Platform Privacy Policy

This Platform Privacy Policy is dedicated to Clients of **Vestberry, s.r.o.,** with its registered seat at Stare Grunty 18, 841 04 Bratislava, company ID no. (IČO): 51 882 540, registered in the Commercial Registry, kept by Bratislava I District Court under Section Sro, Insert no. 130692/B (hereinafter referred to as "**Vestberry**", "**we**" or "**us**") and explains how we handle the Platform Data via our Services or Platform on behalf of our Clients, as defined below.

"**Clients**" are typically venture capital and private equity investors who use our Platform or Services based on master services agreement or similar;

"**Data Processing Agreement**" means the agreement pursuant to the Article 28 GDPR between Clients as controllers and us a their processor;

"**Platform**" means the platform www.app.vestberry.com owned and operated by Vestberry as a portfolio management and reporting software;

"**Services**" are SaaS that Vestberry provides via the Platform to its Clients;

"**Platform Data**" mean any data whether personal data or non-personal data that our clients entrust for our processing by uploading it to the Platform or by providing it to us via use of our Services under the Data Processing Agreement;

General overview

General overview is that Vestberry acts as Clients' processor when providing Services and processing Platform Data via the Platform. We do not process Platform Data as a controller and we do not maintain or take any ownership of the Platform Data. Platform Data is under sole legal control of Clients and its processing is governed by the Data Processing Agreement.

What do we mean by Platform Data?

The Services are provided through our centrally hosted online Platform which is designated to use certain types of information (depending on individual product), that all together we call Platform Data, which includes information sent to or uploaded to us by Clients mainly regarding the venture capital and private equity of their clients. Vestberry stores data it receives from Clients pursuant to a legal contract containing binding obligations on Vestberry, including limiting its processing of personal data only on instruction of the Clients. We may set additional rules for our Clients regarding how data is collected and used for the Services, but such data is collected and used subject to the individual privacy notice for each Clients generally acting as the data controller. Vestberry and its Clients use a number of different technologies to collect data and to provide Services, including cookies, browser local storage, information stored in cookies and browser local storage, clear gifs, pixel tags, web beacons or others.

Is Platform Data personal data?

This question is often asked by our Clients and their legal counsels. We actually believe the vast majority of the Platform Data is not personal data and only poses non-personal economic performance and investment data related to legal persons. However, we cannot rule out that some of the Platform Data is or can be in future linked to a specific individual. We do not see whole complexity of all processing operations and purposes that Clients may use the Platform Data and/or our Platform. In addition, we do process some Platform Data is we always consider personal data, for example login credentials or in general user data about particular end users of the Platform that relates to our Client's employees or representatives. For the benefit of our Clients and from security

perspective, we have opted to approach all Platform Data as personal data although it might turn out that specifically selected pieces of Platform Data is not personal. In any case, we consider all Platform Data as the “Confidential Information” governed by the applicable confidentiality provisions in the master services agreement.

For what purposes our Clients typically process personal data?

Each Client acting as a controller is free to determine its own purposes of processing as regards any Platform Data that is personal data. These are defined in the Data Processing Agreement and should be generally aligned with Clients’ own privacy policy notices. From our observations, certain typical purposes and legal bases are often pursued by our Clients which we have included in the Data Processing Agreement. However, below table provides only generalized information to our Clients for information only and is not legal advice. Clients are solely responsible to rely on sufficient legal basis if and to the extent they believe personal data is included in the Platform Data. If it is, the Data Processing Agreement contemplates that. In any case, we will always process any personal data included in the Platform Data only to the extent required for provision of Services or complying with our rights and obligations under the relevant master services agreement, to the extend allowed by the applicable law.

Typical Client purposes	**Legal grounds typically relied upon by Clients**
Fund management and reporting	Performance of contract pursuant to the Art. 6(1)(b) GDPR and/or Clients’ and their investors’ and/or shareholders’ legitimate interests on managing and reporting within the fund as per Art. 6(1)(f) GDPR
Advanced analysis of the portfolio	Performance of contract pursuant to the Art. 6(1)(b) GDPR and/or Clients’ and their investors’ and/or shareholders’ legitimate interests on advanced analysis of the portfolio as per Art. 6(1)(f) GDPR
Statistical purposes	Legal ground of the original purpose within the regime of compatible purposes under Art. 6(4) GDPR and Art. 89 GDPR, as explained by recital 50 GDPR

The above information is just illustrative and default setting that can be found in our template data processing agreements.

What we handle Platform Data?

We acknowledge confidentiality and value of the Platform Data which we are not exploiting in not allowed way. In particular, we are not:

- selling your personal data to anyone;
- monetizing your personal data by other means;
- claiming ownership over your personal data;
- bartering your personal data for other services or products.

We do not knowingly process personal data relating to children less than 13 years of age (or 16 if the age of consent is higher in a particular country) or permit Clients to provide us with such data. If we become aware that a Client has provided us with any personal data of children, we delete such data from our databases.

