Ambrey Group Privacy Policy

Table of Amendments

Version	Date	Record of Amendment
1.0	Q2 2018	Creation of document
2.0-4.0	Q3 2018-Q4 2020	Review/updated IAW Group developments
5.0	Q1 2021	Updated IAW Group developments
6.0	Q1 2022	Updated IAW Group developments
7.0	Q1 2023	Appendices 1-3 added • Recording of MS Teams Meetings • Stakeholder Screening • Data Control Committee planning
8.0	Q2 2023	Review/ revised IAW with formalisation of Group ISMS
9.0	Q4 2023	Updated IAW Group developments Removal of Ambrey Ltd Nigeria from the policy Additional of Ambrey Analytics to the policy Addition of all intelligence /risk platforms
10.0	Q4 2023	YE Man Review / version control & update to Annex list
11.0	Q3 2024	Updates regarding hard copy record management and Data Cttee agenda to incl Root Cause.
12.0	Q1 2025	AGS Limited added to the policy

Document Ownership

The owners of this document are the Compliance & IT Teams who have authority to review content with senior management and implement revisions.

Amendments will be issued annually or as per requirement.

1. Introduction

Our Privacy Policy applies to the data that Ambrey collects and uses.

References in this Privacy Policy to “Ambrey”, “we”, “us” or “our” mean Ambrey Limited / the Ambrey Group and all subsidiary companies:

- Ambrey Limited Company registration no: 10222741

Ambrey Group registered address - Thorn Business Centre, Rotherwas, Hereford, HR2 6JT, United Kingdom.

- Ambrey Risk Limited Company registration no: 7374749.
- Ambrey International Limited Company registration no: 10095821
- Ambrey Offshore Limited Company registration no: 8592553
- Ambrey Insurance Brokers Limited Company registration no: 12478937
- Ambrey Analytics Limited Company Registration no: 14649343
- Ambrey Services DMCC Company registration number: DMCC 4685.
- Ambrey Global Speciality Limited Company Registration 15830449

Ambrey controls how your personal data is collected and the purposes for which we use your personal data. Ambrey is the "data controller" and the data processor (see notes) for the purposes of the UK Data Protection Act 2018 or the EU Regulation 2016/679 (GDPR).

- Note1: Ambrey Senior Management are Data Managers for the departments they run
- Note2: Ambrey department staff are Data Processers.
- Note3: All stakeholders are Data Processers & IT management are the Data Controller.
    - (refer to section 2)

Data Protection Principles

The Act sets out six data protection principles and various safeguards which must be adhered to. All six principles must be met in order for the Company to comply with the Act.

(i) first data protection principle – processing must be lawful and fair;
(ii) second data protection principle – purposes of processing must be specified, explicit and legitimate;
(iii) third data protection principle – personal data must be adequate, relevant and not excessive;
(iv) fourth data protection principle – personal data must be accurate and kept up to date;
(v) fifth data protection principle – personal data must be kept for no longer than is necessary;
(vi) sixth data protection principle – personal data must be processed in a secure manner.

In our provision of maritime and risk management services Ambrey want all stakeholders to be fully informed and up-to-date with how Ambrey uses data.

If you provide your information ('data') and consent to use it, the manner in which Ambrey use your information is set out in this policy. Ambrey may also process your data under other lawful bases.

This policy is made available to any interested party on the website and is given to new employees. This policy is also an annex in our SOP's and is sent out to third parties, employees, contractors and sub contractors.

Training on data protection and privacy is provided at induction to all employees and consultants and specifically tailored training is provided to data managers and senior managers.

For information on how Ambrey prevents and deals with any data breaches please refer to the Data Breach Policy

If Ambrey share information ('data') with you and you have agreed to operate within the GDPR Regulation guidelines the manner in which Ambrey use this information is set out in this policy.

This Privacy Policy explains the following:

- The types of data that we might collect
- How we store and handle that data
- How we keep data safe
- How we communicate our data processes
- The legal basis on which we manage your data

- How we ensure a high quality of data through keeping the information we store up to date
- How we routinely and securely dispose of personal data in line with timescales stated

Ambrey commit to:

- Managing your data responsibility IAW this Policy and Annexed Compliance Statement
- Routinely reviewing all policy and procedure annually inclusive of data management
- Not removing your data from our systems without your explicit consent to do so
- Not processing unnecessary data about you or keeping any information pertaining to you that is not necessary to our requirements
- Not sharing any personal data for purely marketing purposes without express permission to do so

If you have any queries, questions or would like to report an issue regarding this policy, please contact us: privacy@ambrey.com / +44 (0) 203 503 0330

2. Who we collect data from & why we collect it

When using the term "personal data" in our Privacy Policy, we mean information that relates to you and allows us to identify you, either directly or in combination with other information that we may hold. Your personal data includes, for example, your name, your contact details or data from when you interact with us.

