

1. Introduction

This Policy sets out the obligations of Harmony Energy Storage Ltd, a company registered in England under number 10141078, whose registered office is at Conyngham Hall, Bond End, Knaresborough, North Yorkshire, England, HG5 9AY (“HESL”) regarding retention of personal data collected, held, and processed by HESL in accordance with EU Regulation 2016/679 General Data Protection Regulation (“GDPR”).

The GDPR defines “personal data” as any information relating to an identified or identifiable natural person (a “data subject”). An identifiable natural person is one who can be identified, directly or indirectly, in particular 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, economic, cultural, or social identity of that natural person.

The GDPR also addresses “special category” personal data (also known as “sensitive” personal data). Such data include, but are not necessarily limited to, data concerning the data subject’s race, ethnicity, politics, religion, trade union membership, genetics, biometrics (if used for ID purposes), health, sex life, or sexual orientation.

Under the GDPR, personal data shall be kept in a form which permits the identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

In certain cases, personal data may be stored for longer periods where that data are to be processed for archiving purposes that are in the public interest, for scientific or historical research, or for statistical purposes (subject to the implementation of the appropriate technical and organisational measures required by the GDPR to protect that data).

In addition, the GDPR includes the right to erasure or “the right to be forgotten”. Data subjects have the right to have their personal data erased (and to prevent the processing of those personal data) in the following circumstances:

- a) Where the personal data are no longer required for the purpose for which they were originally collected or processed (see above);
- b) When the data subject withdraws their consent;
- c) When the data subject objects to the processing of their personal data and HESL has no overriding legitimate interest;
- d) When the personal data are processed unlawfully (i.e. in breach of the GDPR);
- e) When the personal data have to be erased to comply with a legal obligation; or

f) Where the personal data are processed for the provision of information society services to a child.

This Policy sets out the type(s) of personal data held by HESL in respect of public consultation activity, the period(s) for which those personal data are to be retained, the criteria for establishing and reviewing such period(s), and when and how it is to be deleted or otherwise disposed of.

For further information on other aspects of data protection and compliance with the GDPR, please refer to HESL's Data Protection Policy.

2. Aims and Objectives

2.1 The primary aim of this Policy is to set out limits for the retention of personal data and to ensure that those limits, as well as further data subject rights to erasure, are complied with.

By extension, this Policy aims to ensure that HESL complies fully with its obligations and the rights of data subjects under the GDPR.

2.2 In addition to safeguarding the rights of data subjects under the GDPR, by ensuring that excessive numbers of data are not retained by HESL, this Policy also aims to improve the speed and efficiency of managing data.

3. Scope

3.1 This Policy applies to all personal data held by HESL for public consultation purposes and in respect of the employment of its staff and by third-party data processors processing personal data on HESL's behalf.

3.2 Personal data, as held by HESL is stored in the following ways and in the following locations:

- a) HESL's servers, located in Conyngham Hall, Bond End, Knaresborough, North Yorkshire, England, HG5 9AY
- b) Third-party servers operated by Microsoft and located within the European Economic Area;
- d) Laptop computers and other mobile devices provided by HESL to its employees;
- e) Computers and mobile devices owned by employees, agents, and sub-contractors
- f) Physical records stored in its premises at Conyngham Hall, Bond End, Knaresborough, North Yorkshire, England, HG5 9AY

4. Data Subject Rights and Data Integrity

All personal data held by HESL is held in accordance with the requirements of the GDPR and data subjects' rights thereunder, as set out in HESL's Data Protection Policy.

4.1 Data subjects are kept fully informed of their rights, of what personal data HESL holds about them, how those personal data are used as set out in Parts 12 and 13 of HESL's Data Protection Policy, and how long HESL will hold those personal data (or, if no fixed retention period can be determined, the criteria by which the retention of the data will be determined).

4.2 Data subjects are given control over their personal data held by HESL including the right to have incorrect data rectified, the right to request that their personal data be deleted or otherwise disposed of (notwithstanding the retention periods otherwise set by this Data

Retention Policy), the right to restrict HESL's use of their personal data, and further rights relating to automated decision-making and profiling, as set out in Parts 14 to 19 of HESL's Data Protection Policy.

