Attachment No. 1 to the Terms of Service – DPA

DATA PROCESSING AGREEMENT (DPA)

This **Attachment No. 1** to the Terms of Service (**DPA**) supplements the provisions of the Terms of Service, as updated between the User and the Administrator (**the Parties**).

The DPA between the Parties is concluded when the User submits a statement acknowledging that they have read and accepted the Terms of Service (and comes into effect on that date).

1. Definitions

1.1. The following terms, when capitalised, have the meanings assigned to them below:

Data Controller	the entity that determines the purposes and means of the Processing of Personal Data (the User);
Data Protection Laws	all laws and regulations relating to data protection and privacy applicable in the European Union (EU) or the EEA governing the processing of Personal Data;
Data Subject	a natural person whose Personal Data is processed by the User (as the Data Controller) and transferred under the DPA for Processing by E-Trade (as the Processor);
EEA	European Economic Area;
E-Trade	E-TRADE SOLUTIONS Sp. z o.o., with its registered office at Gniewomierz 173, 59-241 Legnickie Pole, Poland, entered into the Register of Entrepreneurs of the National Court Register (KRS) under number 0000875181, maintained by the District Court for Wrocław-Fabryczna in Wrocław, IX Commercial Division. NIP (VAT ID): 6912552324, REGON (Business ID): 387822015, with a share capital of 100,000 PLN;
GDPR	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) (OJ L 2016.119.1, dated 2016.05.04);

Meta	WhatsApp Ireland Limited, Merrion Road, Dublin 4 (D04 X2K5), Ireland, registered by the Companies Registration Office Ireland under no. 607470 a Meta group company, operator of the WhatsApp Business Platform
Personal Data	any information relating to an identified or identifiable natural person, meaning a person who can be directly or indirectly identified, such as personal data – first name, last name, residential address, or contact data – email address, phone number;
Processing of Personal Data	any operation or set of operations performed on Personal Data, whether or not by automated means, including: collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction;
Processor	the entity processing Personal Data on behalf of the Data Controller (E-Trade);
Service	the online service at https://dropui.com;
User	You (including affiliated entities) when using E-Trade's services through the Service.
User Data	all Personal Data that E-Trade processes on behalf of the User as a Processor in connection with the use of E-Trade's services through the Service;
Web Push Service	a functionality of the Service enabling the User to send push notifications to subscribers acquired on the User's website;
WhatsApp Service	a functionality of the Service enabling the User to send messages to Recipients via the WhatsApp Business Platform, from a WhatsApp Business number connected by the User.
Email Service	a functionality of the Service enabling the User to send email campaigns to the User's recipients and test messages from the User's verified sending domain.

1.2. All terms used in the DPA, except for those defined directly in the DPA, shall be understood in accordance with Article 4 of the GDPR

2. Entrustment of Personal Data Processing

2.1. The User entrusts E-Trade with Personal Data for Processing in accordance with Article 28 of the GDPR, under the terms, scope, and purpose specified in the DPA, and E-Trade accepts the Personal Data for Processing and commits to process it under the terms specified in the DPA, the GDPR, and Data Protection Laws.

2.2. The Parties mutually agree that, with respect to the Processing of Personal Data, the User is the Data Controller, and E-Trade is the Data Processor. Each Party is obligated to comply with the DPA, the GDPR, and Data Protection Laws.

2.3. The subject matter, duration, nature, and purpose of the Processing, as well as the types of Processing of Personal Data and the categories of Data Subjects, are specified in **Annex A** to the DPA

3. Processing of Personal Data by the User

3.1. The User declares that the User Data (or other Personal Data) entrusted to E-Trade for Processing has been collected in compliance with applicable laws.

3.2. The User is responsible for controlling the Personal Data and is required to fulfil their obligations as a Data Controller under the GDPR and Data Protection Laws, particularly regarding the justification of any transfer of Personal Data to E-Trade and their decisions and actions related to the Processing of Personal Data.

3.3. The User confirms that they have properly informed and obtained all necessary consents or authorisations to enable E-Trade to process the User Data, particularly to ensure the proper provision of services by E-Trade through the Service.

