# Privacy Notice

The purpose of this notice is to provide any person (or 'data subject') in relation to whom Selfpay and Zebrapay, ("we", "us") holds personal data, with details of the information that we collect, how we process it and who we share it with. "You" and "Your" are our customer or person using our services that we collect personal data about.

This privacy notice explains your data protection rights as set out under the General Data Protection Regulation (EU) 2016/679 ("**GDPR**") and the Data Protection Acts 1988-2018 (as may be updated from time to time), both referred to as "Data Protection Law" in this notice.

Certain key terms are used in this policy such as 'personal data', 'processing', and these are defined in the Definitions section included at Annex 1 for ease of reference.

The terms mentioned with capital letters in this Privacy Notice shall have the same meaning as defined in the Terms and conditions.

## Who controls the use of your personal data?

For providing you with the Services, Zebrapay S.A., a company registered in Romania, registration number RO26067497, registered office at Bucharest, 153-155 E Dacia Blv., 2nd District, Romania (hereinafter "**Zebrapay**") and Selfpay Limited, a company registered in Ireland, CRO number 703546, VAT number IE 3829044VH , registered office at Suite 10469, 26/27 Upper Pembroke Street, Dublin 2, D02 X361 ("**Selfpay**") will act together, in their capacity of joint controller, as provided under Article 26 of GDPR. Zebrapay and Selfpay shall be jointly referred to in this Privacy Notice as Joint Controllers.

Joint Controllers have concluded an adequate data processing agreement, regulating their rights and obligations, in order to ensure the legality of the processing of personal data, compliance with the legal obligations and that your rights are handled.

Selfpay is an affiliated company of Zebrapay. The Joint Controllers' services are the performance of payment operations at your direction, to allow the sale-purchase of goods and/or services directly or indirectly (according to the contracts concluded with the partners), such as performing top-up payments, paying the utility bills, purchasing vouchers etc.

## Compliance with principles of data protection law

Joint Controllers adhere to the principles of the data protection law and as a result, your personal data will be:

- Processed lawfully, fairly and in a transparent manner;
- Collected for specified, explicit and legitimate purposes;
- Adequate, relevant and limited to what is necessary;
- Accurate and up-to-date;
- Kept for no longer than is necessary for the specified purpose or purposes; and
- Processed in a manner that maintains the integrity and confidentiality of your data.

## What personal data is collected?

Not all of the types of data covered by this notice will be collected or processed for every data subject whom we process data about. We provide herein a detailed description of the information that Joint

Controllers hold (in both paper or electronic format), where appropriate and permitted by law, respectively:

- "Basic Contact Data" - personal details relating to you: your name, contact details (email address and phone number).
- "Identification information" – identification code on utility bills, unique customer code etc.
- "Payment information" - bank account details (only if required for payments in performance of a contract).

**Where do we collect your personal data?**

Your personal data that we collect will be provided by you through your interactions with us. Basic Contact Data and Identification information will be provided to Joint Controllers by you for the purpose of contacting you in connection with the agreement concluded with you (represented by Selfpay's terms and conditions).

**Purpose for processing your personal data**

Joint Controllers collect personal data for the following purposes:

- To administer our contractual relationship with you.
- To allow oversight of payments by you via Joint Controllers and their commercial partners.
- To comply with legislation specifically applicable to Joint Controllers.
- For the purpose of supporting a legal claim that any of the Joint Controllers might face or to comply with a regulatory or law enforcement body or other authority as required by law.

We have set out further details of our processing operations in respect of your personal data at Annex 2.

Please note that we only share your personal data with our commercial partners in order to make sure that the Services are correctly provided to you. Our commercial partners are the services providers for the Products listed at the SelfPay Payment Stations, such as utility service providers, telecom services providers, online platforms etc.

**Legal basis for processing your information**

We process your personal data in order to provide you with our services and to assist us in the operation of our business. Under data protection law we are required to ensure that there is a legal basis for the processing of your personal data, and we are required to let you know what that basis is.

The primary bases upon which we process your personal data are:

- *Performance of a contract or agreement with you* – we collect and use your information primarily for the purpose of managing our working relationship with you, for example, in order to provide services, to arrange payment of services or to collect payment for our services, to communicate with you, and otherwise to fulfil any contractual obligations owed to you.

