DATA SUBJECTS' RIGHTS – POLICY AND PROCEDURES

February 2019

1 Introduction and Scope

Under Irish and EU data protection and privacy laws, data subjects have the right to be informed about how Ocean Renewable Power Company, Inc. and all its affiliated entities, including but not limited to ORPC Ireland Limited (collectively "ORPC") uses any personal information that it collects and processes about them, and the right to make certain decisions about how that information is used, or processed.

Data subjects have the following rights over their personal information that is processed by **ORPC**. (These rights may occasionally be somewhat restricted, but only in particular circumstances):

a) The right of access to their personal information
b) The right to rectify/correct their personal information
c) The right to erase/delete their personal information (i.e., the "right to be forgotten")
d) The right to 'port' their personal information from one data controller to a new data controller
e) The right to restrict **ORPC**'s processing of their personal information
f) The right to object to **ORPC**'s processing of their personal information

This policy explains how ORPC will respond to an individual's request to exercise their rights (a "**Rights Request**") with respect to their personal information.

Failure to comply with this policy may result in disciplinary action, up to and including dismissal.

2 WHAT IS THE PURPOSE OF THIS POLICY?

ORPC is required to respond to all Rights Requests in a documented, consistent and timely manner, and in a way that complies with applicable data protection and privacy laws.

> All Rights Requests should be completed within 1 calendar month of the receipt of the Rights Request and, where applicable, receipt of the information needed to verify the identity of the requestor, as described in section 4.4(b). If these documents are provided separately, the deadline will be 1 calendar month from the date of receipt of the later document. It may be possible to extend the deadline in certain circumstances as described in section 4.10.

3 WHAT IS THE PURPOSE OF THE PROCESSING?

"Personal information" is any information that relates to an **identified or identifiable living individual**. Different pieces of information, which collected together can lead to the identification of a person, also constitute personal data. Identifiable means they can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, cultural, or social identity of that person. Personal data that has been de-identified, encrypted or **pseudonymized** but can be used to re-identify a person remains personal data and falls within the scope of personal data. Personal data that has been rendered **anonymous** in such a way that the

individual is not or no longer identifiable is no longer considered personal data. For data to be truly anonymized, the anonymization must be irreversible.

Personal information includes, for example:

a) Name and surname
b) Home address
c) Email address, such as name.surname@orpc.co
d) Identification card number
e) Location data (for example the location data function on a mobile phone)
f) Internet Protocol (IP) address
g) Cookie ID
h) Advertising identifier of your phone
i) Data held by a hospital or doctor, which could be a symbol that uniquely identifies a person
j) Images of the individual
k) Bank details
l) Opinions about that individual stated by others

In other words, it is information about an individual whether their name is used or not, so long as it is clear that it is about that individual. It can also refer to information that allows an individual's device to be singled out, so can include cookie identifiers, IP addresses, MAC addresses, unique device identifiers, and other behavioral information that is tied to a unique identifier.

The context of the reference to an individual should also be looked at. So where an individual is simply referred to as having attended a meeting, or is the author of an email, the meeting minutes or the content of the email will not normally be personal information, unless those minutes or content have an individual as their subject matter, but the fact that an individual attended the meeting or sent the email would be personal information about that individual.

4 PROCEDURE FOR RESPONDING TO RIGHTS REQUESTS – WHERE ORPC IS A CONTROLLER

Submitting a Rights Request

a) The following Subject Rights Request forms are available - forms 1a, 2a, 3a, 4a, 5a and 6a in 'Data Subject Rights Procedure and Forms'. These are the forms that can be used to submit Rights Requests, and **ORPC** should encourage individuals to use these forms to make their Requests. Even though **ORPC** provides these forms, **ORPC** may NOT insist on use of these forms but can encourage their use for ease of handling such requests. **ORPC** MUST consider and respond to all requests from individuals relating to their rights.

b) If any **ORPC** employee receives a Rights Request from an individual, that Rights Request must be forwarded to **Sybille Cyr (scyr@orpc.co)** immediately, who will assign the Rights Reequest to a designated individual to handle (the "**Responder**").