4. Processing of User Data by E-Trade

4.1. In connection with the provision of services by E-Trade through the Service to the User, the User entrusts E-Trade with User Data for Processing, and E-Trade processes specific categories and types of User Data solely for the purposes described in the DPA.

4.2. The Parties declare that the DPA sets forth the entirety of the User's instructions regarding the entrustment of Personal Data Processing to E-Trade.

5. User's Obligations

5.1. Subject to the obligations arising from the Terms of Service, the User is obligated to:

a. ensure the security of Personal Data provided through the Account in the Service;

b. ensure the security of User Data transferred to E-Trade (subject to E-Trade's obligations regarding the Processing of Personal Data under the Terms of Service or DPA);

c. provide any notifications or statements required by the GDPR or Data Protection Laws to individuals whose Personal Data is transferred to E-Trade and obtain the necessary consents or authorizations from such individuals in accordance with the GDPR or Data Protection Laws;

d. ensure that Personal Data related to criminal convictions and offenses or related security measures are not transferred for Processing by E-Trade (Article 10 GDPR);

e. review the information provided by E-Trade regarding data security and undertake an independent assessment to verify that the services provided by E-Trade through the Service meet their requirements and legal obligations under the GDPR or Data Protection Laws;

f. in respect of the WhatsApp Service — obtaining Recipients' consent to WhatsApp contact, honouring Recipients' opt-out, and complying with Meta's policies, in particular the WhatsApp Business Messaging Policy;

g. in respect of the Web Push Service — obtaining subscribers' consent to push notifications and honouring their opt-out. The User is solely responsible for the content of messages and notifications and for obtaining the required consents;

h. in respect of contact data imported by the User into the Service — ensuring a legal basis for its processing, the accuracy of the consent information provided, and performance of the information obligation towards Recipients, including under Articles 13 and 14 of the GDPR;

i. The User may connect, within the Service, integrations with external platforms (including email and SMS marketing, CRM systems, analytics tools). Connecting an integration constitutes the User's instruction to transfer Personal Data to the entity selected by the User; the User is responsible for the choice of that entity, the legal basis for the transfer, and its relationship with it. The list of available integrations is presented in the Service and may change.

j. in respect of the Email Service - obtaining and documenting prior marketing consent for the relevant store or website, honouring opt-outs and objections, and ensuring a legal basis and information obligations also for measuring opens and clicks, in accordance with Section 5 of the Terms of Service.

5.2. The User accepts responsibility for the secure use of the services provided by E-Trade through the Service, including the protection of User Data during its transfer to E-Trade and taking all appropriate steps to securely encrypt or back up the User Data transferred to E-Trade.

6. E-Trade's Obligations

6.1. When Processing Personal Data, E-Trade undertakes to secure such data by applying appropriate technical and organisational measures to ensure compliance with the GDPR or Data Protection Laws, including measures that ensure a level of security appropriate to the risk of the rights or freedoms of individuals whose Personal Data is processed, including, among others, measures specified in Article 32 GDPR in conjunction with Article 5(1) and (2) GDPR, as set out in **Annex B** to the DPA.

6.2. E-Trade undertakes to exercise due diligence when Processing entrusted Personal Data.

6.3. E-Trade takes appropriate steps to ensure compliance with the security measures employed by E-Trade, implemented by employees or associates, applicable to the Processing of Personal Data, including ensuring that all persons authorised to process Personal Data are bound by appropriate confidentiality commitments.

6.4. E-Trade agrees to ensure that persons authorised to process Personal Data are bound by confidentiality obligations or are subject to an appropriate statutory duty of confidentiality, as referred to in Article 28(3)(b) of the GDPR. Additionally, E-Trade ensures that such persons will process Personal Data in accordance with the need-to-know principle.

6.5. E-Trade agrees to provide the User with reasonable cooperation and assistance necessary for the User to fulfil their obligations under the GDPR or Data Protection Laws

6.6. E-Trade undertakes, considering the nature of the Processing and the information available to it, to fulfill the obligations set out in Articles 32-36 of the GDPR, including in the areas of Processing security,

reporting Personal Data breaches to the supervisory authority, notifying Data Subjects of a Personal Data breach, conducting data protection impact assessments, and engaging in prior consultations.

