InstaCash Ltd.

Terms and Conditions

Effective from: 1 March 2023

InstaCash Kft. (hereinafter: Service Provider) provides a deferred payment solution as a payment method and related additional services on behalf of its merchant partners (hereinafter: Partner) to their customers and customers (hereinafter referred to as the User) on the https://bnpl.instacash.hu page (hereinafter: Website).

These General Terms and Conditions (hereinafter referred to as: GTC) apply to all services provided through the website indicated above.

1. DETAILS OF THE SERVICE PROVIDER:

Name of Service Provider: InstaCash Limited Liability Company
Headquarters: 1015 Budapest, Szabó Ilonka utca 22. Door 2
Contact: bnpl@instacash.hu
Tax number: 26500469-2-41
Company registration number: 01-09-328893

2. BASIC PROVISIONS

2.1. Issues not regulated in the present GTC and their interpretation shall be governed by Hungarian law, with special regard to the relevant provisions of Act V of 2013 on the Civil Code ("Civil Code") and Act CVIII of 2001 on Certain Issues of Electronic Commerce Services and Information Society Services, as well as Government Decree 45/2014 (II.26.) on the Detailed Rules of Contracts between Consumers and Businesses.

2.2. By accepting these General Terms and Conditions, the User declares that he/she uses the Website at his/her own risk and acknowledges the General Terms and Conditions as binding on him/herself.

3. PROVISIONS RELATING TO THE CONCLUSION OF CONTRACTS

3.1. By accepting the present GTC, the User expressly and irrevocably declares that he is entitled to conclude a contract through the Website. The User acknowledges that it is the User's responsibility to prove the invalidity of the contract.

4. DEFINITION OF RESPONSIBILITIES

4.1. With regard to the fact that the construction of the deferred payment solution and its related parameters are determined by the Service Provider's Partners, the Service Provider cannot take responsibility for the settings under which its Partners make the deferred payment solution available.

4.2. The Service Provider develops the processes related to the use of deferred payment along the needs determined by its Partners, so it cannot take responsibility for any erroneous information resulting from possible inaccuracies.

4.3. When communicating the data and information indicated on the Website, programming them, and uploading the data stored therein, the Service Provider shall act with the utmost care expected of it, however, possible technical, recording and typographical errors may occur. The Service Provider does not take responsibility for any technical, data recording or typographical errors. The Service Provider also excludes its liability for any damages caused by its partners. The Service Provider shall not be liable for any damages or costs that may arise from the use of the Website or its unusable condition, improper operation, malfunction, unauthorized modification of data by anyone, or which may arise from delays in the transmission of information, computer viruses, line or system failures, or other similar reasons.

4.4. In order to provide the service, the Website may contain links to external websites operated by third parties independent of the Service Provider. Browsing such external websites is not covered by these Terms and Conditions. It is the User's sole responsibility to familiarise themselves with the terms of use of the respective website when visiting external websites.

4.5. In the event of rejection of the request, the Service Provider shall not assume any liability for any damages arising from the rejection of the request.

5. TERMS OF USE

5.1. The content and visual representation of the Website are the property of the Service Provider. Without the prior written consent of the Service Provider, it is prohibited to store the content of the Website in whole or in part, or to reproduce, reproduce, copy, distribute or use the Website in any other way. The use of the content of the Website for any commercial purpose is prohibited. Copying with the intention of distribution requires the prior written consent of the Service Provider. All rights in the Website are reserved.

5.2. The Service Provider is entitled to send its newsletters to the e-mail address provided by the User through the Website on the basis of the User's authorization and until the User's withdrawal request to do so.

5.3. If any part of the present GTC becomes invalid or unenforceable does not affect the validity, legality and enforceability of the remaining parts.

6. THE SYSTEM USED FOR THE EXECUTION OF BANK CARD PAYMENTS DURING THE PROVISION OF DEFERRED PAYMENTS

6.1. Online bank card payments are made through the Barion system. The bank card data will not reach the merchant. Barion Payment Zrt., the provider of the service, is an institution under the supervision of the National Bank of Hungary, its license number: H-EN-I-1064/2013.

Az InstaCash Kft.

Privacy Notice

on data processing related to the use of deferred payment

Effective from: 1 March 2023

InstaCash Limited Liability Company (registered office: 1015 Budapest, Szabó Ilonka utca 22. Fsz. door 2, company registration number: 01-09-328893, tax number: 26500469-2-41) as data controller (hereinafter: "**Data Controller 1**") and the [Trader/Service Provider's company name] (registered office: [Trader/Service Provider's registered office], company registration number: [Trader/Service Provider's company registration number], tax number: [Trader/Service Provider's company registration number], tax number: [Trader/Service Provider] tax number]) as data controller (hereinafter referred to as "**Data Controller 2**") inform the data subjects about the data processing related to the deferred payment provided by Data Controller 2 as follows:

1. Joint data processing

Controller 1 and Controller 2 are engaged in joint data processing in connection with the deferred payment available in the webshop operated by Controller 2 at [Webshop URL] **(hereinafter: "**Webshop") (hereinafter referred to as "**Joint Data Controllers**" or "**Data Controllers**")") with regard to the fact that Controller 2 entrusted Controller 1 with the provision of IT services related to deferred payment. The Data Controller 2 processes personal data as the operator of the Webshop and as a merchant, while the Data Controller 1 processes personal data as an IT service provider. The Joint Data Controllers inform the data subjects (hereinafter referred to as "**Client**" or "**Clients**") that their requests related to data processing will be received by Data Controller 1 and answered by Data Controller 1 in the manner specified in Section 6 of this Notice.

