

Privacy Policy

February 2020



Contents

Introduction	1
1 Definitions	1
1.1 “Personal Data”	1
1.2 “Data Controller”	1
1.3 “Data Processor”	2
1.4 “Data Processing”	2
1.5 “Data Subject”	2
1.6 “Cookies”	2
2 GDPR from Human Resources Perspective.....	2
3 GDPR – External Perspective	3
4 EMEC’s GDPR Principles	4
4.1 Accountability.....	4
4.2 Transparency.....	4
4.3 Consent	5
5 EMEC Statement Under GDPR	6
6 Photography and Social Media Marketing	7
7 Personnel Data Retention	7
8 Bases for Processing Data.....	9
8.1 Processing under Contractual/Legal Obligation	9
8.2 Processing for Legitimate Interest.....	9
8.3 Processing under the Basis of Consent	9
8.4 Processing as a Means of Public Task or Interest.....	9
8.5 Processing for Research Purposes.....	9
9 How EMEC Protect Data.....	10
9.1 Paper Data	10
9.2 Electronic Data	10
9.3 Payment Services.....	10
9.4 Third Party Data Sharing.....	11
9.5 Pseudonymization.....	11
10 Data Processing Agreement with IT support contractor	11
11 Rights of ‘Data Subjects’ Under the GDPR in Relation to EMEC	12
11.1 The Right to be Informed	12
11.2 The Right of Access.....	12
11.3 The Right to Rectification	12
11.4 The Right to Erasure.....	12
11.5 The Right to Restrict Processing.....	12
11.6 The Right to Data Portability	13

11.7	The Right to Object.....	13
12	Change.....	13
13	Appendices	14
13.1	Appendix A – Data Retention Table	14

Introduction

EMEC is committed to protecting the rights and freedoms of individuals that share any personal or sensitive information with the Company. This is central to the business' core values as it grows and diversifies in the world of marine renewable energy; and the Company looks to ensure stakeholders understand that privacy across all departments is taken seriously. EMEC endeavours to make stakeholders confident when entrusting the Company with personal information that it is used in the manner expected by that individual or group.

The General Data Protection Regulation (2018) (GDPR) aims to maximise the rights and freedoms of individuals, through implementation of stricter rules and regulations with which all businesses, no matter how big or small, must comply. The GDPR applies to all staff and teams across EMEC and requires each of the business departments to work collaboratively to ensure consistent adherence to the legislation. This privacy policy describes and explains EMEC's practices with regards to personal or sensitive information ('data') and will provide insight into how data is used and protected once under the control of the Company. Please note that policies are subject to change as and when the law and/or the Company changes structurally.

If you have any concerns about how personal data is managed by EMEC, please contact us:

By telephone: 01856 852047

By email: hr@emec.org.uk

In person: The European Marine Energy Centre Limited, The Charles Clouston Building, ORIC, Back Road, Stromness, Orkney, KW16 3AW.

1 Definitions

1.1 "Personal Data"

The term "personal data" in this document and used in connection with the GDPR refers to *"data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller;"* or *"any information relating to an identified or identifiable natural person ('Data Subject')"*. An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to their physical, religious, sexual, physiological, mental, economic, cultural or social identity.

1.2 "Data Controller"

A "data controller" in the GDPR context is defined as *"a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner that any personal data is collected, stored, or to be processed"*. In short, this

refers to the Company who decide what data to obtain upon what basis, and how it is collected, used, stored and erased.

1.3 “Data Processor”

A “data processor”, in relation to GDPR and personal data, means *“any person (other than an employee of the data controller) who processes the data on behalf of the data controller”*. This would refer to anyone who has access to or uses data which EMEC control. As an example, the Company’s IT support contractor acts as a data processor for EMEC and has countersigned a Data Processing Agreement (REF862 in EMEC document register).

1.4 “Data Processing”

The term “data processing” used throughout this document and the GDPR, refers to *“the organisation, adaptation or alteration of the information or data; the retrieval, consultation or use of the information or data; the disclosure of the information or data by transmission, dissemination or otherwise making available, or the alignment, combination, blocking, erasure or destruction of the information or data”*. This refers to the way in which collected data is managed or used by the Company.

