

Privacy Notice

ABIC Enterprise Korlátolt Felelősségű Társaság (limited liability company)

Version: v2.0 · Effective from 26 August 2026

1. Purpose, scope and structure of this notice

ABIC Enterprise Korlátolt Felelősségű Társaság (registered seat: 2724 Újlengyel, Nyári Pál utca 15., Hungary; company registration number: 13-09-240332; tax number: 32807727-2-13; represented independently by Csaba Binó and Balázs Jakobicz, managing directors; electronic contact: info@abicenterprise.com; hereinafter the **Company** or the **Controller**) treats all personal data as confidential and takes the technical and organisational measures necessary to protect personal data.

This notice sets out **for what purposes, on what legal basis, what data, for how long and with whose involvement** the Company processes personal data, and what rights data subjects may exercise.

This notice applies to the following activities of the Company:

#	Processing activity	Data subjects concerned
5.1	Website enquiries and requests for quotation	prospective clients, client representatives
5.2	Contact data of clients, suppliers and partners	staff of contractual partners
5.3	Business development (B2B) outreach and client relationship records	contact persons at target companies
5.4	Newsletters and professional updates	subscribers
5.5	Operation of the website, cookies and log data	website visitors
5.6	Expert database and staffing process	applicants registering as experts
5.7	Data of employees and subcontractors after conclusion of a contract	employees, subcontractors

#	Processing activity	Data subjects concerned
5.8	Enforcement of legal claims, complaint and incident handling	all data subjects

This notice does not apply to processing that the Company carries out **as a processor**, on the instructions of its client, within the framework of a client project. In such cases the client is the controller and the client's own privacy notice applies.

For the detailed rules governing employment relationships and contractor or mandate relationships, the Company uses a separate notice provided directly to the data subject at the time of contracting. That notice is to be read together with this one; in the event of any discrepancy, the activity-specific notice prevails.

2. The controller and its contact details

Name	ABIC Enterprise Korlátolt Felelősségű Társaság
Registered seat	2724 Újlengyel, Nyári Pál utca 15., Hungary
Company registration number	13-09-240332
Tax number	32807727-2-13
Representation	Csaba Binó and Balázs Jakobicz, managing directors, each acting independently
General e-mail	info@abicenterprise.com
Data protection matters	info@abicenterprise.com
Telephone	+36 70 883 3122
Website	https://www.abicenterprise.com
Data protection contact person	Dr. Dániel Jávör, data protection contact person

Data protection officer. Under Article 37 GDPR the Company is not required to designate a data protection officer: it is not a public authority, its core activities do not consist of the regular and systematic monitoring of data subjects on a large scale, and it does not process special categories of data on a large scale. Data protection matters are handled by the Company's **data protection contact person**, who can be reached at info@abicenterprise.com.

3. Definitions

Term	Meaning
GDPR	Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
Personal data	any information relating to an identified or identifiable natural person (the “data subject”); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier – such as a name, an identification number, location data or an online identifier – or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Special category data	data referred to in Article 9 GDPR: data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, genetic and biometric data, health data, and data concerning a person's sex life or sexual orientation.
Processing	any operation or set of operations performed on personal data or on sets of personal data, whether or not by automated means, including collection, recording, organisation, storage, use, disclosure, transmission, restriction, erasure or destruction.
Controller	the body or person that determines the purposes and means of the processing of personal data.

Term	Meaning
Processor	the body or person that processes personal data on behalf of and on the instructions of the Controller.
Recipient	the body or person to which personal data are disclosed, whether or not a third party.
Third country	a country outside the European Economic Area (EEA).
Profiling	any form of automated processing of personal data consisting of the use of those data to evaluate or predict certain personal aspects relating to a natural person – such as performance at work, economic situation, personal preferences or reliability.
Pseudonymisation	the processing of personal data in such a manner that the data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately.
Consent of the data subject	any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
Personal data breach	a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or unauthorised access to, personal data processed.

4. Data protection principles

The Company processes personal data lawfully, fairly and in a manner that is transparent to the data subject. It collects data only for specified, explicit and legitimate purposes, and only to the extent necessary to achieve those purposes. It keeps the data up to date, retains them only for as long as the purpose requires, and protects them by appropriate security measures.

