

## Privacy Policy

**Policy Name:** Online Privacy Policy  
**Organisation Name:** The Octavius Group  
**Date of Last Update:** May 2018

This Privacy Policy sets out information about the online privacy practices of The Octavius Group, as described below (“Octavius”), and the choices you can make about the way your information is collected by us, how it will be used and for what purposes.

### Definitions and interpretation

The following definitions and rules of interpretation apply in this Agreement.

Definitions:

**Authorised Persons:** the persons or categories of persons that the Customer authorises to give the Provider personal data processing instructions as identified in Clause 14.1

**Business Purposes:** the services described in the Master Agreement or any other purpose specifically identified in ANNEX A.

**Data Subject:** an individual who is the subject of Personal Data.

**Personal Data:** means any information relating to an identified or identifiable natural person that is processed by the Provider as a result of, or in connection with, the provision of the services under the Master Agreement; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, I

The Octavius Group includes:

- Octavius Finance
- Octavius Renewables
- Octavius Pharmaceuticals
- Octavius Strategy

By submitting any information to us, or by otherwise accessing or using our websites, you agree to the terms of this Privacy Policy and consent to the policies and practices described herein for Octavius processing of personal data.

### 1. We process your personal data

**Octavius will adhere to Data Protection Legislation:** all applicable privacy and data protection laws including the General Data Protection Regulation ((EU) 2016/679) and any applicable national implementing laws, regulations and secondary legislation in England and Wales relating to the processing of Personal Data and the privacy of electronic communications, as amended, replaced or updated from time to time, including the Privacy and Electronic Communications Directive (2002/58/EC) and the Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2003/2426).

- The Customer and the Provider acknowledge that for the purpose of the

Data Protection Legislation, the Customer is the controller and the Provider is the processor.

- The Customer retains control of the Personal Data and remains responsible for its compliance obligations under the applicable Data Protection Legislation, including providing any required notices and obtaining any required consents, and for the processing instructions it gives to the Provider.

- 

## **2. Personal data collected on our Website**

- The Provider will only process the Personal Data to the extent, and in such a manner, as is necessary for the Business Purposes. The Provider will not process the Personal Data for any other purpose or in a way that does not comply with this Agreement or the Data Protection Legislation. The Provider must promptly notify the Customer if, in its opinion, the Customer's instruction would not comply with the Data Protection Legislation.

- The Provider will maintain the confidentiality of all Personal Data and will not disclose Personal Data to third parties unless the Customer or this Agreement specifically authorises the disclosure, or as required by law. If a law, court, regulator or supervisory authority requires the Provider to process or disclose Personal Data, the Provider must first inform the Customer of the legal or regulatory requirement and give the Customer an opportunity to object or challenge the requirement, unless the law prohibits such notice.

- The Provider will reasonably assist the Customer with meeting the Customer's compliance obligations under the Data Protection Legislation, taking into account the nature of the Provider's processing and the information available to the Provider, including in relation to Data Subject rights, data protection impact assessments and reporting to and consulting with supervisory authorities under the Data Protection Legislation.

- The Provider must promptly notify the Customer of any changes to Data Protection Legislation that may adversely affect the Provider's performance of the Master Agreement.

## **3. Provider's employees**

The Provider will ensure that all employees:

- (a) are informed of the confidential nature of the Personal Data and are bound by confidentiality obligations and use restrictions in respect of the Personal Data;

- (b) have undertaken training on the Data Protection Legislation relating to handling Personal Data and how it applies to their particular duties; and

- (c) are aware both of the Provider's duties and their personal duties and obligations under the Data Protection Legislation and this Agreement.

The Provider will take reasonable steps to ensure the reliability, integrity and trustworthiness consistent with applicable employment law on all of the Provider's employees with access to the Personal Data.

### **Subcontractors**

The Provider may not authorise any third party or subcontractor to process the Personal Data.

**OR**

The Provider may only authorise a third party (subcontractor) to process the Personal Data if:

- (a) the Customer provides prior written consent prior to the appointment of each subcontractor **OR** is provided with an opportunity to object to the appointment of each subcontractor within 7 days after the Provider supplies the Customer with full details regarding such subcontractor;
- (b) the Provider enters into a written contract with the subcontractor that contains terms substantially the same as those set out in this Agreement, in particular, in relation to requiring appropriate technical and organisational data security measures, and, upon the Customer's written request, provides the Customer with copies of such contracts;
- (c) the Provider maintains control over all Personal Data it entrusts to the subcontractor; and
- (d) the subcontractor's contract terminates automatically on termination of this Agreement for any reason.