6.7. E-Trade shall provide the User with all information necessary to demonstrate compliance with the obligations set out in Article 28 of the GDPR in electronic form, such as via email, no later than 14 days from the request.

7. Rights of Data Subjects

7.1. If E-Trade receives a request from an individual concerning User Data, E-Trade, to the extent permitted by law, shall inform the individual to direct their request to the User, who is then responsible for responding to such a request, including, if necessary, by using the functionalities of the services provided by E-Trade through the Service.

7.2. For the avoidance of doubt, the User is responsible for covering any costs arising from the assistance provided by E-Trade to individuals.

8. Erasure of User Data

8.1. Upon the termination of services provided by E-Trade through the Service, for example, in connection with the cessation of services to the User (regardless of the legal or factual basis for such termination), E-Trade shall, upon written request from the User, begin the process of erasing User Data (including any existing copies), unless the GDPR, Data Protection Laws, or applicable legal regulations require the retention of Personal Data.

9. Management of User Data Security Incidents

9.1. E-Trade shall notify the User without undue delay, but no later than within 48 hours, of any security incidents (breaches) involving User Data processed by E-Trade.

9.2. E-Trade shall inform the User of security incidents (breaches) involving User Data through:

a. posting a notification using the functionalities of the Service; or

b. sending an email to the address provided during Account registration.

9.3. The User is responsible for ensuring the accuracy and correctness of the contact information provided in the Service for the entire duration of the DPA.

9.4. In the event of security incidents involving User Data, E-Trade shall take the necessary remedial actions it deems necessary and appropriate to address the causes of such incidents (breaches), including promptly providing the User with:

a. reasonable cooperation and assistance in relation to incidents (breaches) of User Data;

b. reasonable information held by E-Trade regarding incidents (breaches) of User Data;

c. information known to E-Trade about: (i) the nature of the security incident (breach) involving User Data, including the categories and approximate number of affected individuals; (ii) the potential consequences of the security incident (breach) involving User Data; (iii) measures taken to mitigate the consequences of the security incident (breach) involving User Data; (iv) proposed measures to prevent future security incidents (breaches) involving User Data.

9.5. For the avoidance of doubt, E-Trade's notification of a security incident (breach) involving User Data does not constitute an admission of liability for the incident, and the obligations specified in Section 9 of the DPA [Management of User Data Security Incidents] do not apply to security incidents (breaches) involving User Data that were caused by or involved (directly or indirectly) the User (or their employees or associates), entities affiliated with the User, or the User's suppliers (e.g., providers of systems, platforms, services, software, devices, tools, etc.).

9.6. The User agrees to provide E-Trade with the content of any information regarding a security incident (breach) involving User Data that is to be addressed to the supervisory authority, individuals affected by the security incident (breach), or to be made public (e.g., via social media or on the User's website), before such information is released. This should be done in such a way that the content is provided in advance (taking into account any statutory deadlines under the GDPR or Data Protection Laws), allowing E-Trade to provide any clarifications or corrections to such information.

10. Transfer of User Data to a Third Country or International Organisation

10.1. If User Data is transferred to a third country or an international organisation, it is necessary to comply with the requirements set out in **Annex C** to the DPA.

11. Right of Audit

11.1. If required by the GDPR or Data Protection Laws, E-Trade shall directly enable the User to conduct an audit to verify the procedures relevant to the Processing of User Data.

11.2. The User's right of audit will be carried out as follows:

a. The User: (i) shall provide E-Trade with written notice at least 30 days in advance of any proposed audit; (ii) the audit shall take place no more than once every 12 months, except when required by the competent supervisory authority; (iii) the audit shall be conducted in a manner designed to minimise disruption to E-Trade's normal business operations; (iv) the right of audit shall be exercised during E-Trade's business hours;

b. The User or the User's authorised representatives shall maintain the confidentiality of all information obtained as a result of the audit and agree to comply with E-Trade's security rules while on E-Trade's premises. The User acknowledges that they or their representatives may be required by E-Trade to enter into an enhanced confidentiality agreement.