The Company maintains a record of all its processing activities in accordance with Article 30 GDPR and is able to demonstrate compliance with these principles (accountability).

5. The individual processing activities

5.1 Website enquiries and requests for quotation

Aspect	Details
Categories of data processed	name, e-mail address, telephone number, the name of the organisation represented and the data subject's position, together with the text of the message and any attachment to it.
Purpose of the processing	receiving and answering the enquiry, preparing a quotation for the services, and documenting the communication.
Legal basis	Article 6(1)(b) GDPR – where the enquiry concerns the Company's services, the processing is necessary in order to take steps at the data subject's request prior to entering into a contract; Article 6(1)(f) GDPR – for other enquiries, the Company's legitimate interest in answering and documenting business communications addressed to it.
Retention period	12 months from the closure of the enquiry. If a contractual relationship is established, the data continue to be processed in accordance with section 5.2. Where legislation prescribes a longer period, that period applies.
Consequences of failing to provide the data	an e-mail address is required in order to answer the enquiry; without it the Company is unable to reply.

5.2 Contact data of clients, suppliers and partners

Aspect	Details
Categories of data processed	the contact person's name, position, business e-mail address and telephone number, the details of the organisation represented, correspondence arising in the course of the contractual cooperation, and documents relating to performance.
Purpose of the processing	preparing, concluding and performing the contract, maintaining contact, invoicing, and retaining accounting records as required by accounting and tax legislation.
Legal basis	Article 6(1)(b) GDPR – where the contracting party is a natural person (for example a sole trader); Article 6(1)(f) GDPR – in the case of the contact person of a legal-person contracting party, the legitimate interest of the Company and of the partner in maintaining the contact necessary to perform the contract; Article 6(1)(c) GDPR – as regards the data appearing on accounting records, on the basis of Section 169 of Act C of 2000 on Accounting.
Retention period	5 years from the termination of the contractual relationship (the general limitation period under the Hungarian Civil Code), and, in the case of accounting records, 8 years from the creation of the record.

5.3 Business development (B2B) outreach and client relationship records

The Company contacts the **professional contact persons** of organisations likely to be interested in its services for business purposes, and keeps a record of whom it contacted, when and through which channel. The name of a contact person is personal data even where we process it solely in a professional capacity.

Aspect	Details
Categories of data processed	name, position, name of the employing organisation, business contact details, the address of the public professional profile, the date and channel of the outreach, whether a reply was received, and the data subject's country.
Source of the data (Article 14 GDPR)	publicly available professional and corporate sources – the organisation's website, the company register, professional social networks, conferences and industry publications – and data provided by the contact person in person.
Purpose of the processing	presenting the Company's services to organisations potentially concerned, and recording who has requested to be excluded, so that no repeated outreach takes place.
Legal basis	Article 6(1)(f) GDPR – the Company's legitimate interest in establishing business contact and in acquiring business. The Company has carried out a legitimate interest assessment, which is available on request. The electronic communications (“ePrivacy”) rules of the data subject's country also apply to the channel of the outreach; the Company takes these into account for each individual contact.
Retention period	24 months from the outreach where the data subject does not respond. If the data subject objects (“I do not wish to receive further contact”), the Company keeps the data subject on a suppression list solely for the purpose of preventing further outreach, using only the data strictly necessary for that purpose: name, e-mail address and the date of the objection.
Right to object	the data subject may object to outreach based on legitimate interest at any time and without giving reasons, at info@abicenterprise.com or via the unsubscribe link included in the message. Upon objection, the Company ceases the outreach without delay.

5.4 Newsletters and professional updates

Aspect	Details
Categories of data processed	name, e-mail address, the date of subscription, the identifier of the text version accepted at the time of subscription, and delivery and open data.
Purpose of the processing	sending the Company's professional content, newsletters and event invitations.
Legal basis	Article 6(1)(a) GDPR – the data subject's consent. Giving consent is voluntary, is not a condition of any service, and may be withdrawn at any time free of charge. Withdrawal does not affect the lawfulness of processing carried out before the withdrawal.
Retention period	until consent is withdrawn. Thereafter the Company keeps a record of the unsubscription on a suppression list in order to prevent further messages being sent.

