PRIVACY POLICY

Version: 3.0 · Effective from: 10 September 2026

The Czech version of this document is binding; the English version is for information only.
Závazná je česká verze tohoto dokumentu; anglická verze je pouze informativní.

In the course of providing the Coinero services, certain personal data are processed. The processing of personal data is the responsibility of the company MipSoftware s.r.o., with its registered office at Na příkopě 848/6, Nové Město, 110 00 Prague 1, Czech Republic, Company ID No.: 24667021, registered in the Commercial Register kept by the Municipal Court in Prague under File No. C 164643, which operates the Coinero services through the web application operated under the domain coinero.cz and also through the mobile application named Coinero (the “Controller”).

1. DEFINITIONS

“Application” means the web application operated under the domain coinero.cz and the Coinero mobile application, through which the Controller provides its services.

“Client” means a natural person or a legal entity that has entered into an Agreement with the Controller or uses the services provided by the Controller through the Application.

“Data Subject” means a natural person whose personal data the Controller processes, in particular a Client who is a natural person, a prospective client, a representative, a contact person or a beneficial owner of a Client that is a legal entity.

“Agreement” means an agreement for the provision of services concluded between the Controller and the Client.

“GDPR” means 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.

“ZOOU” means Act No. 110/2019 Coll., on Personal Data Processing, as amended.

“AML Act” means Act No. 253/2008 Coll., on Selected Measures against Legitimisation of Proceeds of Crime and Financing of Terrorism, as amended.

“Personal data” generally means any information relating to an identified or identifiable natural person (a Data Subject); an identifiable natural person is a natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, 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.

“Processing of personal data” means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

“Profiling” means automated processing of personal data used to evaluate certain personal aspects of a natural person, in particular the behaviour, reliability or level of risk of that person.

2. PRINCIPLES OF PERSONAL DATA PROCESSING

2.1 The Controller processes personal data in accordance with the GDPR, the ZOOU and other applicable legal regulations.

2.2 In processing personal data, the Controller follows these principles:

(a) it processes personal data lawfully, fairly and in a transparent manner;

(b) it processes personal data only for specified, explicit and legitimate purposes and does not further process them in a manner that is incompatible with those purposes;

(c) it processes only personal data that are adequate, relevant and limited to what is necessary in relation to the purpose of their processing;

(d) it processes accurate and, where necessary, up-to-date personal data and takes reasonable steps to rectify or erase inaccurate data, for which it may require the necessary cooperation of the Data Subject;

(e) it retains personal data in a form which permits identification of Data Subjects for no longer than is necessary for the purposes of their processing;

(f) it processes personal data in a manner that ensures their appropriate security and protection by means of suitable technical and organisational measures.

2.3 The Controller is responsible for compliance with the principles set out in this Article and takes measures to be able to demonstrate such compliance. It reviews the measures taken on an ongoing basis and updates them as necessary.

3. LEGAL BASIS AND PURPOSE OF PERSONAL DATA PROCESSING

3.1 Purposes of personal data processing

The Controller processes the personal data of Clients, prospective clients and other Data Subjects, in particular representatives, contact persons and beneficial owners of Clients, for the following purposes:

(a) negotiations on the conclusion of a contract, the conclusion and performance of a contract, the creation and administration of the Client's account, the authentication of the Client, the management of access to the Application and the provision of services, including the execution of orders and transfers of crypto-assets;

(b) the identification and checking of the Client and other persons concerned, the carrying out of KYC and AML checks, checks of politically exposed persons and of international sanctions, the determination and updating of the risk profile, ongoing monitoring of the business relationship and transactions, blockchain analysis and compliance with obligations in transfers of crypto-assets under the Travel Rule;

(c) communication with the Client, the provision of client support and the sending of operational, security and transactional notifications, including notifications by SMS, email or telephone contact;

(d) compliance with other legal and regulatory obligations of the Controller, in particular the keeping of statutory records, the provision of cooperation to public authorities, compliance with accounting, tax, archiving and reporting obligations, including obligations under the DAC8/CARF rules, where they apply to the Controller;

(e) the prevention and detection of fraudulent or other unlawful conduct, the protection of the Application, Client accounts, information systems, the property and rights of the Controller or third parties, and the establishment, exercise or defence of legal claims;

(f) the carrying out of internal analyses and statistics, the evaluation of the use of the Application and the improvement of the services provided;

(g) direct marketing and the sending of commercial communications under the conditions set out in paragraph 3.3.