#### **4. Security**

The Provider must at all times implement appropriate technical and organisational measures against unauthorised or unlawful processing, access, disclosure, copying, modification, storage, reproduction, display or distribution of Personal Data, and against accidental or unlawful loss, destruction, alteration, disclosure or damage of Personal Data.

The Provider must implement such measures to ensure a level of security appropriate to the risk involved, including as appropriate:

- (a) the pseudonymisation and encryption of personal data;
- (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
- (d) a process for regularly testing, assessing and evaluating the effectiveness of security measures

#### **5 .Personal Data Breach**

The Provider will promptly and without undue delay notify the Customer if any Personal Data is lost or destroyed or becomes damaged, corrupted, or unusable. The Provider will restore such Personal Data at its own expense.

The Provider will within 48 hours and without undue delay notify the Customer if it becomes aware of:

- (a) any accidental, unauthorised or unlawful processing of the Personal Data;
- or

(b) any Personal Data Breach.

Where the Provider becomes aware of (a) and/or (b) above, it shall, without undue delay, also provide the Customer with the following information:

- description of the nature of (a) and/or (b), including the categories and approximate number of both Data Subjects and Personal Data records concerned;
- the likely consequences; and
- a description of the measures taken, or proposed to be taken to address

The Provider will also reimburse the Customer for actual reasonable expenses that the Customer incurs when responding to a Personal Data Breach to the extent that the Provider caused such a Personal Data Breach, including all costs of notice and any remedy as set out in clause 6.6.

## **6. Complaints, data subject requests and third party rights**

The Provider will take such technical and organisational measures as may be appropriate, and promptly provide such information to the Customer as the Customer may reasonably require, to enable the Customer to comply with:

- (a) the rights of Data Subjects under the Data Protection Legislation, including subject access rights, the rights to rectify and erase personal data, object to the processing and automated processing of personal data, and restrict the processing of personal data; and
- (b) information or assessment notices served on the Customer by any supervisory authority under the Data Protection Legislation.
- (c) The Provider must notify the Customer immediately if it receives any complaint, notice or communication that relates directly or indirectly to the processing of the Personal Data or to either party's compliance with the Data Protection Legislation.
- (d) The Provider must notify the Customer within 14 working days if it receives a request from a Data Subject for access to their Personal Data or to exercise any of their related rights under the Data Protection Legislation.
- (e) The Provider will give the Customer its full co-operation and assistance in responding to any complaint, notice, communication or Data Subject request.

## **7. Your rights**

a) **The right to be informed** – We have provided this Privacy Policy to provide you with concise, transparent, intelligible and easily accessible information about how we use your personal data, including specific information depending on whether or not we have obtained your personal data directly from you.

b) **The right of access** – You have right to obtain from us confirmation as to

whether or not personal data concerning you are being processed, and, where that is the case, access to the personal data and the following information:

- (a) the purposes of the processing;
- (b) the categories of personal data concerned;
- (c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;
- (d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
- (e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
- (f) the right to lodge a complaint with a supervisory authority;
- (g) where the personal data are not collected from the data subject, any available information as to their source;
- (h) the existence of automated decision-making, including profiling, and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.
- (i) Where personal data are transferred to a third country or to an international organisation, we will inform you of the appropriate safeguards in place in relation to the transfer.

c) **The right to rectification** – We will rectify without undue delay any inaccurate personal data we hold concerning you, including completing any incomplete personal data.

d) **The right to erasure** (also known as the ‘right to be forgotten’) – You have the right to have us erase all personal data we hold concerning you, without undue delay, in one of the following circumstances:

- (a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
- (b) you withdraw your consent on which the processing is based and there is no other legal ground for the processing;
- (c) you object to the processing and there are no overriding legitimate grounds for the processing, or you objected to the processing in respect to direct marketing;
- (d) the personal data have been unlawfully processed;
- (e) the personal data have to be erased for compliance with a legal obligation in EU or member country law to which our organisation is subject; or
- (f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

We cannot execute your request if the personal data you are asking us to erase is necessary:

- (a) for exercising the right of freedom of expression and information;
- (b) to comply with a legal obligation which requires processing

under EU or a member state's law to which we are subject, or to perform a task in the public interest or in the exercise of official authority vested in us;

