Adatkezelési URL: absolutetantra.com/adatkezeles

PRIVACY POLICY AND NOTICE FOR DATA SUBJECTS

– Effective as of 20 May 2025

(Magyar nyelven az angol alatt)

Introduction

The absolutetantra.com online commercial and service platform is operated by Spirit Service Ltd (registered office: 1 Hova Villas, Hova House, Hove, BN3 3DH, United Kingdom; Company Registration Number: 08593252; UTR Number: 7943000133) – hereinafter referred to as the Data Controller. The Data Controller and its staff are firmly committed to protecting the personal data of their clients and any third parties they engage with, including visitors to the website (collectively referred to as: Data Subjects). They place great importance on respecting the right to informational self-determination.

This Privacy Policy has been created to ensure the Data Controller complies with all relevant data protection laws currently in effect and to provide clear and transparent information to Data Subjects regarding how their personal data is processed. All data processing activities carried out by the Data Controller are governed by this Privacy Policy (hereinafter referred to as: Policy), as well as other internal policies and procedural guidelines.

The General Section of this Policy outlines the fundamental principles and rules applicable to all data processing activities. The Special Section provides specific details and information concerning individual data processing operations. While this Policy offers a comprehensive overview of the primary data processing practices undertaken by the Data Controller, not every type of data processing described herein applies to every Data Subject. When collecting personal data in specific cases, the Data Controller will also provide a brief data protection notice outlining the particular details relevant to that instance.

Please read this entire Policy carefully to fully understand the rules and principles governing how your personal data is processed.

The Data Controller treats all personal data it records or receives as confidential, handling such information in accordance with applicable data protection laws and as outlined in this Privacy Policy. A key principle of the Data Controller is to ensure that every individual retains full control over their own personal data, in line with legal requirements. In addition, the Data Controller takes appropriate steps to safeguard data security, implementing both technical and organizational measures, and establishing internal policies and procedures that uphold data protection and confidentiality standards.

Although the Data Controller has aimed to create a comprehensive framework through this Policy, it may not include every possible data processing activity. In cases where a new type of data processing becomes necessary and is not covered in this Policy, the Data Controller will always

issue a separate data processing notice. This supplementary notice will provide the Data Subjects with relevant and detailed information specific to that particular processing activity.

A current and valid version of this Policy must be kept on file at the Data Controller's registered office and is also available online, including any amendments or updates, at: absolutetantra.com/adatkezeles.

Applicable Legislation

(For a company registered in the United Kingdom that also operates online and is accessible to users within the European Union)

Data Protection

- **UK General Data Protection Regulation (UK GDPR)**
- **Data Protection Act 2018**
  🔗 gov.uk – Data Protection
  🔗 Data Protection Act 2018
- **Regulation (EU) 2016/679 of the European Parliament and of the Council**
  (General Data Protection Regulation – GDPR)
  (Applicable when processing the personal data of EU citizens, even if the company is not established in the EU.)
  🔗 EUR-Lex – GDPR

Accounting and Financial Reporting

- **Companies Act 2006**
- **UK GAAP – UK Generally Accepted Accounting Principles**
  🔗 Legislation – Companies Act 2006
  🔗 FRC – UK GAAP

Taxation

- **Finance Act** *(updated annually)*
- **Taxes Management Act 1970**
- **Companies Act 2006**
- **Money Laundering Regulations 2017**

- **HMRC Guidance**
  🔗 gov.uk – HMRC
  🔗 Legislation – Taxes Management Act 1970

Anti-Money Laundering and Counter-Terrorism Financing

- **Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017**
- **Proceeds of Crime Act 2002 (POCA)**
  🔗 MLR 2017
  🔗 Proceeds of Crime Act 2002

Advertising and Commercial Practices

- **Consumer Protection from Unfair Trading Regulations 2008 (CPRs)**
- **UK Code of Non-broadcast Advertising and Direct & Promotional Marketing (CAP Code)**
  🔗 CPRs 2008
  🔗 CAP Code
- **Directive 2005/29/EC on Unfair Commercial Practices**
  (May be applicable when targeting EU-based consumers)
  🔗 EUR-Lex – Directive 2005/29/EC

Electronic Commerce and Information Society Services

- **Electronic Commerce (EC Directive) Regulations 2002**
  🔗 E-commerce Regulations 2002
- **Directive 2000/31/EC (E-Commerce Directive – EU)**
  (Applicable if the online service is specifically directed at EU users)
  🔗 EUR-Lex – Directive 2000/31/EC

Consumer Contracts, Cancellation and Information Requirements

- **Consumer Contracts (Information, Cancellation and Additional Charges) Regulations 2013**
  🔗 Consumer Contracts Regulations 2013

- **Directive 2011/83/EU on Consumer Rights**
  (Applies when the service is accessible to EU-based consumers)
  🔗 EUR-Lex – Directive 2011/83/EU

General Consumer Protection

- **Consumer Rights Act 2015 (UK)**
  🔗 Consumer Rights Act 2015
- **Directive 2011/83/EU on Consumer Rights**
- **Directive 2005/29/EC on Unfair Commercial Practices**
- **Directive 2000/31/EC on E-Commerce**
- **Directive 2009/22/EC on Injunctions for the Protection of Consumers' Interests**
  🔗 EUR-Lex – Directive 2009/22/EC

Adult Education and Training Services

- **Further and Higher Education Act 1992 (UK)**
- **Skills and Post-16 Education Act 2022**
- **Adult Education Budget (AEB) – funding framework**
  🔗 Further and Higher Education Act 1992
  🔗 Skills and Post-16 Education Act 2022

Prohibition of Unfair Commercial Practices

- **Consumer Protection from Unfair Trading Regulations 2008**
  (Prohibits misleading, aggressive, or otherwise unfair practices aimed at consumers.)
  🔗 Legislation – CPRs 2008

Purpose of the Policy

The purpose of this Policy is to ensure the effective implementation of relevant legal requirements—particularly those set out in the GDPR and UK GDPR—through the consistent application and enforcement of the rules defined herein. To that end, the Data Controller, in alignment with this Policy, its internal regulations, instructions, and established procedural frameworks, aims to:

- safeguard the fundamental rights of Data Subjects concerning the protection of their personal data;

- guarantee compliance with data security obligations and ensure that such requirements are adhered to and enforced throughout all data processing activities;
- define the practical measures to prevent unauthorised access, and establish safeguards against the unlawful alteration, misuse, or disclosure of personal data;
- set out clear and secure procedures for the handling of personal data—whether in physical or electronic form—including its collection, processing, transfer, usage, and destruction;
- and provide Data Subjects with clear, timely, and comprehensive information regarding the processing of their personal data, their rights, and the means available to exercise those rights.

General Provisions

Definitions

For the purposes of this Policy, the following terms shall have the meanings set out below:

"Personal data": any information relating to an identified or identifiable natural person ("data subject"). A person is considered identifiable if they can be directly or indirectly identified, in particular by reference to an identifier such as a name, identification number, location data, online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person. This includes, but is not limited to, names, addresses, phone numbers, IP addresses, and email addresses.

"Processing": any operation or set of operations performed on personal data, whether by automated means or otherwise. This includes, in particular, the collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction of personal data. In essence, any action involving personal data—such as accessing, organising, modifying, or transferring it—constitutes processing.

"Profiling": any form of automated processing of personal data that involves the use of such data to evaluate certain personal aspects relating to a natural person, particularly in order to analyse or predict aspects concerning their work performance, economic situation, health status, personal preferences, interests, reliability, behaviour, location, or movements.

"Pseudonymisation": the processing of personal data in such a manner that it can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to appropriate technical and organisational measures to ensure that the personal data cannot be linked to an identified or identifiable individual.

"Filing system": any structured set of personal data, whether centralised, decentralised, or dispersed according to functional or geographical criteria, which is accessible based on specific criteria and allows the retrieval of data concerning individuals.

"Data Controller": any natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of processing personal data. Where

the purposes and means of processing are determined by Union or Member State law, such law may also specify the identity of the controller or the criteria for its designation.
In this context, the Data Controller is Spirit Service Ltd.

"Data Processor": a natural or legal person, public authority, agency, or other body which processes personal data on behalf of the controller. A processor is any entity or individual acting on the controller's behalf and according to its instructions to carry out specific operations on personal data (e.g., accountant, payroll provider, hosting service, software supplier, email service provider, etc.).

"Recipient": a natural or legal person, public authority, agency, or any other body to whom or with whom the personal data is disclosed, regardless of whether it is considered a third party. However, public authorities that may receive personal data in the framework of a particular legal inquiry under Union or Member State law shall not be regarded as recipients; the processing of such data by those authorities must comply with applicable data protection rules.
Typical recipients include authorities such as tax offices or appointed data processors who receive or access the data.

"Third Party": any natural or legal person, public authority, agency, or body other than the data subject, the controller, the processor, or persons who, under the direct authority of the controller or processor, are authorised to process personal data.
In other words, a third party is any person or entity not directly involved in the data processing operation.

"Data Subject's Consent": any freely given, specific, informed, and unambiguous indication of the data subject's wishes by which they, by a statement or by a clear affirmative action, signify agreement to the processing of personal data relating to them.
Examples include ticking a consent checkbox on a website or signing a written declaration. Silence or inaction does not constitute valid consent under data protection law.

"Personal Data Breach": a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed.
Incidents may include: loss of a device containing personal data (e.g., laptop, mobile phone), cyberattacks, fire in a document archive, misdirected emails, or insecure storage (e.g., discarding unshredded payroll documents), as well as unauthorised copying or transfer of customer or partner data.

"Special Categories of Personal Data": personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership; as well as genetic data, biometric data (where used for identification), health-related data, and data concerning a person's sex life or sexual orientation—due to their sensitive nature, these are subject to stricter protection measures.

"Genetic data": personal data relating to the inherited or acquired genetic characteristics of a natural person that provide unique information about the physiology or health status of that individual. Such data is typically derived from the analysis of a biological sample collected from the individual in question.

"Biometric data": personal data resulting from specific technical processing relating to the physical, physiological, or behavioural traits of a natural person, which allows or confirms the unique identification of that person. Examples include facial images, fingerprints, or retinal scans.

“Health data”: personal data concerning the physical or mental health of a natural person, including information relating to the provision of healthcare services to the individual, where such data reveals information about their health status.

Principles of Data Processing

The processing of personal data must at all times be carried out in accordance with the following core principles:

- **Lawfulness, fairness, and transparency**: Personal data must be processed in a way that complies with relevant legal requirements, is fair towards the data subject, and is transparent. Individuals must be clearly and adequately informed about the key aspects of the processing, such as its purpose, legal basis, and duration.
- **Purpose limitation**: Personal data may only be collected for specific, explicit, and legitimate purposes and must not be further processed in a way that is incompatible with those purposes. Exceptions may apply in the case of processing for archiving in the public interest, scientific or historical research, or statistical purposes.
- **Data minimisation**: The processing of personal data must be limited to what is strictly necessary to achieve the defined purpose. If the objective can be met without processing personal data, or by using less data, then the processing is not justified.
- **Accuracy**: Personal data must be accurate and, where necessary, kept up to date. The data controller must take all reasonable steps to ensure that inaccurate data is corrected or deleted without delay.
- **Storage limitation**: Personal data should be stored in a form which permits identification of data subjects only for as long as is necessary to achieve the intended purpose. Once that purpose has been fulfilled, the data must either be deleted or anonymised so that it can no longer be linked to an identifiable individual.
- **Integrity and confidentiality**: Data must be processed in a manner that ensures appropriate security. This includes protecting the data from unauthorised access, unlawful processing, accidental loss, destruction, or damage by implementing suitable technical and organisational measures. This applies to IT systems, physical storage, and operational procedures alike.
- **Accountability**: The data controller is responsible for ensuring compliance with these principles throughout the entire data processing lifecycle and must be able to demonstrate such compliance when required. To this end, internal policies, documented procedures, and control mechanisms must be established to ensure transparency and traceability of data handling processes, particularly during official audits or inspections.

Purposes and Legal Bases of Data Processing

Purpose of Data Processing

The specific purposes of each data processing activity are determined individually by the Data Controller and are detailed in the Specific Provisions section of this Policy. In general terms, the Data Controller processes the personal data of Data Subjects in connection with its operational activities, particularly for the fulfilment of rights and obligations arising from contractual relationships, and for the legitimate interests pursued by the organisation.

Legal Basis for Data Processing

The legal basis applicable to each processing activity is likewise established separately by the Data Controller and specified in the Specific Provisions section.

According to the GDPR, six legal bases for processing personal data are recognised. The Data Controller selects the appropriate basis depending on the nature and context of the specific processing activity. One of the most commonly used bases is the **consent of the data subject**.

Consent-Based Processing

The consent of the Data Subject must always be given voluntarily, through a clear, affirmative action. Silence, inactivity, or pre-ticked boxes cannot be considered valid consent. Acceptable forms of consent include the signing of a written statement (either as a standalone document or incorporated within a contract), checking a consent box on a website, or clicking a "consent" or "agree" button.

Separate and specific consent must be obtained for each processing activity, and the Data Subject must be given the opportunity to provide or withhold consent independently for each case.