11.3. Before exercising the right of audit, the User and E-Trade shall mutually agree on the reimbursement of costs for which the User will be responsible, including the User's representatives, as well as the schedule and scope of the audit rights.

12. Further Sub-processing of User Data

12.1. E-Trade is entitled to engage another processor (**Subprocessor**) for the further Processing of User Data covered by the DPA. E-Trade shall inform the User of any intended changes concerning the addition or replacement of a Subprocessor, thereby giving the User the opportunity to object to such changes (**Right to Object**).

12.2. E-Trade shall inform the User of any intended addition or replacement of a Subprocessor at least 7 days before that Subprocessor commences Processing User Data. The User may object within that period. If the User objects and does not withdraw the objection, the Subscription Period is shortened correspondingly and ends on the day immediately preceding the commencement of Processing by the new entity, and E-Trade shall refund the User the pro rata portion of the Fee attributable to the unused part of the Subscription Period.

12.3. The list of Subprocessors to which the Data Controller has consented as of the date of the DPA's conclusion is included in **Annex A** to the DPA.

13. Liability

13.1. E-Trade is liable for the Processing of Personal Data that is not in accordance with the DPA, particularly for the unauthorised disclosure of entrusted User Data to unauthorised persons, in accordance with general principles, taking into account the limitation of liability of E-Trade arising from the Terms of Service, unless otherwise required by applicable law.

13.2. The User is liable to the Data Subject, who has the right to compensation for any material or non-material damages caused by the User due to a violation of the rights granted to the Data Subject as a third party beneficiary under the DPA.

14. Duration of the DPA

14.1. The DPA is effective from the date of its conclusion and remains in force until the expiration or termination (cancellation) of the Subscription or the cessation of services provided by E-Trade through the Service to the User

15. Final Provisions

15.1. Only a Party to the DPA is entitled to enforce its provisions, which means that successors or assignees of the Parties are not entitled to enforce the provisions of the DPA. This exclusion shall not apply to legal succession resulting from a transformation of a Party where applicable law provides that universal succession or continuation applies to such transformation.

15.2. The User agrees that any penalties incurred by E-Trade in connection with User Data, arising from or resulting from the User's failure to comply with the obligations under the DPA, the GDPR, or Data Protection Laws, shall be credited against and reduce E-Trade's liability under the DPA.

15.3. The DPA is governed by and interpreted in accordance with the laws of Poland and falls under the jurisdiction of Polish courts, unless otherwise specified by applicable Data Protection Laws.

15.4. Any disputes shall be resolved by the common court having jurisdiction over the registered office of E-Trade.

15.5. In matters not regulated by the DPA, the provisions of the Terms of Service, the GDPR, Data Protection Laws, or the Polish Civil Code shall apply. In the event of any conflict between the DPA and the Terms of Service, the provisions of the DPA shall prevail.

15.6. If any provision of the DPA is found to be invalid, such provision or part thereof shall be deemed removed to the extent necessary, and the remaining provisions of the DPA shall remain unchanged and in full force and effect. If any invalid provision of the DPA becomes valid upon the removal of a part of it,

then it shall apply after making the modifications necessary to render it valid and to reflect the Parties' intentions.

15.7. The DPA is not intended to limit or exclude any rights of Data Subjects provided under the GDPR or Data Protection Laws in any way.

15.8. All annexes to this DPA form an integral part of this Data Processing Agreement.

15.9. Annexes:

a. Annex A – Subject matter, duration, nature, and purpose of the processing, as well as the types of personal data processed and categories of data subjects;

b. Annex B – Appropriate technical and organisational measures;

c. Annex C – Transfer of personal data to third countries or international organisations.

Annex A – Subject Matter, Duration, Nature, and Purpose of Processing, as well as the Types of Personal Data Processed and Categories of Data Subjects

Subject Matter of the Processing of Personal Data: User Data in accordance with the Terms of Service.

