aspects:

I. Data transmission to so-called "Third Countries" without a comparable level of protection under the GDPR:

Personal data may continue to be transmitted to Third Countries (here: to Vietnam) and processed there if the requirements of Art. 44-50 GDPR are complied with. In that regard, the regulations on the transfer to Third Countries (Articles 44-50 GDPR) incorporate in principle the provisions of the previously applicable EU data protection directive, with a few new features.

Specifically, a transfer of personal data to a Third Country (here: to Vietnam) is permitted under Art. 44 GDPR if the data controller and the data processor meet the conditions laid down for data transmission to Third Countries, and if the other provisions of the GDPR are also complied with.

In more detail, data transmission is permitted under the following conditions:

1. If the European Commission has officially decided that an adequate level of protection exists in the Third Country, Art. 45 (3) GDPR.
2. If the European Commission has not taken such official decision, a data controller or data processor may only transfer personal data to a Third Country provided that:
 - a. There are suitable guarantees, and enforceable rights and effective remedies are available, Art. 46 GDPR, amongst other things legally binding and enforceable instruments between public authorities or agencies, Art. 46 (2) (a) GDPR, or
 - b. Internal binding data protection regulations exist, Art. 47 GDPR, or
 - c. Standard data protection clauses exist, that have been adopted by the European Commission or the supervisory authority in a specific procedure, Art. 46 (2) (c) and (d) GDPR.
3. If neither an adequacy decision pursuant to Art. 45 (3) GDPR exists nor appropriate guarantees under Art. 46 GDPR are available, a transfer or a series of transfers of personal data to a Third Country are still permitted under the following conditions:

- a. The data subject has expressly consented to the proposed data transmission, after having been informed of the possible risks of such data transmission without the existence of an adequacy decision and without appropriate guarantees, or
- b. The data transmission is necessary for the performance of a contract between the data subject and the data controller, or for the execution of pre-contractual actions at the request of the data subject, or
- c. The data transmission is necessary for important reasons of public interest.

For DIGI-TEXX customers, depending on the specific case scenario, points 2 or 3 are usually the most relevant.

II. **Security of data processing:**

Article 32 GDPR obliges data processing companies and their subcontractors, including those in Third Countries, to *"take appropriate technical and organizational measures to ensure a level of protection commensurate with the risk"*. According to the GDPR, these measures include, amongst other things:

1. The pseudonymisation and encryption of personal data,
2. the ability to permanently ensure the confidentiality, integrity, availability and resilience of data processing systems and services,
3. the ability to rapidly restore the availability of personal data and access to them in the event of a physical or technical incident,
4. a process for the periodic review and evaluation of the effectiveness of the technical and organizational measures to ensure the security of the data processing.

To this extent, the order processing regulations are largely based on the previous system of paragraph 11 FDPA. What is new is that compliance with the obligations of the data processor to the technical-organizational measures can be evidenced by compliance with internal, binding Data Protection Regulations pursuant to Art. 40 GDPR, or by certification pursuant to Art. 42 GDPR.

III. **Requirements for Data Protection Officers:**

Articles 37-39 GDPR contain detailed requirements for the appointment, position and duties of the mandatory Data Protection Officer.

We hereby confirm that our client DIGI-TEXX is familiar with the requirements of the GDPR and has implemented them as follows:

- DIGI-TEXX has adapted "Technical and Organizational Measures" to meet the requirements of Art. 32 GDPR: Specifically, DIGI-TEXX has implemented internal, binding Data Protection Regulations, which in particular include the rules for risk management, as well as the DIGI-TEXX general security concept, adapted to the specifications of the GDPR. Further, DIGI-TEXX is already ISO 27001 / ISMS certified.
- DIGI-TEXX provides comprehensive initial security standards guidance to each individual employee, and periodically repeats these training sessions.
- DIGI-TEXX has always had a mandatory Data Protection Officer in accordance with both the requirements of the FDPA and ISO 27001 / ISMS, and the Data Protection Officer has already been trained with regards to the new requirements of the GDPR.
- DIGI-TEXX has reviewed and adjusted customer service contracts and their annexes for consistency with the GDPR requirements.
- DIGI-TEXX has adapted its trainings for employees to ensure that employees are fully aware of the requirements of the new GDPR.
- DIGI-TEXX commissions annual internal and external audits, which check compliance with above rules and processes.

We will gladly inform you of further details in a personal conversation at any time.

Sincerely,



Dr. Matthias Dühn, LL.M.

Rechtsanwalt / Foreign registered lawyer (Vietnam)