The Data Subject may withdraw their consent at any time. Withdrawal of consent shall only take effect for the future and does not affect the lawfulness of processing carried out before the withdrawal. Consent can be withdrawn in any form—such as by written notice, email, telephone, or any other clear statement of intent.

Consent by Minors or Persons with Limited Legal Capacity

In the case of individuals under the age of 16 or those with limited legal capacity, valid consent can only be given by the person exercising parental authority or by the appointed legal guardian. Therefore, the processing of personal data relating to individuals under 16 requires the explicit consent of a parent or guardian.

Where there is any uncertainty regarding the existence of valid consent, it must be assumed that consent has **not** been given.

Data Processing for the Performance of a Contract

Where the processing of personal data is required for entering into or fulfilling a contract in which the data subject is one of the parties, such processing is considered lawful and does not require separate consent. This legal basis commonly applies when the contract itself contains personal details of the contracting parties (such as name, address, contact information), or when data must be processed in connection with the provision of a service requested by the data subject.

Data Processing Based on Legal Obligations

If data processing is mandated by law, the Data Controller is obligated to comply. These types of processing activities are considered mandatory, and their scope, purpose, and retention period are determined by the relevant legislation. Numerous statutory obligations require the processing of personal data—for instance, maintaining accounting records, issuing invoices, complying with anti-money laundering regulations, and fulfilling other regulatory duties. In these cases, the legal obligation cannot be waived or substituted with consent.

Processing Necessary to Protect Vital Interests

In exceptional situations, it may become necessary to process personal data to safeguard the vital interests of the data subject or another natural person—especially in cases where the data subject is unable to give consent or act on their own behalf. Such processing is limited strictly to what is essential for the protection of life or physical integrity and is only permitted for the duration of the emergency or incapacity.

Data Processing Based on a Task Carried Out in the Public Interest or Under Official Authority

Since the Data Controller does not operate as a public authority and does not exercise official powers, it does not carry out data processing on this legal basis.

Data Processing Based on Legitimate Interests

Certain processing activities may rely on the legal basis of pursuing a legitimate interest of the Data Controller or a third party. This legal ground is typically based on a right that is recognised by law, a contractual provision, or a commercially justifiable purpose. Unlike processing based on a legal obligation, relying on legitimate interest is discretionary, not mandatory.

Examples of data processing activities based on legitimate interests include:

- promoting or marketing the Data Controller's services,
- optimising the website or other online platforms,
- collecting data on service usage (e.g., through the use of cookies).

It is essential to emphasise that processing under this basis is only lawful if the interests or fundamental rights and freedoms of the Data Subject—particularly regarding the protection of personal data—do not override the legitimate interest. Special care must be taken in cases involving children.

Whenever legitimate interest is used as a legal basis, the Data Controller must conduct a so-called **balancing test**(Legitimate Interest Assessment). This involves identifying the specific purpose and method of processing, then weighing it against the rights and freedoms of the Data Subject. Data may only be processed if the legitimate interest clearly prevails over the data subject's opposing interests.

The result of this assessment must always be documented in writing. Data Subjects may request information about the test and its outcome at any time.

The Data Controller only processes:

- data provided directly by the Data Subject,
- data available in public registers (e.g. company records, sole trader databases),
- or data lawfully shared by third parties.

General Information Regarding the Data Controller's Processing Activities

The Data Controller is legally required to provide Data Subjects with clear, concise, accessible, and easily understandable information about how their personal data is processed. This obligation is fulfilled through the publication of this Privacy Policy, and in each individual case of data collection, by making a brief and specific privacy notice available at the time of data collection.

If you have any questions regarding this Policy, or if you wish to exercise your rights under data protection law (such as the right of access, rectification, erasure, etc.), you are encouraged to contact the Data Controller. Contact details can be found at the end of this Policy and are also included in each specific data processing notice.

The list of data processors (external service providers acting on behalf of the Data Controller) is provided at the end of this Policy. In the Specific Provisions section, each processing activity includes a "Recipients" field indicating the category of data processor involved, based on the type of service they provide (e.g. hosting provider, accountant, mailing service).

Only those individuals or organisations may act as data processors who have entered into a written data processing agreement with the Data Controller, and who provide sufficient guarantees regarding compliance with the **General Data Protection Regulation (GDPR)** and, where applicable, the **UK General Data Protection Regulation (UK GDPR)**. These guarantees must ensure the implementation of appropriate technical and organisational measures to safeguard the rights of Data Subjects and the security of personal data. Data processors are not permitted to use personal data for their own purposes and may only process such data on the documented instructions of the Data Controller.

Under **Article 37(1) of the GDPR**, and the corresponding provisions of **UK GDPR Article 37** and **Section 69 of the Data Protection Act 2018**, the Data Controller is not currently required to appoint a Data Protection Officer. If such an appointment is made in the future, the Data Controller will provide clear and transparent information to the Data Subjects regarding the DPO's contact details and responsibilities.

For each type of data processing activity, the purpose, legal basis, categories of data involved, and the parties with access to the data are described in detail in the Specific Provisions section of this Policy.

Where the legal basis for processing is the legitimate interest of the Data Controller or a third party, this interest is specifically identified and justified within the same section.

The Specific Provisions also identify to whom and for what purpose the personal data may be disclosed—whether to data processors, competent authorities, or third parties.

With regard to data transfers, the Data Controller provides the following information to Data Subjects:

Data Transfers, Retention, and Data Subject Rights – For a UK-Based Company Operating Within the EU

The Data Controller may transmit personal data to courts or public authorities when such processing is necessary to fulfil its legal or contractual obligations or to enforce its legitimate interests. The scope and nature of the data shared will depend on the specific circumstances of the case.

In addition, the Data Controller may be required by law to transfer certain data to public authorities, such as:

- providing invoice or accounting record data to **HMRC (His Majesty's Revenue and Customs)** in accordance with the **Finance Act 2020** and **Taxes Management Act 1970**;
- reporting suspicious transactions to the **National Crime Agency (NCA)** in line with the **Proceeds of Crime Act 2002** and the **Money Laundering, Terrorist Financing and Transfer of Funds Regulations 2017**;
- responding to official audits or investigations where disclosure is legally required.

The Data Controller may also share personal data with authorities or courts to assert its legitimate interests, for example:

- pursuing unpaid invoices,
- supporting criminal complaints when a crime is suspected.

To support the performance of its services and ensure compliance with its obligations, the Data Controller may engage data processors (e.g. hosting providers, accountants, administrative support services). A complete list of such processors is included at the end of this Policy.

Transfers of Personal Data Between the UK and the EU

As the Data Controller is based in the United Kingdom but also offers services to users in the European Union, it ensures that any transfer of personal data between the UK and the EU/EEA complies with applicable regulations.

As of now:

- The **European Commission's adequacy decision** (June 2021) confirms that the UK provides an adequate level of protection under the GDPR, meaning **data can flow freely from the EU to the UK** without additional safeguards.
- Under the **UK GDPR**, **EU/EEA countries are considered adequate**, so **data transfers from the UK to the EU are also permitted**.

If personal data is to be transferred to a **third country outside the UK and EU/EEA** (e.g. the United States, India, or Canada), the Data Controller will only proceed under the following conditions:

- the third country has been granted an **adequacy decision** by either the **European Commission** or the **UK Secretary of State for Digital, Culture, Media and Sport**;

- or, where no such decision exists, **appropriate safeguards** are implemented, such as **Standard Contractual Clauses (SCCs)**, **Binding Corporate Rules (BCRs)**, or appropriate encryption and risk mitigation procedures.

Data Subjects may at any time request further information about the legal basis and safeguards of such international transfers. Additional guidance is available at the European Commission's official website:

👉 https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu_en

Data Subject Rights Related to Personal Data Processing

Right of Access

Data subjects have the right to request confirmation from the Data Controller as to whether their personal data is being processed. Where such processing is ongoing, the data subject has the right to obtain access to the personal data as well as the following information:

- the purposes of the processing;

- the categories of personal data concerned;

- the recipients or categories of recipients to whom the personal data has been or will be disclosed, including recipients in third countries or international organisations;

- where possible, the intended period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;

- the existence of the right to request rectification or erasure of personal data or restriction of processing, and the right to object to such processing;

- the right to lodge a complaint with a supervisory authority (in the United Kingdom: the **Information Commissioner's Office (ICO)** – ico.org.uk);

- where the personal data was not collected directly from the data subject, any available information as to its source;

- the existence of automated decision-making, including profiling, and meaningful information about the logic involved, as well as the significance and possible consequences of such processing for the data subject;

- where personal data is transferred to a third country or international organisation, the data subject has the right to be informed of the appropriate safeguards relating to the transfer (e.g. adequacy decisions, standard contractual clauses, etc.).

If you would like to know whether the Data Controller is processing your personal data, and under what conditions, you may submit an access request at any time.

Upon request, the Data Controller will provide a copy of the personal data undergoing processing. For any additional copies requested, the Data Controller may charge a reasonable administrative fee. If the request is made electronically, the information will be provided in a commonly used electronic format, unless otherwise requested by the data subject.

Right to Rectification

Data subjects have the right to request the prompt correction of inaccurate personal data concerning them. Taking into account the purposes of the processing, they also have the right to request the completion of incomplete personal data, including by providing a supplementary statement if necessary.

If your personal information has changed (e.g. your name, address, or contact details), please inform the Data Controller so that our records can be updated accordingly.

The Data Controller will inform all recipients with whom the personal data was shared of any rectification, unless this proves impossible or involves a disproportionate effort. Upon request, the Data Controller will inform the data subject about these recipients.

Right to Erasure (Also Known as the "Right to Be Forgotten")

The data subject has the right to request that the Data Controller erase their personal data without undue delay. The Data Controller is obliged to comply with this request without undue delay if one of the following grounds applies:

- the personal data is no longer necessary in relation to the purposes for which it was collected or otherwise processed;
- the data subject withdraws their consent on which the processing is based, and there is no other legal basis for continuing the processing;
- the processing is based on the legitimate interests of the Data Controller or a third party, and the data subject objects to the processing, and there are no overriding legitimate grounds for the processing; or the data subject objects to processing for direct marketing purposes;
- the personal data has been unlawfully processed;
- the personal data must be erased in order to comply with a legal obligation under applicable UK law, including the **UK GDPR** or the **Data Protection Act 2018**.

If the Data Controller has made the personal data public and is required to erase it, they will take reasonable steps—taking into account available technology and implementation costs—to inform other data controllers processing the data that the data subject has requested the deletion of any links to, or copies or reproductions of, the personal data.

When the Right to Erasure Does Not Apply

The Data Controller is not required to erase personal data where the processing is necessary for one of the following reasons:

- for exercising the right of freedom of expression and information;
- for compliance with a legal obligation which requires processing under UK law to which the Data Controller is subject;
- for reasons of public interest in the area of public health, in accordance with applicable laws in the United Kingdom;
- for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes, where erasure would seriously impair or render impossible the achievement of those objectives;
- for the establishment, exercise, or defence of legal claims (e.g. in the context of litigation or debt collection).

The Data Controller will inform all recipients to whom the personal data has been disclosed about the erasure, unless this proves impossible or requires disproportionate effort. Upon request, the data subject may receive a list of such recipients.

Right to Restrict Processing

A data subject has the right to request the restriction of processing of their personal data by the Data Controller, under the following conditions:

- The accuracy of the personal data is contested by the data subject, in which case processing may be restricted for a period enabling the controller to verify the accuracy of the data;
- The processing is unlawful, but the data subject opposes the erasure of the data and instead requests restriction of its use;
- The Data Controller no longer requires the personal data for the original purposes of the processing, but the data subject needs the data for the establishment, exercise or defence of legal claims;
- The data subject has objected to processing based on the Data Controller's legitimate interest, and the restriction applies for the duration of the verification of whether the controller's legitimate grounds override those of the data subject.

Where processing has been restricted on one of the above grounds, such personal data may, with the exception of storage, only be processed:

- with the data subject's explicit consent;
- for the establishment, exercise, or defence of legal claims;
- for the protection of the rights of another natural or legal person;
- or for reasons of important public interest in accordance with applicable UK law.

The Data Controller will inform the data subject in advance if the restriction is to be lifted.

The Data Controller is also obliged to notify any recipients with whom the personal data has been shared of the restriction, unless this proves impossible or requires disproportionate effort. The data subject may request information about such recipients.

If your request to restrict processing is granted, the Data Controller will retain your personal data but will not otherwise process it unless one of the above exceptions applies.

Right to Data Portability

The data subject has the right to receive personal data concerning them, which they have provided to the Data Controller, in a structured, commonly used, and machine-readable format. The data subject also has the right to transmit this data to another controller without hindrance from the original Data Controller, provided that:

- the processing is based on the data subject's consent or on a contract; and
- the processing is carried out by automated means (i.e. not manual or paper-based processing).

Furthermore, where technically feasible, the data subject has the right to request that the personal data be transmitted directly from one controller to another.

The exercise of the right to data portability must not adversely affect the rights and freedoms of others.