We collect personal data from you, for example when you work with Ambrey, use our website, use our services or simply contact us. We may also receive your personal data from our suppliers who provide services to you on our behalf (for example when you provide feedback on our services).

We collect, process and issue information/data from the stakeholder groups listed below:

- This is on an individual or company basis

Businesses	Clients	Vessels	Personnel
Shipping Agents	Vessel Owners	Owned	Full Time Employees
Licencing Bodies	Vessel Charterers	chartered	Temporary Employees
Manpower Providers	Vessel Sub Charterers		Consultants
Employment Agencies	Vessel Pool managers		Operational Personnel – security & safety
Flag State Authorities	Vessel Masters		Marine Crew
Insurance Providers	PMSC's		Contractors
IT Providers	Brokers		
Financial Services			
Legal Services			
Certifying / Accrediting Bodies			
Audit Facilitators			

- Note1: All stakeholders listed are Data Processers.
- Note2: Ambrey Senior Management are Data Managers for the departments they run
- Note3: Ambrey department staff are Data Processers.

The nature of the maritime and risk management business means that we have to process and share relevant data on a daily basis, because every task / project is different, and we work with many different suppliers, partners, sub-contractors and clients all over the world.

Each group of stakeholders (clients, people, third-party organisations) has a Data Manager who also acts as the responsible data controller for that particular group.

If you have any queries regarding how Ambrey manage data, you can get in touch at any time privacy@ambrey.com.

3. Categories of data we collect

Special categories of personal data – is more sensitive data and so needs greater protection. Special category data is similar to the concept of 'sensitive personal data' under Data Protection Act 1998 (now superseded by the Act) and includes one of the following types of data:

- Racial or ethnic origin;
- Political opinions;
- Religious or philosophical beliefs;
- Trade union membership;
- Genetic or biometric data processed for the purpose of uniquely identifying an individual;
- Health data;
- Data concerning an individual's sex life or sexual orientation.

The law on data protection sets out several different reasons for which a company may collect and process your personal data, including:

Consent

- We can collect and process data with consent. When collecting and processing personal data we do so in accordance with the necessary requirements and in compliance with GDPR
- *For example, flag approval submission of team details, quarterly declaration of deployment to insurers.*

Contractual obligations

- We need personal data to comply with our contractual obligations.
- *For example, if you want to work for us as a sub-contractor, we may need personal information about such as your employment history to make sure you are qualified to meet the requirements expected from our clients and industry supply chain.*

Legal compliance

- If the law requires us to, we may need to collect and process an individual's data.
- *For example, we can pass on details of people involved in fraud or other criminal activity affecting the Company to law enforcement.*

Legitimate interest

- In specific situations, we require an individual's data to pursue our legitimate interests in a way which might reasonably be expected as part of running our business and which does not materially impact their rights, freedom or interests.
- *For example, if you are a subcontractor who has worked for us before, we may use your email address to contact you about future employment opportunities.*

We may collect and process the following categories of information:

Categories of personal data processed	When do we process the personal data mentioned?	Which legal basis do we rely on for processing your personal data?
Your name and surname and your contact details	When you interact with one of our IT systems	We base the processing on our legitimate interest in running our daily business and being able to provide you with our services.

(email address, job title, telephone number, postal address, passport & NOK information) IT account login details (staff/consultants only)	When you interact with one of our staff When you order or use one of our services	When you order or use one of our services, our processing is based on us being able to fulfil the supply or contractual agreement / order with you.
Information about your (industry) course or event (audits/Cx/Op meetings) bookings, if you require special assistance or if you have specific dietary requirements.	When you book or manage your participation	We base the processing on our legitimate interest in running our daily business and being able to provide you with our services. Insofar as we receive any sensitive information from you, e.g. information on your health or religion, our processing will be based on consent, which we will ask you to provide upon receiving the information. In respect of your ordering of courses and events we may also process you information based on us being able to fulfil the agreement with you for delivering these services.
Your public CV profile covering the professional part.	When you act as a speaker or associated contributor at an Ambrey event	We base the processing on our legitimate interest in being able to inform our clients / workforce (staff/operational personnel) of your credentials relevant to the event you are speaking or contributing to.
Information about your use of our contracts and related transactions	When you use contractual agreements with Ambrey	We base the processing on our legitimate interest in running our daily business and being able to assess how our services are used.
Records about your role within the Ambrey Group and on behalf of Ambrey Group business	When you conduct business on behalf of the Group or others associated with the Group	We base the processing on our legitimate interest in running our daily business in the most efficient way.

