

Allegro Finance sp. z o.o. Privacy protection policy

Appendix of Allegro Finance Terms & Conditions

Section 1. Definitions, Purposes, and Scope of Application of the Policy

DEFINITIONS

1. **Personal Data** — within the meaning of the definition contained in Article 4(1) of the GDPR, personal data are understood as information about a natural person identified or identifiable by one or more specific factors determining, e.g., physical, physiological, genetic, mental, economic, cultural, or social identity, including first and last name, contact number, email address, information provided through User requests or instructions.

2. **Biometric Data** — within the meaning of the definition contained in Article 4(14) of the GDPR

3. **Tax Ordinance** — Act of August 29, 1997 — Tax Ordinance.

4. **PIPL** — Personal Information Protection Law of the People's Republic of China of August 20, 2021.

3. 5. **Policy** — this document

6. **Electronic Communications Law** — Act of July 12, 2024 — Electronic Communications Law.

4. 7. **GDPR** — Regulation of the European Parliament and of the Council (EU) 2016/679 of 27th April 2016 on the protection of natural persons with regard to the processing of personal data and the free movement of such data, and repealing Directive 95/46/EC

8. **Personal Data Protection Act** — Act of May 10, 2028, on the protection of personal data.

5. 9. ~~Anti-Money Laundering Act~~ **Act on Anti-Money Laundering and Countering the Financing of Terrorism** — Act of March 1, 2018, on counteracting money laundering and terrorist financing (consolidated text: Journal of Laws of 2022, item 593, as amended)

10. **Accounting Act** — Act of September 29, 1994, on accounting.

6. 11. **User** — a person using Allegro Finance services or applying for their use.

PERSONAL DATA CONTROLLER, PURPOSES AND SCOPE OF THE POLICY

The controller of personal data of users who are natural persons is Allegro Finance spółka z ograniczoną odpowiedzialnością with its registered office in Poznań, address: ul. Wierzbicice 1B, 61-569 Poznań (hereinafter: „we,” „Allegro Finance,” or the „Company”). This means that the Company determines the purposes and means of processing your Personal Data.

The Policy sets out, in particular, the scope and legal grounds for processing your Personal Data, which we collect in connection with your or your associated parties' use of services we provide. Detailed rules for the processing of Personal Data by Allegro Finance can also be found in the Terms & Conditions issued by us or partners we cooperate with.

The Company's activities are subject to the provisions of law applicable to the protection of personal data, in particular the provisions of the GDPR and the Personal Data Protection Act of May 10, 2018. Should you have questions or concerns about the rules and methods the Company protects your Personal Data, write to our Data Protection Officer:

- email address: iod@allegrofinance.pl,
- postal address: Inspektor Ochrony Danych Allegro Finance sp. z o.o., ul. Wierzbicice 1B, 61-569 Poznań.

Section 2. Source of Personal Data Processed by the Company

We can obtain your data from various sources:

(...)

D. From publicly available sources, including, but not limited to, data published by administrative authorities and courts (e.g., business registers, ineffective bailiff executions, bankruptcies, business bans), documents related to the performance of obligations provided for in the [Act on Anti-Money Laundering and Countering the Financing of Terrorism](#), and concerning the application of national and international restrictive measures;

(...)

Section 3. Scope of Personal Data Processed by the Company

The scope of Personal Data processed by the Company may vary depending on which services or functionalities provided by the Company you use. We process Personal Data necessary for their proper provision and the protection of legitimate business interests.

A unique identification and decision making about the possibility of establishing a relationship with you or a party associated with you, as well as the need to prevent financial crimes may require the processing

of Personal Data not specified in the Policy. As a rule, the Company processes data in the following scope:

(...)