Request for Data Transfer to Another Controller

If your personal data is being processed based on your consent or for the performance of a contract, and such processing is carried out by automated means, you have the right to request that your data be transmitted in a structured, commonly used and machine-readable format, either to you or directly to a third party you designate.

Right to Object

You have the right to object, at any time, on grounds relating to your particular situation, to the processing of your personal data when the processing is:

- carried out in the public interest; or
- based on the legitimate interests of the Data Controller or a third party – including profiling based on those grounds.

In such cases, the Data Controller must cease processing your data unless they can demonstrate compelling legitimate grounds for the processing which override your interests, rights, and freedoms, or the data is needed for the establishment, exercise or defence of legal claims.

Objection to Direct Marketing

Where personal data is processed for direct marketing purposes – including profiling to the extent that it is related to such marketing – you have the right to object at any time to such processing.

If you object, your personal data must no longer be used for direct marketing purposes.

In summary, if the legal basis of processing is the Data Controller's legitimate interest, you have the right to object to such processing at any time.

Automated Individual Decision-Making, Including Profiling

You have the right not to be subject to a decision based solely on automated processing – including profiling – which produces legal effects concerning you or similarly significantly affects you.

This right does not apply where the decision:

- is necessary for entering into, or the performance of, a contract between you and the Data Controller;
- is authorised by applicable UK law or EU law to which the controller is subject and which lays down suitable measures to safeguard your rights, freedoms and legitimate interests;
- is based on your explicit consent.

Where such automated processing is permitted, the Data Controller must implement appropriate safeguards, including the right to obtain human intervention, to express your point of view, and to contest the decision.

Right to Lodge a Complaint with a Supervisory Authority

Without prejudice to any other administrative or judicial remedy, you have the right to lodge a complaint with a supervisory authority if you believe that the processing of your personal data infringes applicable data protection laws.

In the United Kingdom, the competent supervisory authority is:

Information Commissioner's Office (ICO)
📍 Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF
🔗 https://ico.org.uk

If the processing also affects the European Union, you may submit a complaint to the supervisory authority of the Member State of your habitual residence, place of work, or place of the alleged infringement. For example, in Hungary, the competent authority is:

Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH)
🔗 https://naih.hu

Investigation of Complaints by the Supervisory Authority

If you submit a complaint to a supervisory authority, that authority is required to investigate the matter and provide you with information regarding the progress and outcome of the investigation within a reasonable timeframe. This applies particularly in cases that require further examination or cooperation between supervisory authorities.

A complaint may lead to formal proceedings being initiated by the authority against the Data Controller.

Obligation to Respond to Data Subject Requests

If the Data Controller does not take action on your request, they must inform you without undue delay – and at the latest within one month of receiving your request – of the reasons for not acting and of your right to lodge a complaint with a supervisory authority and to seek judicial remedy.

In the United Kingdom, the competent supervisory authority is:

Information Commissioner's Office (ICO)

📍 Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

🔗 https://ico.org.uk

If the data processing falls within the territorial scope of the EU GDPR (e.g., involves EU-based data subjects), you may also submit a complaint to the relevant authority in the Member State of your habitual residence, workplace, or the place of the alleged infringement.

Limitations on Data Subject Rights

Under **UK GDPR Schedule 2** and **Article 23 of the EU GDPR**, national or Union laws may impose restrictions on the rights of data subjects in certain cases, such as when necessary to safeguard national security, public order, or the rights and freedoms of others.

Record-Keeping of Requests

The Data Controller maintains an internal log of all requests made by data subjects and any actions taken in response to those requests.

Judicial Remedies, Compensation, and Liability

If you believe your personal data has been processed in violation of applicable data protection laws – including but not limited to the **UK GDPR**, the **Data Protection Act 2018**, or, where applicable, the **EU GDPR** – you have the right to initiate legal proceedings against the Data Controller or any Data Processor involved in handling your personal data.

You may choose to bring the claim before the court in the UK jurisdiction where you reside or are located. If the processing relates to EU-based individuals, proceedings may also be initiated in their respective Member State courts. The relevant supervisory authority may intervene in the case to support the data subject.

Burden of Proof

The Data Controller or the Data Processor is responsible for proving that the processing complies with the legal obligations established under applicable data protection legislation.

Right to Compensation and Damages

If a Data Controller or a Data Processor causes damage through unlawful processing or by violating data security requirements, they are liable to compensate the individual for the loss incurred.

If a data subject suffers harm to their personal rights or reputation due to a breach of data protection obligations, they may also claim non-material damages (known as **distress compensation** or **moral damages**) from the Data Controller.

The Data Controller is also liable for damage caused by a Data Processor acting on its behalf.

The Data Controller is exempt from liability only if it can prove that the damage or violation occurred due to circumstances beyond its reasonable control and not attributable to its data processing operations.

No compensation is owed if the damage or rights violation resulted from the data subject's own intentional or grossly negligent conduct.

Data Security Requirements

As the Data Controller, **Spirit Service Ltd.** stores personal data either in electronic format, on paper, or both, depending on the nature of the processing activity. The specific methods and storage locations are detailed in the Specific Section of this Policy.

To ensure the confidentiality, integrity, and availability of personal data, the Controller implements appropriate technical and organisational safeguards. The level of protection is determined based on the potential risks associated with data processing, including but not limited to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored, or otherwise processed.

Electronic data is currently stored on servers owned and operated by:

Tárhely.Eu Korlátolt Felelősségű Társaság
Registered office: 1144 Budapest, Ormánság utca 4. X. em. 241
Company registration number: 01-09-909968
Court of registration: Fővárosi Törvényszék Cégbírósága
Website: https://tarhely.eu

Electronic documents created or converted during data processing are archived on these servers as part of a secure storage protocol. This ensures regular data backups and long-term retention in accordance with applicable data protection standards.

The Controller ensures that all workstations and computers are protected with secure login credentials, and access to documents is restricted based on authorisation levels. All systems are

equipped with updated antivirus and anti-malware protection. Periodic backups are conducted on a scheduled basis and maintained with overwrite cycles.

Physical documents containing personal data are stored in locked filing cabinets or secured archive rooms that are protected against fire, water damage, and unauthorised access.

The Data Controller ensures compliance with data security standards through this Policy and supporting internal procedures and instructions. It is also the Controller's responsibility to make sure that employees, contractors, and Data Processors are familiar with these provisions and strictly adhere to them during any data handling operation.

Data Disclosure and Transfer

Spirit Service Ltd., acting as Data Controller, may only transfer personal data to third parties in the following cases and strictly to the specified categories of recipients:

- **For the purpose of fulfilling the specific data processing objective**, personal data may be shared with data processors or other independent controllers who are engaged to carry out tasks necessary to achieve the lawful purpose of the processing;
- **Based on the explicit and informed consent of the data subject**, personal data may be disclosed to any recipient designated or approved by the individual;
- **Where legally required**, or pursuant to an official request or obligation under applicable laws and regulations, personal data may be provided to the competent authorities or institutions as defined by law;
- **In cases involving suspicion of a criminal offence or regulatory violation**, or upon a formal request, the Data Controller is permitted to forward the relevant personal data to criminal investigation authorities, regulatory enforcement bodies, or other entities conducting preliminary or administrative proceedings related to the case.

Data Processing

Spirit Service Ltd., as the Data Controller, may rely on the assistance of third-party service providers—such as administrative partners, accounting professionals, postal or courier services—to support its business operations. These service arrangements often involve the handling of personal data. In such cases, Spirit Service Ltd. remains the Data Controller, while the contracted partner acts as a Data Processor.

The Data Controller only engages Data Processors that provide sufficient guarantees that they will implement appropriate technical and organisational measures in accordance with the **UK General Data Protection Regulation (UK GDPR)**, the **Data Protection Act 2018**, and, where applicable, the **EU GDPR**, to ensure the secure and lawful handling of personal data and the protection of data subject rights.

The roles, responsibilities, and scope of the Data Processor's activities are determined exclusively by the Data Controller, based on written instructions. The Data Processor is not permitted to make

independent decisions regarding the data; it may only process personal data on behalf of the Controller and strictly in accordance with the Controller's directions.

Furthermore, the Data Processor must not use any personal data for its own purposes. It is required to store, retain, or delete the data only as directed by the Data Controller. Sub-processors may only be appointed with the prior written consent of the Data Controller.

A written data processing agreement must be in place for each such arrangement. This agreement must clearly specify at least the subject matter, duration, nature and purpose of the processing, the categories of personal data involved, the categories of data subjects, and the respective obligations, responsibilities, and liabilities of both the Controller and the Processor in accordance with the **UK GDPR** (and, if applicable, the **EU GDPR**). By law, no organisation that has a direct commercial interest in using the data may be appointed as a Processor.

A detailed list of the Data Processors used by the Controller, including their names and scope of processing, can be found at the end of this Privacy Policy.

Special Section – Processing of Partner Data

In the course of its business activities, **Spirit Service Ltd.**, as the Data Controller, maintains contractual and pre-contractual relationships with individual and corporate suppliers and service providers. To perform and manage these relationships—including but not limited to procurement, service delivery, invoicing, and payment—it is necessary to process certain personal data.

This data processing is carried out both on paper (e.g. storage of contracts and related documents at the Controller's registered office) and electronically (secured storage, backup, and archiving).

1. Processing Data of Individual Contractual Partners

Categories of personal data processed:

- Full name
- Residential address
- Mother's maiden name
- Individual entrepreneur registration number, tax number or tax identification code
- Business card details (where applicable)
- Bank account number (where necessary)

Purpose of processing:

- Identification of the contracting party
- Drafting, managing and executing the contract

Legal basis:

- Necessary for the performance of a contract – **UK GDPR, Article 6(1)(b)**
- If the service is offered to individuals in the EU, also applicable under **EU GDPR, Article 6(1)(b)**

Additional contact-related data (if a separate contact person is designated):

- Contact person's name
- Email address
- Telephone number
- Position
- Business card details (where applicable)

Purpose of processing:

- Ensuring ongoing communication with the contractual partner

Legal basis:

- Contractual necessity – **UK GDPR, Article 6(1)(b)**
- Where the contact person differs from the contracting party: Legitimate interest of maintaining effective communication – **UK GDPR, Article 6(1)(f)**

Source of data:

- Directly from the data subject
- From the contracting party if the contact person is designated by them

2. Invoicing and Financial Documentation

Data processed:

- Invoice-related data (e.g. billing name, address, tax identification)

Purpose:

- Issuing invoices and fulfilling record-keeping obligations

Legal basis:

- Compliance with a legal obligation – **UK GDPR, Article 6(1)(c)**
- In accordance with relevant UK accounting and tax regulations:
    - **Companies Act 2006**

- **Taxes Management Act 1970**
- **Finance Acts**
- **HMRC regulations**

Recipients:

- Accountant or bookkeeper (as Data Processor)
- Invoicing software provider (as Data Processor)
- **HM Revenue & Customs (HMRC)** as an independent Data Controller, when required by law

3. Processing of Corporate Partner Data

Data processed (for the representative of the company):

- Name of the individual acting on behalf of the company
- Job title or role
- Business card details (where available)

Purpose:

- Establishing and maintaining the contract

Legal basis:

- Necessary for the performance of the contract – **UK GDPR, Article 6(1)(b)**

Source:

- Directly from the data subject

Additional contact-related data (if other than legal representative):

- Name of contact person
- Email address
- Telephone number
- Position
- Business card data (where applicable)

Purpose:

- Ensuring communication between the Data Controller and the contracting partner

Legal basis:

- Legitimate interest in maintaining business communication – **UK GDPR, Article 6(1)(f)**

Source of data:

- From the contact person or from the legal representative of the contracting entity

Correspondence and Documentation Management

1. Retention of Contractual Documents and Accounting Records

Personal data recorded on contractual documents used to confirm the content and execution of agreements will be retained for **five years** following the termination of the business relationship, in accordance with the general limitation period under civil law. For accounting records such as invoices and receipts, the data retention period is **eight years**, counted from the end of the financial year in which the last record was issued, pursuant to the **UK Companies Act 2006** and applicable accounting principles (**UK GAAP**).

If the legal basis for processing ceases to exist (e.g., the contact person or representative ceases to act on behalf of the partner), the related personal data will be erased without delay.

2. Cash Transactions and AML Obligations

The company does **not accept cash payments exceeding the HUF/GBP equivalent of £6,500 (approx. 3,000,000 HUF)**; payments are exclusively accepted via bank transfer. Consequently, **customer due diligence under the UK Money Laundering Regulations (MLR 2017)** is not required under standard business partner transactions. If such identification becomes necessary, the data subject will be informed separately about the details of the due diligence process.

3. Handling of Incoming Enquiries

Email enquiries received via **hello@absolutetantra.com** email address are reviewed and managed by an authorised staff member, who forwards them internally to the appropriate department. If the enquiry includes personal data, such data will be processed accordingly during this handling process.

Incoming written correspondence is stored digitally under separate archiving rules and also filed in paper format. Incoming emails are manually reviewed, sorted, and then deleted from the inbox after processing.