1.5 “Data Subject”

The “data subject” used throughout this document means *“an individual who is the subject of personal data”*. In other words, the data subject is the individual to whom the data directly relates. The GDPR does not count a data subject as *‘an individual who has died or who cannot be identified or distinguished from others.’*

1.6 “Cookies”

The term “cookies” relates to a text file which contains information relating to a web journey and behaviour online. Cookies can monitor which sections of a website are used most frequently, and from which area of the website users exit or leave the page. This is used as a tool to improve services offered online to internet users and targets areas where users are less satisfied.

2 GDPR from Human Resources Perspective

EMEC collects and maintains personal information about *all* of its employees in accordance with legislation. The organisation is fully committed to protecting and respecting individual data privacy by handling all personal information connected with an individual’s employment with EMEC in accordance with the Data Protection Act 2018.

The legislation applies to *“any business that trades with any EU country and stores the personal data of any EU national within that country”*, thus, EMEC has a legal duty and obligation to handle personal data to deliver contractual obligations to any employee of the Company.

As a business, EMEC collects, processes and transfers personal information about employees, stakeholders and any individual or group they are affiliated with; both in paper form and electronic means. All collection, processing, and transfer of personal information are subject to strict confidentiality and secure privacy safeguards; already in line with the Data Protection Act 2018's predecessor. Security measures put in place by the Company's IT support contractor are enabled to protect personal data from access by unauthorised persons, against unlawful processing, accidental loss, destruction and damage.

Some information must be processed to fulfil a moral and legal obligation to stakeholders, employees and the general public; this refers to organisational processing functions such as:

- Payroll and wage processing;
- Employee annual leave allowance;
- Equal opportunities monitoring of job applicants;
- Staff development and training;
- General recruitment and staffing;
- Administration of bonuses, insurance and the pension scheme;
- Performance management and audits;
- Health and safety/risk management;
- Workplace management and human resource related tasks;
- Protecting EMEC and its workforce from injury, theft, liability, fraud, abuse;
- Compliance with employment law under government legislation;
- Ensuring fairness and equality across the whole organisation with regards to discrimination;
- Determining the effectiveness of promotional campaigns, marketing activities and advertising;
- Better understanding the reach of EMEC's internet presence;
- Tailoring online experiences through EMEC's website and social media functions;
- Processing of government funding claims which include employee salary information.

3 GDPR – External Perspective

As a Company that has a demonstrably large network, EMEC is constantly in touch with stakeholders on a daily basis. Whenever the Company is in contact with an individual through email or through the website, the user in question has consented to the collection of that personal data.

With a public website, <http://www.emec.org.uk/>, EMEC is committed to preserving the privacy of all visitors to the site. The use of the website involves processing data and collecting information about each individual's usage of the site, as well as information about that individual from information posted or shared via the website or through contact forms. By using the EMEC website, each user has consented to the collection, use and potential transfer of information under the terms of this privacy policy; which is available to view on all of the Company's virtual platforms.

The information gathered from collecting data from EMEC's website enables the Company to provide the individual user with access to each separate part of the website and supplies information that may be useful to the user and their experience of the site. EMEC will also use and analyse the information collected to support, improve and develop the website and business.

In particular, EMEC may use collated personal information to contact that individual for their views on the website and may occasionally need to notify that user about important changes or developments to it. However, if an individual/data subject changes their mind about the Company contacting them in the future, they can 'opt out' of this type of correspondence and the Company will respect the individual's wishes in line with the law.

Through the website, "cookies" are used to enhance the user experience with the site. These are stored in a user's web browser to enable EMEC's marketing team to personalize the users' experience online the next time that individual or a new user visits the site. Cookies expedite surfing the internet for the user in question and allow a website to recognise a user's device and tailor the online experience to suit that individual, based on previous online behavioral traits.

