Privacy Notice

Version 2026-10-15 | English

Effective from: 15 October 2026 · version 2026-10-15

This Notice explains how MindsRestart processes the personal data of website visitors, prospective and current clients, minor clients and their legal guardians. It reflects the public website, booking system, quizzes, client portal, email, payments and service delivery as at 15 October 2026.

1. Controller and contact

The controller is Bc. Zdenka Beranová, Company ID No. 74382209, VAT ID CZ8053220560, with registered office at Višňová 97, Voděrádky, 251 01 Říčany, Czech Republic (the “Controller” or “MindsRestart”). Contact for questions and rights requests: info@mindsrestart.com. Website: https://mindsrestart.com.

The Controller has not appointed a data protection officer. Requests may be sent directly to the contact above.

2. People and activities covered

This Notice covers website use, contact and booking forms, creation and security of client accounts, orders and payments, the migraine and childhood-role quizzes, intake questionnaires, informed consent forms, online and in-person sessions, client notes, digital audio materials including preparation and personalised recordings, support communication, complaints and legal obligations.

MindsRestart does not provide healthcare. Nevertheless, information voluntarily shared after explicit consent has been recorded for the subsequent assessment of the suitability and safety of a follow-on service may contain health or psychological data, which are special categories of personal data and receive enhanced protection.

3. Categories of personal data

Area	Examples
Website and security	In the web server’s operational log the IP address, date and time, request and browser details; it is kept for 14 days and serves operation, diagnostics and defence against attacks. In the web application itself the session identifier, CSRF token and security and error records — without the IP address in clear form; short-lived pseudonymised abuse-prevention counters are described in Section 11.
Contact, request and booking	Name, email, optional phone, message or note, service, language, status, price and funding mode. A public request is created without a date or time and also stores its source and the times at which the client acknowledged the Terms and this Notice. Only after the Provider proposes and the client accepts a time is a booking created with the specific date, time, payment status and variable symbol. Neither the IP address nor an open browser identifier is stored with a specific booking or contact enquiry.
Rescheduling proposals and requests	A request without an appointment time for a new session or rescheduling, the related original booking and time where applicable, one or more times proposed by the Provider, online or in-person delivery mode, the time and administrator who verified the in-person room, the Provider’s message, previously recorded client messages, a hash of the one-time link and its validity, request or proposal status, receipt and resolution times, identification of the resolving administrator and related audit data.
Individual cancellation agreements	Booking, immutable version of the exact cancellation terms, amount paid, refund amount, cancellation fee, offer validity, status, exact wording of binding acceptance, control hashes, times of offer, acceptance, withdrawal and actual refund, and related audit data. The client's explanation is not retained beyond what is necessary to reach the agreement.

Area	Examples
Client account	First and last name, email, phone, password hash, email verification, language, account status, pricing or partner group, a record of login attempts (without the IP address) and security tokens.
Service and client file	Individual offer, its status and expression of interest, activated programme, session dates and types, intake questionnaire, assignment, communication, client and internal organisational notes, informed consents and data necessary to assess suitability and safety.
Informed-consent evidence	Signature mode (the client acts personally or is represented by a guardian), document version and language, the exact wording of each statement, decision, date and time, confirmation channel, signer’s name, role and email, guardian identity and authority for a minor, a control fingerprint of the record and one-time-link status. No scan of a paper form or answers from a health questionnaire are uploaded to this record.
Package-contract confirmation	An immutable summary of the individual offer and its control fingerprint, the Terms and Privacy Notice versions, contract-conclusion regime, confirmation recipient, sending and conclusion times, one-time-link status and any two separate statements on early service commencement and early digital-content supply. Only the token hash, not its plaintext value, is stored.
Sensitive data	Health or psychological condition, symptoms, medication, care by other professionals, crisis circumstances, personal and family history or habits where shared and necessary for the service.
Quizzes	The quiz is scored in your browser and answers are not stored. Only if you voluntarily request the result by email do we store the email address, result category, language and request time; the IP address is not stored with the quiz result.

Area	Examples
Recordings and portal	Personalised audio created by the Provider, title, description, file size and duration, validity, playback limit and count, last playback and a pseudonymised browser-identification fingerprint in the playback log (without the IP address).
Payments and accounting	Price, payment method and status, variable symbol, payment date, bank record, billing information and accounting or tax document.
Minors	Child’s name and the fact that a guardian represents the child for the relevant legal act, the guardian’s identity, relationship and authority, contacts, informed consent, the child’s assent/views and necessary safety information.