Legal basis for processing:

- Legitimate interest in maintaining lawful and effective communication – **UK GDPR Article 6(1)(f)**
- In cases where the message relates to an existing contract, the processing is based on **contract performance – UK GDPR Article 6(1)(b)**

Data source:

- The data subject (sender of the enquiry)

4. Outgoing Post (Proof of Mailing and Delivery Receipts)

Proof of mailing (such as certificates of posting or delivery confirmations) related to outgoing postal correspondence is archived together with the relevant letters. These documents serve as evidence of dispatch and delivery.

Processed data:

- Name and address details of recipients

Purpose of processing:

- Maintaining verifiable records of postal correspondence

Legal basis:

- Legitimate interest of the controller in verifying that correspondence has been sent – **UK GDPR Article 6(1)(f)**

Data source:

- The company's internal mailing log or records

Final Provisions and Additional Information

All incoming enquiries are retained in accordance with the retention periods specified in this Privacy Policy, depending on the nature and subject of the request.

Proof of posting and delivery of outgoing correspondence is retained together with the relevant document, and stored in line with the applicable retention periods.

Other Data Processing Not Explicitly Mentioned

The Controller may carry out additional data processing activities not explicitly described in this Privacy Policy. In such cases, prior to any processing, clear and transparent information will always be provided to the data subject, and these processing activities will also fall under the scope of this Policy.

Supervisory Authority – Contact Details

Name: Information Commissioner's Office (ICO)
Head Office: Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF, United Kingdom
Helpline: +44 (0)303 123 1113
Website: https://ico.org.uk
Online complaints form: https://ico.org.uk/make-a-complaint/

This Privacy Policy is effective from **20 MAY 2025** and remains in force until amended or withdrawn.

The Controller reserves the right to unilaterally modify this Policy at any time.

For further clarification or assistance related to this Policy or the interpretation thereof, please contact us via email at **hello@absolutetantra.com**.

ADATKEZELÉSI TÁJÉKOZTATÓ ÉS SZABÁLYZAT

– Hatályos: 2025. május 20. napjától

BEVEZETÉS

Az absolutetantra.com weboldalt működtető Spirit Service Ltd (székhely: 1 Hova Villas, Hova House, Hove, BN3 3DH, Egyesült Királyság; cégjegyzékszám: 08593252; UTR szám: 7943000133) – a továbbiakban: Adatkezelő – és munkatársai elkötelezetten védenek minden olyan személyes adatot, amely az ügyfelekhez vagy más harmadik felekhez, így például a honlap látogatóihoz köthető (a továbbiakban együttesen: Érintettek). Kiemelt jelentőséget tulajdonítanak az egyéni önrendelkezés jogának és a személyes adatok bizalmas kezelésének.

Jelen szabályzat célja, hogy biztosítsa az Adatkezelő működésének összhangját a mindenkor hatályos adatvédelmi előírásokkal, valamint hogy világos és érthető tájékoztatást adjon az Érintettek számára az adatkezelésük módjáról és feltételeiről. Az Adatkezelő az összes adatkezelési tevékenységét a jelen dokumentumban (továbbiakban: Szabályzat), valamint a belső előírásaiban és irányelveiben foglaltak szerint végzi.

A Szabályzat általános része minden adatkezelési műveletre alkalmazandó alapelveket és eljárásokat tartalmaz, míg a különös rész az egyes konkrét adatkezelési helyzetekre vonatkozó előírásokat és információkat részletezi. Bár a dokumentum átfogó képet ad az Adatkezelő főbb adatkezelési gyakorlatairól, fontos megjegyezni, hogy ezek nem minden Érintettre vonatkoznak automatikusan. Az adott adatkezelés megkezdésekor az Adatkezelő külön, rövidített tájékoztatót bocsát az Érintettek rendelkezésére, amely az aktuálisan érintett adatok kezelésének részleteit tartalmazza.

Kérjük, szánjon időt a szabályzat teljes tartalmának áttanulmányozására, hogy átfogó képet kapjon az adatkezelési elveinkről és az Ön jogairól!

Az Adatkezelő a birtokába jutott, illetve számára továbbított személyes adatokat bizalmasan kezeli, a vonatkozó adatvédelmi jogszabályoknak megfelelően és a jelen Szabályzatban meghatározott módon. Elsődleges célja, hogy biztosítsa minden érintett számára a jogot saját személyes adatai feletti rendelkezéshez, összhangban a törvényi előírásokkal. Ezen túlmenően az Adatkezelő minden szükséges technikai és szervezési intézkedést megtesz, valamint külön szabályzatok és eljárási

rendek kialakításával gondoskodik az adatok biztonságáról, a titoktartási és adatvédelmi követelmények tényleges érvényesítéséről.

Bár az Adatkezelő célja a lehető legteljesebb körű adatkezelési szabályozás megalkotása volt, előfordulhatnak olyan új adatkezelési tevékenységek, amelyek ebben a Szabályzatban még nem szerepelnek. Ilyen esetekben az Adatkezelő minden alkalommal külön adatkezelési tájékoztatóval látja el az Érintetteket, amely részletes információkat tartalmaz az adott adatkezelés körülményeiről.

A Szabályzat mindenkor érvényes és frissített példányát az Adatkezelő székhelyén elérhetővé kell tenni, emellett az aktuális Szabályzat és annak módosításai online is megtekinthetők az absolutetantra.com/adatkezeles weboldalon.

VONATKOZÓ JOGSZABÁLYOK

(Egyesült Királyságban bejegyzett, de online az EU-ban is aktív szolgáltatást végző cégre vonatkozóan)

Adatvédelem

- **UK General Data Protection Regulation (UK GDPR)**
- **Data Protection Act 2018**
  🔗 gov.uk – Data Protection
  🔗 Data Protection Act 2018
- **Regulation (EU) 2016/679 of the European Parliament and of the Council** (General Data Protection Regulation – GDPR)
  🔗 EUR-Lex – GDPR

Számvitel és pénzügyi beszámolás

- **Companies Act 2006**
- **UK GAAP – UK Generally Accepted Accounting Principles**
  🔗 Legislation – Companies Act 2006
- 🔗 FRC – UK GAAP
  🔗 **FRC – UK Accounting Standards**

Adózás

- **Finance Act** *(évente frissül)*
- **Taxes Management Act 1970**
- **Companies Act 2006,**

- **Money Laundering Regulations 2017.**
- **HMRC guidance**
  🔗 gov.uk – HMRC
- 🔗 Legislation – Taxes Management Act 1970

Pénzmosás és terrorizmus finanszírozása elleni fellépés

- **Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017**
- **Proceeds of Crime Act 2002 (POCA)**
  🔗 MLR 2017
  🔗 Proceeds of Crime Act 2002
- POCA

Reklámtevékenység és kereskedelmi gyakorlat

- **Consumer Protection from Unfair Trading Regulations 2008 (CPRs)**
- **UK Code of Non-broadcast Advertising and Direct & Promotional Marketing (CAP Code)**
  🔗 CPRs 2008
  🔗 CAP Code
- **Directive 2005/29/EC** on Unfair Commercial Practices
  (kötelező lehet, ha az EU-s fogyasztókat célozza a szolgáltatás)
  🔗 EUR-Lex – Directive 2005/29/EC

Elektronikus kereskedelem és információs társadalmi szolgáltatások

- **Electronic Commerce (EC Directive) Regulations 2002**
  🔗 E-commerce Regulations 2002
- **Directive 2000/31/EC** (E-commerce Directive – EU)
  (akkor alkalmazandó, ha az online szolgáltatás célzottan az EU felhasználókat is érinti)
  🔗 EUR-Lex – Directive 2000/31/EC

Fogyasztói szerződések, elállás, tájékoztatás

- **Consumer Contracts (Information, Cancellation and Additional Charges) Regulations 2013**
  🔗 Consumer Contracts Regulations 2013

- **Directive 2011/83/EU** on Consumer Rights
  (alkalmazandó, ha az EU-s fogyasztók is elérhetik a szolgáltatást)
  🔗 EUR-Lex – Directive 2011/83/EU

Fogyasztóvédelem általánosan

- **Consumer Rights Act 2015 (UK)**
  🔗 Consumer Rights Act 2015
- **Consumer Rights Directive (2011/83/EU)**
- **Unfair Commercial Practices Directive (2005/29/EC)**
- **E-commerce Directive (2000/31/EC)**
- **Directive 2009/22/EC** on injunctions for the protection of consumers' interests *(EU)*
  🔗 EUR-Lex – Directive 2009/22/EC

Felnőttképzés és oktatási szolgáltatások

- **Further and Higher Education Act 1992 (UK)**
- **Skills and Post-16 Education Act 2022**
- **Adult Education Budget (AEB)** – funding regulation
  🔗 Further and Higher Education Act 1992
  🔗 Skills and Post-16 Education Act 2022

Tisztességtelen kereskedelmi gyakorlatok tilalma

- **Consumer Protection from Unfair Trading Regulations 2008**
  A fogyasztók védelme érdekében tiltott, megtévesztő vagy agresszív kereskedelmi gyakorlatokkal szembeni szabályozás.
  🔗 Legislation – CPRs 2008

A SZABÁLYZAT CÉLJA

A jelen Szabályzat célja, hogy a benne foglalt rendelkezések alkalmazásával és következetes betartásával elősegítse a vonatkozó jogszabályi előírások – különösen a GDPR és az UK GDPR – gyakorlati érvényesítését. Ennek érdekében az Adatkezelő a Szabályzatban, valamint egyéb belső szabályzataiban, utasításaiban és eljárásrendjeiben foglaltak mentén biztosítja:

- hogy az Érintettek személyes adatokhoz fűződő alapvető jogai ténylegesen érvényesüljenek;

- hogy az adatbiztonságra vonatkozó követelmények teljesüljenek, azok betartása és betartatása minden körülmények között megvalósuljon;

- az illetéktelen hozzáférések megelőzésének gyakorlati szabályait, valamint azokat a garanciákat, amelyek az adatok jogszerűtlen megváltoztatásának, engedély nélküli felhasználásának vagy nyilvánosságra hozatalának meggátolására irányulnak;

- a papíralapú és elektronikus adatkezelési folyamatok – így a tárolás, feldolgozás, továbbítás, felhasználás és megsemmisítés – pontos és biztonságos rendjét;

- továbbá világos, érthető és időben megadott tájékoztatást nyújt az Érintetteknek személyes adataik kezeléséről, jogaikról és azok érvényesítésének lehetőségeiről.

ÁLTALÁNOS RÉSZ

Fogalom-meghatározások

A jelen Szabályzat alkalmazása során az alábbi kifejezések az alábbi jelentéssel bírnak:

„személyes adat”: minden olyan információ, amely egy meghatározott vagy azonosítható természetes személyre (azaz az „érintettre”) vonatkozik. Az a személy tekinthető azonosíthatónak, aki közvetlenül vagy közvetve, például név, azonosítószám, tartózkodási hely, online azonosító, illetve a személy testi, genetikai, fiziológiai, mentális, gazdasági, kulturális vagy társadalmi azonosságára utaló egy vagy több tényező alapján azonosítható. Ide tartozik többek között a név, lakcím, telefonszám, IP-cím, e-mail cím stb.

„adatkezelés”: bármely olyan művelet vagy műveletsorozat – akár automatizált, akár nem –, amelyet személyes adatokkal végeznek. Ide értendő különösen az adatok gyűjtése, felvétele, rendszerezése, tárolása, megváltoztatása, lekérdezése, megtekintése, felhasználása, továbbítása, nyilvánosságra hozatala, hozzáférhetővé tétele, összekapcsolása, korlátozása, törlése vagy megsemmisítése. Minden olyan tevékenység, amely a személyes adatokkal történik – akár azok megtekintése, módosítása vagy továbbítása –, az adatkezelés körébe tartozik.

„profilalkotás”: a személyes adatok automatizált feldolgozásának azon formája, amely során az adatok alapján a természetes személy valamely tulajdonságát elemzik vagy előrejelzik. Ezek a jellemzők vonatkozhatnak többek között a gazdasági helyzetre, egészségi állapotra, személyes preferenciákra, érdeklődési körre, viselkedésre, tartózkodási helyre, vagy akár a megbízhatóságra is.

„álnevesítés”: a személyes adatok olyan technikai módon történő kezelése, amely biztosítja, hogy azok többé ne legyenek hozzárendelhetők egy meghatározott természetes személyhez, kivéve, ha ehhez külön tárolt kiegészítő információkat használnak. Fontos, hogy ezen információk külön elzártan legyenek kezelve, és megfelelő technikai-szervezési intézkedésekkel legyen kizárva a visszavezethetőség.

„nyilvántartási rendszer”: személyes adatok olyan tagolt struktúrája – legyen az központosított, szétosztott, funkcionális vagy földrajzi alapú –, amelyben az adatok meghatározott szempontok szerint kereshetők és hozzáférhetők.

„Adatkezelő”: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy más szervezet, amely önállóan vagy másokkal közösen meghatározza a személyes adatok kezelésének célját és módját. Amennyiben az adatkezelés célját és eszközeit uniós vagy tagállami jog írja elő, úgy az adatkezelő kijelölésére vonatkozó szabályokat is ezek a jogszabályok határozhatják meg.
Jelen dokumentumban az adatkezelő: Spirit Service Ltd.