3.2 Legal bases of personal data processing

The Controller processes personal data on the basis of the following legal grounds:

(a) the processing is necessary in order to take steps at the request of the Data Subject prior to entering into a contract or for the performance of a contract, under Article 6(1)(b) GDPR;

(b) the processing is necessary for compliance with a legal obligation of the Controller under Article 6(1)(c) GDPR, in particular obligations in the areas of AML, international sanctions, the Travel Rule, accounting, taxes, archiving, regulatory reporting and the provision of cooperation to the competent authorities;

(c) the processing is necessary for the purposes of the legitimate interests of the Controller or of a third party under Article 6(1)(f) GDPR. Those interests are in particular the protection of the Application, Client accounts, information systems, the property and rights of the Controller, the prevention and detection of fraud, the improvement of the services provided, the carrying out of internal analyses, the establishment, exercise and defence of legal claims and direct marketing of the Controller's own similar services to existing Clients;

(d) the Data Subject has given consent under Article 6(1)(a) GDPR, in particular to the sending of commercial communications, where the Data Subject is not an existing Client of the Controller, or to the use of analytics and marketing technologies under Article 11. Consent is voluntary and may be withdrawn at any time.

The legal basis of the performance of a contract applies only where the Data Subject concerned is a party to the contract. The personal data of representatives, contact persons, members of corporate bodies and beneficial owners of Clients that are legal entities are processed by the Controller in particular for the purpose of compliance with legal obligations or on the basis of the legitimate interest in concluding, administering and performing the contractual relationship with the Client.

3.3 Direct marketing and commercial communications

The Controller processes contact details obtained in connection with the provision of services to existing Clients for the purpose of direct marketing and the sending of commercial communications relating to the Controller's own similar services. The legal basis for this processing is the legitimate interest of the Controller under Article 6(1)(f) GDPR. Commercial communications are sent in accordance with Section 7(3) of Act No. 480/2004 Coll., on Certain Information Society Services.

The Client may refuse the use of the Client's electronic contact details for the sending of commercial communications when the contact details are obtained and subsequently at any time, in particular via the link included in every commercial communication. Refusal is free of charge. If the Client objects to the processing of personal data for the purposes of direct marketing, the Controller no longer processes the Client's personal data for that purpose.

Commercial communications are sent to persons who are not Clients of the Controller, and in cases where a commercial communication does not relate to the Controller's own similar services, only on the basis of their prior consent. Consent may be withdrawn at any time, without affecting the lawfulness of processing carried out before its withdrawal.

4. SOURCES OF PERSONAL DATA

4.1 The Controller obtains personal data only to the extent necessary for the purposes set out in this Privacy Policy and on the basis of an appropriate legal ground. It obtains personal data in particular from the following sources:

(a) directly from the Data Subject, in particular upon registration and use of the Application, identity verification, completion of questionnaires, placing of orders, execution of transfers of crypto-assets, submission of documents and in communication with the Controller;

(b) from the Client or persons acting on the Client's behalf, in particular where the Client provides data about the Client's representatives, contact persons, members of corporate bodies, persons in the ownership or control structure or beneficial owners;

(c) in the course of using the Application and providing services, during which data are generated in particular on sign-ins, devices, IP addresses, the manner of use of the Application, orders placed, transfers of crypto-assets, bank accounts, wallets and communication with the Controller, and, where applicable, data obtained through cookies and similar technologies under the conditions set out in this Privacy Policy;

(d) from the activities of the Controller, in particular by evaluating the data provided, carrying out checks, determining the risk profile, monitoring the business relationship and transactions and generating security or AML alerts;

(e) from publicly available sources or sources made accessible by law, in particular public registers, lists and records, the insolvency register, the register of beneficial owners, sanctions lists, sources of information on politically exposed persons and other trustworthy public sources;

(f) from public blockchain networks, in particular in connection with checks of wallet addresses, the origin of crypto-assets and the analysis of transactions;

(g) from external providers and other third parties, in particular from providers of identity verification, AML, sanctions and PEP checks, blockchain analysis, banks, payment service providers, other crypto-asset service providers and providers of analytics or marketing technologies, where the transfer of data is necessary and permitted by legal regulations;

(h) from providers of external registration and sign-in, where the Data Subject chooses to create a Client Account or sign in through an external account, to the extent that the Data Subject decides to make the data available through the relevant provider; and

(i) from public authorities, where the transfer of personal data to the Controller is prescribed or permitted by legal regulations.

