Privacy Notice

on Data Processing Related to the Activities of ATAKÁCS Könyvelő Kft.

Introduction

This Notice ensures compliance with the rules of the General Data Protection Regulation (EU Regulation 2016/679, hereinafter referred to as GDPR) and provides information on how ATAKÁCS Könyvelő Kft. (hereinafter referred to as the Data Controller) processes the personal data of individuals in the course of performing its tasks as detailed below. It outlines the principles and regulations governing this activity and provides insight into the measures taken to protect the data used. Furthermore, it informs data subjects of their rights granted to them for the protection of their interests.

As a Data Controller (and in some cases as a Data Processor), we provide the mandatory information required under Article 13 of the GDPR as follows to data subjects and interested parties.

1. Adatkezelő adatai

Name of data controller:	**ATAKÁCS Könyvelő Kft.**
Seat address:	1065 Budapest, Révay köz 4.
Tax ID:	32653645-1-42
E-mail:	info@atakacs.hu
Phone number:	+3670 611 7254

2. Principles of Personal Data Processing

The Data Controller operates in compliance with the following principles:

- Purpose Limitation Principle: This principle defines the purpose for which the Data Controller stores and uses the personal data of natural persons in the course of its activities.
- Data Minimization Principle: The scope of processed data is appropriate for the given purpose and is limited to what is strictly necessary.
- Accuracy Principle: To ensure compliance with legal requirements and to protect the rights of data subjects, the Data Controller promptly corrects or deletes any inaccurate personal data.

As a Data Controller, we collect personal data directly from the data subjects. We accept as binding all obligations related to the protection of personal data processed in connection with our activities. These obligations help demonstrate to authorities, business partners, and affected clients that we have acted in accordance with the Regulation, the Hungarian Information Act, and other relevant regulations (Accountability Principle).

3. Key Laws Governing Our Data Processing Activities

- Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation – GDPR) on the protection of natural persons concerning the processing of personal data and on the free movement of such data, repealing Directive 95/46/EC
- Act CXII of 2011 on Informational Self-Determination and Freedom of Information (Info. Act)
- Act XLVIII of 2008 on the Basic Conditions and Certain Restrictions of Economic Advertising
- Act I of 2012 on the Labour Code
- Act CL of 2017 on the Rules of Taxation

- Act C of 2000 on Accounting

4. Definitions

- **GDPR**: Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons regarding personal data processing and the free movement of such data, repealing Directive 95/46/EC.
- **Personal Data**: Any information relating to an identified or identifiable natural person, such as an identifier (name, number, location data, online identifier) or data relating to the physical, physiological, genetic, mental, economic, cultural, or social identity of a natural person.
- **Special Categories of Data**: Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership; as well as genetic and biometric data intended for uniquely identifying a natural person, health data, or data concerning a natural person's sex life or sexual orientation.
- **Data Processing**: Any operation performed on personal data or data sets, regardless of the method used, such as collection, recording, organization, structuring, storage, alteration, retrieval, use, disclosure, transmission, alignment, restriction, deletion, destruction, or preventing further use of data, as well as capturing photos, audio, or video recordings, and recording physical characteristics suitable for identification (e.g., fingerprint or palm print).
- **Data Controller**: A natural or legal person, or an entity without legal personality, which alone or jointly determines the purposes and means of personal data processing, makes and executes decisions regarding data processing, or has these carried out by a data processor.
- **Data Processor**: A natural or legal person, or an entity without legal personality, that processes personal data on behalf of the Data Controller.
- **Data Subject**: Any natural person who is identified or identifiable based on specific personal data—either directly or indirectly—through one or more factors. A natural person is identifiable if they can be identified directly or indirectly, particularly based on an identifier such as a name, number, location data, online identifier, or one or more factors.
- **Data Transfer**: Making personal data accessible to a specific third party. Transfers to EEA member states and EU bodies are considered as if they occurred within Hungary.
- **Data Deletion/Erasure**: Rendering data unrecognizable by deleting its content or applying an equivalent method that achieves the same result.
- **Data Breach**: A security breach leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or unauthorized access to transmitted, stored, or otherwise processed personal data.
- **EEA Member State**: A country that is a member of the European Union or a contracting party to the Agreement on the European Economic Area (EEA), as well as any country whose citizens enjoy equal status with EEA citizens based on an international agreement between the EU, its member states, and a non-EEA country.
- **Third Country**: Any state that is not an EEA member state.
- **NAIH**: The Hungarian National Authority for Data Protection and Freedom of Information, the supervisory authority in Hungary under the GDPR.