„Adatfeldolgozó”: olyan természetes vagy jogi személy, hatóság, ügynökség vagy más szervezet, amely az adatkezelő megbízásából és utasítása alapján személyes adatokkal végez meghatározott műveleteket. Adatfeldolgozónak minősül minden olyan külső partner vagy szolgáltató (pl. könyvelő, bérszámfejtő, tárhely- vagy szoftverszolgáltató), aki az adatkezelő nevében eljárva kezeli az adatokat.

„Címzett”: minden olyan természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy egyéb szervezet, akinek a személyes adatot továbbítják vagy aki hozzáfér ezekhez az adatokhoz – függetlenül attól, hogy harmadik félnek minősül-e vagy sem. Azon hatóságok, amelyek törvényi felhatalmazás alapján, például egyedi eljárás keretében hozzáférnek az adatokhoz, nem minősülnek címzettnek.
Címzett lehet például adóhatóság, adatfeldolgozó vagy más jogosult szerv is.

„Harmadik fél”: minden olyan természetes vagy jogi személy, hatóság vagy egyéb szervezet, aki nem azonos sem az érintettel, sem az adatkezelővel, sem az adatfeldolgozóval, illetve nem tartozik azok azon személyei közé, akik az adatkezelő vagy adatfeldolgozó közvetlen irányítása alatt az adatkezeléssel megbízást kaptak.
Vagyis minden olyan fél, aki az adatkezelés folyamatába nem bevont szereplő.

„Az érintett hozzájárulása”: az érintett egyértelmű, önkéntes, megfelelő tájékoztatáson alapuló és konkrét akaratnyilvánítása, mellyel nyilatkozat formájában vagy egy cselekvéssel (pl. weboldalon történő checkbox kipipálásával) kifejezi, hogy beleegyezik a rá vonatkozó személyes adatok kezelésébe.
Fontos: a hozzájárulásnak aktívnak kell lennie – puszta hallgatás, passzivitás nem minősül érvényes hozzájárulásnak.

„Adatvédelmi incidens”: olyan esemény vagy biztonsági hiányosság, amely a személyes adatok véletlen vagy jogsértő megsemmisülését, elvesztését, módosulását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi.
Ide sorolható például: adathordozó vagy mobil eszköz elvesztése, hacker támadás, e-mailek téves címzettnek történő kiküldése, fizetési dokumentumok nem megfelelő tárolása vagy selejtezése, illetve ügyféladatok jogosulatlan másolása.

„A személyes adatok különleges kategóriái”: olyan személyes adatok, amelyek különleges védelem alá esnek, mivel az érintett alapvető jogaira és szabadságaira nézve különösen érzékeny információkat tartalmaznak. Ilyenek például a faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre, szakszervezeti tagságra, egészségi állapotra, szexuális irányultságra vagy biometrikus és genetikai adatokra vonatkozó információk.

„Genetikai adat”: minden olyan személyes információ, amely egy természetes személy örökölt vagy szerzett genetikai tulajdonságaira vonatkozik, és amely az adott személy fiziológiai jellemzőiről vagy egészségi állapotáról hordoz egyedi információt. Ezek az adatok jellemzően a személytől vett biológiai minta – például vér vagy nyál – elemzése útján keletkeznek.

„Biometrikus adat”: olyan személyes adat, amelyet egy természetes személy testi, élettani vagy viselkedési sajátosságai alapján, speciális technikai eljárással állítanak elő, és amely alkalmas az

érintett egyedi azonosítására vagy azonosításának megerősítésére. Ilyen lehet például az arckép, ujjlenyomat vagy retinafelvétel.

„Egészségügyi adat”: olyan személyes információ, amely egy természetes személy testi vagy mentális egészségi állapotára utal. E körbe tartozik az érintett számára nyújtott egészségügyi szolgáltatásokkal kapcsolatos bármely adat is, amennyiben az az érintett egészségi állapotára vonatkozó következtetés levonására alkalmas.

AZ ADATKEZELÉS ALAPELVEI

A személyes adatok kezelése során az alábbi elveket kell érvényesíteni:

- **Jogszerűség, tisztességes eljárás és átláthatóság**: Az adatok feldolgozása kizárólag olyan módon történhet, amely megfelel a vonatkozó jogszabályoknak, tisztességes az érintettekkel szemben, és lehetővé teszi számukra, hogy világos, érthető tájékoztatást kapjanak az adatkezelés minden lényeges körülményéről (például annak céljáról, jogalapjáról, időtartamáról stb.).

- **Célhoz kötöttség**: A személyes adatok kizárólag előre meghatározott, világosan megfogalmazott és jogszerű célból gyűjthetők, és nem kezelhetők ezen célokkal össze nem egyeztethető módon. Kivételt képezhet a közérdekű archiválás, tudományos vagy történelmi kutatás, illetve statisztikai célú további adatfelhasználás.

- **Adattakarékosság**: Csak olyan mértékben és ideig szabad adatokat kezelni, amennyire az az adatkezelés céljának megvalósításához feltétlenül szükséges. Ha az adott cél más módon is elérhető, az adatkezelés nem indokolt.

- **Pontosság**: A személyes adatoknak a valóságnak megfelelőnek kell lenniük, és szükség esetén frissíteni kell azokat. Az adatkezelő köteles minden ésszerű lépést megtenni annak érdekében, hogy a pontatlan adatokat haladéktalanul kijavítsa vagy törölje.

- **Korlátozott tárolhatóság**: Az adatok csak addig őrizhetők meg, amíg az adatkezelés célja ezt indokolja. Az érintett azonosítására alkalmas adatokat a cél megvalósulása után törölni vagy anonimizálni kell, hogy az egyén többé ne legyen beazonosítható.

- **Integritás és bizalmasság**: Az adatkezelést úgy kell megszervezni, hogy az megfelelő technikai és szervezési intézkedések mellett történjen, biztosítva az adatok védelmét a jogosulatlan hozzáférés, jogellenes felhasználás, véletlen elvesztés, károsodás vagy megsemmisülés ellen. Ez magában foglalja az informatikai rendszerek, a fizikai tárolás és a munkafolyamatok biztonságát is.

- **Elszámoltathatóság**: Az adatkezelő kötelessége, hogy az adatkezelés minden szakaszában megfeleljen a fenti elveknek, továbbá képes legyen ezt a megfelelést dokumentált módon igazolni. Ennek érdekében belső szabályzatokat, eljárásokat és utasításokat kell kialakítania, amelyek biztosítják a folyamatok átláthatóságát és ellenőrizhetőségét, különösen hatósági vizsgálat esetén.

AZ ADATKEZELÉS CÉLJAI ÉS JOGALAPJAI

Az adatkezelés célja

Az egyes adatkezelések pontos célját az Adatkezelő minden esetben külön-külön határozza meg, és azokat a szabályzat Különös része részletezi. Általánosságban elmondható, hogy az Adatkezelő az Érintettek személyes adatait a vállalkozás működésével szorosan összefüggő tevékenységei során kezeli, ideértve különösen a szerződéses kapcsolatokból eredő jogok és kötelezettségek teljesítését, valamint a jogos érdekeinek érvényesítését.

Az adatkezelés jogalapja

Az adatkezelés jogalapját az Adatkezelő szintén minden esetben az adott adatkezeléshez igazítva határozza meg, ezek szintén a Különös részben kerülnek rögzítésre.

A GDPR hat különböző jogalapot nevesít, amelyek közül az Adatkezelő az adott adatkezelési tevékenységhez tartozóan alkalmazza a megfelelőt. Az egyik leggyakoribb jogalap az **Érintett hozzájárulása**.

Hozzájáruláson alapuló adatkezelés

Az Érintett hozzájárulása kizárólag önkéntesen, egyértelműen kinyilvánított, aktív magatartással adható meg. A hozzájárulás nem értelmezhető hallgatás vagy passzivitás útján. Érvényes hozzájárulásnak minősül például egy írásos nyilatkozat aláírása (önálló dokumentumban vagy egy szerződésbe foglalva), egy elektronikus felületen történő checkbox kipipálása, vagy egy „hozzájárulok” gombra való kattintás.

Minden adatkezeléshez külön hozzájárulás szükséges, amelyet az Érintett külön-külön jogosult megadni.

Az Érintett bármikor visszavonhatja a korábban adott hozzájárulását. Fontos, hogy a hozzájárulás visszavonása csak a jövőre vonatkozik, a korábban végzett adatkezelések jogszerűségét nem érinti. A visszavonás bármilyen formában történhet – például írásban, e-mailben, telefonon keresztül, vagy egy erre irányuló egyértelmű nyilatkozattal.

Kiskorú vagy korlátozottan cselekvőképes személy esetén: A 16. életévüket be nem töltött személyek, illetve azok, akik cselekvőképességükben korlátozottak, kizárólag akkor adhatnak érvényes hozzájárulást, ha azt helyettük a szülői felügyeletet gyakorló személy, illetve a törvényes képviselő (gyám vagy gondnok) adja meg. Ezért a 16 év alatti Érintettek adatainak kezelése kizárólag szülői vagy gyámi hozzájárulással történhet. Kétség esetén úgy kell tekinteni, hogy a hozzájárulás nem áll fenn.

Adatkezelés szerződés teljesítéséhez kapcsolódóan

Azon esetekben, amikor a személyes adatok feldolgozása elengedhetetlen egy olyan szerződés megkötéséhez vagy teljesítéséhez, amelynek az Érintett maga is részese, az adatkezelés külön hozzájárulás nélkül is jogszerű. Ilyen jogalap alapján történő adatkezelésre tipikusan akkor kerül sor, amikor például a felek között létrejött szerződés tartalmaz személyes adatokat (mint a név, lakcím, elérhetőség stb.), vagy amikor egy szolgáltatás nyújtásához a felhasználó adatait az igénybevétellel összefüggésben kezelni kell.

Adatkezelés jogi kötelezettség teljesítéséhez

Amennyiben jogszabály kötelezi az Adatkezelőt bizonyos adatok kezelésére, az ilyen típusú adatkezelés szintén önálló jogalapot jelent. Ezek az esetek nem választhatók meg szabadon: az Adatkezelő számára kötelező, hogy a törvény által előírt adatkezelési feladatait ellássa. A vonatkozó jogszabályok pontosan meghatározzák, milyen adatokat, milyen célból és mennyi ideig kell kezelni. Ilyen kötelező adatkezelések lehetnek például: a könyvviteli, számviteli nyilvántartások vezetése, számlák kiállítása, pénzmosási előírásoknak való megfelelés, valamint egyéb hatósági kötelezettségek teljesítése.

Adatkezelés közérdekű feladat vagy közhatalmi jogosítvány alapján

Mivel az Adatkezelő nem minősül közhatalmat gyakorló szervnek, így ilyen típusú adatkezelést – amely valamely közérdekű feladat vagy hatósági jogkör gyakorlásához kapcsolódna – nem végez.

Adatkezelés jogos érdek alapján

Egyes adatkezelési tevékenységek olyan jogos érdek érvényesítésén alapulnak, amely az Adatkezelő vagy egy harmadik fél részéről méltányolható és jogszerű célt szolgál. A jogos érdeken nyugvó adatkezelés – szemben a jogszabály által előírt kötelező adatkezeléssel – nem kötelezettség, hanem lehetőség az Adatkezelő számára, amelyet mérlegelés alapján gyakorolhat.

Tipikus példái a jogos érdek jogalapjára épülő adatkezelésnek: az Adatkezelő szolgáltatásainak marketingje és népszerűsítése, a weboldal vagy digitális felületek optimalizálása, valamint a felhasználói szokásokkal kapcsolatos adatgyűjtés – például sütik (cookie-k) alkalmazása.

Fontos megjegyezni, hogy a jogos érdeken alapuló adatkezelés csak akkor jogszerű, ha az Adatkezelő vagy a harmadik fél érdekei nem ütköznek az Érintett olyan alapvető jogaival vagy érdekeivel, amelyek különösen a személyes adatok védelmét szolgálják. Ez különösen érzékeny kérdés, ha az adatkezelés gyermekekre vonatkozik.

Amennyiben az adatkezelés ezen jogalapon történik, az Adatkezelő köteles egy úgynevezett érdekmérlegelési tesztet elvégezni. Ennek során részletesen elemzi az adatkezelés célját, annak eszközeit, és összeveti azzal, hogy az Érintett milyen jogokkal és jogos érdekekkel rendelkezik. Csak abban az esetben kerülhet sor az adatok kezelésére, ha az Adatkezelő vagy a harmadik fél érdeke nyomósabb az Érintett érdekeinél.

Az érdekmérlegelés eredményét az Adatkezelő minden esetben írásban rögzíti. Az Érintettnek joga van tájékoztatást kérni a teszt tartalmáról és annak következtetéseiről.

Az Adatkezelő kizárólag olyan adatokat kezel, amelyeket:

- az Érintett saját maga adott meg közvetlenül;
- nyilvánosan elérhető nyilvántartás (például cégkivonat, egyéni vállalkozók nyilvántartása) tartalmaz;
- harmadik fél jogszerűen rendelkezésre bocsátott.