5. SCOPE AND CATEGORIES OF PERSONAL DATA PROCESSED

5.1 Scope of processing

The Controller processes only the personal data necessary for the purposes set out in this Privacy Policy. The specific scope of processing depends on the position of the Data Subject, the services used, the course of the business relationship and the legal obligations of the Controller. Not all of the categories of personal data listed below are therefore processed about every Data Subject.

5.2 Categories of personal data

The Controller processes in particular the following categories of personal data:

(a) identification data and data from identity documents, in particular first name, surname, birth number (rodné číslo) or date of birth, gender, place and country of birth, citizenship, residential address, signature, photograph, type and number of the identity document, the country or authority that issued it, its period of validity and copies of the identity documents and of other documents used to verify identity;

(b) contact details, in particular correspondence address, email address and telephone number;

(c) data on representation and on the ownership and control structure, in particular data on representatives, contact persons, members of corporate bodies, persons acting under a power of attorney and beneficial owners of the Client, their position and authority to act on behalf of the Client, including powers of attorney and related documents;

(d) data on the Client's account and technical and operational data, in particular the account identifier, data necessary for sign-in and authentication, sign-in history, IP address, approximate location derived from the IP address, basic data on the device, operating system and web browser, and records of security events;

(e) financial, payment and tax data, in particular the bank account number and data on the account holder, payments made, data on income, assets and the origin of funds and crypto-assets, related banking, tax and other supporting documents, data on tax residence and the tax identification number;

(f) data on the use of services and on transactions, in particular data on orders, trades, deposits, withdrawals and transfers of crypto-assets, their date, type, volume, value and frequency, balances, crypto wallet addresses, blockchain transaction identifiers and data on the originator and the beneficiary of a transfer under the Travel Rule;

(g) AML, sanctions and risk data, in particular politically exposed person status, results of sanctions and other checks, the Client's risk profile and risk factors, results of monitoring of the business relationship and transactions, results of blockchain analysis, AML and security alerts and data relating to suspicious or unusual transactions;

(h) communication and client data, in particular the content and history of communication with the Controller, requests, notifications, complaints and grievances, data provided to client support and related documents;

(i) marketing data, in particular data on consents given, objections raised, opt-outs from commercial communications, marketing preferences and commercial communications sent;

(j) external account data: a unique identifier assigned by the external sign-in provider, name, email address or forwarding email address and other data that the Data Subject decides to make available through the provider.

6. RETENTION PERIOD OF PERSONAL DATA

6.1 General rules

The Controller retains personal data only for the period necessary for the purposes for which they are processed or for the period laid down by legal regulations. Where the same data are processed for more than one purpose, the longest applicable period applies, but the data may be used only for the purpose for which their further retention continues.

6.2 Individual retention periods

Personal data are retained in particular for the following periods:

(a) data needed for the creation and administration of the Client's account and the provision of services, for the duration of the contractual relationship; thereafter only to the extent necessary for compliance with legal obligations or the protection of the rights of the Controller;

(b) identification data, copies of documents, data obtained when checking the Client, the risk profile, records of transactions and other data under AML regulations, including data under the Travel Rule, for 10 years from the carrying out of a transaction outside a business relationship or from the termination of the business relationship;

(c) records of services provided, orders and transactions for the period required by the regulations governing the provision of crypto-asset services, generally 5 years, or up to 7 years at the request of the competent authority. Where the ten-year AML period applies to the same records, that longer period applies;

(d) accounting and tax documents generally for 5 or 10 years depending on their type;