"Tracking cookies" collect information about how a user browses and uses EMEC's website, what pages have been visited, how the site was entered and where the user exited it. This data is completely anonymous, but it helps the Company to make improvements to the web experience offered by identifying pages where more visitors may be exiting the website or where visitors may be struggling to find necessary information and move to a different section.

4 EMEC's GDPR Principles

4.1 Accountability

"The controller shall be responsible for and be able to demonstrate compliance with the principles of GDPR". 33 of the 99 articles of the GDPR require evidence to demonstrate compliance with the legislation. EMEC demonstrates this through the measures and safeguards already in place under *older* legislation (Data Protection Act 1998), the strict processes followed, and adherence under the quality management system and official accreditations.

4.2 Transparency

Under the GDPR it is understood that *"any processing of personal data should be lawful and fair. It should be transparent to "natural persons" that the personal data concerning them is collected, used, consulted or otherwise processed and to what extent the personal data will be processed, under defined basis."* Prior to, or at the time of collected data, the purpose for which data is used/processed will be explained to the user in documented form through the privacy policy or verbally. Any data subject will be presented with or directed to a copy of the Company's privacy notice and is given an opportunity to opt in or out regarding data processing (where consent is the basis for processing) and alter the way in which communication

between the two parties is made if they so request. Routes to access information are explained and Subject Access Requests (SARs) shall be recorded and responded to in a timely and thorough matter as required by this legislation. Each individual is made aware of their rights as a data subject.

“The principle of transparency requires that any information and communication relating to the processing of personal data may be easily accessible (to the concerned data subject) and easy to understand; written in clear, plain, language that is concise and easy to read”.

4.3 Consent

The issue of consent as a basis for processing data, is used by EMEC in certain circumstances where there is no legal obligation to process data. Consent is composed of:

‘Any freely given, specific, informed and unambiguous indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed.’ (Articles 4 & 32).

Pre-ticked boxes to obtain consent are not considered to be a valid form of consent under the GDPR, as they may have been under the Data Protection Act of 1998. EMEC does not currently use pre-ticked boxes as a means of obtaining a data subject or natural persons consent.

‘Silence, pre-ticked boxes or inactivity should not therefore constitute consent.’

GDPR states that consent should not be conditional upon sign-up to another service, i.e. coupled together, only giving access to certain areas of a web page if you consent to something prior to that access. This technique was commonly used by UK organisations but is no longer considered valid consent under GDPR:

‘When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.’ (Article 7)

Individuals are informed by the privacy policy (or EMEC representative) that they can withdraw consent at any point and it must be simple to do so, without detriment to the data subject or other aspects of data sharing. This clause is exercised by EMEC when consent is required for the processing of data, for example with market research, or administration activities such as adding a photograph of an employee to an organisational chart or writing a blog post. Please refer to FORM262 GDPR Consent Form.

5 EMEC Statement Under GDPR

- EMEC only uses personal information when necessary, and the way that is expected by the 'data subject'/person in question;
- EMEC strictly adheres to all law and legislation relating to the processing of personal data, under the GDPR;
- EMEC only processes data under the processing basis which will be highlighted to the data subject at the time of collection;
- EMEC makes it easy for a data subject to choose how we communicate with that individual, if that individual wishes us to do so;
- EMEC respects a data subject/natural person's wishes regarding personal information to update, remove, erase, or change the personal information that individual has provided, where the basis for processing allows;
- EMEC never provides any third party with a data subject's personal information (unless legally bound to) without explicit written consent; however, EMEC may occasionally pass aggregate information on the usage of the website to third parties for research purposes - this will not include information that can be used to identify that data subject;
- Unless required or permitted to do so by law, EMEC does not otherwise share, sell or distribute any of the information held on that person without prior and relevant consent;
- EMEC is vigilant in the management of sensitive data and always strives to improve security; exploiting new and secure technologies and reviewing and auditing those measures in place;
- EMEC constantly updates, maintains and implements safeguards to protect privacy through secure policies, secure processes and correct management;
- EMEC make it easy to contact the company should a data subject need to at any time, to answer any questions relating to the data it holds on that natural person/data subject;
- EMEC responds to Subject Access Requests (SAR's) quickly and appropriately under the rules set out by the GDPR, within a 30-day period;
- EMEC adheres to and promotes a culture of strict confidentiality at all times; including the signature of a Non-Disclosure Agreement (NDA) required by all staff and associates of EMEC, safeguarding data to the fullest extent to mitigate risk of a data breach incident;

- EMEC has implemented a Data Breach Standard Operating Procedure (SOP127) which instructs staff on how to record, address and correct a data breach should it occur, which documentation to reference, and to evaluate and establish the root cause of the data breach to continuously improve and apply corrective action.