ÁLTALÁNOS TÁJÉKOZTATÁS AZ ADATKEZELŐ ADATKEZELÉSI TEVÉKENYSÉGEIRŐL

Az Adatkezelőt jogszabály kötelezi arra, hogy az Érintetteket a személyes adataik kezeléséről érthető, világos, tömör és átlátható módon tájékoztassa. Ezt a kötelezettségét a jelen Adatkezelési Szabályzat közzétételével, valamint minden egyes adatkezelés esetében az adatfelvételkor biztosított, rövid adatkezelési tájékoztató útján teljesíti.

Amennyiben Önnek kérdése merülne fel a jelen tájékoztatóval kapcsolatban, vagy élni kíván valamely, az Önre vonatkozó adatkezelési jogával (például hozzáférés, helyesbítés, törlés stb.), kérjük, lépjen kapcsolatba az Adatkezelővel. Az elérhetőségek megtalálhatók jelen Szabályzat záró részében, valamint minden egyedi adatkezeléshez kapcsolódó tájékoztatóban is feltüntetésre kerülnek.

Az Adatkezelés során igénybe vett adatfeldolgozók (megbízott külső szolgáltatók) listáját szintén a Szabályzat végén tüntetjük fel. A Különös rész minden egyes adatkezelésnél a „Címzettek" oszlopban rögzíti az adatfeldolgozó típusát, az általa nyújtott szolgáltatás megnevezésével (pl. tárhelyszolgáltató, könyvelő stb.).

Adatfeldolgozónak kizárólag olyan jogi vagy természetes személy minősülhet, aki írásbeli szerződés alapján vállalja az adatkezeléshez kapcsolódó technikai és szervezési feladatok végrehajtását, és aki garantálja a **General Data Protection Regulation (GDPR)** – illetve az Egyesült Királyságban alkalmazandó **UK GDPR** – szerinti megfelelőséget, különös tekintettel az Érintettek jogainak védelmére és az adatbiztonságra. Az adatfeldolgozónak nincs joga arra, hogy a személyes adatokat saját céljaira felhasználja – kizárólag az Adatkezelő utasításai alapján járhat el.

Az Adatkezelő – a **GDPR 37. cikk (1) bekezdése**, illetve annak angliai megfelelője, a **Data Protection Act 2018, Section 69** és az **UK GDPR Article 37** alapján – jelenleg nem köteles adatvédelmi tisztviselőt kinevezni. Amennyiben a jövőben ilyen kinevezés történik, arról külön tájékoztatásban értesíti az Érintetteket.

Minden egyes adatkezelés célja, jogalapja, az Érintettek által megadott személyes adatok köre, valamint az adatokhoz hozzáférő személyek vagy szervezetek köre a Szabályzat Különös részében részletesen kerül bemutatásra.

Abban az esetben, ha az adatkezelés jogalapja az Adatkezelő vagy egy harmadik fél jogos érdeke, úgy ezt a konkrét jogos érdeket is külön megjelöljük.

Ugyancsak a Különös rész tartalmazza azt is, hogy az egyes adatkezelések során mely címzettek (pl. adatfeldolgozók, hatóságok, egyéb harmadik személyek) kapják meg a személyes adatokat, és milyen célból történik az adattovábbítás.

Az adattovábbítás vonatkozásában az Adatkezelő az alábbi tájékoztatást nyújtja az Érintettek részére:

Adattovábbítás, adatmegőrzés, és az Érintettek jogai – UK székhelyű, EU-ban is aktív vállalkozás esetén

Az Adatkezelő jogosult személyes adatokat átadni bíróságoknak vagy hatóságoknak, amennyiben ez jogi kötelezettségeinek teljesítéséhez vagy a vele szemben fennálló szerződéses kötelezettségek

teljesítéséhez, illetve jogainak érvényesítéséhez szükséges. Az adattovábbítás mértéke és célja mindig az adott ügy természetéhez igazodik.

Továbbá, bizonyos törvényi előírások is szükségessé tehetik adattovábbítást. Ilyen lehet például:

- számlák vagy számviteli bizonylatok tartalmának megküldése az **Egyesült Királyság illetékes adóhatósága**, a **HMRC (His Majesty's Revenue and Customs)** részére, a **Finance Act 2020** és a **Taxes Management Act 1970**előírásai alapján;

- pénzmosás gyanúja esetén történő bejelentés a **National Crime Agency (NCA)** felé a **Proceeds of Crime Act 2002** vagy a **Money Laundering Regulations 2017** szerint;

- adatközlés hatósági vizsgálat vagy jogérvényesítési eljárás során, amennyiben ez elengedhetetlen.

A Data Controller (Adatkezelő) a saját jogos érdekeinek érvényesítése érdekében is továbbíthat személyes adatokat bíróságok vagy hatóságok felé – például:

- követelésbehajtási eljárásban (pl. elmaradt fizetés behajtása),

- bűncselekmény gyanújának bejelentéséhez szükséges adatok továbbítása.

Az Adatkezelő jogosult harmadik feleket, ún. adatfeldolgozókat is bevonni az adatkezelés technikai és adminisztratív támogatására – például: tárhelyszolgáltató, könyvelőiroda, e-mail szolgáltató stb. Az igénybe vett adatfeldolgozók listája a jelen Szabályzat végén található.

Személyes adatok továbbítása az Egyesült Királyság és az EU között

Mivel az Adatkezelő székhelye az Egyesült Királyságban található, de szolgáltatásai az Európai Unió területén is elérhetők, külön figyelmet fordítunk a személyes adatok továbbítására az Egyesült Királyság és az EU/EGT között.

A jelenlegi jogi helyzet szerint:

- az **Európai Bizottság 2021. júniusi megfelelőségi határozata** alapján az Egyesült Királyság „megfelelő védelmi szintet" biztosít a személyes adatok kezelése terén a GDPR értelmében, így az **EU → UK** adattovábbítás **szabadon megengedett**;

- az **UK GDPR** értelmében pedig az **UK → EU/EGT** adattovábbítás is megengedett, mivel az EU tagállamok továbbra is „biztonságos országoknak" minősülnek az Egyesült Királyság jogrendje szerint.

Amennyiben a személyes adatok továbbítása **az EU/EGT-n és az Egyesült Királyságon kívüli** harmadik országba történik (pl. USA, India, Kanada), az Adatkezelő kizárólag az alábbi feltételek mellett végez adattovábbítást:

- ha az adott ország megfelelőségi határozattal rendelkezik az **Európai Bizottság** vagy a **UK Secretary of State for Digital, Culture, Media and Sport** részéről,

- vagy ha az adattovábbításra megfelelő biztonsági garanciák (pl. standard szerződéses feltételek – **Standard Contractual Clauses**, titkosítás, kötelező vállalati szabályok – **Binding Corporate Rules**) mellett kerül sor.

Az Érintettek bármikor jogosultak részletes tájékoztatást kérni az adatátvitel jogalapjáról és biztonsági biztosítékairól, illetve további információkat találhatnak az Európai Bizottság hivatalos oldalán:

👉 https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu_en

AZ ÉRINTETTEK JOGAI A SZEMÉLYES ADATIK KEZELÉSÉVEL KAPCSOLATBAN

Hozzáféréshez való jog

Az Érintett jogosult megerősítést kérni az Adatkezelőtől arról, hogy folyamatban van-e rá vonatkozó személyes adatok kezelése. Amennyiben ilyen adatkezelés zajlik, az Érintett jogosult hozzáférést kapni az alábbi információkhoz:

- az adatkezelés céljai;
- az érintett személyes adatok kategóriái;
- azok a címzettek, illetve címzettek kategóriái, akik számára a személyes adatokat átadták vagy a jövőben átadhatják – ideértve a harmadik országokban vagy nemzetközi szervezeteknél található címzetteket is;
- a tárolás tervezett időtartama, vagy ha ez nem állapítható meg előre, akkor annak meghatározási szempontjai;
- az Érintett azon jogai, hogy kérheti személyes adatainak helyesbítését, törlését, kezelésének korlátozását, továbbá tiltakozhat az adatkezelés ellen;
- a felügyeleti hatósághoz benyújtható panasz lehetősége (az Egyesült Királyságban: **Information Commissioner's Office (ICO)** – ico.org.uk);
- ha a személyes adatokat nem közvetlenül az Érintettől gyűjtötték, akkor azok forrására vonatkozó minden elérhető információ;
- történik-e automatizált döntéshozatal, ideértve a profilalkotást is, valamint az alkalmazott logika, és annak várható következményei az Érintett számára;
- ha az adatokat harmadik országba vagy nemzetközi szervezet részére továbbítják, az Érintett jogosult információt kapni a továbbítás jogalapjáról és az alkalmazott megfelelő biztosítékokról (pl. megfelelőségi határozat, standard szerződéses klauzulák).

Amennyiben Ön tehát szeretné megtudni, hogy az Adatkezelő kezel-e Önre vonatkozó adatokat, és ha igen, milyen formában és milyen feltételek mellett, úgy ezt írásban kérheti az Adatkezelőtől.

Az Adatkezelő – kérés esetén – másolatot bocsát az Érintett rendelkezésére azokról a személyes adatokról, amelyek kezelés alatt állnak. További másolatok esetén az Adatkezelő jogosult adminisztratív költségtérítést felszámítani. Ha a kérelem elektronikus úton érkezik, az adatokat az Adatkezelő elektronikus formátumban adja át, kivéve, ha az Érintett ettől eltérően rendelkezik.

Helyesbítéshez való jog

Az Érintett kérheti az Adatkezelőtől a róla nyilvántartott pontatlan személyes adatok késedelem nélküli helyesbítését. Emellett – a feldolgozás céljának figyelembevételével – jogosult kérni a hiányos adatok kiegészítését, szükség esetén akár külön kiegészítő nyilatkozat útján is.

Kérjük, hogy amennyiben személyes adatai megváltoznak (pl. névváltozás, lakcímváltozás), erről mihamarabb értesítse az Adatkezelőt, hogy a nyilvántartások pontosak és naprakészek maradhassanak.

Az Adatkezelő köteles értesíteni minden olyan címzettet, akivel a helyesbítés előtti személyes adatot közölte – kivéve, ha ez lehetetlen vagy aránytalanul nagy erőfeszítést igényel. Az Érintett kérésére az Adatkezelő tájékoztatást ad ezen címzettekről.

A törléshez való jog (az ún. „elfeledtetéshez való jog")

Az Érintett kérheti, hogy az Adatkezelő indokolatlan késedelem nélkül törölje a rá vonatkozó személyes adatokat. Az Adatkezelő köteles a törlést teljesíteni, ha az alábbi feltételek valamelyike fennáll:

- a személyes adatok már nem szükségesek ahhoz a célhoz, amelyre azokat gyűjtötték vagy kezelték (az adatkezelési cél megszűnt);
- az Érintett visszavonja a hozzájárulását, amely alapján az adatkezelés történt, és nincs más jogalap a további kezelésre;
- az adatkezelés jogalapja az Adatkezelő vagy harmadik fél jogos érdeke, de az Érintett tiltakozik a kezelés ellen, és nincs olyan elsőbbséget élvező jogalap, amely indokolná az adatkezelés folytatását; vagy az Érintett tiltakozik a közvetlen üzletszerzés céljából végzett adatkezelés ellen;
- az adatokat jogellenesen kezelték;
- az adatokat törölni kell egy, az Adatkezelőre vonatkozó jogszabályban (pl. **UK GDPR**, **Data Protection Act 2018**, vagy más kötelező jogi rendelkezésben) foglalt kötelezettség teljesítése céljából.

Amennyiben a személyes adatokat az Adatkezelő nyilvánosságra hozta, és azok törlésére az Érintett kérésére a fenti indokok alapján köteles, az Adatkezelő – figyelembe véve az elérhető technológia szintjét és a megvalósítás költségeit – minden ésszerűen elvárható lépést megtesz annak érdekében, hogy tájékoztassa az ilyen adatokat kezelő más adatkezelőket is a törlés iránti kérelemről. Ez különösen vonatkozik a személyes adatokra mutató linkek, másolatok vagy másodpéldányok eltávolítására irányuló kérés továbbítására.

A törlés megtagadásának jogalapjai

A törlési kérelemnek nem kell eleget tenni, ha az adatkezelés az alábbi célokból továbbra is szükséges:

- a véleménynyilvánítás és a tájékozódás szabadságának gyakorlása érdekében;

- olyan jogi kötelezettség teljesítése érdekében, amely az Adatkezelőre vonatkozik, és amely a személyes adatok megőrzését előírja;
- közegészségügyi célból, amennyiben a kezelés közérdekből történik, és megfelel az Egyesült Királyságban vagy az Európai Unióban érvényes egészségügyi adatvédelmi előírásoknak;
- közérdekű archiválás, tudományos vagy történelmi kutatás, illetve statisztikai célból, amennyiben a törlés veszélyeztetné e célok elérését vagy ellehetetlenítené azokat;
- jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez (pl. folyamatban lévő peres ügyek, követelésbehajtás stb.).