We do not knowingly process sensitive or special categories of personal data, including the following:

- Special categories of personal data as defined in Article 9 of the GDPR, including racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic or biometric data uniquely identifying a natural person, or data concerning a person's sex life or sexual orientation;
- Sensitive data including Social Security Numbers or other Government-issued identity cards, financial account numbers, information about an individual's health or medical conditions or treatments, including genetic, genomic, and family medical history.

The Data Processing Agreement explains that as an immanent feature of our Services, we create for Clients certain aggregated statistical data. Provided rigorous non-identification and Client non-attribution warranties and conditions are met, we are allowed to use this data. The resulting data is not related or linkable to any individual and not even to any specific Client. Rather, this data providers market level overview of investments and trends. Our agreements with Client allow us to also use this data publicly, for example for showcasing our services to other investors or prospect clients. This is data is not Platform Data nor confidential information. Please see the relevant provisions.

Who do we share Platform Data with?

We take confidentiality of Platform Data very seriously and share it to our recipients only on need-to-know basis maintaining the confidentiality of the data recipients. Depending on the purpose of processing and particular circumstances typical recipients of the Platform Data are:

- Providers of platforms for marketing email communication with customers (e.g. Twilio SendGrid)
- Providers of cloud and hosting services (e.g. Amazon Web Services) – as a necessary technology vendors supporting running of the Platform.

We also use sub-contractors to support us in providing services who might process personal data for us. These sub-contractors include mainly developers, hosting, cloud and similar software service providers located or with servers located in the EU/EEA and the US, mainly but not limited to Amazon Web Services, Inc. and SendGrid, Inc. (Twilio SendGrid). We ensure that selection of our sub-contractors and any processing of personal data by them is compliant with the GDPR. We may release personal data and any other information we possess when necessary or appropriate to comply with the law; cooperate with law enforcement or national security requirements; respond to lawful requests; protect the rights of Vestberry or a Client, other Vestberry customers and users, and third parties; or to enforce our terms of use.

What countries do we transfer Platform Data to?

By default, we seek not to transfer your personal data outside the EU and/or European Economic Area where not necessary. However, some of our sub-contractors or the above-mentioned recipients of personal data might be based or their servers might be located in the United States of America (U.S.) or in other country regarded as third party not ensuring adequate level of protection. Any transfer of personal data outside the European Economic Area is done by us only under strict compliance with the GDPR. We ensure the third-party recipients concluded EU model Standard Contractual Clauses (SCC) with us or

follow equivalent safeguards in place to ensure high level of protection of your personal data. Where applicable, we strive to adopt additional safeguards on top of SCC both internally and externally, as stems from Schrems II judgement of the CJEU (C-311/18). If you have any question about cross-border transfer of personal data to these countries, please feel free to contact us. If there is an option to choose between two or more comparable sub-processors, Vestberry shall prefer the sub-processor with the data storage in the EU/EEA.

Protecting your privacy is very important to us also in case of potential transfer of data outside EU/EEA. After Schrems II judgement you as a controllers can rely on us to take all possible steps for processing transfers in accordance with the GDPR. Below you will find a link to reasonable or appropriate guaranties in relation to U.S. transfers:

Sub-contractor	**Privacy**	**Reasonable guarantees under Art. 46 GDPR**
Amazon Web Services	https://aws.amazon.com/compliance/gdpr-center/	EU SCC processor to processor concluded
Twilio SendGrid	https://www.twilio.com/legal/privacy	BCR and EU SCC

How long do we store your personal data?

Where we process personal data on behalf of the Clients, the retention periods are set-out by the them and we have no control over that. As soon as our contract with the Clients ends, we are under obligation to either return all personal data to the Clients or securely erase all personal data, at the choice of the Clients. The same applies to our own purposes of processing which are undertaken only on personal data currently processed by us for the Client. If our contract with the Client ends – by default – we do not keep your personal data for our own purposes. This way, we comply with basic principles relating to processing of personal data such data minimization, storage limitation and purpose limitation.

Subject to our right to retain are (i) copies of transactions between the Clients and Vestberry, (ii) information relating to any dispute or potential fraud, and (iii) any additional information we need to keep protecting our legal rights or the rights of others.

Security Policy

The security of your personal data is important to us. Vestberry follows generally accepted industry standards and has appropriate measures in place to ensure that your data is protected against unauthorized access or use, alteration, unlawful, or accidental destruction and accidental loss. No method of transmission over the internet, or method of electronic storage, is 100% secure, however. Therefore, we cannot guarantee its absolute security. We have adopted appropriate organizational and technical measures required under the GDPR to protect personal data.

Cookies

Vestberry software uses cookies in order to function correctly within provision of Services for our own controllers' purposes. It means that we use cookies and similar technologies on our website or within the Platform when providing the Services in order to enable certain functions of the Service including storing preferences of our Clients.

Changes to this Platform Privacy Policy

We may change this privacy policy from time to time by posting the most current privacy policy and its effective date on our website. In case we change this privacy policy substantially, we may bring such changes to your attention by explicit notice, on our websites.