5.5 Operation of the website, cookies and log data

The Company's public website is available at www.abicenterprise.com, including the careers page (/careers). This section relates to that public website.

Technical log data. In the course of operating the website the system records log data: IP address, browser and device type, the time of the visit, the page viewed and the address of the referring page. Legal basis: the Company's legitimate interest in the secure and proper operation of the website (Article 6(1)(f) GDPR). Retention period: no more than 12 months.

What a cookie is. A cookie is a small data file placed on the visitor's device that the website reads back during the visit. The Company treats technologies similar to cookies — such as the browser's local storage — in the same way as cookies.

Category	What it does	Legal basis and retention period
Strictly necessary	the basic operation of the website, maintaining the session, security, and remembering the cookie setting	legitimate interest – Article 6(1)(f); may be used without consent; no more than 12 months

Category	What it does	Legal basis and retention period
Statistical (analytics)	aggregate measurement of the number and source of visits and of movement within the site, in order to improve the website	consent – Article 6(1)(a); not loaded until consent is given; no more than 12 months, or until consent is withdrawn
Marketing and advertising tracking	the Company does not use such cookies and does not pass data collected on the website to third parties for advertising purposes	—

Consent to statistical cookies may be given via the cookie settings interface displayed on the website, may be refused there just as easily, and may be withdrawn at any time free of charge. Withdrawal does not affect the lawfulness of processing carried out before the withdrawal. The Company uses statistical data in aggregate form; it does not take decisions concerning individual visitors on that basis.

The cookies and browser-side storage actually used are the following. Genuine HTTP cookies arise solely from statistical measurement; all other items remain in the local storage of the visitor's browser and are not uploaded to the Company's servers.

Name	Type	Purpose	Lifetime
_ga, _ga_Y65MER0QJN	HTTP cookie (Google Analytics 4)	traffic measurement	2 years
abic_consent	localStorage	storing the cookie decision	persistent, until deleted
i18nextLng	localStorage	the selected language (HU/EN/DE)	persistent, until deleted
theme	localStorage	light/dark display mode	persistent, until deleted

Name	Type	Purpose	Lifetime
abic_expert_application_draft	localStorage	draft of the application form	deleted upon submission
scroll-pos:*	sessionStorage	remembering the scroll position	until the end of the browser session

Statistical measurement runs within the Google Consent Mode framework: the default state of analytics_storage is “denied”, meaning that the measurement cookie is not placed until consent is given. The Company records the cookie decision in the abic_consent store. The Company does not use marketing or advertising tracking cookies.

The draft of the application form. The application form on the careers page saves a draft while it is being completed, so that an application that has been started can be continued later. The draft remains solely on the visitor's own device, in the browser's local storage (abic_expert_application_draft); it is not uploaded to the Company's servers and is deleted upon submission; it also disappears if the browser data are cleared. If no submission is made, the Company does not become aware of the content of the draft. Only a finally submitted application reaches the Company's server, and it reaches the system managing the expert database only after confirmation of the e-mail address (double opt-in).

Browser settings. Visitors may at any time delete previously placed cookies in their browser settings and block the placing of new ones. If strictly necessary cookies are blocked, certain functions of the website will not work properly.

5.6 Expert database and staffing process

The Company delivers its SAP consulting and digital transformation services using its own staff and contracted subcontractors. For this purpose it maintains an **expert database** of professionals who apply to it with a view to cooperation.

An important distinction. The Company is neither a recruitment agency nor a temporary work agency. It does not process applicants' data in order to sell them to another company, but in order to plan the expert capacity needed to perform its own service contracts. The Company does not sell or rent out its database, and

transfers data to third parties only with the data subject's separate, project-specific consent.

The application route. An application submitted on the careers page does not enter the expert database automatically. The steps of the process are as follows:

Step	What happens
1. Submission and e-mail confirmation	After submission the Company sends a confirmation e-mail. The data become available for processing only after the e-mail address has been confirmed (double opt-in).
2. Separate register	The confirmed application waits in a separate register; at this point it is not yet part of the expert database.
3. Admission decision	A member of our staff opens each application individually and decides whether to admit or reject it.
4. Pre-screened pool	If admitted, the applicant enters the pre-screened pool of the expert database.
5. Qualified pool	An applicant enters this pool only where valid consent, a signed Cooperation Declaration and a processed CV are all available. It is from this pool that the Company approaches professionals with specific project opportunities.