Az Adatkezelő minden olyan címzettet értesít a törlésről, akivel a személyes adatokat korábban megosztotta – kivéve, ha ez lehetetlen vagy aránytalanul nagy erőfeszítést igényel. Az Érintett kérésére az Adatkezelő tájékoztatást ad arról, hogy kiket értesített a törlésről.

A személyes adatok törlésének kérelmezése

Amennyiben Ön úgy ítéli meg, hogy a személyes adatai törlésének feltételei fennállnak, jogosult arra, hogy ezt bármikor kérelmezze az Adatkezelőtől.

Az adatkezelés korlátozásához való jog

Az Érintett kérheti, hogy az Adatkezelő ideiglenesen korlátozza a személyes adatai kezelését, ha az alábbi körülmények bármelyike teljesül:

- Az Érintett vitatja a kezelt adatok pontosságát. Ebben az esetben a korlátozás addig marad fenn, amíg az Adatkezelő ellenőrizni tudja, hogy a vitatott adatok pontosak-e.
- Az adatkezelés jogellenesen történt, azonban az Érintett nem a törlésüket kéri, hanem azt, hogy az Adatkezelő a további felhasználást korlátozza.
- Az Adatkezelőnek már nincs szüksége a személyes adatokra az eredeti célból, viszont az Érintett továbbra is igényt tart azokra jogi eljárás vagy igényérvényesítés céljából.
- Az Érintett tiltakozott az Adatkezelő jogos érdekén alapuló adatkezelés ellen. Ebben az esetben az adatkezelés mindaddig korlátozott marad, amíg nem állapítható meg, hogy az Adatkezelő jogos érdekei elsőbbséget élveznek-e az Érintett érdekeivel és jogaival szemben.

Ha a fenti feltételek alapján az adatkezelés korlátozás alá kerül, akkor az érintett adat kizárólag a következő esetekben kezelhető tovább:

- az Érintett kifejezett hozzájárulásával,
- jogi igény előterjesztése, érvényesítése vagy védelme céljából,
- más természetes vagy jogi személy jogainak védelméhez,
- vagy az Egyesült Királyság (vagy EU) jogrendje szerinti kiemelt közérdek alapján.

A korlátozás feloldásáról az Adatkezelő az Érintettet előzetesen tájékoztatja.

Az Adatkezelő köteles értesíteni minden olyan címzettet, akivel a személyes adatot korábban megosztotta, a korlátozásról – kivéve, ha ez aránytalanul nagy erőfeszítést igényelne vagy lehetetlen. Az Érintett kérésére az Adatkezelő ezekről a címzettekről is tájékoztatást ad.

Amennyiben az Érintett kérelme alapján az adatkezelés korlátozásra kerül, az Adatkezelő az adatokat kizárólag tárolhatja, és azokat kizárólag az Érintett engedélyével vagy jogi igények védelme céljából kezelheti.

Az adathordozhatósághoz való jog

Az Érintett jogosult arra, hogy a róla szóló, általa az Adatkezelő rendelkezésére bocsátott személyes adatokat strukturált, széles körben használt, géppel olvasható formátumban megkapja, és jogosult arra is, hogy ezen adatokat akadálymentesen egy másik adatkezelőnek továbbítsa – feltéve, hogy:

- az adatkezelés jogalapja az Érintett hozzájárulása vagy egy szerződés teljesítése, **és**
- az adatkezelés automatizált módon történik (pl. online rendszer, digitális adatbázisok).

Az Érintett kérheti azt is, hogy az adatok közvetlenül kerüljenek továbbításra az egyik adatkezelőtől a másikhoz, amennyiben ez technikailag megvalósítható. E jog gyakorlása nem sértheti mások jogait és szabadságait, továbbá nem vonatkozik papír alapon tárolt, manuálisan kezelt adatokra.

Az adatok továbbításának kérelmezése más adatkezelő részére

Amennyiben az Ön személyes adatainak kezelése hozzájárulásán vagy szerződés teljesítésén alapul, és az adatok kezelése automatizált módon történik, jogosult arra, hogy kérje az adatai strukturált, elektronikus formában történő átadását akár saját részére, akár egy másik, Ön által megjelölt adatkezelőnek.

Tiltakozáshoz való jog

Az Érintett bármikor jogosult tiltakozni személyes adatainak kezelése ellen, ha az adatkezelés:

- közérdekű feladat végrehajtásához kapcsolódik, vagy
- az Adatkezelő vagy egy harmadik fél jogos érdekén alapul, ideértve az ezen alapokon végzett profilalkotást is.

Tiltakozás esetén a személyes adat a továbbiakban nem kezelhető, kivéve, ha az Adatkezelő képes bizonyítani, hogy az adatkezelést olyan kényszerítő erejű jogos ok indokolja, amely elsőbbséget élvez az Érintett érdekeivel, jogaival és szabadságaival szemben, vagy az adatkezelés jogi igények előterjesztéséhez, érvényesítéséhez vagy megvédéséhez szükséges.

Tiltakozás közvetlen üzletszerzés ellen

Ha a személyes adatokat közvetlen üzletszerzés céljára kezelik (például marketing célú levelezés, hírlevél, remarketing stb.), az Érintett bármikor jogosult tiltakozni az ilyen célú adatkezelés ellen – ideértve a profilalkotást is, ha az ilyen üzleti célhoz kapcsolódik.

Amennyiben az Érintett tiltakozik az ilyen típusú adatkezelés ellen, a személyes adatokat az Adatkezelő e célból többé nem kezelheti.

Összefoglalva: ha az adatkezelés jogalapja az Adatkezelő jogos érdeke, Ön jogosult bármikor kifogással élni a személyes adatai ilyen célú kezelése ellen.

Automatizált döntéshozatal és profilalkotás

Az Érintettnek joga van ahhoz, hogy ne terjedjen ki rá olyan, kizárólag automatizált adatkezelésen – így különösen profilalkotáson – alapuló döntés hatálya, amely rá nézve joghatással bírna, vagy hasonlóan jelentős mértékben érintené.

Ez a jog azonban nem alkalmazható, ha a döntéshozatal:

- az Érintett és az Adatkezelő közötti szerződés megkötéséhez vagy teljesítéséhez elengedhetetlen;
- jogszabályi kötelezettségen alapul, amely egyben megfelelő biztosítékokat is tartalmaz az Érintett jogainak és szabadságainak védelmére (például a **UK GDPR 22. cikk** alapján);
- az Érintett kifejezett hozzájárulásán alapul.

Minden ilyen esetben az Adatkezelő köteles gondoskodni az Érintett megfelelő jogvédelméről, ideértve az emberi beavatkozáshoz való jogot, álláspont kifejtését és a döntés vitatásának lehetőségét.

Panasztételi jog felügyeleti hatóságnál, bírósági jogorvoslat

Az Érintett – függetlenül attól, hogy él-e más közigazgatási vagy bírósági jogorvoslati lehetőséggel – jogosult panaszt benyújtani felügyeleti hatósághoz, ha úgy véli, hogy személyes adatainak kezelése sérti a hatályos adatvédelmi jogszabályokat.

Az Egyesült Királyság területén illetékes felügyeleti szerv:

Information Commissioner's Office (ICO)
📍 Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF
🔗 https://ico.org.uk

Ha az adatkezelés az EU területét is érinti, az Érintett jogosult a lakóhelye, munkahelye vagy az állítólagos jogsértés helye szerinti tagállam felügyeleti hatóságához fordulni (pl. Magyarországon a **Nemzeti Adatvédelmi és Információszabadság Hatóság** – NAIH).

A felügyeleti hatósághoz benyújtott panasz vizsgálata, határidők

Amennyiben az Érintett panasszal fordul egy felügyeleti hatósághoz, a hatóság köteles az ügyet kivizsgálni, és ésszerű határidőn belül tájékoztatást nyújtani az eljárás előrehaladásáról, valamint annak eredményéről. Ez különösen akkor érvényes, ha az ügy további vizsgálatot vagy más felügyeleti hatóság bevonását teszi szükségessé. A panasz alapján a hatóság eljárást is kezdeményezhet az Adatkezelővel szemben.

Adatkezelő válaszadási kötelezettsége

Ha az Érintett az adatkezeléssel kapcsolatos kérelmet nyújt be (pl. törlés, helyesbítés, korlátozás stb.), az Adatkezelő köteles a kérelem beérkezésétől számított legkésőbb 1 hónapon belül tájékoztatást adni a megtett intézkedésekről. Amennyiben nem történik intézkedés, az Adatkezelő köteles indokolni ennek okát, és felhívni az Érintett figyelmét arra, hogy panaszt nyújthat be a felügyeleti hatóságnál, vagy bírósági eljárást kezdeményezhet.

A magyarországi felügyeleti hatóság elérhetőségét a Szabályzat záró szakasza tartalmazza. Az Egyesült Királyság területén az illetékes hatóság:

Information Commissioner's Office (ICO)

📍 Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

🔗 https://ico.org.uk

Jogok korlátozása

Az Érintett adatkezelési jogait korlátozhatják bizonyos esetekben, amennyiben azt az Egyesült Királyságban vagy az EU-ban érvényes jogszabályok (például nemzetbiztonság, bűnüldözés, közigazgatási érdek, közérdek védelme stb.) külön előírják a **UK GDPR Schedule 2** vagy az **EU GDPR 23. cikke** alapján.

Nyilvántartási kötelezettség

Az Adatkezelő köteles belső nyilvántartást vezetni az Érintettek joggyakorlásával kapcsolatos megkeresésekről, valamint az azokkal kapcsolatos válaszairól és intézkedéseiről.

Bírósági jogérvényesítés és kártérítési igény

Az Érintett jogosult bírósághoz fordulni, ha megítélése szerint az Adatkezelő vagy az általa megbízott Adatfeldolgozó a személyes adatokat olyan módon kezeli, amely sérti a hatályos adatvédelmi jogszabályokat – így különösen a **UK GDPR**, a **Data Protection Act 2018**, vagy adott esetben az **EU GDPR** rendelkezéseit.

A jogi eljárást az Érintett választhatja meg: az Egyesült Királyságban lakóhellyel vagy tartózkodási hellyel rendelkező Érintett a helyileg illetékes bíróság előtt is keresetet nyújthat be. Ugyanez vonatkozik az EU területén élő Érintettekre is, akik a saját tagállamuk bíróságán kereshetnek jogorvoslatot.

A bizonyítási teher

Azt, hogy az adatkezelés megfelel a vonatkozó jogszabályi előírásoknak, az Adatkezelő, illetve az Adatfeldolgozó köteles bizonyítani.

Kártérítés és sérelemdíj

Ha az Adatkezelő vagy az általa megbízott Adatfeldolgozó az adatkezelés során jogellenesen járt el, és ezzel másnak kárt okozott – ideértve az adatbiztonsági követelmények megsértését is –, köteles azt megtéríteni.

Amennyiben az Érintett személyiségi joga sérül az adatkezelés következtében, az Érintett jogosult nem vagyoni kártérítésként sérelemdíjat követelni.

Az Adatkezelő az Érintettel szemben akkor is felelős, ha a kárt vagy jogsérelemet a nevében eljáró adatfeldolgozó okozta.

Az Adatkezelő csak abban az esetben mentesül a felelősség alól, ha képes bizonyítani, hogy a kárt vagy a személyiségi jog megsértését olyan, tőle független, elháríthatatlan ok idézte elő, amely kívül esik az adatkezelés körén.

Nem köteles megtéríteni a kárt, és nem jár sérelemdíj, ha az érintett szándékosan vagy súlyosan gondatlanul okozta a jogsértést, vagy a káresemény az Érintett magatartására vezethető vissza.

AZ ADATBIZTONSÁGRA VONATKOZÓ KÖVETELMÉNYEK

A Spirit Service Ltd., mint Adatkezelő, az általa kezelt személyes adatokat elektronikusan és/vagy papír alapon tárolja. A tárolás konkrét módját és helyét az Adatkezelési Szabályzat Különös Része részletezi.

Az adatok védelme érdekében az Adatkezelő minden esetben megfelelő technikai és szervezeti intézkedéseket alkalmaz annak érdekében, hogy megelőzze az adatkezelésből eredő kockázatokat – így különösen a személyes adatok jogosulatlan megismerését, megváltoztatását, törlését, továbbítását, véletlen vagy szándékos megsemmisítését, elvesztését vagy a hozzáférés sérülését.

A digitálisan tárolt személyes adatok jelenleg a **Tárhely.Eu Szolgáltató Korlátolt Felelősségű Társaság** infrastruktúráján kerülnek elhelyezésre.

- Székhely: 1144 Budapest, Ormánság utca 4. X. em. 241
- Cégjegyzékszám: 01-09-909968
- Nyilvántartó bíróság: Fővárosi Törvényszék Cégbírósága
- Weboldal: https://tarhely.eu

Az elektronikus adatkezelés során keletkező vagy elektronikussá átalakított dokumentumok archiválása is a Tárhely.Eu szerverein történik. Az archiválás célja az adatbiztonsági mentések elvégzése és a hosszú távú, biztonságos megőrzés biztosítása.