B. Beneficial owners and persons entitled to represent the User/potential user who is a legal person/imperfect legal person:

- Identification data, e.g., first name(s), last name(s), country of birth, nationality, date of birth, unique identification numbers (e.g., PESEL (Personal ID No.), NIP (Tax Identification Number), REGON (National Business Registry Number)), images of the identity documents with their data (including image, document series and number, expiration date), image, Biometric Data;
 - Contact details, e.g., address of residence, mailing address, contact number, email address;
 - Business information contained, i.a., in the Register of Entrepreneurs of the National Court Register (KRS), the Central Registration And Information On Business (CEIDG), the National Register of Insolvent Debtors, or appropriate foreign registers;
 - Information related to the device used to access the Company's services, e.g., cookies, IP addresses;
 - Other personal data disclosed in the course of using the Company's services (e.g., during the complaints procedure);

C. For persons indicated in sub-paragraphs A and B: Information about inclusion in the sanctions lists, or being a politically exposed person, or being a family member of a politically exposed person, or a person known as a close associate of a politically exposed person within the meaning of the Act on counteracting money laundering and terrorist financing;

D. Parties involved in the distribution of payment instruments we have issued;

- Identification data, e.g., first name(s), last name(s), company name, unique identification numbers (e.g., PESEL (Personal ID No.), NIP (Tax Identification Number), REGON (National Business Registry Number));
- Contact details, e.g., address of residence, mailing address, address of the principal place of business, contact number, email address;
- Business information, e.g., that contained, i.a., in the Register of Entrepreneurs of the National Court Register (KRS), the Central Registration And Information On Business (CEIDG), the National Register of Insolvent Debtors, or relevant foreign registers;

E. Parties to the transaction (persons making the payment and beneficiaries of the payment, including those using payment instruments issued by the Company and those using payment services provided by the Company):

- Identification data, e.g., first name(s), last name(s), company name, unique identification numbers (e.g., PESEL (Personal ID No.), NIP (Tax Identification Number), REGON (National Business Registry Number));
- contact details (e.g. street and house number, postal code, city, e-mail address, telephone number, details given on the delivery form);
- **Transaction data, e.g., the subject matter, course, and procedure of the transaction, bank account numbers, information about payment tools used, information on the complaint procedure - in particular in the case of a refund procedure;
- Information related to the device (including the payment tool) used to carry out the transaction;
 - Other Personal Data that constitutes information accompanying transfers of funds, and disclosed during the complaint procedure;

F. Proxies:

- Identification data, e.g., first name(s), last name(s), unique identification numbers (e.g. PESEL (Personal ID No.), NIP (Tax Identification Number), REGON (National Business Registry Number));
- Contact details, e.g., mailing address, contact number, email address;
- Other Personal Data contained in documents confirming the authorization and disclosed in particular by a proxy (e.g., during the complaints procedure);

G. Legal successors:

- Identification data, e.g., first name(s), last name(s), unique identification numbers (e.g. PESEL (Personal ID No.), NIP (Tax Identification Number), REGON (National Business Registry Number));
- Contact details, e.g., mailing address, contact number, email address;
- Other Personal Data disclosed in particular by a legal successor (e.g., during the complaints procedure).

H. Creditors:

- Identification data, e.g., first name(s), last name(s), unique identification numbers (e.g., PESEL (Personal ID No.), NIP (Tax Identification Number), REGON (National Business Registry Number));
- Contact details, e.g., mailing address, contact number, email address;

- Other Personal Data disclosed in particular by a creditor or public authorities (e.g., in the course of enforcement, security, complaints proceedings, or proceedings related to the assignment agreement).

In the case of direct contact with the User service team/helpline of the Company, its recording may also be processed, about which you will be informed.

The application of financial security measures may involve the processing of data relating to the holding of, or association with, political positions, which is related to the determination under the AML and terrorist financing law. whether:

- you hold a politically exposed position,
- you are a family member of a politically exposed person or a person known to be a close associate of a politically exposed person.

Section 4. The purpose and legal grounds for the processing of your personal data by the Company

Depending on the services or functionalities you use, there are different purposes and legal grounds for processing Personal Data by the Company and periods during which the Company may store or use your Personal Data.