There is no automatic progression at any stage; every admission is decided by a member of our staff.

If the Company rejects an application, it erases the applicant's data within 30 days of the rejection. Thereafter only the minimised evidential log described in section 5.6.6 is retained.

5.6.1 Categories of data processed

Data group	What it contains
Provided by the data subject	name, e-mail address, telephone number, place of residence (country, city), CV and its content (qualifications, work experience, SAP module knowledge, project references, language skills, certifications), the professional data entered in structured form on the application form (specialist category, SAP modules, language skills with levels according to the Common European Framework of Reference [CEFR], region), availability data (from when, on what proportion of time, willingness to work on site), the preferred form of engagement (employment, subcontractor relationship or both), fee expectations, and, in the case of an application as a subcontractor, the details of the business (company name, registered seat, tax number).
Recorded automatically by the system	the application identifier, the time of the application and of the consent, the identifier and language of the text version of the consent, the source of the application (form URL) and its IP address, the time of confirmation of the e-mail address (double opt-in), the confirmation identifier and the IP address of the confirmation, and the version numbers of the documents accepted. These are needed so that the Company can demonstrate the lawfulness of the processing.
Recorded by the Company itself during the process	the status of the application (received, admitted, rejected, qualified), the time of the decision and the identifier of the member of staff taking it, internal professional notes and assessments concerning the applicant, the fact and time of the professional profile being presented to a client or delivery partner, and events relating to the renewal of consent. These data fall within the scope of the right of access under Article 15 GDPR: at the data subject's request the Company also provides information on them, to the extent that this does not adversely affect the rights of others.

Data group	What it contains
Source of the data	as regards the data provided by the applicant, exclusively the data subject. The Company does not collect data for the expert database from CV databases or by purchasing data. Where the Company itself approaches professionals from public professional sources, section 5.6.7 applies; the data of a professional approached in this way enter the expert database only through his or her own application.
Data the Company expressly does not request and does not process	health data, religious or political beliefs, trade union membership, ethnic origin, sexual orientation, criminal offence data, photographs, date of birth and marital status. The Company asks data subjects to omit these from their CVs as well. Should such data nevertheless reach the Company, it erases them and does not take them into account in the selection process.
Consequences of failing to provide the data	submitting an application requires a name, an e-mail address, a CV and availability data — without these the Company cannot assess which project requirement the profile might match, and the application therefore cannot be submitted. Providing a telephone number, place of residence and fee expectations is voluntary; their absence is not an obstacle to applying, but makes it harder to find a suitable project.

5.6.2 Purposes, legal bases and retention periods

Purpose	Legal basis	Retention period
Receiving the application, confirming the e-mail address, and deciding on admission or rejection	consent – Article 6(1)(a)	until the decision; in the case of rejection, from the date of the decision: 30 days

Purpose	Legal basis	Retention period
Internal status, note and assessment data arising during the application process	consent – Article 6(1)(a), together with the Company's legitimate interest in documenting its decisions – Article 6(1)(f)	for the same period as the related applicant data
Storage in the expert database, approaches with project opportunities	consent – Article 6(1)(a)	12 months , renewable
Assessment of an application received for a specific advertised position	steps prior to entering into a contract – Article 6(1)(b)	until the selection process is closed
Sending the professional profile to a client or delivery partner	separate consent – Article 6(1)(a)	until the given selection process is closed
Handling the Cooperation Declaration and demonstrating its performance	contract – Article 6(1)(b), enforcement of legal claims – Article 6(1)(f)	the term of the declaration, plus 5 years
Sending a reminder to renew consent	consent – Article 6(1)(a); the reminder is an inseparable part of managing the consent	until expiry
Demonstrating that consent was given and withdrawn	accountability – Article 5(2), together with the legitimate interest in the establishment, exercise and defence of legal claims – Article 6(1)(f). Article 7(1) is a requirement to demonstrate compliance, not an independent legal basis.	5 years after erasure, in minimised form

Purpose	Legal basis	Retention period
Newsletters, professional updates	separate consent – Article 6(1)(a)	until withdrawal

5.6.3 The four separate consents

The application form contains four independent checkboxes. None of them is pre-ticked, and a separate log entry is created for each:

Checkbox	What it means
storage of the data in the expert database	this is a condition of registration, because without consent there is nothing to store;
acceptance of the Cooperation Declaration	this is a contractual declaration, not a data protection consent; the two have different legal treatment;
sending the professional profile to a client	optional, and may also be given later, on a project-by-project basis;
newsletters and professional updates	optional.