Information about your transactions, including bank details and payment card details	When you purchase Ambrey products or services	We base the processing on us being able to fulfil the purchase agreement or service order with you.
Information about your personal financial, tax and insurance details	When you are contracted to the Ambrey team	We base the processing on us being able to fulfil the payment terms of your contracted agreement with us.
Your communications with us (for example, your emails, letters, telephone calls)	When you contact Ambrey or you are contacted by Ambrey	We base the processing on our legitimate interest in running our daily business and being able to provide you with our services.
Pictures or videos taken at Ambrey events which may include you. Pictures taken during delivery of Ambrey services which may include you. Pictures taken by you during delivery of Ambrey services.	When you participate in a Ambrey event or course or when delivering Ambrey services	We will base the processing on consent, which we will ask you to provide if relevant. In certain circumstances, we may however base the processing on our legitimate interest, if the pictures or videos are of a situational character and does not specifically depict you.
Your posts and messages on social media directed to Ambrey	When you interact with us on social media	We base the processing on our legitimate interest in running our daily business and being able to provide you with our services. We ask that you do not disclose sensitive information such as health information in messages on our social media platforms. If you do so anyhow, we reserve the right to delete such information from platforms we control, unless we have a legal basis

		such as your consent to process the information.
Feedback	When you reply to our requests for feedback or, on occasion participate in company surveys	We base the processing on our legitimate interest in running our daily business and being able to provide you with our services.
Information about how you use our website, from where you access it and what system you use when accessing it and interactive commentary you partake in when using our web based services.	When you navigate to and on our website www.ambrey.com When you navigate to and on our platforms: Fathom, Guardian, Sentinel	We process this information based on your consent and compliance
Information that relates to the services you provide to Ambrey	When you obtain, renew or cancel contractual arrangements with Ambrey	We base the processing on our legitimate interest in running our daily business and being able to provide you with our services.
Historic data	When you no longer hold contractual arrangements with Ambrey	We base the processing on our legitimate interest in being able to document Ambrey history and required reporting to external bodies for audit and legal purposes

4. How we use your personal data

We use your personal data for the following purposes:

In the provision of professional services

When you ask for advice, participate in our delivery of services (ie. commercially, operationally or via training), when attending events or meetings (ie. workshops, audits), when you use our website or products or when recording quarterly / annual statistics / reports, we use your information to perform our services in relation to any of the above. For example, to answer an enquiry, to issue an invoice, to determine who created a contract or to issue an exam certificate.

To communicate with you and manage our business requirements

Occasionally we may need to contact you by email or phone for administrative, commercial or operational reasons. For example, in order to send you information related to your involvement in our delivery of services, invoices, confirmation of bookings and payments, or to notify you of information relevant to the delivery of services (routine and non-routine). Notifications are for

information sharing purposes relevant to the industry and not for marketing purposes.
Your opinion is very important to us, so we may contact you for feedback.
We will use your communications with us and the feedback you may provide in order to manage our relationship with you and to improve our services and experiences for all parties we work with to deliver our business.

To personalise and improve your business experience

We may use your personal data in order to develop our services. For example, if you inform us about your role in the industry and have consented to receive marketing communications, we will be able to send you information relevant to your part of the delivery of our business. (via email or our website).

To share news and information that may be of interest to you

If you have given us your consent to receive marketing material, we may send you marketing communications. *For example, distribution of our Intelligence products.*
Please note that we do not share your contact details or other personal data with other companies for marketing purposes, unless we have first obtained your written consent to do so.
If you do not want to receive communications / notifications from us, you can simply tell us so by contacting us: privacy@ambrey.com / +44 (0) 203 503 0330.
You can also choose to opt out from receiving marketing communications at any time.

To improve services, fulfil our administrative purposes, protect our business interests

The business purposes for which we will use your information include, but are not limited to, accounting, billing and audit, credit or other payment card verification, fraud screening, safety, security and legal purposes, statistical and marketing analysis, systems testing, maintenance and development of our products and services.

