

Mifinity UK Limited Privacy Notice

1. Introduction

1.1 Mifinity is a regulated and licensed online payments company. This notice applies to the companies that are part of the MiFinity Group, the list of MiFinity companies that collect or process personal information according to this notice are MiFinity UK Limited, MiFinity Malta Limited, MiFinity Payments Limited (Ireland), MiFinity Canada Limited, Concentric Data Services Limited (Ireland) and Concentric Data Services Limited (Malta). The reference to MiFinity (including “we”, “us” or “our”) includes the above companies and all relevant group affiliates.

1.2 This policy applies to information we collect about: a) visitors to our website; and b) people who do business with us or register for our service.

1.3 Please read this Privacy Notice carefully to understand our views and practices regarding your personal data, how we use it and how we will treat it. If you do not agree with this Privacy Notice, please do not use our services.

2. Our contact details are:

Address: MiFinity Malta Limited, Level 3 (SUITE 2507), Tower Business Center, Tower Street, Swatar, Birkirkara, Malta.

Email: sales@mifinity.com

Data Protection Representative:

Name: Paul Kavanagh

Email: gdpr@mifinity.com

3. What type of information we may hold about you:

3.1 When you do business with us or register for our service we may collect the following personal information from you: a) your full name, residential address, email address, residence, nationality, IP address, mobile number, date of birth and bank or payment card details and any proof of your identity and/or address that we may request such as passports, drivers licenses and documentation used to verify your address, Politically Exposed Status; b) details of any transactions you carry out through our website and/or mobile application of the fulfilment of your requests; c) details of any bank account (including, but not limited to: account holder, account name, account number, sort code, online banking PIN, Transaction Authentication Number “TAN” and password, available balance and transaction history of your bank account,); d) details of any credit, debit or other card used by you for transactions; e) your participation in any promotion sponsored by us; f) correspondence that you send us; g) calls that we make to you or you make to us; h) surveys that you complete; i) information collected through cookies – please see our cookies policy for more details; and j) your IP address, log-in times, operating system and browser type.

3.2 In order to fulfil our legal obligations to prevent fraud and money laundering, we will obtain information about you from third party agencies, including your financial history, county court judgements and bankruptcies, from credit reference and fraud prevention agencies when you open an account with MiFinity and at any time when we feel it is necessary to prevent fraud and minimise our financial risks.

4 Information about other individuals

4.1 If you appoint a representative to act on your behalf, we would require from the representative:

a) Proof that you have given your representative authority to exercise your data protection rights, or make a complaint for you (such as a letter giving them your authority); and

b) proof of identity of the representative.

Your confirmation that the Representative appointed can:

4.1.1 receive on your behalf any data protection notices; and

4.1.2. give consent to the transfer of your personal data abroad.

5. How we will use the information about you and why:

Lawful basis code:

Using your personal data: Basis of Processing Personal Data

We'll process your personal data:

5.1 As necessary **to perform your contract with you** for the relevant account, policy or service:

- a) To take steps at your request prior to entering into it;
- b) To decide whether to enter into it;
- c) to operate and administer your account and to provide the services that you have requested;
- d) To update our records;
- e) to carry out your instructions to make and receive payments and undertake transactions using our services, including verifying that you have sufficient funds in your nominated bank account to make such payments;
- f) to allow you to participate in the interactive features of our website;
- g) to notify you about changes to our service(s)/this website;

5.2 As necessary **for our own legitimate interests** or those of other persons and organisations, e.g.:

- a) For good governance, accounting, and managing and auditing our business operations;
- b) For financial and identity checks, fraud prevention and detection checks and anti-money laundering;
- c) To monitor emails, calls, other communications, and activities on your account and;
- d) For market research, analysis and developing statistics;
- e) to improve our internal customer training

5.3 As necessary **to comply with a legal obligation**, e.g.:

- a) When you exercise your rights under data protection law and make requests;
- b) For compliance with legal and regulatory requirements and related disclosures;
- c) For establishment and defence of legal rights;
- d) For activities relating to the prevention, detection and investigation of crime;
- e) To verify your identity, fraud prevention and anti-money laundering checks; and
- f) To monitor emails, calls, other communications, and activities on your account.

5.4 Based on **your consent**, e.g.:

- a) When you request us to disclose your personal data to other people or organisations on your behalf, or otherwise agree to disclosures;
- b) To send you marketing communications where we've asked for your consent to do so.

You're free at any time to change your mind and withdraw your consent. The consequence might be that you can't do certain things for you.

6. Marketing

6.1 We may wish to provide you with information about our products and services which we think may be of interest to you. Before sending any marketing material, we will inform you about the purposes of processing and will also collect specific consent (where applicable) from you. We will also provide you with an option to withdraw such consent provided at any point in time. You may reach out to our data protection officer in case of any matters relating to privacy of your personal data.

7. Cookies and other information-gathering technologies

7.1 Our website uses third party cookies. Cookies are text files placed on your computer to collect standard Internet log information and visitor behaviour information. These cookies allow us to distinguish you from other users of the website which helps us to provide you with a good experience when you browse our website and allows us to improve our site.

8. How we protect your information

8.1 We have put in place the following security procedures and technical and organisational measures to safeguard your personal information: a) access to your account is controlled by a password unique to you; b) we store your personal data on secure servers; and c) we automatically encrypt your confidential information in transit from your computer to ours.

8.2 We have implemented measures designed to secure your personal information from accidental loss and from unauthorised access, use, alteration and disclosure. The safety and security of your information is also dependent upon you. If we have given you (or if you have chosen) a password or access code for access to certain parts of our website/portal or mobile applications and similar, you are responsible for keeping this password and/or access code confidential. You must not share your password and/or access code with anyone. You must ensure that there is no unauthorised use of your password and access code. MiFinity will act upon instructions and information received from any person that enters your user ID and password and you understand that you are fully responsible for all use and any actions that may take place during the use of your account.

8.3 You must promptly notify MiFinity of any information you have provided to us which has changed.

8.4 The transmission of information via the internet is not completely secure. Although we will do our best to protect your personal information, we cannot guarantee the security of your information transmitted to our site, unless you are communicating with us through a secure channel that we have provided. Once we have received your information, we will use strict procedures and security features to try to prevent unauthorised access.

8.5 If you are concerned that any of your login details have been compromised, you can change them at any time once you are logged on, but you should always also immediately contact MiFinity Client Services. and tell us why you think your login details have been compromised.

9. Retention of information

9.1 The periods for which we retain your personal information are determined based on the nature and type of information, the MiFinity Service and the country in which they are provided as well as any applicable local legal or regulatory requirements.

9.2 If you use the MiFinity Services, we will retain your personal information as long as necessary to provide you with the services of your choice and any linked legitimate business purpose. That would generally mean we retain your personal information for as long as you are our customer and for a period of time afterwards.

9.3 When our relationship with you ends, we still need to retain certain elements of your personal information for a time no greater than 5 years.

9.4 We can also continue marketing and sending you direct marketing, subject to local laws and where you have not objected to such marketing.

10. Disclosure of Information

10.1 We may disclose your personal information to our associated companies, which means our subsidiaries and any subsidiaries of our shareholder(s) and/or any companies which provide outsourced services to us, who are based in different countries within the EEA and the rest of the World.

10.2 Disclosure of your personal information may be necessary in order to – among other things – fulfil your request, process your payment details, provide support services and monitor fraudulent activities.

10.3 When sending money to a person who you wish to pay, we will pass on certain details to the recipient. Depending on the requirements of that other person and the type of payment involved, we may send other personal details such as your name, address and country of residence if the recipients request this information from us in order to improve the payment process, to reconcile payments with the commercial transaction or to conduct their own anti-fraud and anti-money laundering checks.

10.4 When you open an Account, at intervals of up to every 3 months and at any other time we feel it is necessary to do so to protect our financial interests and prevent money-laundering or fraud, we share certain information about you and your account with MiFinity, which may include financial history and transactions as part of our normal business operations with our banks, payment facilitator partners, credit/debit card processing services, identity verification service providers and credit reference agencies in order to limit our exposure to fraud and other criminal activities and to manage our financial risk. When conducting identification or fraud prevention checks, the relevant parties may retain a record of our query along with your information and may share this information with other fraud prevention agencies.

10.5 We will share your personal information with third parties only in the ways that are described in this Privacy Notice. We do not sell your personal information to third parties. We may also disclose your personal information to:

a) a prospective buyer of our business or a buyer of a substantial number of the shares in our business, if MiFinity is involved in a merger, acquisition, or sale of all or a portion of its assets, you will be notified via email and/or a prominent notice on our website of any change in ownership or uses of your personal data, as well as any choices you may have regarding your personal data; b) the police, the Financial

Conduct Authority, the National Crime Agency and any other lawful enforcement body, regulatory body or court if we are under a duty or required by law to disclose or share your personal data, or to protect the rights, property, or safety of ourselves or our group companies, our customers, or others; and c) third parties we may occasionally use to provide you with the services that you have requested. These third parties will not use your personal information for any other purpose other than for what it was intended for.