(c) for certain reasons of public interest in the area of public health;

(d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in so far as erasing the personal data is likely to render impossible or seriously impair the achievement of the objectives of that processing; or

(e) to establish, exercise or defend legal claims.

e) **The right to restrict processing** – You have the right to request that we restrict specific processing of your personal data, and we will comply, where one of the following applies:

(a) you are contesting the accuracy of your personal data that we hold, while we verify the accuracy of your personal data;

(b) the way we are processing the personal data is unlawful and you oppose the erasure of the personal data and request the restriction of their use instead;

(c) we no longer need the personal data for the purposes of the processing, but you need the personal data to establish, exercise or defend legal claims; or

(d) you have objected to processing in the public interest or in relation to our legitimate interest, pending the verification whether any legitimate grounds we may have override your right.

While you have restricted its processing, we will only store your personal data in question, and may process it only with your consent or to establish, exercise or defend legal claims or protect the rights of another natural or legal person or for reasons of important

public interest. We will notify you before lifting the processing restriction.

f) **The right to data portability** – You have the right to receive from us your personal data that you have provided to us, in a structured, commonly used and machine-readable format, and you have the right to transmit those data to another controller without hindrance from us, where:

(a) the processing is based on consent or on a contract; and

(b) the processing is carried out by automated means.

Where technically feasible, we will transmit your personal data directly to the other controller.

g) **The right to object** – You have the right to object to Phaidon processing your personal data in connection with our legitimate interests in the context of our activities (including profiling), direct marketing (including profiling), and processing for scientific and/or historical research and statistics purposes, where applicable.

h) **Rights with respect to automated decision-making and profiling** – You have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning you or similarly significantly affects you. You can object to your personal data being

used in this way. We are permitted to use automated decision-making and profiling if the decision:

(a) is necessary for entering into, or performance of, a contract between you and us;

(b) is authorised by EU or a member state law to which we are subject and which also lays down suitable measures to safeguard your rights and freedoms and legitimate interests; or

(c) is based on your explicit consent.

Where we engage in automatic decision-making or profiling in connection with a contract between us or further to your explicit consent, we implement suitable measures to safeguard your rights and freedoms and legitimate interests, at least the right to obtain human intervention from us in the course decision-making process, and the opportunity to express your point of view and to contest the decision.

**i) Right to lodge a complaint with your data protection supervisory authority** - In the event you believe that we are processing your personal data otherwise than in accordance with the provisions of the GDPR, you have the right to lodge a complaint with the data protection supervisory authority located in the EU jurisdiction where you reside. For the UK, the supervisory authority is the UK Information Commissioner's Office.

## **8. Links to external websites**

Our website may provide links to third-party companies' websites for your convenience and information. If you access those links, you will leave the Octavius website. Octavius does not control those sites, their content or their privacy practices, which may differ from Octavius. We do not endorse or make any representations about third-party websites. The personal data you choose to give to unrelated third parties is not covered by this Privacy Policy. We encourage you to review the privacy policy of any company before submitting your personal data. Some third-party companies may choose to share their personal data with Octavius; that sharing is governed by that third-party company's privacy policy.

## **7. Children's privacy**

Octavius is committed to protecting the privacy needs of children and we encourage parents and guardians to take an active role in their children's online activities and interests. Octavius does not knowingly collect information from children under the age of 16 and does not target its Website or any of its services to children under the age of 16.

## **8. Keeping your personal data secure**

We are committed to protecting the information you provide us. To prevent unauthorized access or disclosure, to maintain data accuracy, and to ensure the appropriate use of the information, Octavius has in place appropriate technological and operational procedures to safeguard the information we collect.

If you believe Octavius has handled your personal data in a manner that does not comply with this Privacy Policy, please contact us by the means specified below at Section 10 of this Privacy Policy.

### **9. Changes to this Privacy Policy**

If there are updates to the terms this Privacy Policy, we will post those changes and update the revision date in this document, so you will always know what information we collect, how we use it, and what choices you have. For material changes to this Privacy Policy, Octavius will actively notify affected individuals.

### **10. Contacting us**

We value your opinions. If you have comments or questions about our Privacy Policy – as well as if you have any requests or questions regarding our processing of your personal data, please contact the below:

**Email the DPO: RJ Jayaratne**

**Call us: 0208 004 4030**

**Reach us in person or by mail: [rj@octaviusrenewables.com](mailto:rj@octaviusrenewables.com)**