Items 3 and 4 are **not a condition** of registration: an application is complete without ticking them, and the data subject is entered in the database in the same way. Any consent may be withdrawn at any time, free of charge and as easily as it was given.

5.6.4 The 12-month time limit and renewal

The Company retains the data for **12 months** from the date on which consent was given. The reason for this period is the principle of accuracy: the most important elements of an SAP consultant profile – the current project, availability, the most recent module knowledge and fee expectations – typically change within a single project cycle, and the accuracy of the data could therefore not be ensured if they were stored for longer.

The renewal process is as follows:

When	What happens
30 days before expiry	The Company contacts the data subject by e-mail and shows what data it stores about him or her.
7 days before expiry	The Company repeats the reminder.
If confirmed	Processing continues for a further 12 months, and may be repeated an unlimited number of times.
If there is no reply	The Company erases the data automatically and permanently.

If there is no reply, the Company erases the data automatically and permanently. Silence is not consent. The Company regards only an express renewal statement as a renewal — not the opening of an e-mail, a click on a link, or a reply to a project offer.

Self-service interface. The Company includes in every outgoing e-mail a personal link, requiring no login, through which the data subject can view and update the data stored, renew or withdraw consent, and request erasure of the data. Erasure takes no more steps than registration did.

5.6.5 Transfer of data to a client or delivery partner

The Company sends the professional profile to a client or delivery partner only where the data subject has consented **in advance, expressly and in respect of the given project**. Before requesting that confirmation, the Company specifies:

- **to whom** the profile will be sent (a named client, not a general description),
- **for which position,**
- **exactly what** will be sent (a full CV or an anonymised professional profile),
- **how long** the confirmation remains valid.

As a first step — where the client's selection process allows this — the Company sends an **anonymised professional profile** that does not contain the data subject's name or current employer.

From the moment the profile is sent, the client becomes an **independent controller** and acts in accordance with its own privacy notice. The Company

stipulates in its contracts that the client may use the profile solely for the given selection purpose and must erase the data of unsuccessful candidates once the process is closed. If the data subject later requests erasure from the Company, the Company erases its own systems, but can no longer erase the copy lawfully transferred to the client earlier. The data subject must be aware of this before giving the confirmation.

5.6.6 What the Company retains after erasure

Under Article 7(1) GDPR the Company must be able to demonstrate that valid consent was in place. For this reason it retains, after erasure, only a minimised evidential log:

Item retained	Why
A salted hash of the e-mail address	not the e-mail address itself, but an irreversible hash of it
The time of consent	to demonstrate that valid consent was in place
The time of withdrawal or expiry	to demonstrate when the processing ceased
The identifier of the text version	to demonstrate which version of the text the data subject accepted
What the Company does not retain	name, CV, telephone number and any other data capable of identifying the person
Retention period of the log	5 years

5.6.7 Sourcing professionals from public professional sources

Because professionals in niche SAP areas are available only in limited numbers, the Company also identifies professionals itself from public professional sources and contacts them, inviting them to apply to the expert database. This is processing separate from and independent of that described in sections 5.6.1–5.6.6, because at this stage the data do not originate from the data subject.

Aspect	Details
Categories of data processed	name, the address of the public professional profile, current or former role and employer, area of specialisation and module knowledge, region, and the date and channel of the outreach and whether a reply was received. At this stage the Company does not process CVs, fee expectations or private contact details.
Source of the data (Article 14 GDPR)	publicly available professional sources — professional social networks, conference and speaker lists, professional publications and company websites. The Company does not purchase data and does not collect data from CV databases.
Legal basis	Article 6(1)(f) GDPR — the Company's legitimate interest in identifying the expert capacity needed to perform its service contracts. The Company has carried out a legitimate interest assessment, which is available on request. The Company provides the information required by Article 14 GDPR at the latest upon first contact, within the outreach message itself.
Retention period	12 months from the outreach where the data subject does not reply. In the event of a negative reply the Company erases the data without delay and — in order to prevent further outreach — keeps the data subject on a suppression list, retaining only the name, the contact details and the date of the objection.

