Persate

LEGAL DOCUMENT

Last updated: 28 May 2026

PRIVACY POLICY

Preamble

This Privacy Policy describes the rules for processing information about you, including personal data and cookies. This Privacy Policy should be read together with the Terms of Service of persate.com, in particular with respect to definitions. This Privacy Policy also governs the rules for data processing within the AI Assistant Service and the Legislative Monitoring Service.

§ 1. General Information

1. The service provider is: PERSATE simple joint-stock company (prosta spółka akcyjna) with its registered office in Sochaczew, address: ul. Warszawska 62 lok. 4, 96-500 Sochaczew, entered into the register of entrepreneurs maintained by the District Court for Łódź-Śródmieście in Łódź, XX Commercial Division of the National Court Register under KRS number: 0001205038, NIP: 8371886321, REGON: 543232081.
2. The Provider is the Controller of personal data with respect to data voluntarily provided by Users when visiting the service, creating an Account, using services, or participating in various informational activities conducted by the Provider (e.g., newsletters). Where the User uses the AI Assistant Service and provides the Service with personal data of third parties stored in external cloud data services or directly uploads such data to the Service, the Provider acts as a data processor within the meaning of Article 28 GDPR, while the User remains the controller of such data.
3. Data provided by Users for the purpose of using the services is used in the process of launching and providing those services. This primarily includes: a) technical launch of services, b) registration and management of the User Account, c) notification of planned technical work and failures, d) notification of significant configuration changes, e) notification of changes to terms and policies, f) provision of technical support, including responses to User inquiries, g) clarifications regarding billing, h) direct commercial contact – if requested by the User ("Book a Demo"), i) sending product information by e-mail and other communication channels – if the User has consented to such forms of contact, j) provision of the AI Assistant Service, including access to files and data of the User stored in external cloud data services connected by the User to the Service, and to files and data uploaded by the User directly to the Service, k) provision of the Legislative Monitoring Service, including delivery of legislative notifications to the e-mail address or other communication channel indicated by the User.
4. The Service collects information about Users and their behaviour in the following ways: a) through data voluntarily entered in forms, which is entered into the Provider's systems, b) through use of the Provider's services, c) through storage of cookie files ("cookies") on end devices, d) through storage

of technical information in http server logs and other network services and applications of the Provider (system logs).

§ 2. Detailed Information on Personal Data Processing

1. Personal data processing is carried out in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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), hereinafter referred to as ("GDPR"), taking into account the provisions of the Act on electronic services and other universally applicable laws.
2. Personal data controller: a) The Provider is the controller of personal data. b) Controller contact details: ul. Warszawska 62 lok. 4, 96-500 Sochaczew, e-mail: mbednarczyk@persate.com.
3. Providing personal data is voluntary; however, the Provider informs that unless otherwise indicated in the content of individual forms (e.g., that providing data is optional), the Provider's services cannot be used anonymously or under a pseudonym. Accordingly, refusal to provide data may result in refusal to conclude an agreement and provide the ordered service.
4. Categories of processed data, purposes and legal bases: a) Registration and management of the User Account, including designation of the Account Administrator and management of sub-accounts: i. Scope of data: first and last name/company name, e-mail address, password (stored in encrypted form), authentication credentials of an external identity provider (Google, Microsoft) – if the User uses external login, first and last name and e-mail address of the Account Administrator and persons granted access to sub-accounts, and any other data provided by the User. ii. Purpose: conclusion and performance of services, in particular the Account Service Agreement or Premium Service Agreement. iii. Legal basis: Article 6(1)(b) GDPR – performance of a contract. iv. Retention period: for the duration of the Account Service Agreement, and after its termination for the period necessary to handle any complaints or pursue/defend claims, but no longer than the expiry of the limitation period. b) AI Assistant Service – integration with external cloud data services/data uploaded directly to the Service: i. Scope of data: authorization tokens enabling access to resources and data in external cloud data services designated by the User (in particular Google Drive, Microsoft OneDrive), file metadata (names, dates, types, sizes), file content – solely to the extent necessary for the execution of a specific User query to the AI Assistant. ii. Purpose: provision of the AI Assistant Service consisting of intelligent search, categorization and analysis of the User's files. iii. Legal basis: Article 6(1)(b) GDPR – performance of a contract. iv. Retention period: tokens are invalidated immediately upon disconnection of the integration by the User or upon deletion of the Account. v. Special information: The Provider does not process the User's data from external cloud data services/files uploaded directly to the Service for purposes other than providing the AI Assistant Service to the given User, in particular does not use them for marketing purposes and does not share them with third parties without separate, explicit consent of the User, except in cases arising from mandatory applicable law. c) Legislative Monitoring Service: i. Scope of data: e-mail address or other contact details indicated by the User as the notification delivery channel (e.g., messenger identifier), configuration of Monitoring Topics and Key Phrases defined by the User. ii. Purpose: provision of the Legislative Monitoring Service, i.e., automatic tracking of selected legislative topics and delivery of legislative event notifications to the User, including in particular those resulting from AI analysis of sessions of the