(e) data and records processed for the purposes of DAC8/CARF for the period laid down by legal regulations, at least 5 and at most 10 years after the end of the relevant reporting period;

(f) data needed to handle complaints, grievances and legal claims for the period of their handling and subsequently for the relevant limitation periods, generally 3 years. Where proceedings are ongoing or a longer statutory period applies, the data may be retained for longer;

(g) technical, operational and security records for the period necessary to secure the Application, prevent fraud and investigate security events;

(h) contact details of existing Clients for direct marketing for the duration of the contractual relationship and for no longer than 2 years after its termination, and in any event no longer than until an objection is raised or the Client opts out;

(i) data processed on the basis of consent for the period stated when consent is given, but in any event no longer than until consent is withdrawn.

After marketing is refused, the Controller may retain a minimal record of the electronic contact and of the objection raised, in order to ensure that the person concerned is not added to the marketing mailing list again and so that it can demonstrate compliance with its obligations.

6.3 Erasure and anonymisation

After the relevant period expires, the Controller securely erases or anonymises personal data without undue delay, unless another legal ground exists for their further retention. Anonymised data that can no longer be linked to a specific person may continue to be retained.

Erasure from backup copies takes place as part of their regular rotation; until then, the data in backups are not routinely used.

The Controller cannot itself change or erase data recorded on a public blockchain network. After the relevant period expires, the Controller erases or anonymises data retained in the Controller's own systems, or restricts their link to a specific Data Subject. This does not affect the retention of limited pseudonymised security indicators under paragraph 6.2(g), where they continue to be necessary for the prevention and detection of fraud.

7. RECIPIENTS AND TRANSFERS OF PERSONAL DATA

7.1 The Controller makes personal data available only to the extent necessary, where this is needed for the provision of services, compliance with a legal obligation or the protection of the rights and legitimate interests of the Controller.

Depending on the nature of the service provided, the recipients may act as processors, independent controllers or joint controllers of personal data. Processors may process personal data only on the basis of a contract, in accordance with the instructions of the Controller and while ensuring an appropriate level of protection of personal data.

7.2 Personal data may be made available in particular to:

(a) providers of IT, cloud, hosting, communication and security services who ensure the operation, maintenance, security and support of the Application and related systems;

(b) providers of services for identity verification, AML, sanctions and PEP checks and blockchain analysis, where their involvement is necessary for compliance with legal obligations, risk management or the security of the services provided;

(c) banks, payment institutions and crypto-asset service providers, where this is necessary for the execution of an order, a transfer of crypto-assets or the provision of another service;

(d) providers of email, SMS and other communication services and of client support services, where this is necessary for communication with the Client, the sending of security and operational notifications or the provision of support;

(e) providers of external registration and sign-in, where the Data Subject chooses to create a Client Account or sign in through an external account;

(f) accounting, tax, audit, legal and other professional advisers, where the transfer of personal data is necessary for the provision of their services, compliance with legal obligations or the protection of the rights of the Controller;

(g) providers of analytics, measurement and marketing services, where the Controller uses the relevant services and the conditions laid down by this Privacy Policy are met, in particular the requirement of prior consent to the use of optional technologies; and

(h) competent public authorities and other authorised persons, in particular the Czech National Bank, the Financial Analytical Office, the authorities of the Financial Administration of the Czech Republic, courts, authorities involved in criminal proceedings, enforcement officers, notaries or insolvency administrators, where making the personal data available is prescribed or permitted by legal regulations.

7.3 When crypto-assets are transferred, the Controller transmits, in the cases prescribed by legal regulations, the data on the originator and the beneficiary of the transfer to another crypto-asset service provider or, where applicable, to another authorised entity, in order to comply with the obligations relating to the information accompanying transfers of crypto-assets (the Travel Rule).

7.4 In some cases, personal data may be transferred or made available to recipients outside the European Economic Area. In such a case, the Controller ensures appropriate protection of personal data, in particular on the basis of a decision of the European Commission on an adequate level of protection, standard contractual clauses adopted by the European Commission or another mechanism permitted by the GDPR. Where necessary in view of the nature of the transfer, the Controller also adopts supplementary technical or organisational measures.

The Controller provides the Data Subject, on request, with information about the protection mechanism used or the possibility of obtaining a copy of it.