2. Applicable law

The most important legal regulations applied during data processing:

- 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 (hereinafter referred to as the "**GDPR")**
- Act CXII of 2011 – on the Right of Informational Self-Determination and on Freedom of Information (hereinafter: "**Infotv.**").

3. Scope of data processed, purpose, legal basis and duration of data processing

3.1. In the context of deferred payment, the Joint Controllers process personal data as follows:

Processed personal data	**Purpose of data processing**	**Legal basis of data processing**	**Duration of data processing**
Private Individual in the case of a Client Name (last name, first name) Place and date of birth Mother's name Address Tax identification number Amount and term of deferred payment	Establishing, performing and registering a deferred payment contract	Article 6(1)(b) of the GDPR) The processing is necessary for the performance of a contract to which the data subject is a party or it is necessary to take steps at the request of the data subject prior to the conclusion of the contract	For 5 years from the termination of the deferred payment contract

Monthly Installment Amount			
In case of a sole proprietorship Client Name (last name, first name) Seat Registration number Tax number Amount and term of deferred payment Monthly Installment Amount	Establishing, performing and registering a deferred payment contract	Article 6(1)(b) of the GDPR) The processing is necessary for the performance of a contract to which the data subject is a party or it is necessary to take steps at the request of the data subject prior to the conclusion of the contract	For 5 years from the termination of the deferred payment contract
Results of the financial due diligence carried out by Data Controller 1	Making a decision to grant deferred payments	It is in the interest of Data Controller 2 to provide deferred payment only to Clients who are expected to be solvent (Article 6(1)(f) of the GDPR)	Until a decision is made on granting deferred payments
Telephone number	Deferred payment contract validation	Article 6(1)(b) of the GDPR) The processing is necessary for the performance of a contract to which the data subject is a party or it is necessary to take steps at the request of the data subject prior to the conclusion of the contract	Until the deferred payment contract is validated
Credit card number	Monthly Payment Deduction from the Client	Article 6(1)(b) of the GDPR) The processing is necessary for the performance of a contract to which the data subject is a party or it is necessary to take steps at the request of the data	Until the purchase price is fully satisfied

		subject prior to the conclusion of the contract	
Credit card number Email address Telephone number	Compliance monitoring	The legitimate interest of the Data Controllers in the full performance of the contract for deferred payment (Article 6(1)(f) of the GDPR)	For 5 years from the termination of the deferred payment contract
Email address Telephone number	Marketing inquiries	Article 6(1)(a) of the GDPR Client's consent	For 2 years from the termination of the deferred payment contract

4. Transfer of personal data, data processors

The personal data specified in Section 3 of this Policy may be accessed by the representatives of the Joint Data Controllers and their employees performing tasks related to deferred payment.

In connection with the deduction of the monthly instalment, the Joint Data Controllers shall be responsible for **Barion Payment Zrt.** payment service provider (registered office: 1117 Budapest, Irinyi József utca 4-20. 2nd floor, company registration number: 01-10-048552) as a data processor.

In addition to the above, in the cases specified by law, the Joint Data Controllers are also entitled or obliged to transfer personal data to the organization entitled to act at the request of the competent authorities or for the purpose of enforcing the legal claim that has arisen.

5. Automated decision-making (including profiling):

Profiling under Article 4(4) of the GDPR is any form of automated processing of personal data in which personal data are used to assess certain personal characteristics relating to a natural person, in particular to analyse or predict characteristics relating to performance at work, economic situation, state of health, personal preferences, interests, reliability, behaviour, location or movement.

The Data Controllers inform the Clients that prior to the conclusion of the contract for deferred payment, the Data Controller will carry out 1 financial due diligence, during which profiling will also take place. However, this does not take place within the framework of joint data management as set out in this Policy, but within the framework of independent data processing carried out by Data Controller 1, in which case the data protection policy of Data Controller 1 performed as an independent data controller, available at https://instacash.hu/szabalyzatok-es-tajekoztatok/adatvedelmi-szabalyzat/ address, shall be applicable.

No automated decision-making, including profiling, will take place during data processing.

6. Rights of Clients

The Data Subject may enforce the rights set out in Chapter III of the GDPR in connection with the data processing described in this Policy as follows:

Withdraw consent

The Client has the right to withdraw his/her consent to the processing of his/her personal data at any time without justification, without any financial or other obligation on the part of the Client. The withdrawal of consent does not affect the lawfulness of the data processing up to the point of withdrawal.

Right of access and information

The Client has the right to receive feedback on whether his or her personal data is being processed and, if so, to be granted access to the information related to the processing (purpose of processing, categories of personal data, data on the source of the personal data, etc.). The Client may also request a copy of the personal data that is the subject of data processing.

Right to rectification

The Client has the right to request the correction or completion of his/her personal data processed by the Joint Controllers.

Right to erasure

The Client is entitled to request the Joint Controllers to delete the personal data they have processed if one of the following reasons applies:

- the personal data is no longer necessary for the purposes for which it was collected or otherwise processed;
- the Client withdraws his/her consent on which the data processing is based and there is no other legal basis for the data processing;
- the Client objects to the processing and there is no overriding legitimate reason for the processing;
- the personal data have been unlawfully processed;
- the personal data must be erased in order to comply with a legal obligation under Union or Member State law applicable to the Joint Controllers;
- Personal data was collected in connection with the provision of information society services.

However, the right to erasure is not unlimited, it may be limited by the provisions of the relevant EU and domestic data protection legislation.

Right to restriction of processing

The Client is entitled to request the restriction of data processing in the following cases:

- the Client contests the accuracy of the personal data, in which case the restriction applies to the period that allows the Joint Controllers to verify the accuracy of the personal data;
- the data processing is unlawful and the Client requests the restriction of data processing instead of deleting the data;

- the Joint Controllers do not need the personal data for the purposes of the processing, but the Client requires them for the establishment, exercise or defence of legal claims; or
- the Client objected to the processing; in this case, the restriction shall apply for the period until it is established whether the legitimate reasons of the Joint Controllers take precedence over the legitimate reasons of the Client.

Following the restriction of data processing, the personal data subject to the restriction may only be processed with the consent of the Clients, with the exception of storage, or for the establishment, exercise or defence of legal claims, or for the protection of the rights of another natural or legal person, or for reasons of important public interest of the Union or a Member State.

Furthermore, Clients have the right to receive their personal data provided to the Joint Controllers electronically and to transmit them to another controller.

Right to object

The Client has the right to object to the processing of his or her personal data if the processing is carried out for the purpose of direct marketing. In this case, the data subject to the objection may no longer be processed for the purpose of direct marketing.

In matters related to its complaints, the Client has the right to report it to the competent data protection supervisory authority.

7. General rules of the exercise of law:

The Data Controller 1 shall inform the Client of the measures taken in response to the request without undue delay, but no later than within 30 days from the receipt of the request. If necessary, taking into account the complexity of the application and the number of applications submitted by the Clients, this deadline may be extended by a further two months. The Data Controller 1 shall inform the Client of the extension of the deadline within 30 days of receipt of the request, indicating the reasons for the delay.

The Data Controller 1 shall provide the information and measures to the Clients free of charge. If the Client's request is clearly unfounded or excessive, especially due to its repetitive nature, the Data Controller 1, taking into account the administrative costs associated with providing the requested information or information or taking the requested action:

a) charge a reasonable fee, or

b) may refuse to take action on the basis of the request.

The burden of proving the clearly unfounded or excessive nature of the request lies with Data Controller 1.

If the Joint Controllers have reasonable doubts about the identity of the natural person submitting the request, they may request the provision of additional information necessary to confirm the identity of the Client.

8. Options for enforcing rights:

Clients may contact the representative of the Joint Data Controllers, Data Controller 1 at any time in connection with the processing of their personal data, at the following contact details:

Email address: bnpl@instacash.hu

Data Controller 1 is obliged to respond to the incoming requests in the manner and within the deadline specified in Section 6 of this Policy.

In the event of a violation of its rights, the Client may turn to the court against the Joint Data Controllers. The court proceeds in the case out of turn. The Joint Data Controllers are obliged to prove that the data processing complies with the provisions of the law. The adjudication of the lawsuit falls within the competence of the regional court, and in the capital city the jurisdiction of the Metropolitan Court. The lawsuit may also be brought before the tribunal of the Client's domicile or residence.

In case of a complaint regarding the processing of his or her personal data, the Client may also turn to the National Authority for Data Protection and Freedom of Information (dr. Attila Péterfalvi, President of the National Authority for Data Protection and Freedom of Information, postal address: 1363 Budapest, Pf.: 9., address: Falk Miksa u. 9-11, 1055, Phone: +36 (30) 683-5969, e-mail: ugyfelszolgalat@naih.hu; website: www.naih.hu).

Az InstaCash Kft.

Privacy Policy

Effective from: 18/04/2025

The identity of the data controller, the purpose of the policy

Name of the data controller: InstaCash Kft. (hereinafter: "InstaCash")
Registered office: 1015 Budapest, Szabó Ilonka utca 22. 2.
Email: info@instacash.hu

The purpose of the Privacy Policy (hereinafter referred to as the Policy) is to regulate InstaCash's personal data processing processes and ensure the rights of data subjects, complying with the requirements of the applicable legislation.

InstaCash does not carry out any **activity as a multi-agent of financial services as defined in the InstaCash Act with regard to certain financial services appearing on the website of InstaCash**.The Magyar Nemzeti Bank has terminated its activities in accordance with its activity licence H-EN-I-6/2020 issued by the Magyar Nemzeti Bank.

From now on, the activities of InstaCash Kft. will no longer fall under the scope of Act CCXXXVII of 2013 on Credit Institutions and Financial Enterprises (hereinafter: Hpt.).

The Company does not have a license issued by the National Bank of Hungary to carry out financial services activities, and it does not carry out lending or debt purchase activities pursuant to Section 3 (1) b) and (l) of the Credit Act. The Company does not provide financial services on a commercial basis, does not disburse money loans, and does not purchase the claims of other natural or legal persons for the purpose of enforcing them.

Based on the above, InstaCash Kft. does not qualify as a financial institution and does not perform any financial activity determined on the basis of the provisions of the InstaCash Act.

1. BASIC CONCEPTS AND SCOPE

1.1. Scope of the Policy

1.1.1. Personal scope

The scope of the Policy extends to i) persons performing data processing or data processing activities performed by InstaCash (employees or persons in a legal relationship with InstaCash for other work purposes) and ii) those natural persons in connection with whom InstaCash processes or processes personal data (data subjects), or – if Hungarian law orders the application of Regulation (EU) 2016/679 of the European Parliament and of the Council to such persons: under the conditions and by the deadline specified therein – for the data subject and his or her relatives.

1.1.2. Material scope

The scope of the policy covers personal data processed or processed by InstaCash as a data controller or data processor.

2. RELATED REGULATIONS AND LEGISLATION

The following pieces of legislation are particularly significant and contain background information from the point of view of the policy:

- Regulation (EU) 2016/679 of the European Parliament and of the Council 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 (the "General Data Protection Regulation" or "Regulation");
- Act V of 2013 on the Civil Code ("Civil Code");
- Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information ("Privacy Act");
- Act I of 2012 on the Labour Code ("Labour Code").
- Act XLVIII of 2008 on the Basic Conditions and Certain Restrictions of Commercial Advertising Activities,
- Act CVIII of 2001 on Certain Issues of Electronic Commerce Services and Information Society Services,
- Act CXIX of 1995 on the Processing of Name and Address Data for the Purposes of Research and Direct Marketing
-

3. BASIC CONCEPTS

3.1. Data management

Any operation or set of operations performed on personal data or data sets by automated or non-automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

3.2. Controller

The natural or legal person, public authority, agency or any other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

3.3. Processing

The natural or legal person, public authority, agency or any other body that processes personal data on behalf of the controller.

3.4. **Data breach**
A breach of security that results in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

3.5. **Special categories of personal data**
Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, as well as genetic and biometric data for the purpose of uniquely identifying natural persons, health data and personal data concerning the sex life or sexual orientation of natural persons.

3.6. **Consent of the data subject**
Voluntary, specific, well-informed and unambiguous indication of the data subject's will, by which the data subject indicates by a statement or an unambiguous affirmative act that he or she consents to the processing of personal data concerning him/her.

3.7. **Pseudonymisation**
Processing of personal data in such a way that, without the use of additional information, it is no longer possible to determine which specific natural person the personal data relates, provided that such additional information is stored separately and it is ensured by taking technical and organisational measures that such personal data cannot be linked to identified or identifiable natural persons.

3.8. **EEA State**
A Member State of the European Union and another State party to the Agreement on the European Economic Area, as well as a State whose national enjoys the same legal status as a national of a State party to the Agreement on the European Economic Area on the basis of an international treaty concluded between the European Union and its Member States and a State not party to the Agreement on the European Economic Area.

3.9. **Third Party**
A natural or legal person, public authority, agency or any other body which is not the same as the data subject, the controller, the processor or the persons authorised to process personal data under the direct direction of the controller or processor.

3.10. **Third country**
Any state that is not an EEA state.

3.11. **Joint data management**
If the purposes and means of data processing are determined jointly by InstaCash with other data controller(s).

3.12. **National Data Protection Authority (NAIH)**

3.13. **Profiling**
Any form of automated processing of personal data in which personal data is used to evaluate certain personal characteristics relating to a natural person, in particular to analyse or predict characteristics relating to performance at work, economic situation, state of health, personal preferences, interests, reliability, behaviour, location or movement.

3.14. **Personal data**
Any information relating to an identified or identifiable natural person ("data subject"). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, a 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.

4. INSTACASH AS A DATA CONTROLLER

PRINCIPLES

4.1. In order to enforce the data subjects' right to their personal data, InstaCash respects the principles of data protection law applicable to our services – as laid down in the above-mentioned legislation – thus:

4.1.1. Data should only be obtained and processed fairly and lawfully. It ensures that the personal data is accurate and, where necessary, kept up to date, and takes all reasonable steps to promptly delete or rectify any personal data that is inaccurate with regard to the purposes of the processing.

4.1.2. Data may only be stored for specific and lawful purposes and may not be used in any other way.

4.1.3. Personal data must be proportionate to the purpose for which they are stored and must comply with that purpose and not go beyond it.

4.1.4. The method of storage of personal data must be such that the data subject can only be identified for as long as is necessary for the purpose for which they are stored.

4.1.5. InstaCash always complies with the restrictions laid down by law during the recording, recording and processing of personal data, and informs the data subject of its activities by electronic mail as requested.

4.1.6. In certain cases – official courts, police requests, legal proceedings, copyright, property or other infringements or reasonable suspicions of these, the violation of the interests of InstaCash, the endangerment of the provision of its services, etc. – InstaCash makes available the data of the data subject to third parties. In addition to the above, InstaCash is entitled to make available the data of the data subject to its subcontractors who are required and used for the provision of its services, who are in a contractual relationship with it and who are subject to confidentiality obligations. The data subject releases InstaCash within the scope specified in this section in order to maintain its confidentiality obligation.

4.1.7. When determining the method of data processing and during data processing, InstaCash implements appropriate technical and organizational measures aimed at implementing data protection principles on the one hand, and incorporating the guarantees necessary for the protection of the rights of data subjects into the data processing process on the other.

4.1.8. InstaCash implements appropriate technical and organizational measures to ensure that only personal data that is necessary for the specific purpose of data processing is processed. These measures cover the amount of personal data collected, the extent to which they are processed, the duration of their storage and their availability. In particular, those measures are intended to ensure that personal data cannot be disclosed to unauthorised third parties without the intervention of the natural person.

4.1.9. InstaCash processes personal data in such a way that it is able to verify compliance with the above principles.

4.1.10. Proposals for the regulation and modification of personal data protection are the responsibility of the managing director of InstaCash, who consults the company's data protection officer beforehand. If any employee of InstaCash detects a circumstance affecting the company's personal data processing (receives a request for data processing from a data subject, experiences a personal data breach, or comes into possession of any other relevant information), he/she is obliged to immediately notify the managing director of InstaCash and forward the relevant documents to him/her. The managing director shall immediately notify the company's data protection officer of this information.

5. LEGAL BASIS FOR DATA PROCESSING

5.1. Personal data is processed by InstaCash only in the following cases:

5.1.1. If the data subject has given consent to the processing of their personal data;

5.1.2. If the processing is necessary for the performance of a contract to which the data subject is a party or it is necessary to take steps at the request of the data subject prior to entering into a contract;

5.1.3. If the processing is necessary for compliance with a legal obligation to which InstaCash is subject;

5.1.4. If the processing is necessary for the performance of a task carried out in the exercise of a public interest authority;

5.1.5. If the processing is necessary for the protection of the vital interests of the data subject or of another natural person;

5.1.6. If the processing is necessary for the purposes of the legitimate interests pursued by InstaCash or by a third party, unless those interests are overridden by the interests or fundamental rights and freedoms of the data subject which require the protection of personal data, in particular if the data subject is a child;

5.2. If the legal basis of the data processing is the legal basis specified in Section 5.1.6, it is necessary to conduct a balancing of interests test. In the context of this test,

5.2.1. It is necessary to determine what constitutes the legitimate interest of InstaCash or the third party;

5.2.2. It is necessary to examine what constitutes the interests or fundamental rights and freedoms of the data subject that require the protection of personal data;

5.2.3. Preliminary assessment shall be made on the basis of the factors described in points 5.2.1 and 5.2.2;

5.2.4. Compared to the result of the preliminary assessment, if the result of the balancing of interests is unclear, additional guarantees must be associated with the protection of the rights of the data subject.

5.2.5. Based on the principle of accountability (point 4.1.9), the performance of the assessment described in points 5.2.1 to 5.2.4 and its outcome shall be documented.

6. PURPOSE OF DATA PROCESSING

6.1. The purpose of data processing is the operation, maintenance and development of the mobile and/or web application (hereinafter referred to as the "Application") provided by InstaCash Kft., as well as to enable the use of the services available through the Application, and to perform them in a secure, lawful and contractual manner.

6.2. The Operator processes the personal data of the data subjects exclusively for the following specific purposes:
- to provide registration and login functions for the Application,
- creating, managing and identifying the user account,
- performing technical operations necessary for the operation of the Application (e.g. logging, error handling, backups),
- statistical analyses and developments carried out in order to increase the quality of service,
- Receiving and managing user feedback,
- fulfilling the obligations prescribed by law,
- for the purpose of pursuing a legitimate interest, in particular to maintain IT security or to establish, exercise or defend legal claims.

7. SPECIAL CATEGORIES OF PERSONAL DATA

7.1. Data belonging to special categories of personal data are processed by InstaCash only on the basis of the explicit consent of the data subject.

7.2. In the absence of the consent specified in Section 5.1.1, InstaCash shall return the document sent by the data subject containing data belonging to a special category of personal data to the data subject without making a copy.

7.3. The consent under Section 5.1.1 shall be duly documented.

8. DATA SUBJECT'S RIGHT TO INFORMATION

8.1. InstaCash primarily obtains their personal data from the data subjects, in which case the declaration of consent and information annexed to this Policy shall apply. If the personal data is not obtained from the data subject, InstaCash will provide the data subject with the following information:

8.1.1. the identity and contact details of InstaCash and its representative;

8.1.2. contact details of InstaCash's Data Protection Officer;

8.1.3. the purpose of the planned processing of personal data and the legal basis for the processing;

8.1.4. categories of personal data concerned;

8.1.5. recipients or categories of recipients of personal data; if any, the information specified in the General Data Protection Regulation in the case of transfers of personal data to third countries;

8.1.6. the duration for which the personal data will be stored or, if this is not possible, the criteria for determining this period;

8.1.7. if the legal basis for data processing is the legal basis set out in Section 5.1.6, then the legitimate interest of InstaCash;

8.1.8. The fact that the data subject may request from the controller access, rectification, erasure or restriction of processing of personal data concerning him or her, and the right of the data subject to data portability;

8.1.9. In the case of data processing based on consent, the right to withdraw consent at any time, which does not affect the lawfulness of the processing carried out on the basis of consent before its withdrawal;

8.1.10. The right to lodge a complaint with the NAIH as a supervisory authority;

8.1.11. the source of the personal data and, where applicable, whether the data originated from publicly available sources;

8.1.12. the fact of automated decision-making, including profiling, and, at least in these cases, comprehensible information on the logic used and the significance of such processing and the likely consequences for the data subject;

8.2. The information described in Section 7.1 must be disclosed within a reasonable period of time from the date of receipt of the personal data, taking into account the specific circumstances of the processing of personal data, but no later than one month. If personal data are used for the purpose of maintaining contact with the data subject, the information must be disclosed at least at the time of the first contact with the data subject.