Polish Sejm and Senate. iii. Legal basis: Article 6(1)(b) GDPR – performance of a contract. iv. Retention period: for the duration of the Premium Service. Configuration of Monitoring Topics and Key Phrases is deleted immediately upon the User's withdrawal from the Legislative Monitoring Service or upon deletion of the Account. d) Handling "Book a Demo": i. Scope of data: e-mail address, message content. ii. Purpose: taking action at the request of the person before possible conclusion of a contract, commercial contact. iii. Legal basis: Article 6(1)(f) GDPR – legitimate interest, i.e., handling commercial correspondence. iv. Retention period: for the duration of correspondence and until expiry of the limitation period for any claims. e) Handling complaints and technical support: i. Scope of data: first and last name/company name, e-mail address, description of the reported problem, technical logs necessary for its diagnosis. ii. Purpose: handling complaints and providing technical support. iii. Legal basis: Article 6(1)(b) GDPR – performance of a contract; Article 6(1)(c) GDPR – compliance with a legal obligation. iv. Retention period: for the duration of the complaint handling process and until expiry of the limitation period for claims. f) Analytics and service quality improvement: i. Scope of data: anonymized data about the use of the Service (application events, navigation paths, session time), IP address (truncated). ii. Purpose: analysis and improvement of the Service's functionality and services. iii. Legal basis: Article 6(1)(f) GDPR – the Provider's legitimate interest in improving the quality of services offered. iv. Retention period: until effective objection is raised or the processing purpose ceases, but no longer than 24 months. g) Establishment, pursuit or defence of claims: i. Scope of data: all data necessary for the fulfilment of this purpose, in particular data from Account history and correspondence. ii. Purpose: legal protection of the Provider. iii. Legal basis: Article 6(1)(f) GDPR – the Provider's legitimate interest. iv. Retention period: until expiry of the limitation period for claims.

5. In certain situations, the Provider as the controller of personal data has the right to transfer personal data to other recipients if this is necessary for the performance of the concluded contract or fulfilment of obligations resting on the Controller. This applies in particular to the following categories of recipients: a) authorized employees and associates of the Controller who use the data to perform services, b) providers of external authentication services (Google, Microsoft) – for login processing, c) operators of external cloud data services (in particular Google – Google Drive, Microsoft – OneDrive) – solely to the extent necessary for authorization and access to the User's resources within the AI Assistant Service, d) providers of artificial intelligence models and infrastructure, as well as providers of cloud infrastructure (including file storage, database hosting, transactional e-mail delivery, audio/video transcription) – to the extent necessary for the provision of specific Service functions. The complete, current list of data processors (sub-processors) together with the country of processing is set out in § 8 of this Policy. The Provider ensures that these entities are obligated to process data solely on documented instructions from the Provider and apply adequate data protection measures, e) law firms – in particular for the purpose of pursuing or defending claims, f) public authorities – solely on the basis and to the extent arising from applicable law.
6. Users' personal data may be transferred outside the European Economic Area (EEA) – in particular to the United States of America – only in connection with the use of services from sub-processors listed in § 8. The transfer takes place on the basis of: a) European Commission adequacy decisions (EU-US Data Privacy Framework, Article 45 GDPR) – with respect to entities certified under the DPF, b) standard contractual clauses approved by the European Commission (Article 46(2)(c) GDPR), c) other transfer mechanisms set out in Article 46 GDPR ensuring an adequate level of data protection.

Information on the transfer basis applicable to a specific sub-processor is provided in § 8. The Provider maintains a register of transfer bases used and makes it available to Premium Users on request.

7. The Controller does not use automated decision-making, including profiling referred to in Article 22(1) and (4) GDPR, with respect to personal data processed through the Service.
8. Where a User using the AI Assistant Service is the controller of personal data of third parties contained in resources stored in external cloud data services/files uploaded by the User directly to the Service (e.g., data of clients, employees, contractors), the Provider processes such data solely as a data processor within the meaning of Article 28 GDPR. In such case: a) The User is obligated to ensure an appropriate legal basis for processing personal data of third parties through the Service before granting the Service access to these resources, b) the detailed terms of data processing entrustment, including the Provider's obligations and guarantees as a data processor, are set out in a separate Data Processing Agreement concluded with the User upon request or automatically available as an annex to the Premium Service terms, c) The Provider processes personal data of third parties solely on documented instructions from the User (as controller), solely to the extent and for the purpose necessary for the provision of the AI Assistant Service, and ensures that persons authorised to process such data have committed to maintaining confidentiality.
9. When the User designates an Account Administrator and grants access to sub-accounts to specific persons/groups of persons, the User acts as the controller of personal data of those persons within the meaning of Article 4(7) GDPR. The User is obligated to: a) ensure an appropriate legal basis for processing personal data of the Account Administrator and sub-account users before granting them access to the Account through the Service, b) fulfil the information obligation referred to in Article 13 GDPR towards those persons in relation to the processing of their data by the Provider in connection with use of the account/sub-accounts assigned to them, c) not share with the Service personal data of persons for whom the User does not have an appropriate legal basis.

§ 3. User Rights

1. Each User has the following rights: a) Right of access (Article 15 GDPR) – to obtain confirmation as to whether data is being processed, and if so – to access it and obtain a copy. b) Right to rectification (Article 16 GDPR) – to request correction of inaccurate data or completion of incomplete data. c) Right to erasure (Article 17 GDPR) – to request deletion of data when it is no longer necessary for the purposes for which it was collected, when consent has been withdrawn, or when data was processed unlawfully. d) Right to restriction of processing (Article 18 GDPR) – to request suspension of processing in cases specified in the GDPR. e) Right to data portability (Article 20 GDPR) – to receive data in a structured, commonly used, machine-readable format (applies to data processed on the basis of consent or contract in an automated manner). f) Right to object (Article 21 GDPR) – against processing based on the legitimate interest of the Controller, including profiling. The right to object cannot be exercised where there are compelling legitimate grounds for processing that override the interests, rights and freedoms of the User, in particular for the establishment, exercise or defence of claims. g) Right to withdraw consent – at any time, without affecting the lawfulness of processing carried out before its withdrawal. h) Right to lodge a complaint with the President of the Personal

Data Protection Office (ul. Stanisława Moniuszki 1A, 00-014 Warsaw; www.uodo.gov.pl), if the User considers that the processing violates GDPR provisions.

2. To exercise the above rights, please contact the Controller at the e-mail address indicated in § 2(2)(b). The Controller shall handle the request without undue delay, no later than within one month of receiving it. This period may in justified cases be extended by a further two months, of which the Controller shall inform the User (Article 12(3) GDPR).

§ 4. Information in Forms

1. The Service collects information voluntarily provided by the User, including personal data, if provided.
2. The Service may save information about connection parameters (timestamp, IP address).
3. Data provided in a form is processed for the purpose arising from the function of the specific form – e.g., for handling a service demonstration request or Account creation. In each case, the context and description of the form clearly indicates its purpose.

§ 5. Administrator Logs

Information about User behaviour in the Service may be subject to logging. Such data is used solely for the purposes of Service administration and technical diagnostics.

§ 6. Information About Cookies

1. The Service uses cookies.
2. Cookies are IT data, in particular text files, which are stored on the User's end device and are intended for use with the Service's websites. Cookies usually contain the name of the website from which they originate, the storage time on the end device, and a unique number.
3. The entity placing cookies on the User's end device and accessing them is the Provider.
4. Cookies are used for the following purposes: a) maintaining the User's session (after logging in), so that the User does not need to re-enter authentication data on each sub-page of the Service, b) remembering User preferences and application settings, c) analytics and statistics on Service usage – solely after obtaining the User's consent.
5. The Service uses two main types of cookies: "session" cookies and "persistent" cookies. Session cookies are temporary files stored on the User's end device until logging out, leaving the website, or closing the browser. Persistent cookies are stored on the User's end device for the time specified in the cookie parameters or until deleted by the User.
6. Installation of non-essential cookies (in particular analytical and marketing cookies) on the User's end device occurs only after the User has given consent via the cookie banner displayed during the first visit to the Service.
7. Cookies placed on the User's end device may also be used by entities cooperating with the Provider.

§ 7. Managing Cookies

1. If the User does not wish to receive cookies, they may change their browser settings. We note that disabling cookies essential for authentication, security and user preference maintenance processes may make using the Service difficult or, in extreme cases, impossible.
2. To manage cookie settings, select from the list below the web browser you use and follow the instructions: a) Edge (https://support.microsoft.com/en-us/microsoft-edge/view-and-delete-browser-history-in-microsoft-edge-00cf7943-a9e1-975a-a33d-ac10ce454ca4), b) Chrome (https://support.google.com/chrome/answer/95647?hl=en), c) Safari (https://support.apple.com/en-gb/guide/safari/sfri11471/mac), d) Firefox (https://support.mozilla.org/en-US/kb/clear-cookies-and-site-data-firefox), e) Opera (https://help.opera.com/en/latest/web-preferences/#cookies); Mobile devices: a) Android (Google Chrome) (https://support.google.com/chrome/answer/95647?hl=en), b) Safari (iOS) (https://support.apple.com/en-us/105082).

§ 8. Sub-processor Register

1. The Provider engages the following sub-processors (data processors) to provide specific Service functions:

Sub-processor	Function in the Service	Processing region	Transfer basis outside the EEA
Supabase Inc. / Supabase EU GmbH	Database hosting, authentication system	European Union (Frankfurt)	Not applicable (EEA)
CloudFerro S.A.	Storage of User files and recordings (object storage)	Poland (EEA)	Not applicable (EEA)
Anthropic, PBC	Claude language models (AI Assistant, content analysis)	United States	SCC
Google LLC / Google Cloud (Vertex AI)	Gemini models (OCR, document analysis)	European Union and United States	EU-US DPF + SCC
OpenRouter, Inc.	AI model gateway (embeddings, reranking)	United States	SCC
ElevenLabs, Inc.	Audio/video transcription	United States	SCC
Resend, Inc.	Transactional e-mail delivery (notifications, password reset, alerts)	United States	SCC
Google LLC	OAuth/Google Drive (only when the User connects a Google account); Google Analytics (only with User consent)	United States, EEA	EU-US DPF + SCC
Microsoft Corporation	OAuth/OneDrive (only when the User connects a Microsoft account)	United States, EEA	EU-US DPF + SCC

2. The Provider may update the sub-processor list from time to time in connection with Service development, changes of service providers, or security requirements. The current list is made available to Premium Users on request together with information on the scope of data entrusted. A material change of sub-processor is preceded by appropriate prior notice to the Account Administrator of the organisation.
3. With respect to each sub-processor, the Provider enters into a data processing agreement satisfying the requirements of Article 28 GDPR and verifies the technical and organisational data protection measures applied by that sub-processor.