For each of the purposes of processing, we have specified the legal basis and the maximum period for the storage of Personal Data. [For clarity, we primarily indicate the legal basis under the GDPR, supplementing it with references to additional legal provisions or, in the case of Users who are also subject to the PIPL, indicating an additional legal basis \(this applies where the legal bases under the GDPR and the PIPL do not overlap\).](#) After the indicated period, we will not use your Personal Data for the indicated purpose. However, this does not mean that we will delete them in every case. We will retain your Personal Data for the longest period indicated for specific services of the Company. For example, if you opt out of the Company's services, we will stop processing your Personal Data for the purpose of providing the Company's services. We will store them for the period provided by law, for example to enable the exercise of your rights, and to be able to comply with legal obligations provided for in accounting, tax and anti-money laundering regulations.

If artificial intelligence (AI) systems or models are used, the Company processes Personal Data on the basis of a legitimate interest, [or, in the case of Users who are also subject to the PIPL, concurrently as part of performing the agreement concluded with you or based on your consent](#), unless the specific use requires other legal grounds, which we will specifically indicate in such cases.

Below we have described standard actions on Personal Data in connection with the use of services or functionalities provided by the Company. More detailed information on the processing of Personal Data when using certain services may also be found in the Terms & Conditions of those services.

CONCLUDING AN AGREEMENT WITH THE COMPANY AND ITS PERFORMANCE

Applying for the use of Allegro Finance services requires, in principle, the Company obtaining the Personal Data of Users, their representatives, and the beneficial owners of their business activity.

In connection with the performance of services, we process your Personal Data according to the rules described in the table. In addition, your Personal Data may be processed for other purposes, including analytical and marketing purposes, and to guarantee the security of our services, as you will learn from further sections of this part of the Policy. For the purposes described in this part, we may use artificial intelligence (AI) systems or models.

Purpose of Personal Data processing	Legal grounds for Personal Data processing	Period of storage of Personal Data for a specific purpose (retention period)
Taking steps related to the conclusion of an agreement with the User who is a natural person for electronically provided services and in the scope of payment services	Article 6(1)(b) of the GDPR (necessary for entering into and perform an agreement) – Personal Data required for the conclusion of the agreement	Until the service is discontinued, or until it is found that the service can no longer be provided
Taking steps related to the conclusion of an agreement with the User through a representative for electronically provided services and in the scope of payment services	Article 6(1)(f) of the GDPR (legitimate interest of the Company, consisting in establishing a relationship with the User) <i>or, in the case of Users who are also subject to the PIPL, concurrently as part of performing the agreement concluded with the Company—</i> Personal Data necessary to conclude an agreement	Until the service is discontinued, or until it is found that the service can no longer be provided
Application of financial security measures provided for in the anti-money laundering regulations	Article 6(1)(c) and Article 9(2)(g) of the GDPR in conjunction with Article 34 of the <i>Act on Anti-Money Laundering and Countering the Financing of Terrorism Act</i> .	5 years from the end of the cooperation with you/a party associated with you, or from the last occasional transaction, except where the supervisory authority instructs that Personal Data be stored for longer
Handling complaints, including solving technical problems	Article 6(1)(b) of the GDPR (legitimate interest of the Company in the protection of the Company's and the User's rights) <i>or, in the case of Users who are</i>	Until the processing of the complaint completed, or until the technical issue is resolved

	also subject to the PIPL, concurrently as part of performing the agreement concluded with the Company	
Exercise or defense of legal claims arising from an agreement or related to the provision of services, including debt collection or participation in court, arbitration, and mediation proceedings	Article 6(1)(f) of the GDPR (legitimate interest of the Company in the protection of the Company's rights) <i>or, in the case of Users who are also subject to the PIPL, concurrently as part of performing the agreement concluded with the Company</i>	Until the last day of the calendar year following the expiration of a 3 years' period after the service is discontinued. If necessary, personal data will be processed until the final completion of civil, enforcement, administrative, or criminal proceedings that require the processing of Personal Data
Exercise or defense of legal claims in connection with applying for and not concluding an agreement for Allegro Finance services	Article 6(1)(f) of the GDPR (legitimate interest of the Company in the protection of the Company's rights) <i>or, in the case of Users who are also subject to the PIPL, concurrently as part of performing the agreement concluded with the Company</i>	12 months starting from the year following the year in which the agreement was not concluded
Execution of public authority decisions	Article 6(1)(c) (processing is necessary for compliance with a legal obligation under specific regulations)	Until the purpose of processing has been fulfilled
Compliance with statutory obligations under tax and accounting regulations	Article 6(1)(c) of the GDPR in conjunction with Article 70 § 1 of the Tax Ordinance Act and Article 74 of the Accounting Act (processing necessary for compliance with a legal obligation) <i>or other applicable regulations</i>	5 years from the beginning of the year following the fiscal year in which the economic event requiring the processing of your Personal Data occurred

(...)

