PRIVACY POLICY

1. INTRODUCTION

This Policy aims to set out, in plain terms, our practices regarding the processing of the personal data you provide to us when using the ovolus.com platform.

The protection of your personal data is a priority for us. For this reason, our Platform operates in full compliance with 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 with Greek law.

This Policy contains everything you need to know about the processing of your Personal Data. We recommend that you read it carefully. This Policy has been adopted and applies to your use of the services we provide and forms part of the terms and conditions governing those services. By accepting those terms and conditions in order to use our services, you expressly accept this Policy. If you do not agree with the practices and procedures described in this Policy, you may not use our services.

2. DEFINITIONS – SCOPE OF APPLICATION

For the purposes of this Policy, the following terms have the meanings set out below, unless the context clearly indicates otherwise:

GDPR	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.
Data	Information relating to Users, whether or not it constitutes Personal Data.
Personal Data	Any information relating to natural persons whose identity is known or can be ascertained. Information relating to legal persons does not constitute Personal Data.
Investor	Any natural or legal person who submits, through the Platform, an offer to invest in crowdfunding projects with

	a view to acquiring transferable securities for crowdfunding purposes, in accordance with our Terms and Conditions for the provision of our Services.
Project	The business activity or activities which a Project Owner finances, or seeks to finance, through an Offer.
Regulation (EU) 2020/1503	Regulation (EU) 2020/1503 of the European Parliament and of the Council of 7 October 2020 on European crowdfunding service providers for business, and amending Regulation (EU) 2017/1129 and Directive (EU) 2019/1937, as in force from time to time.
Project Owner	Any legal person seeking to raise funding through the Platform, in accordance with our Terms and Conditions for the provision of our Services.
Platform	The website ovolus.com, which we operate for the provision of crowdfunding services, and which constitutes a publicly accessible internet-based information system within the meaning of Regulation (EU) 2020/1503.
Offer	A communication by One Three Capital, through the Platform, containing sufficient information on the terms of the offer and the Project being offered to enable the Investor to invest in the Project.
Services	The crowdfunding services we provide through the Platform.
Users	Investors and Project Owners collectively, regardless of whether they hold active investments or active Offers, respectively, on the Platform.

This Policy governs our collection and processing of your Data in the context of providing our Services to you through the Platform.

The Platform may contain third-party plug-ins and/or links through which you are directed to third-party websites. Your use of those plug-ins or links may result in the collection of your Data by those third parties, whom we do not control, and we therefore cannot guarantee the protection of your Data by those third parties, nor are we liable for any non-compliance on their part with the applicable legislative and regulatory framework on the protection of personal data. Before using any third-party plug-ins or websites, please review their own privacy and personal data protection policies.

3. DETAILS OF THE CONTROLLER

The company under the name "One Three Capital Crowdfunding Services Société Anonyme", established in the Municipality of Amaroussion, Attica, at 21 Sifnaion Aggeioplaston Street, postal code 15125, is the Controller of the Personal Data which you provide to us, or which we collect about you, in accordance with this Policy.

4. PROCESSING PRINCIPLES

The processing of your Data is based on the following principles:

- Lawfulness, fairness and transparency in processing.
- Purpose limitation.
- Data minimisation.
- Accuracy and up-to-date status of the Data being processed.
- Integrity and confidentiality of processing.
- Storage limitation.
- Compliance with the applicable legislative and regulatory framework.

5. HOW WE COLLECT DATA

We collect Data relating to you in a number of ways:

1. When you provide it to us directly:

- when you create an account on the Platform;
- when you complete an Investor or Project Owner profile;
- when you submit requests, queries or complaints;
- when you subscribe to our newsletter;

- when you contact us by email, telephone or other means.

2. When we collect it automatically through your use of the Platform:

device information, IP address, date and time of access, browser information, operating system, referring URL, cookies and similar technologies (e.g. for authentication, security and usage statistics). For further information, please refer to our separate Cookies Policy.