8. SECURITY OF PERSONAL DATA

8.1 Personal data are processed mainly in electronic form. The Controller has adopted appropriate technical and organisational measures corresponding to the nature, scope and risks of the processing. As necessary, these measures include in particular access rights management, secure user authentication, encryption, backups and measures to ensure the confidentiality, integrity, availability and resilience of systems and personal data.

8.2 Access to personal data is granted only to persons duly authorised by the Controller or its processor who need such access to perform their employment or contractual duties, and only to the extent necessary.

8.3 The authorised persons are bound by a contractual or statutory duty of confidentiality and may process personal data only on the basis of the relevant instructions of the Controller, unless European Union or Czech law provides otherwise.

9. OBLIGATION TO PROVIDE PERSONAL DATA AND CONSEQUENCES OF NOT PROVIDING THEM

9.1 The provision of certain personal data is a statutory or contractual requirement or a requirement necessary to enter into the Agreement. The Client must provide such data if the Client wishes to use the relevant services of the Controller, in particular for the purposes of identity verification, compliance with obligations under the legal regulations governing measures against money laundering and terrorist financing, the creation and administration of the Client Account and the conclusion and performance of the Agreement.

9.2 Without the provision of these data, the Controller cannot verify the identity of the Client, create or administer the Client Account, conclude or perform the Agreement, execute an order or provide the relevant service.

9.3 The provision of personal data for the purposes of processing based on consent is voluntary. Not giving consent or withdrawing it does not affect the provision of basic services; the Controller will merely not carry out the processing for which consent is required.

The Client may refuse the sending of commercial communications at any time, simply and free of charge, in particular via the opt-out link included in every commercial communication. Refusing commercial communications does not affect the provision of other services.

10. RIGHTS IN CONNECTION WITH THE PROCESSING OF PERSONAL DATA

10.1 The rights set out in this Article belong to every natural person whose personal data the Controller processes (the “Data Subject”). The individual rights may be exercised under the conditions laid down by the GDPR and their scope depends in particular on the purpose and legal basis of the processing.

10.2 Right of access. The Data Subject has the right to ask the Controller to confirm whether it processes the Data Subject’s personal data. Where the Controller processes personal data, the Data Subject has the right to obtain a copy of them and the following information:

(a) the purposes for which the personal data are processed and the categories of personal data concerned;

(b) to whom the personal data have been or will be made available or, as the case may be, which categories of recipients are concerned, in particular if they are located outside the European Economic Area;

(c) the period for which the personal data will be stored or, as the case may be, the criteria by which that period is determined;

(d) the source from which the Controller obtained the personal data, if it did not obtain them directly from the Data Subject;

(e) the right to request the rectification or erasure of personal data or the restriction of their processing, to object to the processing and to lodge a complaint with a supervisory authority;

(f) the safeguards applied in transfers of personal data outside the European Economic Area or to an international organisation; and

(g) any automated decision-making, including basic information about the procedure used and its possible consequences for the Data Subject.

10.3 Right to rectification. Where the Data Subject’s personal data are inaccurate or out of date, the Data Subject may request their rectification or updating. Where personal data are incomplete, the Data Subject may request that they be completed or, as the case may be, provide additional information or a statement. The Controller carries out the rectification or completion without undue delay.

10.4 Right to erasure (“right to be forgotten”). The Data Subject may request that the Controller erase the Data Subject’s personal data without undue delay where:

(a) the personal data are no longer necessary for the purposes for which they were collected or processed;

(b) the Data Subject has withdrawn consent and there is no other legal ground for further processing;

(c) the Data Subject has objected to the processing and there are no overriding legitimate grounds for its continuation, or has objected to the processing for the purposes of direct marketing;

(d) the personal data have been processed unlawfully; or

(e) the personal data must be erased for compliance with a legal obligation.

The right to erasure is not absolute. The Controller does not erase personal data where their further processing is necessary in particular for compliance with legal obligations under AML, sanctions, tax, accounting or other legal regulations or for the establishment, exercise or defence of legal claims.