USER SERVICE AND CONTACT FORM

(...)

In relation to the handling of content addressed to the Company, including through the contact form, we process your Personal Data according to the rules described in the table. Your Personal Data may also be processed for other purposes, including analytical and marketing purposes, and to guarantee

the security of our services. Continue reading to learn more. For the purposes described in this part, we may use artificial intelligence (AI) systems or models.

Purpose of Personal Data processing	Legal grounds for Personal Data processing	Period of storage of Personal Data for a specific purpose (retention period)
Contacting Users, including for the purposes of providing services and User service, through the available communication channels, in particular email, telephone, contact form	Article 6(1)(b) of the GDPR (necessary for the performance of an agreement)	Until the service is discontinued
Handling Users' requests submitted in particular to the customer service department and via the contact form, when they are not directly related to the performance of the agreement	Article 6(1)(f) GDPR (legitimate interest of the Company in responding to received queries) or, in the case of Users who are also subject to the PIPL, concurrently as part of performing the agreement concluded with the Company	Until a response is given or the request is granted
Exercise or defense of legal claims arising from an agreement or related to the provision of services, including debt collection or participation in court, arbitration, and mediation proceedings	Article 6(1)(f) of the GDPR (legitimate interest of the Company in the protection of the Company's rights) or, in the case of Users who are also subject to the PIPL, concurrently as part of performing the agreement concluded with the Company	Until the last day of the calendar year following the expiration of a 3 years' period after the service is discontinued. If necessary, Personal Data will be processed until the final completion of civil, enforcement, administrative, or criminal proceedings that require the processing of Personal Data

MARKETING ACTIVITIES

The Company may also use your Personal Data to carry out marketing activities, including where you provide your Personal Data or give your consent to their processing. In return, the Company makes content or services available to you. For the purposes described in this part, we may use artificial intelligence (AI) systems or models.

Purpose of Personal Data processing	Legal grounds for Personal Data processing	Period of storage of Personal Data for a specific purpose (retention period)
Contacting Users for purposes related to	Article 6(1)(f) of the GDPR in conjunction with Articles 398 and	Until the consent to receive messages or information is

permitted activities, available communication channels, including email, text/MMS, and push, and telephone contact	marketing through electronic channels, text/MMS, and telephone contact	399 of the Electronic Communications Law Article 10 of the Act on Electronically Supplied Services or Article 172 of the Telecommunications Law (legitimate interest of the Company in the promotion of the Company's or third-party goods or services in connection with expressed consent for a communication channel) or, in the case of Users who are also subject to the PIPL, concurrently based on the expressed consent	withdrawn (based on the provisions of the Act on Electronically Supplied Services or the Telecommunications Law), or until an effective objection to Personal Data processing for marketing purposes is expressed
--	--	---	---

ANALYTICAL AND STATISTICAL ACTIVITIES AND SURVEYS

Provisions of the [Act on Anti-Money Laundering Act and Countering the Financing of Terrorism](#) require Allegro Finance to apply financial security measures, which often involve analyzing the activities of Users and their associated parties.

Allegro Finance may also be required by regulatory authorities to provide aggregated or individual reports and analyzes concerning Users and their associated parties.

In addition, your Personal Data may be processed by the Company for analytical and statistical purposes. In this case, we use your Personal Data to improve functionality and quality of services.

Though surveys sent to Users, i.e., via email, the Company may collect Personal Data from Users, which can be used to examine Users' preferences and adjust the Company's offer to their expectations. Such Personal Data are also used for statistical analyses.