3. When we receive it from third parties in connection with the Services:

- from our payment services provider (such as Secupay), in pursuit of our legitimate interests;
- from our identity verification and KYC provider (such as Shufti), in the context of identity verification, document validation and, where applicable, biometric verification;
- from publicly accessible sources/registers, to the extent necessary for our purposes (e.g. verification of Project Owners' corporate details).

The Data you provide to us must be accurate, complete and up to date, and you are required to notify us promptly of any changes, in particular where this is necessary for the provision of the Services or for our compliance with our legal obligations (e.g. KYC/AML).

6. WHAT DATA WE COLLECT

Depending on your relationship with us (Investor, Project Owner, Platform visitor) and the Services you use, we may collect and process the following categories of Data:

6.1 Identification and contact data

- Full name and father's name.
- Identity card/passport details (document number, date of issue/expiry, issuing authority).
- Date of birth, place of birth, citizenship/nationality.
- Tax identification number (TIN), competent tax authority, country of tax residence.
- Residential address/registered office, correspondence address.
- Contact details (telephone, email).

- Platform account details (username, password).
- If you are a legal person, we collect corresponding information on the company (name, registered office, corporate structure/management, etc.) and the personal data of the natural persons who manage and/or represent it.

6.2 KYC/AML and identity verification data

In the context of our legal obligations (e.g. prevention of money laundering) and of the appropriateness assessment of Investors and Project Owners, we collect:

- Copies/photographs of identification documents (ID card, passport, driving licence).
- A "selfie" or other means of confirming that the person in the document is the same as the user.
- Information extracted from identification documents by means of optical character recognition (OCR) or equivalent processes.

For the provision of identity verification services, we work with specialised identity verification providers (such as Shufti), and they may process:

- identity data contained in your documents;
- data resulting from the biometric processing of facial images (facial recognition);
- in certain cases, where required by the configuration of the service, additional sensitive information contained in the documents (e.g. religion, gender, blood group).

Processing of such special categories of data is carried out only to the extent strictly necessary for the purposes of identity verification and in accordance with the conditions of the GDPR.

6.3 Financial and transactional data

For the provision of our Services and the execution of investments/funding rounds, we collect:

- the financial and investment profile of the Investor;
- financial information of the Project Owner, including data on solvency/creditworthiness;
- information on investments/participations and on the progress of the Projects;

- details of transactions carried out through the Platform (amounts, dates, type of transaction, etc.).

For the execution of payments, we work with a payment services provider (Secupay). In this context, the provider may collect personal information relating to you in accordance with its own policy; such information may constitute personal data. Before using any of the Services, please familiarise yourself with the provider's policy; acceptance of that policy is a prerequisite for using the Services.

6.4 Technical data and cookies

When you browse the Platform, we automatically collect certain technical data, such as:

- IP address, date and time of access;
- browser type and version, operating system;
- pages visited, duration of visit, basic usage statistics.

We use cookies and similar technologies for:

- the operation and security of the Platform (e.g. session cookies, authentication cookies);
- the analysis of Platform usage and the optimisation of our Services,

as set out in our Cookies Policy, where you can also find information on cookie management options.

6.5 Special categories of data and minors

As a general rule, we do not systematically collect or process special categories of data (e.g. data concerning health, sexual orientation or political opinions), other than such data as may be contained in identification documents and processed solely for KYC/identity verification purposes, as described above.

We do not collect or process Personal Data of persons under the age of eighteen (18).

If you become aware that such data has been provided to us, please contact us so that we can delete it without delay, unless its retention is required by law.

7. PURPOSES AND LEGAL BASES OF PROCESSING

We collect and process your Data for the following purposes:

- to provide our Services to you [legal basis: performance of a contract to which you are a party, or pre-contractual steps taken at your request – Article 6(1)(b) GDPR];
- to fulfil, in the context of providing our Services, our obligations arising from the applicable legislative and regulatory framework, and to comply with decisions of the competent Authorities [legal basis: compliance with a legal obligation – Article 6(1)(c) GDPR];
- to safeguard our legitimate interests [legal basis: our legitimate interest – Article 6(1)(f) GDPR];
- to safeguard the quality and security of the Services we provide [legal basis: our legitimate interest – Article 6(1)(f) GDPR];
- to provide you with support in connection with our provision of the Services [legal basis: performance of a contract to which you are a party, or pre-contractual steps taken at your request – Article 6(1)(b) GDPR];
- to request information from you regarding your use of our Services and to understand how you use them, so as to optimise them [legal basis: our legitimate interest – Article 6(1)(f) GDPR];
- to handle any complaints and to respond to all kinds of requests you address to us [legal basis: your consent and the performance of the contract to which you are a party – Article 6(1)(a) and (b) GDPR];
- to send you any changes to our terms and policies and other similar information [legal basis: our legitimate interest – Article 6(1)(f) GDPR];
- for statistical purposes, provided that the Data have been anonymised [legal basis: our legitimate interest – Article 6(1)(f) GDPR];
- in relation to Personal Data collected via CCTV on our premises, for the purposes of safeguarding the security of our premises and protecting our property and that of our employees [legal basis: our legitimate interest – Article 6(1)(f) GDPR];
- to send you details about our products and Services and for marketing purposes, only where you have previously given us your specific consent to do so [legal basis: your consent – Article 6(1)(a) GDPR]; you may withdraw your consent at any time, although such withdrawal does not affect the lawfulness of processing carried out on the basis of consent before its withdrawal. Withdrawal is effected by means of a written notice submitted, in paper or electronic form, to One Three

Capital (addressed to the Data Protection Officer) and takes effect from the date of its submission onwards.

We will not collect or process your Data for any purpose other than that for which it was collected, unless we have notified you in advance of such change and obtained your prior consent, where required.

Please note that the processing of your Data is also possible without your knowledge or consent, where this is permitted or required by law.

Where you provide your explicit consent, we may subject your Personal Data to automated processing, including profiling.

If you choose not to provide us with your Data, this may limit, or even make it impossible for you, to use our Services.

8. WHO HAS ACCESS TO YOUR DATA

The Data we collect from you may be transferred, for the purposes set out in Section 7 of this Policy, to the following recipients:

- our employees;
- our partners to whom we have entrusted, in whole or in part, the processing of Data in the context of providing our Services, such as KYC providers and payment providers, for the fulfilment of our obligations in the provision of our Services, for the optimisation and security of those Services, for the purposes of marketing our products and services, and for handling your requests;
- any third party to whom transfer is required to be made pursuant to the applicable legislative and regulatory framework, or pursuant to a court decision, such as the competent Authorities;
- professional advisers such as lawyers, certified auditors and accountants, in order to safeguard our legitimate interests;
- third parties at your request or following your specific consent thereto;
- another business entity, in the event of a sale or merger of One Three Capital with that entity, without however the terms of processing of your Data set out in this Policy being thereby altered.

Transfer of Personal Data to a third country or international organisation: The transfer of your Personal Data to a third country or international organisation may take place

only where an adequate level of protection is ensured by the third country or the international organisation according to an adequacy decision of the European Comission. Otherwise, the Company may transfer Personal Data to a third country or international organisation only under the strict conditions provided for by the GDPR (eg. Special agreement).

Staff training: We ensure that our staff, including our executives, are fully informed and trained on all matters relating to Data protection and on their compliance with the related obligations arising from the GDPR, the applicable legislative and regulatory framework, and the policies and procedures we have adopted.

Processing by third parties: Where we use third-party partners to process your Data in the context of this Policy, we enter into a written data processing agreement with them, by which we ensure that their processing of your Data is carried out under the terms provided for in this Policy.

9. HOW LONG WE RETAIN YOUR DATA

Your Personal Data are stored and processed through information systems owned and operated by us, or by third-party technical service providers. Processing is carried out exclusively by specifically authorised personnel, as set out above. Your Personal Data are retained for as long as is strictly necessary to serve the contractual or legal purposes for which they were disclosed to the Controller and, in any event, no longer than ten (10) years from the termination of any relationship with the Controller.

10. SECURITY OF YOUR DATA

We have implemented appropriate technical and organisational measures to ensure the confidentiality and the lawful retention, processing, protection and safe storage of your Data, in order to prevent unlawful or unauthorised processing, accidental or unlawful destruction, loss or alteration, unauthorised disclosure or unauthorised access, in compliance with the applicable legislative and regulatory framework. These measures are designed:

- to implement the data protection principles at the design stage of our systems and applications, so that the requirements of the GDPR are continuously met and the rights of Users are protected (data protection by design); and

- to ensure by default that only those Data which are necessary for each specific purpose of processing are processed, only for the strictly necessary period, and that they are accessible only to the strictly necessary group of people (data protection by default).

These measures are reviewed and updated whenever this is considered necessary. In this context:

- we have adopted and continuously apply a Policy and procedures for maintaining the confidentiality and ensuring the integrity, availability and reliability of our processing systems and services;
- we have adopted a Business Continuity Plan, ensuring that, in the event of a physical or technical incident, the availability of, and access to, the Data can be restored promptly and without delay;
- we ensure that we collect and process only the Data strictly necessary for the relevant purpose of processing;
- we ensure that the processing of Data complies with the principles of lawfulness, fairness and transparency;
- we take care to ensure the accuracy and timely updating of the Data being processed;
- we limit access to the Data to those persons who need it for the proper and lawful performance of their assigned duties, and only to the extent that such access is necessary;
- we ensure that any natural person under our supervision who has access to Data processes such Data only on our instructions and within the limits of those instructions, and under the terms we have set for the processing of Data;
- we have adopted simple, easy-to-implement and effective procedures for the exercise of your rights in relation to your Data;
- we have adopted procedures for the pseudonymisation or encryption of Data, as appropriate, where considered necessary;
- we carry out periodic testing, assessment and evaluation of the adequacy of our procedures and of the effectiveness of the technical and organisational measures in place for ensuring the security of the retention and processing of Data.

Record of processing activities: One Three Capital, as Controller, maintains a record of the processing activities for which it is responsible, which includes the following information:

- the name and contact details of One Three Capital, of its representatives and of the Data Protection Officer;
- the purposes of the processing;
- a description of the categories of data subjects and of the categories of Personal Data;
- the categories of recipients to whom the Personal Data have been or will be disclosed, including recipients in third countries or international organisations;
- where applicable, transfers of Personal Data to a third country or an international organisation, including the identification of that third country or international organisation;
- where possible, the envisaged time limits for the erasure of the different categories of Data;
- where possible, a general description of the technical and organisational security measures it has adopted and implements.

Data breach: Any breach of this Policy, as well as of the applicable legislative and regulatory framework on the protection of Data, and, in general, any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Data transmitted, stored or otherwise processed, constitutes a Data breach.

In the event of a Data breach:

- where the Data are Personal Data, we shall notify the breach to the Hellenic Data Protection Authority without undue delay and, where feasible, within 72 hours of becoming aware of it, unless the breach is unlikely to result in a risk to the rights and freedoms of Users;
- we shall promptly inform the Data Protection Officer, who shall take all necessary measures and undertake all action required to contain the breach, prevent its further spread and remedy it. The Data Protection Officer shall keep a record of the Data breaches that occur, assess their causes and document each

breach, recording the factual circumstances surrounding it, its consequences and the remedial measures taken;

- where the Data are Personal Data and the breach is likely to result in a high risk to the rights and freedoms of Users, we shall communicate the breach of their Personal Data to the affected Users without undue delay, as provided for in the GDPR.

11. YOUR RIGHTS

In accordance with the provisions of the GDPR, you have the following rights as Data Subjects of the Data we collect and process:

- **Right to information and access** to the Data relating to you and to receive information about such Data, including its origin, the purposes of processing, the recipients or categories of recipients, and the retention period.
- **Right to rectification** of inaccurate Data and to completion of incomplete Data.
- **Right to erasure** of the Data; this right is, however, subject to the retention of such Data for a minimum specified period, in order to comply with a legal obligation or to safeguard our legitimate rights, under the applicable legislative and regulatory framework.
- **Right to restriction of processing** of the Data, where the accuracy of the Data is contested, where the processing is unlawful, or where the purpose of the processing no longer applies, provided that there is no lawful ground for retaining the Data.
- **Right to data portability**, i.e. transfer of the Data to another controller, provided that the processing is based on your consent and is carried out by automated means. The fulfilment of this right is subject to our lawful rights and obligations to retain the Data.
- **Right to object** to the processing of your Data on grounds relating to your particular situation, in cases where the Data are processed for the performance of a task carried out in the public interest or for the purposes of the legitimate interests pursued by us or by a third party. Following your exercise of this right, we shall no longer process your Data, unless we demonstrate compelling and legitimate grounds for processing which override your interests, rights and freedoms, or for the establishment, exercise or defence of legal claims.

Your requests in relation to your Personal Data and the exercise of your rights are to be submitted to the Data Protection Officer at the email address complaints@ovolus.com or via the link https://ovolus.com/general-information/. We undertake to do everything necessary to respond to your requests in accordance with the conditions set out in the applicable legislative and regulatory framework; however, the fulfilment of one of your rights may not be possible, in particular where its exercise is restricted by other provisions. In such case, we will inform you of the reasons why your right could not be fulfilled.

In any case, you have the right to lodge a complaint, report or formal grievance with the Hellenic Data Protection Authority (1-3 Kifisias Avenue, Athens / contact@dpa.gr) on any matter concerning your Personal Data.

Both the information we provide to you under Articles 13 and 14 GDPR, and any communication, as well as our actions to respond to your requests for the exercise of your rights under Articles 15 to 22 and Article 34 GDPR, are provided free of charge. However, where your requests are manifestly unfounded or excessive, in particular due to their repetitive nature, we may either charge you a reasonable fee for our actions, taking into account our administrative costs as the case may be, or refuse to act on your request.

12. DATA PROTECTION OFFICER

We have appointed a Data Protection Officer, who is properly and in good time involved in all matters relating to the protection of personal data. In particular, the Data Protection Officer assumes the following duties:

a) informs and advises us and our executives/employees of their obligations arising from the GDPR, the applicable legislative and regulatory framework, and the policies and procedures we have adopted in relation to the protection of Personal Data;

b) monitors compliance by us and our employees/executives who process Personal Data in any way with our obligations under the GDPR, the applicable legislative and regulatory framework, and the policies and procedures we have adopted in relation to the protection of Personal Data, including the allocation of responsibilities, the awareness-raising and training of staff involved in processing operations, and the related audits;

c) provides advice, where requested, on data protection impact assessments and monitors their implementation;

d) cooperates with the Hellenic Data Protection Authority;

e) acts as the point of contact for Users on any matter relating to the processing of their Personal Data and the exercise of their rights; and

f) acts as the point of contact for the Hellenic Data Protection Authority on matters relating to the processing of Personal Data by us.

In performing his/her duties, the Data Protection Officer has due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of the processing.

Contact details of the Data Protection Officer we have appointed: complaints@ovolus.com

13. VALIDITY – REVISION OF THE POLICY

This Policy applies from the date of its publication on the Platform. We may amend this Policy in order to comply with the applicable legislative and regulatory framework or to optimise it. Any such change will be incorporated into the revised version of the Policy, which will from time to time be published on the Platform and will take effect from the date of its publication. By using the Platform and/or our Services after the publication of the revised Policy, you declare that you agree to its terms.