5. Data Processing Procedures

All business partner, employee, or client data we obtain during our activities, in any form or to any extent, is processed in accordance with this Privacy Notice, with a commitment to confidentiality, in compliance with the GDPR and relevant Hungarian legal regulations.

We lawfully store and organize personal data received as part of our business activities and use it to the necessary extent within the legal framework.

Data processing is immediately discontinued once its purpose is fulfilled or ceases to exist. Additionally, we assess termination requests from data subjects.

We do not engage in profiling or automated decision-making.

6. Details of Data Processing Related to Our Activities, by Purpose

6.1 Contacting Us

- **Data Subjects**: Natural persons or representatives of legal entities who contact us for inquiries.
- **Purpose of Data Processing**: Establishing contact, maintaining communication, and providing information.

Type of data	Legal basis	Keep on record
nem	GDPR 6. article (1) sec. a); your agreement	Until withdrawal of agreement, up to maximum 5 years
e-mail address		
phone number		

Data Processing Procedure: If you provide us with your contact details via email or phone, we will use them for communication and to provide information related to our services.

Providing the above data is not mandatory; however, without it, we will be unable to maintain contact with you. You may withdraw your consent at any time without justification. This will not affect the lawfulness of data processing carried out before the withdrawal based on your prior consent. Consent can be withdrawn by sending a request to the specified email address, which we will process as soon as possible, but no later than five (5) working days.

6.2 Contracting with Partners and Clients

Data Subjects: Any service provider, client, or business partner entering into a contract. This may include natural persons acting as sole proprietors on their behalf or representatives of a business entity or organization.

Purpose of Data Processing: Performance of the Contract.

Type of data	Legal basis	Keep on record
name	GDPR 6. article (1) sec. b), contract fulfilment	Until the end of contractual relationship, up to maximum 5 years
signature		
self-employed tax id		
self-employed address		
e-mail address	GDPR 6. article (1) sec. b), necessary for communication	
phone number		

The processing of the above personal data is essential for entering into, fulfilling, and maintaining communication (collaboration) related to the contract.

6.3 Data Processing Related to Our Accounting Services

- **Data Subjects**: All our clients.
- **Purpose of Data Processing**: The lawful performance of the services agreed upon in the contract.

Type of data	Legal basis	Keep on record
account information: self-employed name, address, tax ID bank account number	GDPR 6. article c); Fulfilling legal requirements; Accounting act no. C. of 2000	Until the end or termination of contractual relationship.
Salary, social security, other personal data of clien enmployees required by law		

Data Processing Procedure: The processing of the above personal data is essential for fulfilling our contractual services, and the scope of the processed data is determined by legal regulations. We process this data as a data processor on behalf of our client (the data controller), and we do not use or store it for our own purposes. At the end of the assignment, we return all data to the data controller.

During our activities, we use various accounting and administrative software programs, whose service providers may have system administrator-level access to stored data.