Data recorded on a public blockchain network cannot, given its technical nature, be changed or erased. However, in the cases laid down by the GDPR, the Controller erases the related personal data from its own systems, unless legal or technical reasons prevent it.

10.5 Right to restriction of processing. The Data Subject may request that the Controller temporarily restrict the processing of the Data Subject's personal data where:

(a) the Data Subject contests the accuracy of the personal data, for the period necessary for the Controller to verify their accuracy;

(b) the processing is unlawful, but the Data Subject requests only the restriction of their use instead of erasure;

(c) the Controller no longer needs the personal data, but the Data Subject requires them for the establishment, exercise or defence of legal claims; or

(d) the Data Subject has objected to the processing, for the period during which it is assessed whether the legitimate grounds of the Controller override the rights and interests of the Data Subject.

During the restriction, the Controller generally only retains the personal data. Otherwise, it may process them only with the consent of the Data Subject, for the establishment, exercise or defence of legal claims, for the protection of the rights of another person or for reasons of important public interest. Before the restriction is lifted, the Controller informs the Data Subject in advance.

10.6 Right to data portability. Where the processing is based on consent or is necessary for the performance of the Agreement and is carried out by automated means, the Data Subject has the right to receive the personal data that the Data Subject has provided to the Controller in a structured, commonly used and machine-readable format. Where technically feasible, the Data Subject may request that the personal data be transmitted directly to another controller.

10.7 Right to withdraw consent. Where the Data Subject has given the Controller consent to the processing of personal data, the Data Subject may withdraw it at any time, in whole or in part. Withdrawing consent must be as easy as giving it and may be done via the Controller's contact details or in another manner that the Controller offers for the given processing.

After consent is withdrawn, the Controller ends the processing carried out solely on its basis. If it has no other legal ground for the further retention of personal data, it erases the data processed solely for the given purpose.

The withdrawal of consent does not affect the lawfulness of processing carried out before its withdrawal or processing based on another legal ground. The withdrawal of consent does not affect the provision of services that do not depend on that consent.

10.8 Right to object. The Data Subject may, on grounds relating to the Data Subject's particular situation, object at any time to the processing of personal data based on the legitimate interest of the Controller, including profiling related to that processing.

After an objection is raised, the Controller no longer processes the personal data unless it demonstrates compelling legitimate grounds for the continuation of the processing that override the interests, rights and freedoms of the Data Subject, or the processing is necessary for the establishment, exercise or defence of legal claims.

Where personal data are processed for the purposes of direct marketing, the Data Subject may object at any time and without stating a reason, in particular via the opt-out link included in the commercial communication. The objection also applies to any profiling related to direct marketing. Once it has been

exercised, the personal data will no longer be processed for the purposes of direct marketing.

The right to object does not apply to processing necessary for compliance with legal obligations of the Controller, in particular obligations under AML, sanctions, tax or other legal regulations.

10.9 Automated evaluation and human assessment. The Controller uses automated rules to check whether an order, a transfer of crypto-assets, a withdrawal of funds or another operation exceeds a set limit or meets another condition requiring additional verification.

If such a condition is met, the execution of the operation may be temporarily suspended or restricted until an authorised person carries out the necessary verification and individual assessment.

A final decision that would produce legal effects concerning the Data Subject or similarly significantly affect the Data Subject is not based solely on automated processing.

10.10 Exercise of rights. The Data Subject may exercise the Data Subject's rights by email at podpora@coinero.cz or in writing at the address of the Controller's registered office: MipSoftware s.r.o., Na příkopě 848/6, Nové Město, 110 00 Prague 1, Czech Republic.

The Controller handles the request without undue delay and at the latest within one month of receiving it. Taking into account the complexity or number of requests, it may extend this period by a further two months. It informs the Data Subject of the extension and the reasons for it within one month of receiving the request.

Where the Controller has reasonable doubts about the identity of the applicant, it may request additional information necessary to verify it. Exercising the rights is free of charge; however, in the case of manifestly unfounded or excessive requests, the Controller may charge a reasonable fee or refuse the request.

10.11 Right to lodge a complaint. The Data Subject has the right to lodge a complaint with the Office for Personal Data Protection, Pplk. Sochora 27, 170 00 Prague 7, uoou.gov.cz, or with another competent supervisory authority.