§ 9. Biometric Data and Special Categories of Data

1. As part of the public proceedings recording analysis function (in particular broadcasts of sessions of the Polish Sejm, Senate, and other public bodies), the Service may process: a) the image of persons appearing in the recording – for the purpose of identifying speeches of specific speakers (e.g., parliamentarians, witnesses at public hearings), b) voice characteristics – for the purpose of separating utterances of individual speakers (diarization) and attributing transcriptions to the speaker.
2. To the extent that the processing described above constitutes processing of special categories of data within the meaning of Article 9(1) GDPR: a) the legal basis is Article 9(2)(e) GDPR (data manifestly made public by the data subject) – limited exclusively to public persons appearing in recordings of a public nature, b) the analysis results are used solely for the creation of speech chronologies, summaries, and legislative notifications for Users – they are not used for profiling of natural persons or for taking decisions concerning specific individuals, c) biometric features used for identification (face embeddings, voice embeddings) are not shared with third parties for purposes other than the provision of the Service.
3. A User who uses the analysis function for their own private recordings (e.g., internal meetings of the organisation) bears responsibility for ensuring an appropriate legal basis, including – where necessary – separate consent from the participants, in relation to the processing of their biometric data. The Provider in this regard acts as a data processor within the meaning of Article 28 GDPR.
4. The Provider does not use the biometric data processed for purposes other than those arising from a specific User assignment (recording analysis) or Service function (recognition of public persons in public recordings).

§ 10. Privacy and Security Controls

1. A User using the Premium Service has the option to limit the scope of data transferred to external sub-processors through Account configuration of the organisation. The following mechanisms are available: a) disabling transmission of document content to external OCR models – in such case, text extraction from files is carried out solely within functions available in the Provider's infrastructure, b) disabling transmission of content fragments to external vectorisation (embedding) models – this affects the scope of the semantic search function, c) disabling transmission of queries to external reranking models, d) limiting the scope of daily e-mail reports to the title, source and link of the

document only, with the full content omitted, e) disabling enrichment of data about public persons with external public sources (e.g., Wikipedia). Activation of the above mechanisms takes place at the organisation (Premium Account) level and applies to all Users within that organisation.

2. Access by members of the Provider's technical support team to the User's private files is permitted exclusively: a) at the request of the Account Administrator of the organisation in connection with handling a support request, or b) in cases necessary for the performance of legal obligations resting on the Provider (e.g., requests from competent public authorities). Each access requires a justification and is logged in an audit log including information on the time, the identifier of the employee, and the case number. The Account Administrator of the organisation has the right to receive an extract from the audit log concerning their organisation on request.
3. The Provider applies technical and organisational data protection measures appropriate to the risk of processing, including: a) encryption of connections (TLS) and of data at rest, to the extent provided by infrastructure sub-processors, b) isolation of data of individual organisations at the database level (multi-tenant isolation), c) two-factor authentication (2FA/MFA) available to Account Administrators, d) regular backups and recovery procedures, e) logging and monitoring of significant security events.
4. The Provider maintains a record of processing activities in accordance with Article 30 GDPR and – with respect to particularly risky operations – a data protection impact assessment (DPIA) in accordance with Article 35 GDPR.

§ 11. Final Provisions

1. Polish law governs this Privacy Policy.
2. Disputes between the Provider and the User shall be resolved by the court competent for the registered office of the Provider. Where the User is also a Consumer, all disputes shall be resolved by the common courts competent in accordance with the provisions of the Code of Civil Procedure.
3. Matters not regulated by this Privacy Policy shall be governed by the provisions of the Civil Code, the GDPR, and other mandatory applicable provisions of Polish law.
4. This Privacy Policy is effective from 28 May 2026.