8.3. The exercise of the right to information may only be refused in the cases set out in Article 14(5) of the GDPR.

9. RIGHT OF ACCESS OF THE DATA SUBJECT

9.1. InstaCash will provide feedback on the data subject's request as to whether their personal data is being processed and, if such processing is in progress, they will provide access to the personal data and access to the following information:

9.1.1 the purposes of the processing;

9.1.2. categories of personal data concerned;

9.1.3. the recipients or categories of recipients to whom the personal data have been or will be disclosed, including, in particular, recipients in third countries or international organisations;

9.1.4. where applicable, the envisaged period for which the personal data will be stored or, if this is not possible, the criteria for determining that period;

9.1.5. the data subject's right to request the controller to rectify, erase or restrict the processing of personal data concerning him or her, and to object to the processing of such personal data;

9.1.6. the right to lodge a complaint with a supervisory authority;

9.1.7. if the data was not collected from the data subject, all available information on their source;

9.1.8. the fact of automated decision-making, including profiling, and, at least in these cases, comprehensible information on the logic used and on the significance of such processing and the likely consequences for the data subject.

9.1.9. If personal data is transferred to a third country, the data subject has the right to be informed of the safeguards for the transfer.

9.2. InstaCash provides the data subject with a copy of the personal data subject to data processing. For additional copies requested by the data subject, InstaCash may charge a reasonable fee based on administrative costs. If the data subject has submitted the application electronically, the information must be provided in a commonly used electronic format, unless the data subject requests otherwise. The right to request a copy must not adversely affect the rights and freedoms of others.

10. RIGHT TO RECTIFICATION AND ERASURE

10.1. At the request of the data subject, InstaCash shall rectify the inaccurate personal data concerning him or her without undue delay, and – taking into account the purpose of data processing – upon the request of the data subject, it shall ensure the completion of the incomplete personal data, including by means of a supplementary statement.

10.2. At the request of the data subject, InstaCash shall delete the personal data relating to him or her without undue delay if:

10.2.1. the personal data is no longer necessary for the purposes for which it was collected or otherwise processed;

10.2.2. the data subject withdraws his/her consent on which the data processing is based and there is no other legal basis for the data processing;

10.2.3. the data subject objects to the processing of their data and there is no overriding legitimate reason for the processing, or objects to the use of their data for direct marketing purposes;

10.2.4. the processing of the data subject's personal data is unlawful;

10.2.5. the personal data must be erased in order to comply with a legal obligation imposed by EU or Member State law applicable to InstaCash;

10.2.6. Personal data was collected in connection with the provision of information society services to children.

10.3. The rights set out in Section 9 may only be restricted in the case of exceptions set out in the General Data Protection Regulation.

10.4. InstaCash will inform all recipients to whom the personal data has been disclosed of any correction or deletion, unless this proves impossible or requires a disproportionate effort. At the request of the data subject, InstaCash will inform the data subject about these recipients.

11. RIGHT TO RESTRICTION OF PROCESSING

11.1. At the request of the data subject, InstaCash restricts data processing if:

11.1.1. the data subject contests the accuracy of the personal data, in which case the restriction applies to the period that allows the data controller to verify the accuracy of the personal data

11.1.2. the processing is unlawful and the data subject opposes the erasure of the data and instead requests the restriction of their use

11.1.3. the controller no longer needs the personal data for the purpose of data processing, but the data subject requires them for the establishment, exercise or defence of legal claims;

11.1.4. the data subject has objected to the processing carried out on the basis of a legitimate interest or for a purpose of public interest; In this case, the restriction applies to the period until it is established whether the legitimate reasons of the data controller take precedence over the legitimate reasons of the data subject.

11.2. InstaCash informs all recipients to whom the personal data has been disclosed of any restriction of processing, unless this proves impossible or requires a disproportionate effort. At the request of the data subject, InstaCash will inform the data subject about these recipients.

12. RIGHT TO DATA PORTABILITY

12.1. The data subject shall have the right to receive the personal data concerning him or her, provided to InstaCash, in a structured, commonly used, machine-readable format, and shall have the right to transmit such data to another data controller if:

12.1.1. the processing is based on consent or a contract under the General Data Protection Regulation as a legal basis, or

12.1.2. The processing is carried out by automated means.

12.2. The rules of the General Data Protection Regulation shall be applied to exclude and limit the application of the right to data portability.

13. RIGHT TO OBJECT

13.1. The data subject may at any time object to the processing of data for reasons relating to his or her particular situation for purposes of public interest or legitimate interest, including profiling. In this case, InstaCash may no longer process the personal data, unless it proves that the processing is justified by compelling legitimate grounds which override the interests, rights and freedoms of the data subject or which are related to the establishment, exercise or defence of legal claims.

13.2. This right must be explicitly brought to the attention of the data subject at the first contact at the latest, and the relevant information must be displayed clearly and separately from any other information.

14. AUTOMATED DECISION-MAKING, PROFILING

14.1. InstaCash will only apply decisions based solely on automated data processing, including profiling, which have legal effects on the data subject or similarly significantly affect him/her, if:

14.1.1. necessary for the conclusion or performance of a contract between InstaCash and the data subject;

14.1.2. is made possible by EU or domestic law applicable to InstaCash, which also lays down appropriate measures for the protection of the rights and freedoms and legitimate interests of the data subject

14.1.3. based on the explicit consent of the data subject.

14.2. The General Data Protection Regulation applies to further requirements for automated decision-making and professionalisation.

15. INCIDENT MANAGEMENT AS A DATA CONTROLLER

15.1. InstaCash shall report the personal data breach to the NAIH without undue delay, if possible, no later than 72 hours after becoming aware of it. The notification, if any, must be made in the form and manner specified by the authority, in accordance with the authority's regulations (e.g. on the interface or hot-line designated by the authority). If the data protection authority does not create an interface, it must be done with the mandatory content elements of the notification.

15.2. If the personal data breach is not likely to entail a risk to the rights and freedoms of natural persons, the notification does not need to be made. This decision is made by the executive, considering all the circumstances of the case, after seeking the opinion of the Data Protection Officer.

15.3. InstaCash keeps a record of personal data breaches, indicating the facts related to the personal data breach, its effects and the measures taken to remedy it. If the supervisory authority determines mandatory content elements for the recording of breaches, then the breach record table must be prepared with this content.

15.4. InstaCash shall inform the data subject of the personal data breach without undue delay if the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons. This decision is made by the managing director after consulting the DPO, taking into account all the circumstances of the case on which he is making a note.

15.5. An exception to the notification of the data subject is if

15.5.1. InstaCash has implemented appropriate technical and organisational safeguards and applied those measures with respect to the data affected by the personal data breach, in particular measures, such as the use of encryption, which make the data incomprehensible to persons who are not authorised to access the personal data; or

15.5.2. Following the personal data breach, InstaCash has taken additional measures to ensure that the high risk to the rights and freedoms of the data subject is no longer likely to materialise; or

15.5.3. Disclosure would require a disproportionate effort, in which case the data subjects would have to be informed by means of publicly published information or a similar measure would have to be taken to ensure that the data subjects are equally effectively informed.

16. JOINT DATA MANAGEMENT

16.1. In the case of joint processing, InstaCash and the sub-controllers shall determine in the agreement concluded between them the division of their responsibilities for the fulfilment of the obligations set out in the General Data Protection Regulation, in particular in relation to the exercise and provision of the rights of the data subjects. In the agreement, InstaCash and the other data controllers appoint a contact person for the data subjects.

16.2. The essence of the agreement referred to in Section 15.1 shall be made available to the data subject.

16.3. The rights of the data subject shall also be ensured if the data subject wishes to exercise them in a manner other than the agreement referred to in Section 15.1.

17. USE OF A DATA PROCESSOR

17.1. As a data controller, InstaCash only uses data processors that comply with the requirements of the General Data Protection Regulation. The data processing agreement must be concluded in writing and must comply with the content requirements set out in this section.

17.2. The data processing agreement shall stipulate that the data processor may not use an additional data processor, and a general authorisation or the possibility of a specific authorisation for the use of an additional data processor shall be recorded. If the processor also uses the services of an additional processor for certain specific processing activities carried out on behalf of InstaCash, the same data protection obligations as those set out in the contract between InstaCash and the processor shall be imposed on this sub-processor by means of a contract or other legal act under Union or Member State law.

17.3. The data processing agreement shall stipulate that the processor shall process the personal data only on the basis of written instructions from InstaCash, including the transfer of personal data to a third country or international organisation, unless the processing is required by the Union or Member State law applicable to the data processor; in this case, the data processor shall notify InstaCash of this legal requirement prior to data processing, unless this is prohibited by the relevant law for reasons of important public interest.

17.4. The contract must ensure that the persons authorised to process personal data are bound by confidentiality or are subject to an appropriate obligation of confidentiality based on law;

17.5. The contract must stipulate that the data processor ensures the data security requirements set out in the General Data Protection Regulation.

17.6. The contract shall stipulate that the data processor will assist InstaCash to the extent possible by appropriate technical and organizational measures in order to fulfil its obligations in terms of responding to requests related to the exercise of the rights of the data subject.

17.7. The contract must stipulate that the data processor assists InstaCash in exercising its obligations regarding the security of data processing, the reporting of personal data breaches to the authorities, the informing of data subjects about personal data breaches, as well as data protection impact assessment and prior consultation.

17.8. The contract shall stipulate that after the completion of the data processing, the data processor shall delete or return all personal data to InstaCash and delete the existing copies, unless EU or Hungarian law requires the storage of personal data.

17.9. The contract shall stipulate that the data processor shall provide InstaCash with all information necessary to verify the fulfilment of the obligations set out in the General Data Protection Regulation, as well as to enable and facilitate audits carried out by InstaCash or another auditor appointed by it, including on-site inspections.

17.10. The contract shall stipulate that the data processor shall immediately inform InstaCash if it considers that any of its instructions violate this General Data Protection Regulation or any other Hungarian or EU data protection provision.

18. RECORD OF DATA PROCESSING AND DATA PROCESSING ACTIVITIES

18.1. InstaCash keeps a record of its data processing with the content specified in Annex 1.

18.2. The Data Protection Officer is responsible for keeping records. It is the obligation of InstaCash employees to report to the official any planned activities related to the processing of personal data or data processing. The Data Protection Officer will introduce the change in the relevant register after obtaining a legal opinion, if necessary.

19. FINAL PROVISIONS

LEGAL REMEDIES

19.1. In the event of an alleged infringement of rights related to the processing of their personal data, any data subject may also turn to the competent court of law, or to the Metropolitan Court of Budapest in the capital, or may file a complaint with the National Authority for Data Protection and Freedom of Information (1024 Budapest, Szilágyi Erzsébet fasor 22/C., ugyfelszolgalat@naih.hu, +36-1-3911400, www.naih.hu) The person concerned may also initiate the lawsuit before the court competent for his or her place of residence or residence, at his or her choice.

Annexes to the Privacy Policy:

- Annex 1.sz Registration of data processing pursuant to Article 30 (1) of the General Data Protection Regulation

- Annex 2.sz Record of data breaches

Budapest, 18 April 2025

1. **Annex No.: Register of data processing operations pursuant to Article 30(1) of the General Data Protection Regulation**

Name of the data controller: InstaCash Kft.
Contact details of the data controller: 1015 Budapest, Szabó Ilonka utca 22. fszt 2., info@instacash.hu

A) Data processing in connection with customers and business partners

Purpose of data processing (Process)	Stakeholders Categories	Personal data processed	Legal basis for data processing	Data transfer/processing Disclosure	Deletion deadline
Communication with the client (phone, email) in order to provide the technical background related to the commercial loan	Customers/Users	Username Email address Last name and first name No Age Telephone number	Contribution		Immediately after deleting a registration
Complaint handling	Customer service workers Customers/Complainants	Telephone conversations, content of email communication, date, calling number, number called, person of the call handler, reason for this in the case of an unhandled call, time of the	Contribution		5 years for complaint and response rules on the

		conversation, waiting time, Employee-related status changes (call answering, outgoing call, break, meeting, lunch break, administrative work, e-mail management, personal customer reception, training)			

B) Financial due diligence of Clients to determine eligibility for deferred payment

Purpose of data processing (Process)	Stakeholders Categories	Personal data processed	Legal basis for data processing	Data transfer/processing Disclosure	Deletion deadline

Determining eligibility for deferred payment	Customers using deferred payment	Account Information and Other Financial Information Provided by Clients	Client's consent	The Client's account information is obtained by Aggreg8 Limited Liability Company, which is forwarded to Instacash Kft. for the purpose of conducting financial due diligence Instacash Kft. forwards to its partner providing deferred payment information on whether the conditions for deferred payment are met or not	Until the information on determining eligibility for deferred payment is communicated to the deferred payment partner

InstaCash Kft. performs profiling during the financial due diligence and automated decision-making as follows:

InstaCash Kft. provides IT services to its partners providing deferred payments, which also includes the financial due diligence of the Clients. In the course of the financial due diligence, Instacash Kft. performs calculations in an automated manner based on the Client's account information and other financial data in order to determine whether the Client is expected to be able to perform the contract for deferred payment in accordance with the parameters set by the partners providing the deferred payment. If the result of the due diligence is positive, InstaCash Kft. will notify its partner providing the deferred payment, who may provide deferred payment to the Client based on this. If the result of the due diligence is negative, InstaCash Kft. will report this fact to its partner providing the deferred payment, which may refuse to provide the deferred payment on this basis.

InstaCash Kft. expressly draws the attention of the Clients to the fact that, apart from the above, it does not share financial information about the Clients with its partners providing deferred payment.

C) Other data processing

Purpose of data processing (Process)	Categories of stakeholders	Personal data processed	Legal basis for data processing	Data transmission/ data processing	Deletion deadline
Electronic filing system	Correspondents	Contact information	The legitimate interest of InstaCash Kft.		5 years
Technical operation of the website, protection of the website against illegal activities	Website visitors	IP addresses and related technical data (operating system, time of visit, requested files, etc.)	The legitimate interest of InstaCash Kft.		2 months

C) List of data processors

Incident Time/Detection Time	Tax number	Scope and number of people affected by the incident
Loginet Systems Ltd	14461862-2-43	Operation
COMNICA Ltd.	14242036-2-43	Provision of services (call center application, customer due diligence application)
RackForest Zrt.	14671858-2-41	Provision of service (hosting)
Aggreg8 Ltd.	25930423-2-06	Provision of services (Electronic account history information sharing)
Barion Payment Zrt.	25353192-2-43	Provision of service (payment solution)

instacash

2. Appendix No.: Incident Registration

Incident Time/Detection Time	Scope of personal data concerned	Scope and number of people affected by the incident	Circumstances and impact of the incident, measures taken to eliminate the incident