6 Photography and Social Media Marketing

As an organisation with an emphasis on comprehensive marketing and branding; it is expected as part of EMEC's daily operations that images and photographs may be taken and published, to carry out a business function effectively by the Commercial Team.

“As a basis for processing, it is possible to justify the taking and processing of photographs under the ‘Legitimate Interest’ clause especially if you are working under contract where the taking and processing of personally identifiable data is required for you to carry out your contract”.

This is the case when EMEC has been a partner or affiliate on any project as it is expected that photos will be taken to perform marketing or public relations functions and promote the business as much as possible.

EMEC will not take or publish photographs unless there is a legitimate reason for doing so. EMEC staff will ensure that freedom of choice is given to participants with regards to ‘opting out’, and individual’s rights regarding the GDPR and photography will be made clear by reference to the privacy policy or by speaking to the EMEC representative.

With regards to marketing activities done through social media channels, where the issue of consent and data use is concerned, the large social networking sites utilised such as Facebook, Twitter, Instagram, LinkedIn, and YouTube are covered by the terms and conditions and privacy policies of each of these software tools.

‘Due to existing legislation known as EU-US Privacy Shield, US organisations (including social media application providers) can self-certify and commit to this framework agreement which underpins their protection of EU citizen data entrusted to them’.

EMEC's direct mail and/or marketing activities for existing business relationships are based on legitimate interest or consent, from which each ‘data subject/natural person’ has the ability and clear choice to opt-out. EMEC carry out regular checks against mailing/contact lists to ensure they are up to date and fit for purpose.

7 Personnel Data Retention

Both the GDPR and the Data Protection Act 2018 do not specifically dictate how long an organisation should keep personal data. EMEC store data for no longer than necessary for the designated processing purpose – the length of time given to retain personal data on a data subject is relative to why it was collated initially.

As an example; applicants for employment that do not successfully reach the end of the recruitment process with EMEC have their data erased electronically and in paper form after 6 months from EMEC first obtaining it, unless otherwise arranged with the human resources department (if a candidate requests to have their CV kept on file for future vacancies, or this is discussed between the candidate and the panel).

The process of full erasure upon a staff member leaving, is executed under the contract EMEC have in place with the Company's IT support contractor, undertaking complete erasure to those wishing to exercise the right (given the basis for processing is consent, or the basis by which the data was gathered is now invalid with no purpose for retention).

EMEC seeks to act under each individual's best interests and respects any expression of wish intimated to the Company.

If a data subject currently works for EMEC, that person's personal data will be kept for as long as is deemed reasonable, for the duration of their employment as is valid. After termination of contract, that employee's information will be erased after 6 years as the law requires for financial record keeping. It is archived securely until that date. The extent of erasure would be dependent on the *type* of information from which the data subject is requesting erasure from, as this right can only be exercised under the basis of consent, and is possible *only*, on the basis that there is no legal or contractual obligation to retain this data for longer than the expressed length of time.

If a data subject is a stakeholder of EMEC; the organisation stores any data collected for no longer than necessary for purpose, and where requested or instructed, explain why data has been retained and under what basis.

'We will retain your information for a reasonable period; or as long as we are bound to under law.' (Articles 12-14).

Personal data will need to be retained for longer in some cases than in others due to its nature. How long EMEC retain different categories of personal data is evaluated on a case-by-case basis regarding business needs. A judgement is then made regarding:

- the current and future value of the information;
- the costs, risks and liabilities associated with retaining that information; and
- the ease or difficulty of making sure it remains accurate and up to date.

If it continues to be necessary to hold the data for one of the reasons set out in Schedules 2 and 3 of the Data Protection Act (such as the performance of a public function or compliance with employment law), then EMEC will retain it for as long as that reason applies.

Under the GDPR, retaining personal data for longer than required will now become a liability that is sanctionable. Please refer to Appendix A for details on the Data Retention Table.

8 Bases for Processing Data

8.1 Processing under Contractual/Legal Obligation

This basis is used by EMEC when required by law to process personal data, holding full data controller responsibility for processing activities. EMEC cannot negate its responsibility by ‘handing over’ responsibility for the processing to another data controller or data processor. EMEC is held accountable regarding all data processing activities, collection, storing and erasure. A legal basis for processing data is used where the performance of contractual obligation will be compromised if no processing takes place. To satisfy the data subject’s needs relating to employment, processing must take place in the context of contractual obligation.

8.2 Processing for Legitimate Interest

EMEC uses this basis for processing data where it is used, processed or stored in a way the “data subject” or “natural person” would expect, which also poses a minimal threat to that data subject’s privacy or security. This is the most commonly used basis by EMEC company-wide.

8.3 Processing under the Basis of Consent

EMEC uses the basis of consent to process information gathered from a ‘data subject’ or ‘natural person’, where they have expressed their willingness to provide this data verbally or in documented form, for the process highlighted to them. EMEC ensures that consent is freely given, unambiguous, clear, and the option for the data subject to ‘opt out’ is understood and simple to request, without detriment to the data subject. This basis is most commonly used by the administration and marketing departments for related functions.

8.4 Processing as a Means of Public Task or Interest

This basis is used by EMEC when it processes data in the “exercise of official authority”; covering public functions and powers set out in law; to perform a specific task in the public interest which is required by a governing body. This is mandatory.

8.5 Processing for Research Purposes

EMEC uses this basis for conducting research under projects or instruction. Qualitative or quantitative information may be used/gathered depending on the type of project in question and the desired outcomes and/or deliverables. If required by government to process data, this basis may override personal interest if performing in the public’s best interest.

9 How EMEC Protect Data

9.1 Paper Data

Any information processed in paper form relating to an employee of EMEC, past, current or prospective future; is securely stored in a filing cabinet in the EMEC office in Stromness. Authorised members of staff have access to this. EMEC does not keep any paper documents for longer than necessary and review and shred data on a regular basis to ensure the basis for processing is relevant and intact, the information is up-to-date and is accurate.

9.2 Electronic Data

Any personal information relating to or regarding an EMEC employee is managed by the Finance Director and authorised members of staff have access to information as required by their role. EMEC and its IT support contractor have a Data Processing Agreement in place (May 2018, REF862 in EMEC's Document Register) which outlines how data is managed, erased and rectified, who has access to this data, and under what circumstances it is accessible to the company. EMEC's IT support contractor does not process data without clear instruction from the data controller. EMEC is also bound by contract relating to the non-disclosure of any information. As such, all instructions are logged properly and there is documented evidence to support this process, the dates they occurred, who requested assistance and for what purpose.

9.3 Payment Services

Legally and mandatorily, EMEC shares sensitive information with the Company's payroll contractor in order for them to process payroll and deposit wages into each employee's nominated bank under contract. Under law, all financial information stored within the employee's nominated bank of choice is confidential and protected by comprehensive security measures that the nominated bank or building society has in place. All financial information sent to Scholes is sent through a secure portal that the payroll contractor implemented in May 2018 under the GDPR directive; which is also password protected. Authorised members of staff have access to the portal as required by their role. The portal ensures that data cannot be intercepted by unauthorised users; but does mean that information is shared with a third-party; with whom EMEC have a non-disclosure contract agreement.

In addition, EMEC share sensitive financial and personal information with the Company's pension provider (a pension associate) which is a legal requirement from all employers in the UK; thus, a contractual obligation exists under the scheme. EMEC's pension provider is a large, governed body that has the capacity and security in place to deal with large quantities of data for different organisations. Authorised staff have accounts registered to make contributions for staff as directed.

EMEC's legal proceedings are handled by the Company's solicitors; who may in certain circumstances have or require access to sensitive data or any third-party information relating to any legal grievance, disciplinary or court proceedings, acting

on behalf of EMEC if required to do so. Given the sensitive nature of this data, any solicitor or legal body may not divulge this information without the data subject's consent unless acting in the public's best interest or statutory law.

9.4 Third Party Data Sharing

Due to the nature of EMEC as a not-for-profit organisation, personal data relating to employees must be shared with other bodies in order to claim grant funding for specific projects. As an example, EMEC works closely with Highlands and Islands Enterprise (HIE), a key stakeholder of the company from whom funding is occasionally available and sharing of information is necessary for claims. This is the case with many of EMEC's project partners, such as INTERREG who provide the company with funded projects.

EMEC also employs human resources consultants, who provide the Company with advice relating to HR matters which can include sensitive or personal information. There is a contract in place with this service provider to ensure data security.

9.5 Pseudonymization

Pseudonymization is a technique concerning data management and de-identification by which; *“personally identifiable information fields within a data record are replaced by one or more artificial identifiers, or ‘pseudonyms’. A single pseudonym for each replaced field or collection of replaced fields makes the data record less identifiable while remaining suitable for data analysis and data processing.”*

EMEC's marketing team (where possible) pseudonymize data gathered from external or internal sources for specific tasks to mitigate risk of potential data breaches within the organisation due to the 'link ability' between data and the individuals concerned. This is only an applicable technique where sensitive data gathered can be linked to its originator.

10 Data Processing Agreement with IT support contractor

EMEC has a legally binding agreement with a local IT support business which details their responsibilities as EMEC's 'data processor' and EMEC's responsibilities as the 'data controller' to which they report. In place is a non-disclosure agreement, and data processing agreement (REF862 in EMEC document register) - legally binding contracts which forbid the Company's IT support contractor from discussing any data they may be exposed to or subject to when providing the required IT support and services throughout EMEC. Within EMEC's internal intranet function, there is a section which refers to 'IT Issues' – under this tab, EMEC employees are able to request any changes or insignificant tasks they require assistance with, with regard to a specific asset or program and the IT support contractor, acting as the 'data processor', monitor this log and act accordingly to complete logged requests. Problems are reported directly to the IT support contractor by phone or email to the company's helpdesk.

11 Rights of 'Data Subjects' Under the GDPR in Relation to EMEC

EMEC encourage any individual who shares information with the company to refer to this policy.

11.1 The Right to be Informed

EMEC are transparent about the type of data held on individuals and how it is managed, and the concerned 'data subjects' have the right to be informed about what data EMEC possess relating to them, why they have it, how it is processed, for what purpose and how long it is kept. The organisation's primary concern is maximising security and solidifying trust between the company as a data controller and its data subjects. EMEC encourage staff to understand what data the company holds related to them and why.

11.2 The Right of Access

'Data subjects' are able to access the information held on them through a 'Subject Access Request' or SAR. EMEC responds to SAR's quickly (within the 1-month/30 days) time frame as outlined by GDPR requirement, and thoroughly, undertaking a full investigation into the subject following the Data Breach SOP127. The data held should be clear, concise, accurate and meet data portability specifications so, the data subject could take that information and use it for another purpose if desired.

11.3 The Right to Rectification

The 'data subject' has a right to have any information held on them that is incorrect or inaccurate updated and corrected - EMEC do this in a secure and timely manner, at the request of any individual directly concerned.

11.4 The Right to Erasure

The 'data subject' has a right to have any data held on them in EMEC's records fully erased after the basis for processing becomes invalid; for example, after another candidate secures the job that the data subject applied for during the recruitment process. If a data subject wishes, the information obtained under the basis of consent that was in place can be withdrawn at any point - for example, providing the company with an email address for direct marketing which the data subject wishes to cease – EMEC erases this data when the right is exercised, under the basis of consent for processing.

11.5 The Right to Restrict Processing

The 'data subject' has the right to restrict the processing of their personal data held on them. For example, the data subject can allow EMEC to store data, but not process it in a certain manner, even under a lawful basis. This only applies in certain circumstances and, depending on the basis, can be overruled.

11.6 The Right to Data Portability

Information held on a 'data subject' must be clear and specific enough that the 'data subject' can take that information held on them and use it for their own purposes across different services. EMEC stores data in an accurate, readable format, and allows the data subject access to their information should they request it (under the correct process) and wish to edit what is held on that data subject.

11.7 The Right to Object

Individuals from which EMEC collects, stores, processes or retains personal data, have the right to object to its use for different purposes; for example, to stop data provided previously from being used for a different processing purpose than originally consented to, hence the 'opt in/out' clause. The marketing team frequently gather data externally; thus, this right needs to be made clear to data subjects prior to the collection of data, at the time of first contact and throughout the communication EMEC has with a 'data subject'.

12 Change

EMEC may revise the privacy policy occasionally. The most current version of the privacy policy will govern EMEC's use of personal data and will be viewable through direct contact or media channels. If a change is made to this policy, the user will be notified by contacting those who provided consent. By continuing to access or use the Company's services after these changes have been implemented, the data subject agrees to be bound by the revised privacy policy.

EMEC reserves the right at any time to modify policy documents, the consent forms, internal SOP's and processes under instruction from management.

EMEC also accepts modifications made to these documents in line with statutory law, the best interests of the Company and the best interests of our stakeholders.

13 Appendices

13.1 Appendix A – Data Retention Table

EMEC Data Retention Table	Such As...		
Recruitment Documents	CVs, cover letters, proof of eligibility to work in UK, schedules, interview notes from panel, task documents produced in interview	If successful – filed in staff file (locked cabinet) and scans moved into ‘S’ drive for HR management. All applications for a post are archived into EMEC’s ‘S’ recruitment drive.	If unsuccessful – all paper documents are shredded after 6 months and electronic records destroyed by the Company’s IT support contractor unless consent has been obtained to keep longer.
Employee Information	Any sensitive data such as D.O.B, emergency contact details, qualifications scans, proof of eligibility to work in the UK, staff development reviews, financial information, payroll, employment references	If still employed by EMEC, all documentation listed left is deemed necessary for the fulfilment of the employment contract and under lawful legislation and should be kept as long as that individual is employed.	If not employed by EMEC, documents must be destroyed after 6 years , in line with HMRC/financial requirements, with the exception of health and safety records.
Intranet Functions	Sickness and absenteeism log, staff development and training log, holiday recording, timesheets	If employed by EMEC, these functions must all be recorded to carry out the duties listed in the employment contract in line with business functions.	If no longer employed by EMEC, all records are taken off the intranet and archived once the individual has left – not visible to other intranet users. This happens quickly after departure. After 6 years these

			are then destroyed permanently.
Accounts	Email accounts under Outlook, account to log in to EMEC Server, Scholes secure portal	If employed currently – necessary in order to do the work as laid out in the job description for each post	If no longer employed by EMEC, this information is disabled by the Company’s IT support contractor after 6 months. If shared account, the other employee can get access granted by the Company’s IT support contractor if this was the case prior.
Pieces of Work	Reports, documents, pieces of work produced	In past, present or future employment, once the employment contract is signed any work produced by an employee is the property of EMEC and shall as such, be surrendered to EMEC and becomes the company’s property.	This is an important part of the terms and conditions of EMEC employment and is applicable to each employee across all levels at any stage.
Clients or Partner Work	As stated in the terms and conditions of agreement or contract between	Unless specific instruction in place otherwise, keep for as long as necessary for project purpose. If under contract,	

EMEC and the client.

work will belong to EMEC and or client.

The European Marine Energy Centre Limited

The Charles Clouston Building, ORIC, Back Road, Stromness, ORKNEY, KW16 3AW

Tel: 01856 852060

Email: info@emec.org.uk

Web: www.emec.org.uk

Registered in Scotland no.SC249331

VAT Registration Number: GB 828 8550 90

Uncontrolled when printed