For a public request, legal acknowledgement is recorded when the request is submitted. If the client later accepts a specific time and a booking is created, the exact wording and original time of that acknowledgement are carried into the booking evidence; the later administrative processing time is not substituted. A request for a session already covered by an agreed package neither implies nor creates a new legal acknowledgement.

4. Sources

We obtain data mainly from you through the website, client portal, one-time link, email, phone, signed paper forms and the service itself. A guardian also supplies data about a minor; after an age-appropriate explanation, the Provider records the child’s views. Payment data come from bank records. Technical data arise when the website and portal are used. A partner transfers data only after informing you and identifying a legal basis; the source and scope are available on request.

5. Purposes and legal bases

Purpose	GDPR legal basis
Responding to an enquiry, checking basic offer suitability and pre-contract steps	Article 6(1)(b) – steps at your request before a contract; for a general non-contractual enquiry, Article 6(1)(f) – legitimate interest in replying.
Booking, contract formation/performance, sessions, portal, support and recordings	Article 6(1)(b) – performance of a contract.
Payments, invoicing, accounting and tax	Article 6(1)(b) and (c) – contract and legal obligations.
Website/portal security, abuse prevention, login and audit logs	Article 6(1)(f) – legitimate interest in security, integrity and fraud prevention.
Legal protection, complaints and disputes	Article 6(1)(f) – legitimate interest in establishing, exercising or defending claims; where applicable Article 6(1)(c).
Operational first-party audience measurement without an advertising profile	Article 6(1)(f) – legitimate interest in improving and securing the website; you may object. A non-essential technology is stored on or read from a device only with consent where required by law.
Entry questionnaire for assessment and preparation	Separate explicit consent under Article 6(1)(a) and, for health data, Article 9(2)(a) GDPR; Article 6 explains the conditions and consequences of refusal.
Voluntary delivery of a quiz result by email	Explicit consent under Article 9(2)(a) GDPR — the result may indicate health or psychological state. Scoring itself happens only in your browser and stores nothing.
Voluntary testimonial, photograph or client story	Article 6(1)(a) – separate consent specifying scope and channels; for sensitive data also Article 9(2)(a).

Purpose	GDPR legal basis
Exceptional disclosure in an immediate threat to life	Article 6(1)(d) and, where sensitive data must be processed and the person cannot consent, Article 9(2)(c). This is not a routine service basis.
Evidence of informed service acknowledgement, consents and withdrawals	Article 6(1)(b) GDPR for a contractual acknowledgement; Article 6(1)(a) for separate voluntary consents and, for health data, also Article 9(2)(a). Retaining evidence after the purpose ends relies on Article 6(1)(f) — demonstrating lawfulness and protecting legal claims.
Confirmation of an individual offer and evidence of an early-performance request or statement	Article 6(1)(b) and (c) GDPR — concluding and performing the contract and complying with consumer-information duties. Subsequent limited retention relies on Article 6(1)(f) — demonstrating the contractual process and protecting legal claims.
Individual cancellation agreement, its acceptance, settlement and refund	Article 6(1)(b) GDPR — amendment and settlement of the contractual relationship; Article 6(1)(c) also applies to accounting and payment records. Subsequent limited retention relies on Article 6(1)(f) — evidence of the agreement and protection of legal claims.

MindsRestart does not currently operate a newsletter or routine marketing mailings. Before introducing such a purpose, the notice and forms will be updated; marketing consent must not be a condition of service.

6. Health and psychological data

For routine processing of health or psychological data in the subsequent assessment of the suitability and safety of a follow-on service, its individual tailoring, service delivery, creation of personalised materials including an audio recording, safety notes and the voluntary delivery of a quiz result by email, we rely on separate, specific and explicit consent under Article 9(2)(a) GDPR. A generic form statement saying “I consent to personal-data processing” does not replace that explicit consent.

Creating, storing and securely making available digital audio materials agreed in the individual offer, including a preparation recording and each personalised recording, forms part of contractual performance under Article 6(1)(b) GDPR, not a separate optional purpose. Where their content is based on health or psychological data, the explicit Article

9(2)(a) consent described above also applies to that work. We do not request separate consent merely for the existence of those agreed materials.

Initial assessment and consultation preparation use a separate entry questionnaire. Before answers are made available, we require explicit consent for this specific purpose. The questionnaire must be completed; without consent and the necessary answers, the system does not allow the client to proceed with preparation. Refusal or withdrawal pauses preparation and the next step is agreed with the Provider; the account, agreed appointment and contract are not automatically cancelled. Statutory client rights remain unaffected. Before consent, only general objectives and practical arrangements can be discussed, without detailed enquiry into or recording of health data. Questionnaire consent does not replace the separate consents required for a follow-on service.

Consent may be withdrawn at any time in the client portal or by emailing info@mindsrestart.com; withdrawal is not retroactive. A portal withdrawal is recorded immediately and the Controller receives an email alert. Processing these data is necessary for safe assessment, individual adaptation and continuation of the chosen follow-on service. Without consent the follow-on service cannot start and, after withdrawal, it cannot continue; the Controller may discuss with you whether another service is possible without that processing. Existing bookings are not cancelled automatically by withdrawing consent, and the Controller will agree the next steps with you. After withdrawal, limited data may be retained where necessary for a specific legal claim under Article 9(2)(f); this does not authorise continued routine use for client work.

Informed consent to a method or service is separate from consent to processing sensitive data. Likewise, acknowledging receipt of this Notice is not consent to unnecessary processing.

7. Required and optional data

Name, email, selected service and information necessary for safety and payment are contractual requirements; without them the request or service cannot be handled. A specific appointment is not required in the initial request because the Provider proposes it later, but an accepted time is necessary before a booking for a specific session can be created. Phone and most information in a general contact form are optional. Clients do not enter free-form messages or time preferences when requesting a new appointment, requesting a reschedule or responding to a proposed time; the Provider offers another time based on her availability. Do not put more sensitive information in free text than necessary. Website fields must be marked according to their actual requirement.

8. Recipients and processors

Recipient / category	Role and scope
Contabo GmbH	EU VPS hosting and technical infrastructure storing the website, database, encrypted client recordings and operational logs.
William OPTIK s.r.o., Company ID No. 117 51 011	Processor for the technical operation of the website under the Wagnerprojekt brand: administration, security, development, support, server operation and first-party audience measurement on the processor’s server in the EU; access only as necessary and on the Controller’s instructions.
Cloudflare, Inc.	Turnstile protects the contact form against automated submissions. It processes technical browser signals including the IP address; we do not send the message or other completed form fields to it. Details: Turnstile privacy addendum.
Webglobe, s.r.o.	SMTP relay and related domain/email infrastructure; it is not the current host of the website or client database.
Microsoft Ireland Operations Limited	Operation of the official info@mindsrestart.com mailbox in Microsoft 365.
Google Ireland Limited	Encrypted off-site backups; depending on configuration, onward processing outside the EEA may occur.
Československá obchodní banka, a. s.	Processing bank payments as an independent controller.
Accounting, tax or legal adviser	Only data necessary for accounting, tax, review or a legal claim; processor or independent controller depending on the role.
Public authorities	Only where required by law or necessary to protect rights or safety.
X-team, foundation or other partner	No automatic disclosure. Data are shared for a specific joint or follow-on service only after prior information on roles and legal basis.

MindsRestart does not use Calendly for the current website and does not currently offer PayPal or Revolut as payment methods. Before a new supplier is engaged, its legal basis, security, processing agreement and any international transfer will be assessed and this Notice updated.

9. Transfers outside the EEA

The main website and database are hosted in the EU. Some Microsoft and Google support services may involve access or onward processing in third countries. A transfer takes place only under a valid European Commission adequacy decision (including the EU–US Data Privacy Framework for a certified recipient), Standard Contractual Clauses with supplementary measures, or another lawful derogation. Details of the applicable mechanism are available from the Controller.

10. Retention

Category	Standard period / criterion
General enquiry or contact form without a contract	12 months after receipt of the message, or the last reply recorded in the system; longer only for a specific claim or legal obligation.
Booking, contract, programme and ordinary client records	During the engagement and normally for 5 years afterwards for continuity, complaints and claims. A documented individual review then follows; deletion or anonymisation takes place once there is no specific legal or legitimate reason for further retention.
Entry questionnaire – draft	Up to 14 days from starting the draft, always within any shorter remaining preparation-content period.
Entry questionnaire – questions and answers	Up to 90 days from creation of the preparation case. Closure shortens the remaining period to at most 30 days and never extends the original 90-day limit. Refusal or withdrawal of consent in the portal removes the content and blocks further use. Expired content is inaccessible and the next daily cleanup physically deletes it.
Evidence of entry-questionnaire consent and withdrawal	Kept separately without answers for five years after the purpose ends, then removed by the daily retention task.
Necessary health or psychological content notes from a follow-on service	During the service and no more than 3 years after the last performance. This is a separate record with its own purpose and applicable consent; it does not extend retention of the entry questionnaire or justify copying the whole questionnaire into the client file. Longer retention requires a specific legal ground.
Sensitive free text in appointment requests and proposals	For the time needed to arrange the appointment and no more than 3 years after the last actual performance; longer only for a specific ongoing claim or legal duty. Necessary business and status records may remain for the ordinary client-record period.