The Company does not transfer data processed in this way to clients or delivery partners. If the data subject applies, his or her data move into the consent-based processing described in sections 5.6.1–5.6.6, and the record created during sourcing ceases to exist; the Company does not maintain the two sets of records in parallel.

5.7 Data of employees and subcontractors after conclusion of a contract

Where an employment contract or a contractor or mandate agreement is concluded, the processing relating to the expert database ceases and new processing begins: processing connected with the performance of the

relationship, payroll, contribution and tax returns, working time records, and participation in client projects.

Aspect	Details
Legal basis	performance of the contract (Article 6(1)(b)), compliance with legal obligations to which the Company is subject (Article 6(1)(c) — in particular Act I of 2012 on the Labour Code, social security and tax legislation, and the Accounting Act), and the establishment, exercise and defence of legal claims (Article 6(1)(f)).
Retention period	for the period prescribed by law, or, in the absence of such a provision, for 5 years from the termination of the relationship. As regards data prescribed by pension insurance legislation, the longer statutory period applies.

The Company provides the detailed notice directly to the data subject at the time of contracting.

5.8 Enforcement of legal claims, complaint and incident handling

The Company records, investigates and answers the complaints, personal data breaches and data subject requests it receives.

Aspect	Details
Legal basis	compliance with a legal obligation (Article 6(1)(c) — Articles 12, 30, 33 and 34 GDPR), together with the Company's legitimate interest in the establishment, exercise and defence of legal claims (Article 6(1)(f)).
Retention period	5 years for data subject requests, the replies to them and the breach register; in the event of a legal dispute, until the end of the limitation period following the final closure of the case.

6. Processors and recipients

6.1 Access within the Company

Personal data are accessible to the Company's managing directors and to those members of staff who need such access to perform their duties. Access is restricted through authorisation levels, tied to individual user accounts and, in the case of the expert database, logged: it can be traced who viewed a profile and when. Members of staff are bound by an obligation of confidentiality.

6.2 Processors

The Company uses IT and back-office services for its activities. These providers process personal data on behalf of the Company, solely on the Company's written instructions and under a contract meeting the requirements of Article 28 GDPR, and may not use the data for their own purposes.

The categories of processors engaged are as follows:

Category	Activity	Place of storage
Hosting and cloud provider	storing the data, operating the applications	EEA
E-mail and office services provider	e-mail communication, document management	EEA
Application management and customer relationship system	recording applications and enquiries	EEA
Newsletter and notification system	sending system messages, renewal reminders and newsletters	outside the EEA (USA) — under the DPF or SCCs (see section 7)
Process automation platform	running the application and notification workflows	EEA
Accounting service provider	bookkeeping, payroll	Hungary
Document and CV processing service	machine reading of submitted CVs and conversion into structured data	outside the EEA (USA) — under the DPF or SCCs (see section 7)

Category	Activity	Place of storage
Artificial intelligence provider	supporting the matching of professional profiles with project requirements; the provider may not use the data for its own purposes or for model training	outside the EEA (USA) — under the DPF or SCCs (see section 7)
Web analytics provider	producing website traffic statistics, solely on the basis of the visitor's consent	EEA

The Company maintains a **list of its processors by name** at any given time and makes it available to data subjects free of charge on request at info@abicenterprise.com.

6.3 Other recipients

Recipient	On what conditions
Clients and delivery partners	solely on the basis of the separate, project-specific consent described in section 5.6.5, as independent controllers.
Legal, accounting and tax advisers	subject to an obligation of confidentiality, to the extent necessary.
Authorities and courts	on the basis of a statutory obligation, to the extent of their request.

The Company does not sell or rent personal data and does not disclose them to third parties for marketing purposes.

7. Transfers to third countries

The Company stores and processes personal data primarily within the European Economic Area.