11. Overseas transfers

11.1 The information you provide may be transferred to countries outside the European Economic Area (EEA) that do not have similar protections in place regarding your data and restrictions on its use as set out in this policy. However, we will take steps to ensure adequate protections are in place to ensure the security of your information.

12. Your Rights

12.1 Access to your personal data – You have the right to request a copy of the information that we hold about you. If you would like a copy of some or all of your personal information, please send an email to gdpr@mifinity.com or send a letter to MiFinity Malta Limited, Level 3 (SUITE 2507), Tower Business Center, Tower Street, Swatar, Birkirkara, Malta.

12.2 Correction of personal data – We want to ensure that your personal information is accurate and up to date. If any of the information that you have provided to MiFinity changes, for example if you change your email address or name, please let us know the correct details by sending an email to gdpr@mifinity.com. You may ask us to correct and/or remove information you think is inaccurate.

12.3 Right to withdraw consent – Where we have relied upon your consent to process your personal data, you have the right to withdraw that consent. It is important to know that by withdrawing your consent MiFinity may have to end the relationship because we rely on your data so that we can provide you with a service.

12.4 Right of erasure (also known as 'right to be forgotten') – You can request either verbally via our Client Services or in writing to gdpr@mifinity.com for us to erase your personal data where there is no compelling reason, such as our own Anti-Money Laundering requirements, to continue processing. This right only applies in certain circumstances; it is not absolute right.

12.5 Right to data portability – This right allows you to obtain your personal data that you have provided to us with your consent or which was necessary for us to provide you with our products and services in a format which enables you to transfer that personal data to another organisation. You may have the right to have your personal data transferred by us directly to the other organisation, if this is technically feasible.

12.6 Right to restrict processing of personal data – You have the right in certain circumstances to request that we suspend our processing of your personal data. Where we suspend our processing of your personal data, we will still be permitted to store it, but any other processing of this information will require your consent, subject to certain exemptions.

12.7 Right to object to processing of personal data – You have the right to object to our use of your personal data which is processed on the basis of our legitimate interests. However, we may continue to process your personal data, despite your objection, where there are compelling legitimate grounds to do so or we need to process your personal data in connection with any legal claims.

13. Monitoring

13.1 We may monitor and record communications with you (such as telephone conversations and emails) for the purpose of quality assurance, training, fraud prevention and compliance.

14. Communicating with you

14.1 We may contact you by email to the primary email address registered on your account with MiFinity or by telephone to the contact number(s) you have provided when registering for your account with MiFinity. You can change your primary email address and/or contact number at any time.

14.2 You may also receive system-generated transactional emails such as confirmation of uploads, notification of receipt of payments, notification of password changes, etc. which are necessary for the proper operation and administration of your account.

14.3 Phishing is the name given to attempts to steal personal details and financial account details from a website user. "Phishers" use fake or "spoof" emails to lead users to counterfeit websites where the user is tricked into entering their personal details, such as credit card numbers, user names and passwords. WE WILL NEVER SEND EMAILS ASKING YOU FOR SUCH DETAILS AND OUR STAFF WILL NEVER ASK YOU FOR YOUR PASSWORD. If you do receive such an email or are asked for your password by anyone claiming to work for us, please forward the email or report the incident to our Data Protection Officer at phishing@mifinity.com or by contacting MiFinity Client Services.

15. Your consent

15.1 By submitting your personal information you consent to the use of that information as set out in this policy.

16. Changes to Privacy policy

16.1 We keep our Privacy Notice under regular review. If we change our Privacy Notice, we will post the changes on this page, and place notices on other pages of the website, so that you may be aware of the information we collect and how we use it at all times. We reserve the right to make changes to our Privacy Notice at any time, without notice, where such change is required by applicable legislation.

17. Links to other websites

17.1 Our website contains links to other websites. This Privacy Notice applies to this website and our mobile applications, so when you access links to other websites you should read their own privacy policies.

18. Filing a Complaint

18.1 If you are not satisfied with how we manage your personal data, you have a right to make a complaint. Please email your complaint to the Data Protection Officer at gdpr@mifinity.com, if you feel that your complaint has not been dealt with to your satisfaction you can contact the Information Complaints Office (ICO) or depending on your location then your local Data Protection Authority.