Category	Standard period / criterion
Genuinely orphaned appointment request without a client account	It is anonymised no later than after 5 years: name, email, phone, free text and the public token are removed. Only the necessary business and status skeleton, such as the service, price, payer, outcome and audit times, remains unless a specific legal duty or claim prevents anonymisation.
Accounting and tax documents	10 years after the relevant tax period where VAT rules require; other accounting records for their statutory period.
Request to receive the quiz result by email	90 days after the request; then automatic deletion.
Client account and login attempts	Active during the engagement. On termination the account is blocked and archived; ordinary business records remain only until the retention date, normally 5 years. Separate security logs and failed attempts: no more than 12 months.
Programme digital audio materials	Access for the period stated in the offer or portal. The audio file and database record are physically deleted no later than 90 days after access ends; on client archiving or approved complete deletion, immediately. Earlier deletion is possible on request unless a specific legal reason prevents it.
Playback tokens and logs	Token until expiry or use; playback logs no more than 12 months for security and technical incidents.
Internal audit log of operations on client data	5 years from the entry, as part of the client records; then deletion.
Audit snapshot before archiving or deletion	Only to demonstrate safe completion of the operation and protect claims, no later than the client-record retention date, normally 5 years; the snapshot must not extend a shorter period applying to particular data.
Web server operational log (incl. IP address)	14 days from the entry; then automatic deletion.

Category	Standard period / criterion
Form and login abuse-prevention counters	After 24 hours of inactivity, the file is scheduled for deletion by the next daily retention task; in normal operation, no later than 48 hours after the last attempt.
Operational web analytics	Monthly cleanup deletes records older than 14 months, within 15 months of creation in normal operation; this includes interaction maps and visit recordings.
Evidence of consent and contractual confirmations	During the purpose and normally for 5 years afterwards to demonstrate lawfulness and protect claims; withdrawal is recorded. After five years, each item is reviewed individually and retained longer only for a specific documented reason.
Individual cancellation agreements and settlement	The offer until acceptance, withdrawal or its stated expiry; the immutable accepted agreement, accounting link and evidence of the actual refund normally as part of the contractual and payment records under the relevant rows above.
One-time links for package early-performance decisions	Until use, cancellation or the stated expiry. The immutable contract summary and resulting statements are retained as contractual evidence under the preceding row.
One-time consent links	Normally 7 days after issue, until use or cancellation. Only the token hash is stored in the database; expired and used requests are removed by the retention task, while evidence of the resulting decision remains under the preceding row.
Backups	Cyclically overwritten under the security schedule; deleted data may temporarily remain in an inactive encrypted backup until overwrite and are restored only after a disaster.

Once the standard five-year period has expired, the Controller conducts a documented review at least annually to determine whether a specific legal or legitimate need remains for each immutable contract summary, acceptance or confirmation. Automated cleanup does not remove this contractual evidence merely because the record has reached a particular age; longer retention may be necessary, in particular during a dispute, complaint or another legal obligation. Once the specific reason ceases, approved deletion or anonymisation follows.

When a paying or served client is archived, login is blocked, recordings are removed, and booking, package, session and accounting data remain under restricted access until the retention date. An account with no actual service use may be fully deleted after a limited audit record is created. A monthly task removes archives after their retention date and a daily task automatically enforces the periods for quiz requests, contacts, expired recordings, audit snapshots, short-lived rate-limit counters and security logs.

The automated retention step for the new appointment requests and proposals is not yet enabled. Until it is introduced safely, the Controller applies the three- and five-year periods above through a controlled manual review; this technical circumstance does not extend those periods.

During a complaint, dispute, audit or legal duty, the relevant part may be restricted from ordinary use for as long as necessary. Periods are reviewed and data are kept beyond them only for a specific reason.

11. Cookies, local storage and analytics

Technology	Purpose and duration
MR_SESSION	Essential secure website/portal session for login and form protection; normally ends with the session or according to security settings.
CSRF token in session	Prevents forged form submission; session duration.
Cloudflare Turnstile	Security check of the contact form before storing the message and sending e-mail; it evaluates technical visit signals, not the message text.
Web server operational log	The server records the IP address, time, request and browser details — necessary for operation, troubleshooting and automatic defence against repeated login attempts. Logs are kept for 14 days and then deleted automatically; they are not used for analytics.

The web application itself — bookings, client portal, forms, quizzes and the consent records — stores neither the IP address nor the open browser-identification string in its database. The exception is a pseudonymised hash of the browser identification stored with a short-lived playback token and in the playback log, as described in Article 3; it protects the recording and limits token misuse. The public appointment-request token, proposal-link token and electronic-consent token are stored only as hashes, never in plaintext. Electronic

consent evidence also stores the time, channel, person, version, exact wording and its hash. The paper route stores the same evidence data, not a scan. To protect forms, logins and access-token issuance, the application briefly stores outside the database only attempt times, any blocking period and a pseudonymised technical identifier. Depending on the protected action, that identifier is derived from the IP address, email address or internal account ID using HMAC-SHA-256 and a separate secret key; it does not contain the source value in clear form. It remains pseudonymised personal data, not anonymous data. After 24 hours of inactivity, the file is scheduled for deletion by the next daily retention task.

Technologies essential for a session, security or a requested function may be used without cookie consent. If the website starts storing or reading non-essential analytics or marketing identifiers, they will remain disabled until freely given consent and an explicit consent choice with equal accept and reject options will be shown first. Rejection will not block core functions.

We analyse website traffic and use with our own analytics tool provided as part of the Wagnerprojekt service (William OPTIK s.r.o., business ID 11751011). It helps us improve the content, usability and operation of the website. Measurement runs on our processor’s server in the EU, uses no analytics cookies and creates no advertising profile. We do not link analytics records to your name, e-mail address or client account.

The data includes pages visited, referring page, time, language, device and browser type, screen size, loading performance and approximate location derived from the IP address. The IP address is not stored in analytics records; technical identifiers nevertheless distinguish visits and link events to them. On selected public pages we also analyse clicks, movement around the page and scrolling, including interaction maps and replay of selected visits. Text is masked and forms and their contents are excluded from this recording. This behaviour tracking is not used in the client portal, administration or entry questionnaire.

Measurement serves our legitimate interest in improving our website under Article 6(1)(f) GDPR. You may object at info@mindsrestart.com. A monthly cleanup removes analytics records older than 14 months, so in normal operation they are deleted within 15 months of creation.

12. Quizzes and automated scoring

Quizzes automatically assign a result category and generate a non-binding explanation. The result is not a diagnosis, treatment recommendation or decision producing legal or similarly significant effects, so it is not Article 22 automated decision-making. A human always assesses suitability for a service individually.

Answers are never sent anywhere or stored — scoring happens only in your browser. Only if you request the result by email are the email address and result category stored with your

explicit consent; full answers are never stored. Marketing use of name/email requires separate optional consent.

13. Minors

For a minor, data are processed only as necessary for assessment, contract, safety and service delivery. Consent for special-category data is given by a person authorised to represent the child; the child receives age-appropriate information and their views are taken into account according to age and maturity. A guardian must not receive more of the child's confidential communication than necessary for safety, parental responsibility and service organisation.

Public quizzes and general forms are not intended for a child to submit identifiable sensitive data without guardian involvement. If such a submission is discovered, we will review, restrict and, in the absence of a legal basis, delete it.

14. Your rights

Subject to the GDPR, you may request access and a copy, rectification, erasure, restriction and portability; object to legitimate-interest processing; withdraw consent; and not be subject to a solely automated decision with significant effects. Rights may be limited by legal duties, other persons' rights or the need to establish, exercise or defend a claim.

Send a request to info@mindsrestart.com. We may reasonably verify identity to protect data. We respond without undue delay, normally within one month; a complex request may be extended by two further months under the GDPR.

You may complain to the Czech Data Protection Authority, Pplk. Sochora 27, 170 00 Prague 7, Czech Republic, https://uoou.gov.cz. We encourage you to contact MindsRestart first so the matter can be resolved directly; this does not restrict your right to complain.

15. Security

We use access controls, separate administrative and client sessions, hashed passwords and tokens, encrypted transport, attempt limits, audit/security logs, encryption of client recordings at rest, time-limited access and encrypted backups. Access is limited to people who need it and are bound by contractual or legal duties. No system can, however, be described as absolutely secure.

If a personal-data breach occurs, we assess the risk, take remedial action and comply with any duty to notify the Czech Data Protection Authority and affected individuals.

16. Changes

This Notice takes effect on 15 October 2026 (version 2026-10-15). The current version is published on the website. For a material change of purpose, recipient, technology or legal basis, new information will be provided before the changed processing begins and fresh consent obtained where required.