In connection with the performance of analytical and statistical activities, we process your Personal Data according to the rules described in the table. Your Personal Data may also be processed for other purposes, including in particular to guarantee the security of our services, as you will learn from further sections of this part of the Policy. For the purposes described in this part, we may use artificial intelligence (AI) systems or models.

Purpose of Personal Data processing	Legal grounds for Personal Data processing	Period of storage of Personal Data for a specific purpose (retention period)
Carrying out analyzes provided for in the Act on Anti-Money Laundering and	Article 6(1)(c) of the GDPR in conjunction with Article 34 of the Act on Anti-Money Laundering and Countering the Financing of	Results of the analyzes will be stored for 5 years from the time of their completion, except where the

Countering the Financing of Terrorism Act	Terrorism or other applicable regulations Act	supervisory authority instructs that Personal Data be stored for longer
Preparation and sharing of reports and analyzes provided for in specific regulations	Article 6(1)(c) of the GDPR	In accordance with the regulations on the basis of which the reports and analyzes were prepared
Conducting analytical and statistical activities	Article 6(1)(f) of the GDPR (legitimate interest of the Company in analyzing Users' activity, including activity history, to optimize the services provided and to increase their quality) or, in the case of Users who are also subject to the PIPL, concurrently as part of performing the agreement concluded with the Company	Until the end of the storage period of the User's Personal Data in connection with another active purpose of processing, or until an effective objection to Personal Data processing is expressed
Conducting surveys, research, and analyses on the services provided, including in terms of functioning, improving their operation, or estimating the main interests and needs of Users	Article 6(1)(f) of the GDPR (legitimate interest of the Company in analyzing User activity to optimize the services provided) or, in the case of Users who are also subject to the PIPL, concurrently as part of performing the agreement concluded with the Company	Personal Data are processed in real time and, therefore, they will be stored until the User no longer uses the services provided by the Company (that is, until the User completes a survey or analysis)

ENSURING SECURITY OF THE SERVICES PROVIDED AND ENFORCING THE TERMS & CONDITIONS

Where necessary, in order to ensure the security of services, including IT resources or the security of other Users **and continuity of the Marketplaces or Mobile Application**, ~~services, or functionalities~~, the Company may automatically obtain and record your Personal Data transmitted to the server by web browsers or your devices.

In order to guarantee an adequate security level and prevent abuse and fraud, the Company may obtain and record Personal Data transmitted to the server by web browsers or your devices, **as well as via the interaction with the Marketplaces itself** ~~(which include, in particular~~ **including**: technical components of the device, **software parameters, browser settings, location data, and information on the use of the Marketplaces** ~~how it is used, your browser settings, and details of your viewing behavior on Allegro)~~ in such a way as to create a unique digital "fingerprint" of the devices or instances of applications that you use. **The Company may use such a digital "fingerprint" for additional authentication of the User, including as part of the authentication methods. These measures help to prevent abuse and fraud.**

In order to counteract abuse, fraud, activities that violate rules of morality, the Allegro Terms & Conditions, and attempts to use your Account without authorization, the Company provides Lexisnexis Risk Solutions (EUROPE) Limited with Personal Data and certain Personal Data from your online interactions. These data allow querying the anonymous digital identity network (DIN) consisting of events originating from the entities participating in the network. Personal data outside the IP address is provided by us in a masked form in such a way that it is not possible to identify you. Information about the processing of data by Lexisnexis Risk Solutions (EUROPE) Limited can be found [here](#).

In order to prevent abuse, fraud, ~~and~~ **or** acts that violate the terms of our services, applicable laws (including national or international restrictive measures), or **acts** that negatively affects security, we automatically process Personal Data relating to the use of our services and products, including analyzing links with other parties whose personal data we process. For the purposes described in this part, we may use artificial intelligence (AI) systems or models. **In cases where the links or risk signals are ambiguous, automated decisions are subject to initial verification by authorized employees of the Company.**

In order to counteract the occurrences listed above, we will make decisions in your case based on automatic data processing, including profiling.

These actions may have an effect of limiting the ability to use the services or functionalities, e.g. automatic suspension **or** reinstatement of the ability to use our services, their individual functionalities, **or** payouts of collected funds.