Duration of the Processing of Personal Data: For the Subscription Period (while the User has an active Subscription in the Service until the Subscription expires or is canceled/terminated) or for the duration of the services provided by E-Trade to the User

Nature of the Processing of Personal Data: E-Trade provides tools that support the development of websites and applications in the form of a service through the Service, allowing Users, in particular, to create pop-ups or other similar tools. Under the WhatsApp Service and the Web Push Service, E-Trade processes Recipients' Personal Data on the User's behalf, respectively, to send WhatsApp messages from a number connected by the User and to send push notifications to the User's subscribers. Under the WhatsApp Service, E-Trade also processes messages and files sent by Recipients to the User, in order to make them available to the User within the Service. Under the Email Service, E-Trade processes Recipients' Personal Data on the User's instructions to prepare, queue and send campaigns and handle consent, opt-outs, suppressions, delivery events and statistics for opens and clicks. Messages are sent from the User's sending domain through the infrastructure listed in this Annex. Test messages are sent to the User's Account email address.

Purpose of the Processing of Personal Data: The purpose of Processing Personal Data is the provision of services by E-Trade to the User.

Categories of Data Subjects::

a. Users – any natural person visiting the Service or using its functionalities;

b. Data Subjects – any natural person whose Personal Data is processed (stored or collected) through the services provided via the Service.

Types of Personal Data Processed:

a. transaction data (e.g., sales history, payments, refunds, bonuses, discounts);

b. user interaction data (e.g., website visits, click tracking, call recordings, social media activities, posts, likes, comments, survey responses, complaints, feedback);

c. location data (e.g., geographic location data, GPS position, movement profiles);

d. financial data (e.g., income, expenses, ratings);

e. identification data (e.g., first name, last name, company name, phone number, email address);

f. contact data (e.g., phone number, email address);

g. accounting data (e.g., bank account details, tax identification number);

h. attitudes and beliefs (e.g., customer opinions);

i. biometric data (e.g., age, gender);

j. biographical data (e.g., profession, education).

k. WhatsApp communication data (Recipients' phone numbers, WhatsApp profile name, message and template content, content and files sent by Recipients, delivery and read statuses);

l. web push subscription data (endpoint address and encryption keys, subscriber identifier, device and browser data, IP address, geolocation data, engagement data);

m. contact data imported or created by the User (contact details, tags and additional attributes assigned by the User, contact source, consent status and history).

n. email communication data: Recipients' email addresses and identifiers, data used in message content or personalisation, campaign content and subject, sender and domain details, the source, status and history of consent and opt-outs, sending identifiers and timestamps, acceptance, delivery, delay and bounce statuses, spam complaints, suppression lists, open and click data and technical event data made available by the provider, including IP address and email-client or browser data. This scope does not include retrieving the content of Recipients' private mailboxes or handling their replies within the Service.

User Consent for Sub-processing: The User consents to E-Trade entrusting the Processing of Personal Data to another Sub-processor for further Processing, in accordance with Section 12 of the DPA:

• Other Sub-processors within the EEA:

Jamna Software Sp. z o.o. with its registered office in Stargard, ul. Powstańców Warszawy, No. 10A, Apt. 4, 73-110 Stargard, entered in the Register of Entrepreneurs of the National Court Register maintained by the District Court Szczecin-Centrum in Szczecin, XIII Commercial Division of the National Court Register under number 0000848802. NIP (VAT ID): 8542432361, REGON (Business ID): 386829417, with a share capital of 50,000 PLN;

Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen, Germany — infrastructure hosting and storage of User Data;

Vercom S.A. (EmailLabs), registered office in Poznań (61-569), Poland, KRS 0000535618, NIP 7811765125, REGON 300061423 — email delivery, including notifications/digests containing lead data;

WhatsApp Ireland Limited, 4 Grand Canal Square, Dublin, Ireland — delivery of messages under the

WhatsApp Service. Data may be transferred to WhatsApp LLC and Meta Platforms, Inc. in the United States under terms established by Meta, including Standard Contractual Clauses;

Functional Software, Inc. (Sentry), application error monitoring (may include access to Personal Data contained in error reports); data stored in the EU region (Frankfurt), with possible access from the USA under Standard Contractual Clauses.