Certain providers engaged by the Company — typically in the context of technical support — may also access data from outside the EEA. Any such transfer is in every case based on one of the safeguards set out in Chapter V GDPR:

Safeguard	What it means
Adequacy decision	an adequacy decision of the European Commission — in the case of the United States, for providers certified under the EU–US Data Privacy Framework
Standard contractual clauses (SCCs)	the standard contractual clauses adopted by the European Commission, supplemented where necessary by additional technical and organisational measures

The Company stores the data held in the expert database and the CVs submitted within the European Economic Area, in data centres in Ireland and Germany. A defined set of data is, however, processed by providers established in the United States of America: the artificial intelligence provider that performs machine reading of CVs and supports the matching of professional profiles, and the provider that sends system messages and reminders. These transfers take place on the basis of one of the safeguards described above — certification under the EU–US Data Privacy Framework or standard contractual clauses. The artificial intelligence provider processes the data solely on the Company's instructions; it may not use them for its own purposes or for model training.

At the data subject's request, the Company provides information on which providers involve a transfer outside the EEA and on what safeguard it is based, and makes available a copy of the safeguard applied.

8. Automated decision-making, profiling and artificial intelligence

In the processing activities described in sections 5.1–5.5 and 5.7–5.8 of this notice, the Company **does not use** automated decision-making or profiling.

In the case of the expert database (section 5.6), the Company also supports the matching of professional profiles with open project opportunities by IT means, including a solution based on artificial intelligence. This qualifies as **profiling** within the meaning of Article 4(4) GDPR, and the Company therefore provides the following information:

What the system does. Applicants already provide part of their professional data in structured form on the application form. In addition, the system also

reads the submitted CV by machine and records the professional data contained in it in structured form — that is, the uploaded file is not merely stored but also processed. The system then ranks, on the basis of the professional data in the profile — SAP module knowledge, years of experience, project references, language skills, availability, region — which profiles may match a given project requirement.

What the system does not do. It does not take decisions. Who is approached, whose profile is presented to the client and who drops out of the process is in every case **decided by a member of our staff, exercising genuine judgement**, and that decision is documented. The system does not by itself exclude anyone from the process.

It follows that the Company **does not take decisions based solely on automated processing within the meaning of Article 22 GDPR**. The data subject may nevertheless at any time request an explanation of the criteria applied and raise an objection to the assessment concerning him or her at info@abicenterprise.com.

Generative artificial intelligence in communications. Where the Company uses artificial intelligence (for example a chatbot) in its communications with prospective clients or applicants, it states this clearly at the start of the communication.

EU legislation on artificial intelligence. The Company monitors the application of the European Union's Regulation on artificial intelligence (AI Act) and documents the classification of the system supporting the ranking of candidates, as well as its own role in relation to that system. Should the obligations under that Regulation become applicable to the Company, the Company will separately inform data subjects that they fall within the scope of such a system.

9. Data security measures

Taking into account the state of the art, the costs of implementation, and the nature, scope and risks of the processing, the Company applies appropriate technical and organisational measures. These include in particular:

Measure	Details
Access management	authorisation levels, individual user accounts, the need-to-know principle, and multi-factor authentication in critical systems.
Encryption	transmission of data over an encrypted channel (TLS), and encryption of stored data wherever the provider makes this available.
Logging	logging of access to personal data and of processing operations, with a profile-level access log in the case of the expert database.
Backup and recovery	regular backups, verification of recoverability, and a rotational deletion rule for backups that extends erasure requests to the backups as well.
Automated erasure	machine calculation of retention periods and scheduled execution of erasure, without human discretion.
Organisational measures	confidentiality obligations for staff, data protection information and training for them, and internal procedures.
Processor control	conclusion of the contract required by Article 28 and verification of providers' security levels.

The Company designs and operates its systems so as to ensure authorised access, the integrity and authenticity of the data, and protection against unauthorised access, alteration, disclosure or destruction.

10. Handling personal data breaches

Case	Action and deadline
Every breach	The Company enters it in a register, recording the fact of the breach, its effects and the measures taken to remedy it.

Case	Action and deadline
Where the breach is likely to result in a risk to the rights and freedoms of data subjects	Notification to the Hungarian National Authority for Data Protection and Freedom of Information within 72 hours of becoming aware of it.
Where the breach is likely to result in a high risk	The Company also informs the data subjects without delay and in clear and plain language.