- *Where required by applicable law* - Joint Controllers are required to maintain records that can include personal data, such as mandatory reporting, tax and accounting requirements. In particular, Joint Controllers process personal data relating to our customers to facilitate the customers making payments and recording evidence of those payments having been made.

- *To fulfil our legitimate business interests* - Joint Controllers also process your personal data to pursue our legitimate business interests, which shall include planning for, conducting and monitoring the activities of Joint Controllers, providing service information etc. Examples include sharing statistical information amongst the Zebrapay group, however, your personal data shall be anonymised in advance of such sharing.

For your convenience, we have put together a table at Appendix 2, setting out examples of the purpose of Joint Controllers' processing, what categories of data we use and the legal basis. Joint Controllers will only use your information for the purposes for which it was collected, unless we reasonably consider that we need it for another purpose that is compatible with the original purpose. If we need to use your information for an unrelated but compatible purpose, we will notify you in advance of our use of your information and explain the legal basis for this. Note that we will process your information without your knowledge or consent only when this is required or permitted by applicable law, or in the event of a merger or acquisition of Joint Controllers.

Joint Controllers will not use your personal data for any marketing or promotional purposes.

Joint Controllers do not carry out automated decision-making processes with personal data.

**Who do we share your personal data with?**

You should be aware that Joint Controllers disclose your personal information to the commercial partners, but will only do so where it is consistent with the purposes outlined above and under appropriate lawful instructions and under an appropriate data processing agreement compliant with Data Protection Law. Your personal data will be shared between Zebrapay and Selfpay, as we act jointly for providing you the Services.

When required, Joint Controllers will disclose your personal data to professional advisors, in order to establish its legal position.

Joint Controllers will also disclose your personal data in response to a valid, legally compliant request by a competent authority or in response to a court order or otherwise in compliance with any applicable law, regulation, legal process or enforceable governmental request or other statutory requirement; to detect, prevent or otherwise address fraud, security or technical issues; or to protect against imminent harm to the rights, property or safety of Joint Controllers, its employees, its members or the public, as required or permitted by law.

Joint Controllers will ensure through contracts and data processing agreements that third parties with whom your personal data is shared, apply appropriate security measures to protect your data from loss, misuse and unauthorised access or disclosure.

**Transfers outside of the European Economic Area (EEA)**

Joint Controllers do not transfer personal data outside the European Economic Area unless the recipient is in a country for which the European Commission (EC) has issued an adequacy decision, or, if the country does not have an adequacy decision, Joint Controllers have taken appropriate steps to safeguard your personal data in compliance with Chapter V of the GDPR. In particular, Joint Controllers are likely to utilise EC approved Standard Contractual Clauses and ensures that appropriate technical and organisation security measures are also in place to protect your personal data. Joint Controllers will carry out a risk assessment in respect of such data transfers.

## Retention of personal data

Joint Controllers will retain your personal data in accordance with our record retention policy. This policy operates on the principle that we keep personal data for no longer than is necessary for the purpose for which we collected it. It is also kept in accordance with any legal requirements that are imposed on us. This means that the retention period for your personal data will vary depending on the type of personal data. For further information about the criteria that we apply to determine retention periods, please see below:

- *Statutory and regulatory obligations* – we have certain statutory obligations to retain personal data for set periods of time which we are obliged to comply with.

- *Business requirements* – As we only collect personal data for defined purposes, we assess how long we need to keep personal data in order to meet our reasonable business purposes.

Joint Controllers will permanently delete your personal data when the relevant retention period has expired.

## Data breaches

Breaches of personal data held by Joint Controllers will be reported to the Data Protection Commission if assessed to be a notifiable breach within 72 hours any of the Joint Controllers becoming aware that a notifiable breach occurred. Based on the agreement concluded between Joint Controllers, each of the Joint Controller hold the responsibility to act without undue delay when becoming aware of the data breach, in order to minimize/eliminate the risk and to carry out all the required assessment in order to make sure that all the legal obligations are complied with.

## Safeguards

Joint Controllers take the security of your data very seriously and has implemented an information security policy which describes the technical, procedural and physical measures in place to protect your data from loss, misuse and unauthorised access or disclosure. Joint Controllers also maintain reasonable procedures to help ensure that such data is reliable for its intended use and is accurate, complete and current.