- RLB-60 Bt. (Business Administration Software)
  - Privacy Policy: https://www.rlb.hu/Adatkezelesi_tajekoztato.html
- SBA Group Zrt. (Cashbook Software)
  - Privacy Policy: https://cashbook.hu/informaciok/adatkezelesi-tajekoztato/
- Nyíltbankolás Zrt. (www.bankszamlakivonat.hu)
  - Privacy Policy: https://portal.bankszamlakivonat.hu/privacy-policy
- NAV ÁNYK (Hungarian Tax Authority's Electronic Filing System)
  - Privacy Policy: https://nav.gov.hu/footer-tartalmak/adatvedelem

To ensure the security of certain data related to our work, we also use password-protected cloud storage services.

- Google Drive (USA)
  - Privacy Policy: https://policies.google.com/privacy?hl=hu#europeanrequirements
- Dropbox (USA)
  - Privacy Policy: https://www.dropbox.com/privacy

6.4 Processing of Job Applications and Applicant Data

- **Data Subjects**: Individuals applying for job opportunities.
- **Purpose of Data Processing**: Evaluating applications and notifying applicants.

Type of data	Legal basis	Keep on record
applicant's gender	GDPR 6. article (1) sec. a), agreement	Until withdrawal of agreement, up to maximum 6 months after decision
birth place, date		
personal address		
education, experience		
signature		

e-mail address		
phone number		
face picture occasionally		

Data Processing Procedure: Applicants for a given job opportunity submit their résumés (CVs) and cover letters, which may contain personal data that the applicant considers important for a successful evaluation. Providing the above data is not mandatory; however, without it, we cannot evaluate the application or notify the applicant of the outcome.
Applicants may withdraw their consent at any time without justification. This will not affect the lawfulness of data processing carried out before the withdrawal based on prior consent. Consent withdrawal requests can be sent via email, and we will process them as soon as possible, but no later than five (5) working days.

6.5 Data Processing Related to Employment

- **Data Subjects**: Individuals employed under a legal employment relationship with us.
- **Purpose of Data Processing**: Administrative processes related to employment in compliance with legal requirements.

Type of data	Legal basis	Keep on record
Personal identifiers	GDPR 6. article (1) c) legal compliance; Act on Labour Code no. I. of 2012. Act on Rules of Taxation no. CL of 2017 Accounting act no. C. of 2000 Act on Pensions no. LXXI of 1997 (…)	Certain categories of personal data related to employment must be retained according to legal requirements, and cannot be disposed of: Personal data related to establishing, terminating employment, and pension eligibility cannot be discarded. Data related to salary payments and payroll processing cannot be discarded. Personal data associated with an employee being designated as a contact person is stored by the Data Controller in accordance with the Accounting Act and tax regulations for a period of 8 years.
personal address		
employment data		
numbers of official papers		
work organisation infos		
social security, salary details		
contact details: email address, address, phone number		
other data required by law		

Data Processing Procedure: The purpose of providing the above data is to comply with the administrative requirements set by law for employment. Providing this data is mandatory.

6.6 Handling of Data Protection Complaints

- **Data Subjects**: Any natural person (data subject) who believes their rights have been violated.
- **Purpose of Data Processing**: Identification, conducting the complaint procedure, and maintaining communication.

Type of data	Legal basis	Keep on record
name	GDPR 6. article (1) sec. c); Fufilling legal requirements 2016/679 (EU) order (GDPR)	5 years after closing the case
mother's name		
email address		
phone number		
info about objections		

Data Processing Procedure: Any data subject has the right to file a complaint regarding our data processing activities if they believe their rights have been violated. Providing the necessary data is required for investigating the complaint and maintaining communication to ensure a lawful procedure. Without this data, we cannot identify the complainant or process the complaint.

6.7 Invoice Management and Accounting

- **Data Subjects**: Any natural person whose information appears on an invoice.
- **Purpose of Data Processing**: Document management in compliance with **accounting laws**.

Type of data	Legal basis	Keep on record
name	GDPR 6. article c); Fulfilling legal requirments; Accounting act no. C. of 2000	8 years after the year of issuing the invoice
tax ID, address		

Data Processing Procedure: In the case of sole proprietors, invoices may contain personal data. We retain this data in compliance with the Accounting Act. Providing the necessary data is required by legal regulations. Failure to provide this data will result in the invoice being invalid.
We store invoice-related data electronically using the Számlázz.hu service.