A Spirit Service Ltd. által használt számítógépek és munkaállomások felhasználói jelszóval védettek, a hozzáférés korlátozott, kizárólag a feladat ellátásához szükséges személyek számára engedélyezett. A hálózaton minden eszköz naprakész vírusvédelmi és rosszindulatú szoftverek

elleni védelemmel van ellátva. Az adatokról rendszeres, ciklikus biztonsági mentés készül, amely felülírással működik.

A fizikai dokumentumtárolás is biztonsági előírások szerint történik: a személyes adatokat tartalmazó iratok zárható szekrényben vagy biztonságos irattárban kerülnek elhelyezésre, víz- és tűzvédelmi szempontokat is figyelembe véve.

Az adatbiztonság fenntartásáról és folyamatos érvényesítéséről a jelen Szabályzat rendelkezései mellett külön belső utasítások és biztonsági szabályzatok gondoskodnak. Az Adatkezelő biztosítja, hogy minden érintett munkatárs, megbízott és adatfeldolgozó megismerje ezen előírásokat, és az adatkezelés során azoknak megfelelően járjon el.

ADATTOVÁBBÍTÁS

A Spirit Service Ltd., mint Adatkezelő, személyes adatokat kizárólag az alábbi esetekben, és kizárólag az alábbi címzettek részére továbbíthat:

- **az adatkezelés céljának megvalósítása érdekében**, olyan adatfeldolgozók vagy önálló adatkezelők részére, akik az adott feladat elvégzéséhez szükségszerű módon részt vesznek az adatok kezelésében;
- **az érintett előzetes, kifejezett hozzájárulása alapján**, bármely olyan címzett részére, akinek részére az érintett engedélyezi az adatok átadását;
- **jogszabályban meghatározott kötelezettség teljesítése érdekében**, vagy hatósági felszólítás alapján, a vonatkozó jogszabályokban nevesített hatóságok, szervek vagy intézmények részére;
- **amennyiben bűncselekmény vagy szabálysértés gyanúja merül fel**, illetve hivatalos megkeresés érkezik, az adatok átadásra kerülhetnek a nyomozó hatóság, a szabálysértési hatóság, illetve az előkészítő eljárást folytató illetékes szerv részére.

ADATFELDOLGOZÁS

A Spirit Service Ltd., mint Adatkezelő, működésének biztosítása érdekében jogosult külső szolgáltatók – például adminisztrációs, könyvelési, postai vagy futárszolgálati partnerek – közreműködését igénybe venni. Ezeknek a szolgáltatásoknak a nyújtása során gyakran elkerülhetetlen bizonyos személyes adatok kezelése is. Ilyen esetekben a Spirit Service Ltd. továbbra is az adatkezelői minőségét őrzi meg, míg a megbízott szolgáltató adatfeldolgozóként (processor) jár el.

Az Adatkezelő kizárólag olyan adatfeldolgozókkal működik együtt, akik megfelelő garanciákat nyújtanak arra vonatkozóan, hogy a személyes adatok kezelését a **UK GDPR**, a **Data Protection Act 2018**, valamint – ha alkalmazandó – az **EU GDPR** rendelkezéseinek megfelelően végzik. E garanciák közé tartoznak a megfelelő technikai és szervezeti biztonsági intézkedések, valamint a dokumentált adatkezelési eljárások is.

Az Adatfeldolgozó személyes adatokkal kapcsolatos feladatainak körét, valamint jogait és kötelezettségeit az Adatkezelő határozza meg, írásban rögzített utasítások alapján. Ezeknek az utasításoknak a jogszerűségéért az Adatkezelő felelős. Az Adatfeldolgozó nem hozhat saját hatáskörben döntést az adatok kezeléséről, és kizárólag az Adatkezelő által kijelölt módon kezelheti azokat.

Az Adatfeldolgozó nem jogosult a tudomására jutott személyes adatokat saját céljaira felhasználni, azokat csak az Adatkezelő előírásai szerint tárolhatja, kezelheti és – szükség esetén – törölheti. A személyes adatok feldolgozása során harmadik adatfeldolgozót kizárólag az Adatkezelő előzetes jóváhagyásával vehet igénybe.

Az adatfeldolgozásról minden esetben írásos szerződést kell kötni, amely egyértelműen meghatározza az adatkezelés célját, időtartamát, természetét, az érintett adatok típusát, az érintettek körét, valamint az Adatkezelő és az Adatfeldolgozó közötti felelősségi viszonyokat, és a **UK GDPR (illetve EU GDPR)** szerinti elvárásokat. Jogszabályi előírás alapján olyan fél nem bízható meg adatfeldolgozással, aki a feldolgozandó személyes adatok üzleti célú hasznosításában érdekelt lehet.

Az Adatkezelő által igénybe vett adatfeldolgozók részletes listáját – megnevezéssel és feladatkörrel – a jelen Adatkezelési Szabályzat végén külön fejezet tartalmazza.

EGYÉB RENDELKEZÉSEK

Szolgáltató partnerek adatkezelése

Az adatkezelő – a Spirit Service Ltd. – tevékenysége során szükségszerűen kapcsolatba kerül olyan természetes és jogi személyekkel, akik beszállítói vagy szolgáltatói jogviszonyban állnak a céggel, vagy ilyen kapcsolat létesítésére törekednek. A partnerekkel megkötött szerződések teljesítéséhez, illetve az azzal kapcsolatos jogi, pénzügyi és adminisztratív kötelezettségek teljesítéséhez az Adatkezelő bizonyos személyes adatokat is kezel.

Az adatok kezelése egyrészt papír alapon történik (például a szerződések és bizonylatok fizikai tárolása az Adatkezelő székhelyén), másrészt elektronikus formában kerül mentésre és archiválásra, a megfelelő adatbiztonsági intézkedések betartása mellett.

1. Magánszemély szerződéses partnerek adatai

Kezelt adatok köre:

- Név, lakcím, anyja neve
- Egyéni vállalkozói nyilvántartási szám, adószám vagy adóazonosító jel
- Névjegykártya adatok (ha rendelkezésre áll)
- Bankszámlaszám (csak ha szükséges)

Adatkezelés célja:

- A szerződéses partner azonosítása

- A szerződés előkészítése és teljesítése

Jogalap:

- A szerződés teljesítéséhez szükséges adatkezelés – **UK GDPR Article 6(1)(b)**
  (és ha az EU-s érintettek adatait is kezelik: **EU GDPR Article 6(1)(b)** is)

Kapcsolattartás céljából kezelt további adatok:

- E-mail cím, telefonszám
- Kapcsolattartó megjelölése esetén: neve, beosztása, elérhetősége, névjegykártya adatai

Jogalap:

- A szerződés teljesítése – **UK GDPR 6(1)(b)**
- Amennyiben a kapcsolattartó nem azonos a szerződő féllel: jogos érdek – **UK GDPR 6(1)(f)**
  (azaz az adatkezelő jogos érdeke a folyamatos és biztonságos üzleti kommunikáció biztosítása)

Adatok forrása:

- Érintettől közvetlenül, vagy a kapcsolattartó kijelölése esetén a szerződő féltől

Számlázási adatok kezelése

Kezelt adatok:

- Számlázási adatok

Adatkezelés célja:

- Számlák, bizonylatok kiállítása és megőrzése

Jogalap:

- Jogszabályi kötelezettség teljesítése – **UK GDPR 6(1)(c)**
- Megfelelő brit számviteli szabályozás: **Companies Act 2006**, **Finance Act**, **HMRC regulations**

Címzettek:

- Könyvelő és számlázási szolgáltató (mint adatfeldolgozók)
- HM Revenue & Customs (HMRC), mint önálló adatkezelő, ha jogszabály ezt előírja

2. Jogi személy szerződéses partnerek adatai

Kezelt adatok köre:

- Az adott cég képviseletében eljáró természetes személy neve, beosztása
- Névjegykártya információ (ha rendelkezésre áll)
- Kapcsolattartó elérhetőségei (név, e-mail, telefonszám, beosztás)

Adatkezelés célja:

- Szerződéses viszony létrehozása és teljesítése
- Folyamatos kapcsolattartás fenntartása

Jogalap:

- Szerződéses kötelezettség teljesítése – **UK GDPR 6(1)(b)**
- Jogos érdek a kapcsolat folyamatos biztosítása céljából – **UK GDPR 6(1)(f)**

Adatok forrása:

- Közvetlenül az érintettől, vagy jogi személy partnertől

Beérkező és kimenő levelezés, dokumentumkezelés

1. A szerződéses dokumentumok adatmegőrzési ideje

A szerződés teljesítésének igazolásához, illetve a megállapodás tartalmának bizonyításához szükséges személyes adatokat az adatkezelő a jogviszony megszűnését követően legfeljebb 5 évig kezeli, összhangban a polgári jog szerinti általános elévülési idővel. Az olyan dokumentumok esetében, amelyek számviteli bizonylatnak minősülnek (pl. számlák), az adatkezelés időtartama az adott bizonylat kiállításának évét követő 8 év a **UK Companies Act 2006** és a **UK GAAP**előírásainak megfelelően.

Amennyiben a szerződés megszűnését követően az adatkezelés jogalapja már nem áll fenn (pl. a képviseleti vagy kapcsolattartói minőség megszűnik), az adatokat haladéktalanul törölni kell.

2. Készpénzes teljesítés és ügyfél-azonosítás

A Spirit Service Ltd. nem fogad el 3,000,000 HUF-nak megfelelő összeg feletti készpénzes teljesítést, kizárólag banki utalás útján történő fizetést. Ennek következtében az **Anti-Money Laundering (AML)** kötelezettségek – ideértve a Pmt. (Hungarian Act LIII of 2017) szerinti ügyfélazonosítást – a jelen gyakorlat alapján rendszerint nem alkalmazandók. Amennyiben mégis felmerül ilyen igény, a Társaság külön, részletes tájékoztatást nyújt az érintett számára az azonosítás körülményeiről.

3. Beérkező megkeresések kezelése

A **hello@absolutetantra.com** e-mailre érkező kérdések, megkeresések feldolgozása az erre kijelölt munkatárs hatáskörébe tartozik. A beérkező megkeresések a szervezet megfelelő részlegeihez

kerülnek továbbításra. Ennek során az adott megkeresésben szereplő személyes adatok kezelése szükségessé válhat.

Az elektronikus úton érkező megkeresések egyedi szabályozás alapján archiválásra kerülnek, digitálisan tárolva, valamint nyomtatott formában is iktatva. Az e-mail fiókokban beérkező levelek manuális szűrést követően, a feldolgozás után törlésre kerülnek.

Jogalap:

- Jogos érdek a vállalat hatékony és szabályszerű működéséhez fűződő érdeken alapulva – **UK GDPR Article 6(1)(f)**
- Amennyiben a megkeresés meglévő szerződéshez kapcsolódik, az adatkezelés jogalapja a szerződés teljesítése – **UK GDPR Article 6(1)(b)**

Forrás:

- Az érintett (a megkeresést küldő személy)

4. Kimenő postai küldemények (feladóvevények és tértivevények)

A társaság által kiküldött levelek és csomagok postai feladóvevényei, valamint a tértivevények a küldemény visszaérkezését követően archiválásra kerülnek, együtt az adott levél példányával. A nyilvántartás célja a postai feladás és kézbesítés igazolása.

Kezelt adatok:

- Címzéshez kapcsolódó személyes adatok

Cél:

- A postai küldemények dokumentált kezelése, a feladás és kézbesítés igazolása

Jogalap:

- Jogos érdek az adatkezelő oldalán, a levelezés hiteles igazolására – **UK GDPR Article 6(1)(f)**

Forrás:

- Az adatkezelő postázási nyilvántartási rendszere

Záró rendelkezések és kiegészítő információk

A beérkező megkeresések tartalmától és tárgyától függően azokat a jelen Adatkezelési Tájékoztatóban meghatározott megőrzési idő szerint tároljuk.

A kimenő levelezéshez kapcsolódó feladóvevények és tértivevények minden esetben az adott küldeményhez kapcsolva, az arra vonatkozó megőrzési időszaknak megfelelően kerülnek archiválásra.

Egyéb, nem részletezett adatkezelések

Az Adatkezelő a jelen Adatkezelési Tájékoztatóban külön nem részletezett adatkezelési műveleteket is végezhet. Ilyen esetekben az adatkezelés megkezdése előtt az érintett mindig világos és átlátható tájékoztatást kap. Ezek az adatkezelések is a jelen Tájékoztató hatálya alá tartoznak.

Felügyeleti Hatóság – Elérhetőségek

Név: Information Commissioner's Office (ICO)
Székhely: Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF, United Kingdom
Telefon: +44 (0)303 123 1113
Weboldal: https://ico.org.uk
Online panaszbejelentés: https://ico.org.uk/make-a-complaint/

Jelen Adatkezelési Tájékoztató **2025. május 20. napjától** érvényes, és hatályban marad visszavonásáig vagy módosításáig.

Az Adatkezelő fenntartja a jogot, hogy a Tájékoztatót bármikor egyoldalúan módosítsa.

Ha a dokumentummal kapcsolatban bármilyen kérdésed vagy értelmezési bizonytalanságod merül fel, kérjük, írj nekünk a következő e-mail címre: **hello@absolutetantra.com**.