(...)

Section 5. Users' Rights in the Context of Personal Data Processing and How to Exercise Them

We enable the exercise of all your rights under the GDPR, i.e., the rights described in Articles 15-22 of the GDPR **and** PIPL. Below is a detailed description of these specific rights.

The **right of access to Personal Data** allows you to obtain information on the processing of your Personal Data by the Company, including in particular on the purposes and legal grounds for such processing, the scope of the data held, parties to whom your data are disclosed, and the planned date of erasure of these data.

To **obtain a copy of your Personal Data** processed by the Company, you can exercise your right in this respect.

You can exercise your **right to rectify your Personal Data** if you notice that your Personal Data are inaccurate or incomplete. In this case, we undertake to remove the discrepancies or errors in the Personal Data processed and to supplement such Personal Data if they are incomplete.

You can exercise your **right to erasure of your Personal Data** if:

- Your Personal Data are no longer necessary for the purposes for which they were collected or otherwise processed by the Company;
- You withdraw your consent to the processing of Personal Data or object to the processing of your Personal Data, and there are no other legal grounds for their processing;
- Your Personal Data are processed unlawfully.

You can exercise your **right to restrict the processing of Personal Data** if:

- You notice that your Personal Data are inaccurate — you can request the restriction of the processing of your Personal Data for a period allowing us to check the correctness of such data;
- Your Personal Data are being processed unlawfully, but you do not wish them to be erased;
- We no longer need your Personal Data, but you may need them for exercise or defense of legal claims;
- You object to the processing of Personal Data — until it is determined whether the legitimate grounds on our side override the grounds for objection.

You can exercise the **right to Personal Data portability** if the processing of your personal data is based on your consent or a contractual relationship between you and the Company, and if this processing is carried out by automated means.

You can exercise the **right to object to the processing of your Personal Data for marketing purposes** at any time if your Personal Data are processed for marketing purposes, without the need to justify such objection.

[In the case of Users who are also subject to the PIPL regulations, the right to object or refuse processing is granted in line with the rules and to the extent provided for in the GDPR and the relevant PIPL regulations.](#)

You can exercise the **right to withdraw consent to the processing of Personal Data** that you previously expressed at any time; withdrawal of your consent will not affect the lawfulness of the processing that was carried out on the basis of consent before its withdrawal.

You can exercise your **right to human intervention, express your point of view, and contest an automated decision taken against you** at any time if an automated decision has been taken against you that produces legal effects or similarly significantly affects you.

Note also that you have the **right to lodge a complaint** regarding our processing of your Personal Data with the supervisory authority, i.e., the President of the Personal Data Protection Office (address: Prezes Urzędu Ochrony Danych Osobowych, ul. Moniuszki 1A, 00-014 Warszawa).



In addition, if you are a User subject to the PIPL, you also have the right to have the personal data processing rules explained to you. For this purpose, you may contact the Company as described in Part 9 of the Policy. At the same time, we indicate that the Policy serves as the primary point of reference for exercising this right.

Section 6. Personal Data Recipients

The recipient of personal data is any third party to which the Company discloses your Personal Data — regardless of whether it acts on our behalf or processes data on its own behalf.

The recipients of your Personal Data may be:

- A. Parties authorized to receive such data under the law, including competent judicial authorities, in particular as part of Allegro Finance fulfilling its obligations provided for in the law and related to the provision of payment services;
- B. To the extent and for the time necessary to provide or perform services (including payment institutions) and in relation to these services — third parties, including parties engaged by Allegro Finance to perform actions related to the provision of services or which participate in (and benefit from) such services;
- C. Allegro sp. z o.o., to counteract fraud on the Allegro platform in connection with the payment services provided;
- D. Other parties, if this results from the rules or terms of services provided by us and this Policy.

We cooperate with specialized providers of data storage services, analytical services, debt collection services, and IT services. In this case, your Personal Data will be processed exclusively on behalf of and for the purposes of Allegro Finance in accordance with the concluded data processing agreements. The company also cooperates with entities offering tools based on artificial intelligence (AI) systems or models.