Partner and Privacy Policy:

- KBOSS.hu Kft. (Számlázz.hu)
  - Privacy Policy: https://rendezveny.szamlazz.hu/adatvedelmi-tajekoztato/

- Access to Invoice Data by Tax Authorities: The competent tax authority has lawful access to invoice information.

Tax Authority Information:

- NAV (Hungarian Tax Authority)
  - Contact: kbpavig@nav.gov.hu
  - Privacy Policy: https://nav.gov.hu/footer-tartalmak/adatvedelem

7. Data Transfers and Disclosures

In certain cases, we transfer personal data to third parties as part of our activities. Data transfers may occur in paper or electronic form, ensuring that data is accessible only to the intended recipient.

Methods of Data Transfer:

- Paper-based transfer: Personal delivery or postal mail, addressed to a specific recipient.
- Electronic transfer (email): Personal data is not included in the email text. If necessary, personal data is sent as an attached Excel file or compressed file, always protected with a unique password. Whenever

possible, we avoid direct data transfers and instead use a password-protected cloud database where clients upload information for our processing. Clients can also view/download accounting records and reports from this platform.

We do not transfer personal data to third countries or international organizations.
In addition to the partners listed above, we transfer data to the following organizations, either as data processors or independent data controllers, under the legal basis of "contract performance" or "legal compliance."

Additional Partners and Their Privacy Policies:

- CIB Bank Zrt.
  - Privacy Policy: https://www.cib.hu/document/documents/CIB/vhk_adatkezelesi_190325_2.pdf
- Hosting (Domain) Service Provider: Rackhost Zrt.
  - Privacy Policy: https://www.rackhost.hu/privacy-policy

8. Data Security

We ensure the security of the personal data we process through technical and organizational measures and the implementation of appropriate procedures.

- Access Restriction: Only employees whose duties require access to personal data can access it.
- Risk Management: When designing and operating our IT system, we assess and minimize potential risks.
- Threat Monitoring: We monitor security threats (e.g., viruses, hacking attempts, denial-of-service attacks) and take timely measures to prevent and mitigate them.
- Physical Security: We protect IT equipment and paper-based records from unauthorized access and environmental hazards (e.g., water, fire, power surges).
- System Monitoring: We continuously monitor our IT systems to detect potential security incidents.
- Reliable Service Providers: We prioritize reliability when selecting service providers involved in system operations.

9. Rights of Data Subjects under GDPR (Articles 15-20)

Data subjects have the following rights regarding their personal data:

- Right to information
- Right of access
- Right to rectification
- Right to erasure ("right to be forgotten")
- Right to restriction of processing
- Right to data portability
- Right to object

You can exercise your rights by contacting us at **info@atakacs.hu**.

Right of Access

You may request confirmation of whether we are processing your personal data. If processing is ongoing, you have the right to access your personal data and receive information about the security measures applied.

Right to Rectification

Upon request, we will promptly correct any inaccurate personal data and complete any missing information.

Right to Erasure ("Right to Be Forgotten")

We will delete your personal data without undue delay if:

- The data is no longer needed for the original purpose.
- The processing was based on consent, and you withdraw that consent with no other legal basis for processing.
- The personal data was processed unlawfully.
- Legal regulations require the deletion of the data.

Exceptions:
We cannot delete personal data if processing is necessary for:

- Legal claims (e.g., defense in legal proceedings).

Right to Restriction of Processing

Upon request, we will limit the use of your personal data so that it is only used for specific purposes.

Right to Data Portability

If this does not infringe on the rights and freedoms of others, we will provide your data in a structured, commonly used, machine-readable format, or, upon request, directly transfer it to another data controller.