Employees who handle personal data covered by this policy are trained on the information security policy and how to correctly collect, process, store and delete data in accordance with each of the Joint Controllers' data protection policy. The employees of Joint Controllers are provided with data protection training.

## Your rights

You have various rights under Data Protection Law, subject to certain exemptions and requirement, in connection with our processing of your personal data:

- ***Right to access the data*** – You have the right to request a copy of the personal data that we hold about you, together with other information about our processing of that personal data.

- ***Right to rectification*** – You have the right to request that any inaccurate data that is held about you is corrected, or if we have incomplete information, you may request that we update the information such that it is complete.

- ***Right to erasure*** – You have the right to request us to delete personal data that we hold about you. This is sometimes referred to as the *'right to be forgotten'.*

- ***Right to restriction of processing or to object to processin***g – You have the right to request that we no longer process your personal data for particular purposes, or to object to our processing of your personal data for particular purposes.

- ***Right to data portability*** – You have the right to request us to provide you, or a third party, with a copy of your personal data in a structured, commonly used machine readable format.

- ***Right to complain*** - You have the right to lodge a complaint with the Data Protection Commission if you are unhappy with our processing of your personal data.

- ***Right to withdraw your consent*** – When we process your personal data on the basis of your consent, you are free to withdraw that consent at any time by contacting us using the contact details below. Please note that if you withdraw your consent we may not be able to continue providing you with the service to which the consent related.

Based on the data processing in place, Joint Controllers hold the obligation of ensuring all the necessary technical and organizational measures for handling in compliance with the legal obligations the data subjects' rights and for responding without undue delay, and in any case, within the legal deadline to the requests sent by the data subjects.

In order to exercise any of these rights, please get in touch using the contact details set out below. Given the affiliation between the Joint Controllers and the intra-group relations, the Joint Controllers have appointed a single point of contact for handling data subjects' requests, as set out below.

**Changes to this privacy notice**

The provisions of this notice may be altered by Joint Controllers from time to time.  you will be informed of any alteration of the privacy notice via the e-mail address that you provided us.

**Queries and complaints**

Joint Controllers, part of the same group, have appointed a data protection officer. If you have any queries or complaints in connection with our processing of your personal data, you can get in touch with us using the following contact details:

- **E-Mail**: dpo@selfpay.com

Complaints may also be submitted to the Data Protection Commission which is the Data Protection Authority for Ireland (see www.dataprotection.ie):

- **Post:** Data Protection Commission
  21 Fitzwilliam Square South
  Dublin 2
  D02 RD28

Ireland

- **E-Mail**: info@dataprotection.ie

- **Online forms:** https://forms.dataprotection.ie/contact

**Annex 1 – Key Definitions:**

**"Data Protection Commission"** is the Irish supervisory authority in the European Union.

"**Data Protection Law"** means the General Data Protection Regulation (EU) 2016/679 ("**GDPR**") and any national implementing laws, regulations and secondary legislation, as amended or updated from time to time, in Ireland and any successor legislation to the GDPR or the Data Protection Acts 1988-2003.

**"consent"** of the data subject means any freely given, specific, informed an unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her – such as a written/electronic statement or an oral statement.

**"data controller"** means the legal person or company who determines the purposes and means of the processing of personal data, e.g. Selfpay.

**"data processor"** means a person or company who processes personal data on behalf of the data controller

**"data subject"** means an identifiable natural person who is the subject of the personal data, e.g. the user, an employee, an employee of an Selfpay member organisation;

**"personal data"** means any information relating to an identified or identifiable natural person (data subject).

**"processing"** means any operation which is performed on personal data, where automated or not, such as collection, recording, organisation, structuring, storage, adaptation, retrieval, consultation, use, disclosure by transmission, dissemination, alignment or combination, restriction, erasure or destruction.

**"special categories of data"** means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data and data concerning health or a person's sex life or sexual orientation.

**ANNEX 2**

| **Processing Purpose** | **Categories of Personal data use** | **Legal basis** |
|---|---|---|
| For providing you with Selfpay services | Basic contact information<br>Identification information<br>Payment information | Performance of contract |
| Managing and improving the services provided by Selfpay | Basic contact information<br>Identification information<br>Payment information | Legitimate interest |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |