

DATA PROCESSING POLICY OF

VIS KFT.

LIMITED LIABILITY COMPANY

RELATED TO DATA TRANSFER TO FOREIGN COUNTRIES

Data processor

Company name: **VIS Korlátolt Felelősségű Társaság**

Abbreviated name: **VIS Kft.**

Registered seat: **1118 Budapest, Muskotály street 11.**

Tax No.: **25861321-2-43 (EU VAT No.: HU25861321)**

Company registration No.: **01-09-293127**

European Unique Identifier (EUID): **HUOCCSZ.01-09-293127**

CHAPTER I GENERAL PROVISIONS

1. Introduction

The Company hereby states that it performs its data processing activity – by taking the adequate internal rules, technical and organizational measures – in a way that it will comply with (including, but not limited to) the provisions of the GDPR and the Privacy Act, as well as to the related legal statutes.

CHAPTER II DATA TRANSFER TO FOREIGN COUNTRIES

2. Data transfer to foreign countries

According to the GDPR, personal data can only be transferred to third countries if the person concerned provides his/her explicit approval or if the “adequate protection” of personal data given is assured.

We take care of the safe storage and transfer of personal data of visitors and registered users. That is why we only transfer data outside the European Economic Area (EEA) (the member states of the EU, moreover Norway, Iceland and Liechtenstein), particularly to the U.S. if it complies with the data protection regulations and the method of data transfer provides adequate protection to your data.

We provide data processing services exclusively to the enterprises of the VIS Kft. group of companies registered within the European Union and the U.S.

2. Application of BCR (binding corporate rules):

Based on the Directive of the European Parliament and the Council No. 95/46/EC, the Privacy Act creates the possibility to transfer personal data to foreign countries if the data processor establishes adequate guarantees by applying BCR to protect the private life, fundamental rights and freedoms, as well as to exercise the related rights of private individuals.

3. EU-U.S. Privacy Shield:

The Committee of the European Union adopted the EU-U.S. Privacy Shield on 12th July 2016, which – in line with the requirements set out by the Court of Justice of the European Union - intends to provide real and efficient protection for the residents of the EU, the personal data of whom are transferred to the United States of America and to create a clear legal situation for those companies, for which intercontinental data transfer is essential. The EU-U.S. Privacy Shield takes care of the efficient protection of rights related to personality, provides guarantees

against data access by the government of the U.S. and sets out strict obligations to companies, which can receive personal data from the EU.

The EU-U.S. Privacy Shield is based on a declaration of compliance, as a result of which the American companies are obliged to comply with several data protection principles, namely the Principles of the EU-U.S. Privacy Shield Framework (hereinafter called: Principles). The Principles shall apply to both data controllers and data processors. Data processors must be at all times obliged in a contract to act exclusively on the basis of the instruction given by the data controller. el. Following the first declaration the companies are obliged to make a repeated declaration annually, provided that they intend to receive personal data from the EU based on the Privacy Shield.

American companies intending to use the privacy shield are obliged to register into the system at the US Department of Commerce. The obligations of companies acting on the basis of the rules of the privacy shield are governed by the so-called "data protection principles". The Department of Commerce shall liable for the management and control of the privacy shield, as well as to assure that the companies shall fulfil their obligations. The companies shall have a data protection regulation complying with the data protection principles for the certification. They also have to annually renew their "membership" existing in the privacy shield. Should they fail to do so, they cannot receive and use personal data originating from the EU in the future in this framework.

The participation of a given American company in the privacy shield can be examined on the website of the US Department of Commerce, on the list of organizations participating in the privacy shield (<https://www.privacyshield.gov/welcome>). The list contains the data of organizations participating in the privacy shield, as well as the type of personal data used and the type of services they provide.