If you need detailed information about the above-mentioned entities, such as contact details, specific purposes, means of transferring Personal Data, and the categories of Personal Data transferred, contact us as specified in Part 9 of the Policy.

Section 7. Transfers of Personal Data to Countries Outside the European Economic Area

Your Personal Data may be transferred outside the European Economic Area, including to:

- ~~SFDC UK, Ltd (SalesForce) with its registered office in London, UK, in connection with the use of Personal Data processing services offered by this party to ensure the provision of services by Allegro Finance.~~

- Regulatory DataCorp Limited, with its registered office in London, UK, in connection with the use of services to support analyses aimed at preventing money laundering and terrorist financing.
- In the event of transactions for a party or for an account maintained by a financial institution located outside the European Economic Area, Personal Data may be transferred by the Company outside the European Economic Area on a one-time basis for the purpose of executing that specific transaction. The transfer of Personal Data is necessary for the performance of the agreement between the Company and the person using the services of the Company, as well as for the execution of the transaction itself.

At the same time, as part of cooperation with processors, data processing may be further entrusted to parties that may transfer data to countries outside the European Economic Area. Parties that systematically process data for Allegro Finance include:

- Genesys Cloud Services BV with its registered office in Amsterdam, the Netherlands, in connection with the use of Personal Data processing services offered by this party to ensure the provision of services offered by the Company as part of Allegro Finance;
- Google Cloud Poland sp. z o. o. with its registered office in Warsaw, Poland, in connection with the use of Personal Data processing services offered by this party and provided outside the European Economic Area to ensure the provision of payment services by Allegro Finance;
- Lexisnexis Risk Solutions (EUROPE) Limited, based in Dublin, Ireland, in connection with the use of the ThreatMetrix service to ensure the security of the provision of services by the Company offered on Allegro;
- Microsoft Ireland Operations, Ltd with its registered office in Dublin, Ireland, in connection with the use of Personal Data processing services offered by this party to ensure the provision of services offered by the Company as part of Allegro Finance;
- SFDC Ireland, Ltd (SalesForce) with its registered office in Dublin, Ireland, in connection with the use of Data processing services offered by this party to ensure the provision of services by Allegro Finance;
- Snowflake Computing Netherlands, B.V. with its registered office in Amsterdam, the Netherlands, in connection with the use of Personal Data processing services offered by this party to ensure the provision of services offered by the Company as part of Allegro Finance.

Allegro Finance always relies on mechanisms ensuring an adequate level of protection, i.e., by using standard contractual clauses for the transfer of Personal Data to Personal Data processors established in third countries, as approved by the European Commission. To obtain copies of such clauses, contact us at: iod@allegrofinance.pl.

In the case of Users (Sellers) who are established or reside in the People's Republic of China or conduct business from the People's Republic of China, Personal Data may be transferred outside the People's

Republic of China to the entities indicated above. The Company will comply with all the requirements provided for in applicable laws, such as:

- obtaining a separate consent, if consent is the legal basis for processing;
- carrying out a data protection impact assessment;
- obtaining a positive verification in the scope of cross-border transfer, if required.

If you need detailed information about the above-mentioned entities, such as contact details, specific purposes, means of transferring Personal Data, and the categories of Personal Data transferred or procedures for exercising rights against recipients under applicable local laws, contact us as specified in Part 9 of the Policy.

~~Where you are transacting for an entity or account with a financial institution located outside the European Economic Area, Personal Data may be transferred by the Company outside the EEA on a one-off basis in order to complete a specific transaction. The transfer of Personal Data is necessary for the performance of the contract between the Company and the person using the Company's services, as well as for the transaction itself.~~

Section 8. Contact Details

You can receive more information about the processing of your Personal Data, including answers to questions about the scope of the Privacy Protection Policy, by contacting our Data Protection Officer.

Email address: iod@allegrofinance.pl

Postal address: Inspektor ochrony danych Allegro Finance sp. z o.o., ul. Wierzbicice 1B, 61-569 Poznań.

You can also contact the Data Protection Officer via the contact form.

If the Seller has additional support, the relevant information or assistance in obtaining it may also be provided by the Account Manager.