11. COOKIES AND SIMILAR TECHNOLOGIES

11.1 The Controller uses cookies and similar technologies in the Application, in particular local storage, sign-in tokens, device identifiers and measurement codes. These technologies serve to ensure the functioning and security of the Application and, on the basis of the Data Subject's consent, also to analyse its use, to measure the effectiveness of advertising and for marketing purposes.

11.2 Necessary technologies. The Controller uses, without consent, technologies necessary for sign-in, user authentication, management of the user session, protection of Client Accounts, prevention of fraud and abuse and ensuring the secure operation of the Application. Necessary technologies include in particular sign-in cookies and tokens, security identifiers and technologies used to store the Data Subject's choice regarding cookies.

The use of necessary technologies cannot be switched off via the cookie settings, because without them some functions of the Application could not be provided securely. This does not affect the rights of the Data Subject under Article 10 of this Privacy Policy.

Related security and audit records may also be retained in pseudonymised form where this is necessary for the prevention and detection of fraud, compliance with legal obligations or the protection of the rights of the Controller. Their retention period is determined by the Article governing the retention period of personal data.

11.3 Analytics technologies. On the basis of consent, the Controller may use technologies that make it possible to evaluate traffic, the manner in which the Application is used, its technical functioning and any errors. These technologies may record in particular information about the pages visited, the time and manner of use of the Application, the approximate location and technical data about the browser and the device.

Where the data obtained are also used for advertising purposes or linked to advertising services, the Controller treats the technologies concerned as marketing technologies for the purposes of consent choices.

11.4 Marketing technologies. On the basis of consent, the Controller may use technologies for measuring the effectiveness of advertising campaigns and conversions, evaluating interactions with advertising, retargeting and displaying personalised advertising.

In connection with their use, information may be processed in particular about the visit to the Application, interaction with advertising, the performance of a certain action or conversion and technical data about the browser and the device.

The Controller will not transmit to the providers of these technologies the Client's email address, telephone number or other directly identifying data, not even in hashed form, unless the Data Subject has been informed of such processing in advance and an appropriate legal basis has been ensured for it.

11.5 External registration and sign-in. The Application may allow the creation of a Client Account and sign-in through an external provider. If the Data Subject chooses this method, the Controller may obtain from the provider a unique user identifier, name, email address or forwarding email address and other data that the Data Subject decides to make available.

These data are processed for the purpose of creating, linking, securing and administering the Client Account and enabling sign-in. The legal basis is the taking of steps prior to entering into the Agreement or the performance of the Agreement under Article 6(1)(b) GDPR. The use of an external account is voluntary.

11.6 Consent to optional technologies. Analytics and marketing technologies that store or read data in the Data Subject's device may be activated only on the basis of the Data Subject's prior consent. The legal basis for the related processing of personal data is consent under Article 6(1)(a) GDPR.

The Data Subject may allow or refuse analytics and marketing technologies separately via the cookie banner. The consent given may be changed or withdrawn at any time via the "Cookie settings" link, which is permanently available in the Application. Not giving consent or withdrawing it does not affect the ability to use the basic functions of the Application or the lawfulness of processing carried out before its withdrawal.

Until consent is given, as well as where it is not given or is withdrawn, analytics and marketing identifiers are neither stored nor read in the Data Subject's device. In this mode, the measurement code may transmit limited technical data to the provider of the measurement service without the use of analytics or marketing identifiers, for the purpose of producing aggregate statistics and statistical estimates of traffic. The Controller carries out this limited processing on the basis of its legitimate interest in measuring and evaluating the use of the Application under Article 6(1)(f) GDPR. Only after consent is given are analytics or marketing technologies that store or read data in the device activated, and measurement then takes place to the extent described in paragraphs 11.3 and 11.4.

11.7 Providers and overview of technologies. A current overview of the cookies and similar technologies actually used is available through the “Cookie settings” interface. For each technology, its name, provider, category, purpose and duration are stated in particular. The Controller updates this overview before a new technology or provider is deployed.

Where the use of these technologies involves transfers of personal data outside the European Economic Area, the conditions set out in the Article governing the transfer of personal data apply.