Amazon Web Services EMEA SARL, 38 Avenue John F. Kennedy, L-1855, Luxembourg - Amazon Simple Email Service (Amazon SES) infrastructure and services necessary for email campaign delivery, delivery events, open and click measurement and sending suppression. Additional AWS entities may participate in processing under the AWS GDPR Data Processing Addendum and AWS's published subprocessor list; information: https://aws.amazon.com/compliance/gdpr-center/.

Data for the Email Service are handled in the AWS region specified in the service configuration; the default module configuration provides for Europe (Frankfurt). Message delivery requires transferring data to the recipient's email provider, whose location depends on the address selected by the User. The AWS region's location does not mean that all processing takes place exclusively in the EEA. Transfers of Personal Data by E-Trade or its subprocessors outside the EEA take place under Chapter V of the GDPR using an appropriate transfer basis, including Standard Contractual Clauses where required. The AWS GDPR Data Processing Addendum applies in respect of AWS. The User is responsible for ensuring that its own sending instructions and recipient selection comply with applicable data protection rules.

Annex B – Appropriate Technical and Organisational Measures

Technical and Organisational Measures

Confidentiality:

- □ Protection against unauthorised access to data processing systems (e.g., keys, electronic access cards, smart cards, electronic door opening devices, security personnel, security guards, alarm systems, video surveillance systems);
- □ Protection against unauthorised use of systems (e.g., passwords, automatic locking mechanisms, two-factor authentication, encryption of data carriers);
- □ Standard processes for assigning permissions, logging access, and periodic verification of assigned authorisations, especially for administrative user accounts;
- □ Pseudonymization – core identifying attributes of personal data are removed and stored separately during data processing;
- □ Data classification system, in line with obligations under legal requirements, contracts, or internal control procedures (e.g., classification into confidential, secret, restricted, internal, public, or open data).
- □

Integrity and Accountability:

- □ Control of unauthorised reading, copying, modification, deletion, or transmission (e.g., encryption, VPN, electronic signatures);
- □ Control of personal data entry (e.g., logging, document management);
- □ Protection against accidental or unlawful destruction or loss (e.g., backup policies, power backup systems, surge protectors, antivirus protection, firewalls, contingency plans, security controls at the infrastructure and application levels, standard processes related to staff departures);
- □ Rapid recovery capability;
- □ Data and metadata erasure schedules.

Periodic Review and Assessment Procedures:

- □ Data protection management, including regular employee training;
- □ Incident response management;
- □ Default privacy settings;
- □ No processing without appropriate instructions from the Data Controller (e.g., clear terms for processing agreements and sub-processing agreements, rigorous selection of processors and other subprocessors, audits, inspections

Annex C – Transfer of Personal Data to Third Countries or International Organisations

Transfer of Personal Data to Third Countries or International Organisations

The transfer of personal data to third countries or international organisations is permissible only under the following conditions:

1) The processing of personal data must comply with the provisions of the GDPR;
2) The transfer of personal data to controllers, processors, or other recipients in third countries or international organisations must not compromise the level of protection of natural persons as ensured by the GDPR, including any onward transfers to third countries and international organisations.
3) **The transfer of personal data to third countries is permissible based on a decision by the Commission determining an adequate level of protection**. A data transfer based on such an adequacy decision does not require special authorisation from the supervisory authority. When assessing whether the level of protection is adequate, the Commission takes into account, in particular, the following elements: the rule of law, respect for human rights and fundamental freedoms, relevant legislation—both general and sector-specific—including in the areas of public security, defence, national security, and criminal law, as well as the access of public authorities to personal data and the implementation of such legislation; data protection principles, professional conduct rules, security measures, including rules for onward transfers of personal data to another third country or international organisation that are observed in that country or international organisation; case law; the existence of effective and enforceable rights for data subjects whose personal data is transferred, including their right to effective administrative and judicial redress; the existence and effective functioning of at least one independent supervisory authority in the third country or with regard to the international organisation, tasked with ensuring and enforcing compliance with data protection regulations—including possessing appropriate powers to enforce compliance, assist, and advise data subjects in exercising their rights, and cooperate with supervisory authorities of Member States; as well as the international commitments undertaken by the third country or international organisation, or other obligations arising from legally binding conventions or instruments, and participation in multilateral or regional systems, particularly in the area of data protection. The Commission publishes in the Official Journal of the European Union and on its website a list of third countries, territories, and specified sectors within a third country, as well as international organisations, for which it has adopted an adequacy decision or determined a lack thereof. **Decisions adopted by the Commission under Article 25(6) of Directive 95/46/EC remain in force until they are amended, replaced, or repealed by a Commission decision, which currently applies to** Andorra, Argentina, Canada (commercial activities), the Faroe Islands, Guernsey, Israel, the Isle of Man, Japan, Jersey, New Zealand, Switzerland, Uruguay, and the United Kingdom.
4) The transfer of personal data to third countries is permissible subject to the provision of appropriate safeguards.
5) **Appropriate safeguards may be ensured without requiring special authorisation from the supervisory authority through:**
    a) a legally binding and enforceable instrument between public authorities or bodies;
    b) binding corporate rules;

c) standard data protection clauses adopted by the Commission pursuant to the examination procedure;

d) standard data protection clauses adopted by a supervisory authority and approved by the Commission pursuant to the examination procedure;

e) an approved code of conduct together with binding and enforceable commitments of the controller or processor in the third country to apply appropriate safeguards, including with regard to the rights of data subjects;

f) an approved certification mechanism together with binding and enforceable commitments of the controller or processor in the third country to apply appropriate safeguards, including with regard to the rights of data subjects

6) Appropriate safeguards may be provided subject to the authorisation of the competent supervisory authority through:

a) contractual clauses between the controller or processor and the controller, processor, or recipient of the personal data in the third country or international organisation;

b) provisions of administrative arrangements between public authorities or bodies that include enforceable and effective rights for data subjects.

7) In the absence of a Commission decision determining an adequate level of protection or the absence of appropriate safeguards, including binding corporate rules, the transfer of personal data to a third country or international organisation, whether single or repeated, may only take place under the condition that

a) the data subject, having been informed of the potential risks that may arise for them due to the lack of an adequacy decision and the absence of appropriate safeguards, has explicitly consented to the proposed transfer;

b) the transfer is necessary for the performance of a contract between the data subject and the controller or for the implementation of pre-contractual measures taken at the data subject's request;

c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;

d) the transfer is necessary for important reasons of public interest. The public interest must be recognised in the law of the Union or the law of the Member State to which the controller is subject;

e) the transfer is necessary for the establishment, exercise, or defence of legal claims;

f) the transfer is necessary to protect the vital interests of the data subject or other persons where the data subject is physically or legally incapable of giving consent;

g) the transfer is made from a register which, according to Union law or the law of a Member State, is intended to provide information to the public and is open to consultation by the public or any person who can demonstrate a legitimate interest—but only to the extent that the conditions for such consultation set out in Union or Member State law are met in the particular case. The transfer must not involve the entirety of the personal data or entire categories of personal data contained in the register. If the register is accessible to persons with a legitimate interest, the transfer shall be made only at the request of those persons or where they are to be the recipients

8) **If the transfer cannot be based on any of the previously defined grounds, including provisions related to binding corporate rules, and none of the exceptions applicable in specific situations apply, the transfer to a third country or international organisation may only take place if the transfer is not repetitive, concerns only a limited number of data subjects, is necessary due to compelling legitimate interests pursued by the controller, which are not overridden by the interests or rights and freedoms of the data subject. The controller must assess all the circumstances surrounding the data transfer and, based on this assessment, ensure suitable safeguards for the protection of personal data.** The Data Controller must inform the supervisory authority about the transfer. In addition to the information referred to in Articles 13 and 14 of the GDPR, the controller must also provide the data subject with information about the transfer and the compelling legitimate interests pursued by the controller. The Data Controller or the Processor must document the assessment and the appropriate safeguards in their records.