

## Privacy notice - On the processing of personal data of natural person contacts of the senior management and business partners

### Preamble

The Data Subject must be notified about the processing prior to the start of processing. If requested, the Privacy Notice must be made available to the Data Subject in electronic or paper form. As for the management of the contracting process, if, after contracting, the Data Subject objects to processing, this may result in the cancellation of the contract.

### Processing the personal data of natural person contacts of the senior management and business partners

In compliance with the provisions of Act CXII of 2011 on Informational Self-Determination and Freedom of Information and Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (hereinafter referred to as: General Data Protection Regulation or GDPR), ATTRACT Kft. as the Data Controller hereby notifies the senior management and natural person contacts of business partners with whom it has a contractual relationship about the processing of their personal data.

#### 1. The Controller

<b>Company name of the Controller:</b>	ATTRACT Kft.
<b>Address of the Controller:</b>	H-7622 Pécs, Siklósi út 1/1.
<b>Tax number of the Controller:</b>	11777364-2-02
<b>Company registration no. of the Controller:</b>	02-09-066227
<b>Telephone number of the Controller:</b>	+36 72 551 642
<b>E-mail address of the Controller:</b>	<a href="mailto:contact@nosiboo.com">contact@nosiboo.com</a>
<b>Name of the data protection officer (if any):</b>	-
<b>Contact details of the data protection officer:</b>	-

## 2. The personal data processed

### 2.1 Categories of data processed, the purpose and legal basis of processing

Personal data	Purpose of processing	Legal basis of processing
<b>In case of a senior manager: Surname and first name, title, telephone number and e-mail address (if included in the contract)</b>	Contract management, business process support and communication	Pursuant to Article 6 paragraph (1) item (b) (performance of a contractual obligation), item (c) (performance of a legal obligation) and item (f) (legitimate interest) of Regulation (EU) 2016/679 of the European Parliament and of the Council
<b>In case of a contact person: Surname and first name, title, telephone number and e-mail address</b>	Communication regarding order fulfilment, scheduling, quality management coordination and other general administration issues	Pursuant to Article 6 paragraph (1) item (f) (legitimate interest) of Regulation (EU) 2016/679 of the European Parliament and of the Council

### 2.2 Duration of data processing (storage)

The Controller shall store the personal data in its possession for 5 (five) years after the termination of the contractual relationship. The accounting records and supporting documents generated during the contract period shall be kept by the Controller for the current year and subsequently for a period of 8 (eight) years pursuant to Section 169, paragraph (1) of Act C of 2000 on Accounting.

### 2.3 Profiling during data processing

No profiling is being performed during data processing.

## 2.4 Automated decision-making during data processing

No automated decision-making is being performed during data processing. If this changes, the Controller shall provide the Data Subject with the possibility of manual, human intervention.

## 2.5 Source of the personal data processed

The personal data processed by the Controller come directly from the Data Subject.

## 2.6 Data transfer

Data are transferred to:

Category	Company name, registered seat, activity
<b>Processors (entities performing the technical tasks related to processing operations)</b>	<p>Pintér-Audit Könyvvizsgáló Kft. (seat: H-7634 Pécs, Kovács Béla utca 6.) – Accounting</p> <p>Réder &amp; Réder Kft. (seat: H-7624 Pécs, Jurisics Miklós utca 5. 3. em. 8) – System administrator and hosting services</p> <p>DIGI Távközlési és Szolgáltató Kft. (seat: H-1134 Budapest, Váci út 35.) – Fixed-line internet services</p> <p>MiniCRM Zrt. (seat: H-1075 Budapest, Madách Imre út 13-14.) – Customer relationship management software</p> <p>Microsoft Ireland Operations Ltd. (One Microsoft Place, South County Business Park Leopardstown Dublin 18, D18 P521 / Microsoft Corporation, 15010 NE 36th Street, Microsoft Campus Building 92, Redmond, WA 98052) – MS Office365 provider</p> <p>Telenor Magyarország Zrt. (seat: H-2045 Törökbálint, Pannon út 1.) – Management of company fleet telephones</p> <p>Magyar Telekom Nyrt. (seat: H-1097 Budapest, Könyves Kálmán krt. 36.) – Provision of fixed telephone services</p>

Data are transferred to:

Category	Company name, registered seat, activity
<b>Recipients (the natural or legal person, public authority, agency or any other body with whom or to which the personal data are disclosed)</b>	GLS General Logistics Systems Hungary Csomag-Logisztikai Kft. (seat: H-2351 Alsónémedi, Európa u. 2.) – Home delivery of parcels Magyar Posta Zrt. (seat: H-1113 Budapest, Dunavirág utca 2-6.) – Postal mail delivery

Data transfers to third countries:

Category	Company name, registered seat, activity
<b>Third (non-EU) countries</b>	Microsoft Ireland Operations Ltd. (One Microsoft Place, South County Business Park Leopardstown Dublin 18, D18 P521 / Microsoft Corporation, 15010 NE 36th Street, Microsoft Campus Building 92, Redmond, WA 98052) – MS Office365 provider

In addition to the above, the personal data of the Data Subject may also be accessed by employees of the Controller to the extent and for the duration necessary for the performance of their duties at work.

## 2.7 Joint processing

There is no joint processing of data.

## 2.8 Access to personal data and data security measures

**Restriction of access:** Documentation containing personal data is handled with appropriate security measures in place, and the scope of persons authorized for access is restricted.