11. Summary of retention periods

Processing	Retention period
Website enquiry	12 months from closure
Data of contractual partners	5 years from the termination of the relationship
Accounting records	8 years
B2B business development outreach	24 months; suppression list in the event of an objection
Newsletter	until consent is withdrawn
Website log data and cookies	no more than 12 months, or as per the cookie setting
Expert database	12 months, renewable
Cooperation Declaration	its term, plus 5 years
Demonstration of consent (minimised log)	5 years after erasure
Employment and subcontractor relationships	as prescribed by law, or, failing that, 5 years
Data subject requests, breach register	5 years
Applications received but not yet assessed	until the decision on admission or rejection

Processing	Retention period
Rejected applications	30 days from the rejection
Draft of the application form	until submission, in the visitor's browser; disappears when the browser data are cleared
Recording of cookie consent	no more than 12 months, or until consent is withdrawn
Sourcing of professionals from public sources (5.6.7)	12 months from the outreach; immediate erasure in the event of a negative reply

12. Rights of data subjects

Data subjects may exercise the following rights using the contact details given in section 2.

Right	What it means
Right to information and of access (Articles 13–15)	information as to whether the Company processes data about the person and, if so, what data, for what purpose, for how long and to whom they are transferred; the right to request a copy of the data processed
Right to rectification (Article 16)	correction of inaccurate data and completion of incomplete data
Right to erasure (Article 17)	erasure of the data where the purpose has ceased, consent has been withdrawn, or the processing is unlawful
Right to restriction of processing (Article 18)	“blocking” of the data until contested accuracy or lawfulness has been clarified
Right to data portability (Article 20)	in the case of automated processing based on consent or on a contract, provision of the data in a machine-readable format
Right to object (Article 21)	objection to processing based on legitimate interest; in the case of direct marketing, without any conditions

Right	What it means
Right to withdraw consent (Article 7(3))	at any time, free of charge and as easily as it was given; withdrawal does not affect the lawfulness of prior processing
Rights relating to automated decision-making (Article 22)	the right to obtain human intervention, to express one's point of view and to contest the decision

Procedure. The Company complies with requests without undue delay and in any event **within one month**. That period may be extended by a further two months — taking into account the complexity and number of the requests; the Company informs the data subject of any such extension within the original time limit. Information and action are provided free of charge, unless the request is manifestly unfounded or excessive, in particular because of its repetitive character.

Identification. Where the Company has reasonable doubts concerning the identity of the person making the request, it may request further information for identification purposes. The Company uses data requested for identification solely for that purpose and erases them once the matter is closed.

13. Remedies

Complaint to the Company. Data subjects may at any time contact the Company directly using the contact details given in section 2. The Company investigates and answers the complaint.

Complaint to the supervisory authority.

Name	Hungarian National Authority for Data Protection and Freedom of Information (NAIH)
Address	1055 Budapest, Falk Miksa utca 9-11., Hungary
Postal address	1363 Budapest, Pf. 9., Hungary
Telephone	+36 (1) 391-1400
E-mail	ugyfelszolgalat@naih.hu
Website	www.naih.hu

Judicial remedy. Data subjects may bring an action before the courts if their rights are infringed. Such actions fall within the competence of the regional court (törvényszék) and may, at the data subject's choice, also be brought before the regional court with jurisdiction over his or her domicile or place of residence. The court deals with such cases as a matter of priority.

14. Amendment of this notice and version control

The Company reserves the right to amend this notice. The version in force is available at all times at <https://www.abicenterprise.com/adatkezelesi-tajekoztato>.

The Company notifies data subjects whose data are processed on the basis of consent — that is, those registered in the expert database and newsletter subscribers — of any material amendment in advance, by e-mail.

Every version has its own version number and effective date. The Company archives earlier versions so that it can be traced which version of the text the data subject was aware of when giving consent.

Version	Effective	Change
v1.0	[date]	website enquiries (the earlier /privacy-policy document, which the present version replaces in its entirety)
v2.0	26 August 2026	full notice: processors and place of storage, transfers to third countries, expert database and staffing process (the application route, double opt-in, admission decision), sourcing of professionals from public sources, B2B outreach, cookies and cookie consent, artificial intelligence, remedies

ABIC Enterprise — Complexity made simple.