5. Technical and Organisational Data Security Measures

5.1 The following technical measures are in place within HESL to protect the security of personal data.

Please refer to Parts 24 to 28 of HESL's Data Protection Policy for further details:

- a) All emails containing personal data must be encrypted;
- b) All emails containing personal data must be marked "confidential";
- c) Personal data may only be transmitted over secure networks;
- d) Personal data may not be transmitted over a wireless network if there is a reasonable wired alternative;
- e) Personal data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely. The email itself and associated temporary files should be deleted;
- f) Where personal data are to be sent by facsimile transmission the recipient should be informed in advance and should be waiting to receive it;
- g) Where personal data are to be transferred in hardcopy form, it should be passed directly to the recipient, sent using Royal Mail Recorded and a secure courier service;
- h) All personal data transferred physically should be transferred in a suitable container marked "confidential";
- i) No personal data may be shared informally and if access is required to any personal data, such access should be formally requested from the Company Data Protection Representative.
- j) All hardcopies of personal data, along with any electronic copies stored on physical media should be stored securely;
- k) No personal data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of HESL or not, without authorisation;
- l) Personal data must be handled with care at all times and should not be left unattended or on view;
- m) Computers used to view personal data must always be locked before being left unattended;
- n) No personal data should be stored on any mobile device, whether such device belongs to HESL or otherwise without the formal written approval of the Company Data Protection Representative and then strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is absolutely necessary;
- o) No personal data should be transferred to any device personally belonging to an employee and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of HESL where the party in question has agreed to comply fully with HESL's Data Protection Policy and the GDPR;

- p) All personal data stored electronically will be stored in the cloud either on HESL's Office365 Tenancy or using secure cloud-based databases. Backups of these services will be made automatically by the service-prover and will be encrypted;
- q) All electronic copies of personal data should be stored securely using passwords and encryption;
- r) All passwords used to protect personal data should be changed regularly and must be secure;
- s) Under no circumstances should any passwords be written down or shared. If a password is forgotten, it must be reset using the applicable method. IT staff do not have access to passwords;
- t) All software should be kept up-to-date. Security-related updates should be installed not more than three months;
- u) No software may be installed on any Company-owned computer or device without approval

5.2 The following organisational measures are in place within HESL to protect the security of personal data. Please refer to Part 29 of HESL's Data Protection Policy for further details:

- a) All employees and other parties working on behalf of HESL shall be made fully aware of both their individual responsibilities and HESL's responsibilities under the GDPR and under HESL's Data Protection Policy;
- b) Only employees and other parties working on behalf of HESL that need access to, and use of, personal data in order to perform their work shall have access to personal data held by HESL;
- c) All employees and other parties working on behalf of HESL handling personal data will be appropriately trained to do so;
- d) All employees and other parties working on behalf of HESL handling personal data will be appropriately supervised;
- e) All employees and other parties working on behalf of HESL handling personal data should exercise care and caution when discussing any work relating to personal data at all times;
- f) Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed;
- g) The performance of those employees and other parties working on behalf of HESL handling personal data shall be regularly evaluated and reviewed;
- h) All employees and other parties working on behalf of HESL handling personal data will be bound by contract to comply with the GDPR and HESL's Data Protection Policy;
- i) All agents, contractors, or other parties working on behalf of HESL handling personal data must ensure that any and all relevant employees are held to the same conditions as those relevant employees of HESL arising out of the GDPR and HESL's Data Protection Policy;
- j) Where any agent, contractor or other party working on behalf of HESL handling personal data fails in their obligations under the GDPR and/or HESL's Data Protection Policy, that

party shall indemnify and hold harmless HESL against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

6. Data Disposal

Upon the expiry of the data retention periods set out below in Part 7 of this Policy, or when a data subject exercises their right to have their personal data erased, personal data shall be deleted, destroyed, or otherwise disposed of as follows:

6.1 Personal data stored electronically (including any and all backups thereof) shall be deleted as follows:

6.1.1 Electronic documents that pertain in its entirety to the subject will be double deleted. The recycle bin deletion is a weekly automated task and double checked by individual staff.

6.1.2 Where electronic documents pertain to and include other subjects then redaction will be used in line with the guidance of the ICO.;

6.2 Special category personal data stored electronically (including any and all backups thereof) shall be deleted securely using the following method:

- a) Data will be deleted from the cloud servers;
- b) Immediately the user will empty the "Deleted Items" folder;
- c) Once deleted, the emails remain on the server hosted by Microsoft for another 30 days. On reaching the 30-day limit the files will be permanently deleted;
- d) During this time all data are fully encrypted using Bit Locker encryption on the hosted Microsoft servers.

6.3 Personal data stored in hardcopy form shall be shredded and recycled;

6.4 Special category personal data stored in hardcopy form shall be shredded and recycled.

7. Data Retention

7.1 As stated above, and as required by law, HESL shall not retain any personal data for any longer than is necessary in light of the purpose(s) for which those data are collected, held, and processed.

7.2 Different types of personal data, used for different purposes, will necessarily be retained for different periods (and its retention periodically reviewed), as set out below.

7.3 When establishing and/or reviewing retention periods, the following shall be taken into account:

- a) The objectives and requirements of HESL;
- b) The type of personal data in question;
- c) The purpose(s) for which the data in question is collected, held, and processed;
- d) HESL's legal basis for collecting, holding, and processing that data;
- e) The category or categories of data subject to whom the data relates;
- f) The limitations of law applying to the overall project that HESL has worked on.

7.4 If a precise retention period cannot be fixed for a particular type of data, criteria shall be established by which the retention of the data will be determined, thereby ensuring that the data in question, and the retention of those data, can be regularly reviewed against those criteria.

7.5 Notwithstanding the following defined retention periods, certain personal data may be deleted or otherwise disposed of prior to the expiry of its defined retention period where a decision is made within HESL to do so (whether in response to a request by a data subject or otherwise).

7.6 In limited circumstances, it may also be necessary to retain personal data for longer periods where such retention is for archiving purposes that are in the public interest, for scientific or historical research purposes, or for statistical purposes. All such retention will be subject to the implementation of appropriate technical and organisational measures to protect the rights and freedoms of data subjects, as required by the GDPR.

Data Reference	Type of Data	Purpose of Data	Review Period	Retention Period or Criteria	Comments
Name	Name	To enable us to identify a data subject who is participating in a public consultation process	Every 12 months whilst the project is still active	12 years after the project completion	Data will be archived and not reused once the full project has been completed e.g. once construction is complete. Data may be anonymised and used for research purposes at any time up to the deletion period.
Postal address	Postal address	To enable us to contact a data subject to discuss the project on which a public consultation is being held	Every 12 months whilst the project is still active	12 years after the project completion	Data will be archived and not reused once the full project has been completed e.g. once construction is complete. Data may be anonymised and used for research purposes at any time up to the deletion period.
Telephone number	Telephone number	To enable us to contact a data subject to discuss the project on which a public consultation is being held	Every 12 months whilst the project is still active	12 years after the project completion	Data will be archived and not reused once the full project has been completed e.g. once construction is

					complete. Data may be anonymised and used for research purposes at any time up to the deletion period.
Email address	Email address	To enable us to contact a data subject to discuss the project on which a public consultation is being held	Every 12 months whilst the project is still active	12 years after the project completion	Data will be archived and not reused once the full project has been completed e.g. once construction is complete. Data may be anonymised and used for research purposes at any time up to the deletion period.
Gender	Gender	To enable us to ensure that public consultation programmes and activities have taken into account the demographic makeup of a particular geography	Every 12 months whilst the project is still active	12 years after the project completion	Data will be archived and not reused once the full project has been completed e.g. once construction is complete. Data may be anonymised and used for research purposes at any time up to the deletion period.
Date of birth	Date of birth	To enable us to ensure that public consultation programmes and activities have taken into account the demographic makeup of a particular geography To ensure that we are not collecting data from anyone under the age of 16	Every 12 months whilst the project is still active	12 years after the project completion	Data will be archived and not reused once the full project has been completed e.g. once construction is complete. Data may be anonymised and used for research purposes at any time up to the deletion period.
Age Group	Age Group	To enable us to ensure that public consultation	Every 12 months whilst the project is still active	12 years after the project completion	Data will be archived and not reused once the full

		programmes and activities have taken into account the demographic makeup of a particular geography To ensure that we are not collecting data from anyone under the age of 16			project has been completed e.g. once construction is complete. Data may be anonymised and used for research purposes at any time up to the deletion period.
Opinions	Opinions	Opinions of data subjects as part of statutory and non-statutory public consultation exercises	Every 12 months whilst the project is still active	12 years after the project completion	Data will be archived and not reused once the full project has been completed e.g. once construction is complete. Data may be anonymised and used for research purposes at any time up to the deletion period.
Home ownership	Home ownership	To enable us to ensure that public consultation programmes and activities have taken into account the demographic makeup of a particular geography	Every 12 months whilst the project is still active	12 years after the project completion	Data will be archived and not reused once the full project has been completed e.g. once construction is complete. Data may be anonymised and used for research purposes at any time up to the deletion period.

8. Roles and Responsibilities

8.1 HESL's Company Data Protection Representative is Peter Kavanagh – planning@harmonyenergy.co.uk.

8.2 The Company Data Protection Representative shall be responsible for overseeing the implementation of this policy and for monitoring compliance with this Policy, HESL's other Data Protection-related policies (including, but not limited to, its Data Protection Policy), and with the GDPR and other applicable data protection legislation.

8.3 The Company Data Protection Representative shall be directly responsible for ensuring compliance with the above data retention periods throughout HESL.

8.4 Any questions regarding this Policy, the retention of personal data, or any other aspect of GDPR compliance should be referred to the Company Data Protection Representative.

9. Implementation of Policy

This Policy shall be deemed effective as of 14th April 2020. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

This Policy has been approved and authorised by:

Peter Kavanagh
CEO
Harmony Energy Storage Ltd

Date: 14 April 2020

Due for review by: 15 April 2021