4.1 RECEIPT OF THE REQUEST

a) When the Responder receives a Rights Request, they should review that request. If that Rights Request is not submitted using one of the forms provided, the Responder should fill out the relevant Rights Request Form using the information provided, as best as possible.

b) The Responder should:
    i. Check that the identity of the requestor has been verified. If a Rights Request is made

by an individual other than a current employee, **ORPC** is only required to comply with the Rights Request if the individual making the request supplies **ORPC** with information that allows **ORPC** to confirm their identity. For users with accounts with **ORPC**, this could include requiring the user to log in before submitting the request. Otherwise, this should comprise **proof of identity**. Proof of identity may include any information specific to a requestor's use of the service that would not generally be known, such as the requestor's last login date, or amount of an invoice received. If the information requested includes that requestor's address, photo or other sensitive information, additional proof of identity may be requested (e.g. copy of ID card or another official document). When requesting proof of identity, the Responder should provide the data subject the opportunity to obscure or redact information that is not necessary for identification. The Responder should contact the requestor to ask for such information if it has not been provided (see forms 1b, 2b, 3b, 4b, 5b and 6b).

ii. Review the scope of the Rights Request for clarity. If it is not clear, the Responder should contact the requestor to request further information using the relevant form set out (see forms 1b, 2b, 3b, 4b, 5b and 6b). The types of further information that may be required are set out in the information about each particular right.

c) Once the Responder has received any additional information required about the scope of the request and appropriate identification documents from the requestor, they should then determine whether the Rights Request is valid. Information about whether a Rights Request is valid is set out in the information about each particular right.

d) If the Rights Request is not valid, the Responder should contact the requestor and explain the reasons why the Rights Request is not valid using the relevant form (see forms 1d, 2d, 3d, 4d, 5d and 6d).

e) If the Rights Request is valid, the Responder should acknowledge the Rights Request using the relevant form (see forms 1c, 2c, 3c, 4c, 5c and 6c) and comply with the request as set out below.

4.2 COMPLYING WITH THE RIGHTS REQUEST

f) The Responder should follow the appropriate steps for complying with the relevant type of Rights Request. Relevant considerations with respect to each right are set forth in the descriptions of the rights (see document 'Data Subject Rights Procedure and Forms'). It is important for the Responder to record the steps taken when responding to the Rights Request.

g) In some cases, complying with a Rights Request will require third parties (e.g. service providers and other third parties with which **ORPC** shares Personal Information) to take certain actions, for example to update their records in response to a request to correct/rectify personal information, or to delete personal information they hold in response to a request for erasure/deletion. The arrangements applicable to the respective responsibilities of the Controller and third-party Processors must be detailed in a Data Processing Contract that complies with Article 28(3). The Responder should therefore contact all third parties who hold Personal Information relating to the relevant individual using the relevant form (see forms 1e, 2e, 3e, 4e, 5e and 6e) and ask that they comply with the Rights Request and confirm to Responder that they are doing so. Where appropriate, the details of some of the third parties that might be relevant for each type of Rights

Request are set out.

h) If, due to the scope of the Rights Request, it is possible that complying with the Rights Request will take longer than 1 calendar month, the Responder should inform **Sybille Cyr**. After receiving sign-off from **Sybille Cyr**, the Responder should contact the requestor using the relevant form (see forms 1f, 2f, 3f, 4f, 5f and 6f) to inform the requestor that the response to the Rights Request may be delayed. This should not be a typical circumstance, and the Responder should document the reasons why the deadline was not met both internally, and to the requestor.

i) Once the Rights Request has been completed, the Responder should prepare a report that sets out how the Rights Request has been completed. This report should contain a description of all steps taken to determine whether the Rights Request was valid, and all steps taken to comply with the Rights Request. The Responder should then contact the requestor using the relevant form (see forms 1g, 2g, 3g, 4g, 5g and 6g).to confirm that the Rights Request has been completed, attaching the report.

j) Any additional information collected to verify the identity of the requestor should be deleted at a set period of time after the identity has been verified, in accordance with the Records Retention Policy.

5 PROCEDURE FOR RESPONDING TO RIGHTS REQUESTS – ORPC IS A PROCESSOR

a) Where **ORPC** receives a Rights Request from an individual in its capacity as a processor (i.e., the personal information to which the Rights Request relates is processed by **ORPC** in the course of providing services to a client who is the Data Controller), ORPC should pass that request promptly to that data controller, i.e., the entity for whom they are providing a service, and should not respond to the request unless authorized to do so in writing by the data controller. The arrangements applicable to the respective responsibilities of the Controller and the Processor must be detailed in a Data Processing Contract that complies with Article 28(3).

b) ORPC will also be required to provide reasonable assistance to the data controller when the data controller is responding to that request, or a similar request received by the Controller, for example by carrying out searches on its own systems. Again, the arrangements applicable to the respective responsibilities of the Controller and the Processor must be detailed in a Data Processing Contract that complies with Article 28(3) of the GDPR.