In the context of company processes, documentation containing personal data is stored separately in a structured system. Hardcopy documentation is stored in a lockable office. The office is equipped with an alarm system for property protection and personal safety purposes.

**Data security measures:** A business e-mail system is used in the data processing process. Cloud-based storage is protected by access right management and password protection. Data are transferred to controllers via this platform. The network is protected by virus protection and firewalls. Security backups are made at regular intervals. Personal data are stored in a structured system, in the software used by the company. Central password and access right management is in place.

The Data Controller shall choose the IT tools it uses in such a way that the data processed are accessible to those authorised to access them, their authenticity is ensured, their integrity is verifiable, and they are protected against unauthorised access.

The Data Controller's IT system and network are protected against computer fraud, espionage, sabotage, vandalism, fire and flood, computer viruses, computer intrusions and attacks that could lead to denial of service. The Data Controller ensures security through server-level and application-level protection procedures.

Electronic messages transmitted over the internet, regardless of the protocol (e-mail, web, ftp, etc.), are vulnerable to network threats that could lead to fraudulent activity or the disclosure or modification of information.

The Controller shall take all reasonable precautions to protect against such threats. It monitors systems in order to record any security discrepancies and to provide evidence of any security incidents. However, it is well known – and therefore, known to those concerned – that the internet is not 100% secure. The Data Controller is not liable for any damage caused by an indefensible attack, despite the utmost care.

## 2.9 Other data processing

The Controller informs the Data Subject that the authorities and other bodies authorised by law may contact the Controller for the purpose of providing information, communicating or transmitting data or documents. However, in this case, the Controller shall disclose personal data only to the extent strictly necessary for the purpose of the request.

## 3. Rights of the Data Subject

**Right to request and receive information** – The Data Subject has the right to request and receive information on the method of personal data processing prior to the start of processing.

**Right to rectification** – The Data Subject has the right to request the rectification of personal data, if the personal data stored at the Controller are untrue or incorrect and they can prove this.

**Right to access** – The Data Subject has the right to request from the Controller the personal data stored concerning the Data Subject.

**Right to data portability** – The Data Subject has the right to request the personal data stored concerning them digitally, in a table form.

**Right to review automated decision-making** – The Data Subject has the right to request the manual review of all processes where the Controller has used automated decision-making with legal effect concerning the Data Subject.

**Right to object** – Where the legal basis is based on legitimate interest or public authority, the Data Subject may object to the processing of their personal data, but such objection does not imply the immediate erasure of their data.

**The right to restrain** – If the Data Subject does not consider that the Controller is entitled to process their personal data, they may request the suspension of the processing during the investigation.

#### 4. Lodging complaints

The Data Subject has the right to lodge complaints with the data protection authority. The Data Subject may turn to the Hungarian National Authority for Data Protection and Freedom of Information as follows:

<b>Name:</b>	Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH) [Hungarian National Authority for Data Protection and Freedom of Information]
<b>Registered seat:</b>	H-1055 Budapest, Falk Miksa utca 9-11.
<b>Postal address:</b>	H-1374 Budapest, Pf.: 603.
<b>E-mail:</b>	<a href="mailto:ugyfelszolgalat@naih.hu">ugyfelszolgalat@naih.hu</a>
<b>Telephone number:</b>	+36 (1) 391-1400
<b>Fax number:</b>	+36 (1) 391-1410
<b>Website:</b>	<a href="https://naih.hu">https://naih.hu</a>

#### 5. Legal remedy

The provisions on legal remedy are set out in Act CXII of 2011 on Informational Self-Determination and Freedom of Information.

If the Data Subject has objected to processing, the Controller investigates the objection within the shortest time possible from the submission of such request, but within 15 days at the latest, makes a decision on the substantiation of the request and informs the applicant of the decision in writing. If the Data Subject does not agree with the decision made by the Controller, or if the Controller fails to observe the above due date, the Data Subject has the right to turn to the court within 30 (thirty) days of the communication of the decision or from the deadline specified.

In the event of the violation of their rights or in the above cases, the Data Subject may file action with a court against the Controller. The court proceeds in the action as a matter of urgency. Alternatively, such proceedings may also be brought before the court competent according to the Data Subject's residence or place of stay.

Entities or persons that otherwise have no legal capacity may also be parties to the court action. The data protection authority may intervene in the proceedings in the interest of a ruling in the Data Subject's favour.

The Controller shall compensate for any and all damage caused by the unlawful processing of the Data Subject's data or a breach of the data security requirements. If the Controller violates the Data Subject's privacy through the unlawful processing of the Data Subject's data or a breach of the data security requirements, the Data Subject may claim compensation from the Controller. The Controller is also liable for damage caused to the Data Subject by the processor, and the Controller shall also pay the Data Subject compensation for any breach of the Data Subject's personal rights by the processor.

The Controller is released from the liability for the damage caused and the obligation to pay compensation for personality rights breach if the Controller can prove that the damage was caused or the Data Subject's personal rights were violated due to a cause beyond its reasonable control and the scope of processing. The damage shall not be paid and no compensation may be claimed if the damage was caused or the violation of rights caused by the violation of the personality rights arose from the wilful misconduct or gross negligence of the Data Subject.

Date and place of entry into force: Pécs, 14 January 2022