Right to Information

At any time during the processing period, you may request details about how we process your personal data. We will respond within 30 days with a clear, written explanation of:

- The data we process.
- The purpose, legal basis, and duration of processing.
- Any data transfers (recipients and reasons).

Right to Object

If you object to data processing, we will review your request within 15 days and provide a written response. If we deny your request for rectification, restriction, or erasure, we will explain our legal and factual reasons within 30 days.

10. Other Provisions Regarding Data Processing

End of Data Processing

We will delete any personal data if:

- The purpose of data processing has ended.
- There is no valid legal basis for processing.

- The data subject withdraws consent or objects to processing.
- Legal regulations require deletion.

Data Blocking Instead of Deletion If deletion would violate the data subject’s legitimate interests, we will block (restrict) the data instead. In this case, data is retained only for as long as the purpose of blocking remains valid.

11. Handling of Data Protection Complaints

Complaint Procedure

We handle as a complaint any written request from a data subject that concerns a violation of this Privacy Notice or any data protection issue.

Complaints can be submitted:

- By email to info@atakacs.hu
- By postal mail to our official mailing address

Required Complaint Information

Complaints must include:

- Complainant’s name, address (email), and phone number
- Date of the incident
- Detailed description of the issue
- Signature of the complainant
- Consent to process personal data related to the complaint

Without this information, we cannot investigate the complaint and will notify the complainant accordingly.

Complaint Handling Process

- We use the complainant's personal data exclusively for handling the complaint.
- We do not share this data with third parties except when legally required (e.g., court or regulatory authorities).
- We do not use complaint data for business purposes.

Response Time:

- We will investigate and respond in writing within 30 days via the same method the complaint was received (email or postal mail).
- If a 30-day response time is insufficient, we will notify the complainant and provide a final response within three months.
- If the complaint is justified, we will inform the complainant of the corrective action taken.
- If the complaint is denied, we will provide a written explanation of our decision and inform the complainant of their further legal options.

Further Legal Options

If dissatisfied with our response, you may file a complaint with the National Authority for Data Protection and Freedom of Information (NAIH):

Contact Information:

- Address: NAIH, 1055 Budapest, Falk Miksa u. 9-11, Hungary
- Email: ugyfelszolgalat@naih.hu
- Phone: +36 (1) 391 1400
- Website: www.naih.hu

Alternatively, you may initiate legal proceedings in a **court of law**.

12. Data Breaches and Incident Management

Definition of a Data Breach

A data breach refers to any action, intervention, or omission that results in the unlawful processing or handling of personal data. This includes, but is not limited to:

- Unauthorized access, alteration, transmission, or disclosure of personal data.
- Deletion or destruction of personal data.
- Accidental destruction or damage of personal data.

If you become aware of a data breach related to our activities, please report it as soon as possible via:

- **Email: info@atakacs.hu**
- **Phone: +36 70 611 7254**

Incident Handling Procedure

As a Data Controller, we record all breach reports and immediately begin an investigation.

- If the breach involves an IT system, we notify the relevant service providers responsible for database operation.
- We collect all necessary information to:
    - Identify the breach.
    - Reduce potential damages.
    - Develop further countermeasures.

Recorded information includes:

- Time and location of the breach.
- Description, circumstances, and impact of the incident.
- Type and amount of compromised data.
- Affected individuals.

Notification to Authorities

In compliance with legal requirements, we report all significant data breaches to the National Authority for Data Protection and Freedom of Information (NAIH) within 72 hours.

Data Protection Officer (DPO)

As a Data Controller, we do not process large volumes of sensitive personal data as part of our core activities. Additionally, we are not a public authority, meaning we are not legally required to appoint or employ a Data Protection Officer (DPO).

Amendments to This Privacy Notice

As a Data Controller, we reserve the right to update and amend this Privacy Notice in line with:

- Legal changes.
- Operational or procedural updates.

The most recent version of this Privacy Notice will always be available at our company.

Budapest, March 2025

ATAKÁCS Könyvelő Kft.