Compliance purposes

We may also use your personal data for the following:

- A legal obligation which requires processing by law or in order for us to be able to establish, enforce, or defend against legal claims.
- Insurance reporting and management procedures
- Audit and due diligence purposes

5. Your rights

You have legal rights under EU data protection legislation.

Below is a summary, to read the full regulation refer to the General Data Protection Regulation (Regulation (EU) 2016/679) https://gdpr-info.eu/ sections 3–5:

- Access rights. You are entitled to be informed as to whether Ambrey is processing personal data about you. If we are, you are entitled to information regarding, among other things, which personal data we are processing, the purposes of the processing, which external recipients have access to your personal data, and how long we save your personal data.
- Data portability rights. You have a right to receive a copy of the personal data which you have provided to Ambrey, in a structured, commonly used, and machine-readable format. You also have the right to require that Ambrey transfers this personal data to another controller of personal data. The right to data portability applies to personal data which is processed in an automated manner and which is based on your consent or on an agreement to which you are a party.
- Correction of wrong or incomplete data. You have a right to request that Ambrey corrects erroneous or incomplete information about you.
- Deletion of data. You have a right to require Ambrey to delete your personal data under certain circumstances, for example where the personal data is no longer necessary for the purpose for which we collected it.

- Right to object to processing of data. You have the right, under certain circumstances, to object to Ambrey's processing of your personal data.
- Right to object to direct marketing. You have the right at any time to object to Ambrey processing your personal data for direct marketing purposes. If you object to such processing, Ambrey must discontinue all direct marketing to you without undue delay.
- Right to restrict the processing of personal data. You have the right to require Ambrey to restrict its processing of your personal data in certain circumstances. For example, if you have denied that your personal data is correct, you can request a restriction on the processing during a period of time which allows Ambrey to verify whether the personal data is correct.
- Right to withdraw consent for use of data. If our processing is based on your consent, you have the right to withdraw your consent to our processing of your personal data at any time. Such withdrawal does not affect the lawfulness of our processing based on your consent before its withdrawal.
- Complaints. If you have any complaints regarding Ambrey's processing of your personal data, you are entitled to file such complaints with the Data Protection Authorities (Information Commissioners Office – ICO - https://ico.org.uk/)

6. Security of your personal data

- Ambrey are committed to taking appropriate technical and management measures to protect your personal data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data that we hold / process about you.
- Ambrey identifies, assesses and manages information security risks. Please refer to the Information Security Policy for further detail.
- Ambrey provides regular information security awareness training for all staff, including temporary, locum or contracted employees, to ensure they are all aware of and fulfil their responsibilities.
- When you provide your personal data to us, this information is held on a secure private cloud and associated financial software. Entry to this software is on a 'need to' basis prevent unauthorised physical access, damage and interference to personal data and to provide the minimum access to information.
- Ambrey has appropriate password security procedures and 'rules' for information systems and has a process in place to detect any unauthorised access or anomalous use.
- All Ambrey hardware has been identified, documented and classified its hardware and software assets and assigned ownership of protection responsibilities and the security of mobile working and the use of mobile computing devices. All Ambrey hardware is configured to reduce vulnerabilities and to ensure it provides only the functionality and services required. *For example anti malware software on laptops provided to staff.*
- As described in this Privacy Policy, we may disclose your personal data to third parties when delivering our business services. Any third party Ambrey discloses your personal data to has been issued a compliance statement requesting / requiring the data is managed in line with the EU Regulation.
- The information that you provide to us will be held on hosted systems not owned by us, which are located in premises of an appointed third party within the EU.
- We may also allow access to your information by our employees who act as data processors on our behalf for the purposes described in this Privacy Policy or for other purposes for which your consent or compliance has been granted.
- Ambrey has a process to securely dispose of records and equipment when no longer required.
- Ambrey routinely backs-up electronic information to help restore information in the event of disaster.

7. Retention of personal data

We will retain your personal data for as long as we need it in order to fulfil our purposes set out in this Privacy Policy.

We may also save your personal data for a longer period of time where necessary in order to fulfil the following:

- A legal obligation which requires processing by law or in order for us to be able to establish, enforce, or defend against legal claims.
- Insurance reporting and management procedures
- Audit and due diligence purposes

8. Website

Ambrey use Google Analytics and our website collects visitor data to analyse traffic on our sites. This information helps us understand your interests and helps us improve our website.

When you visit our site www.ambrey.com or MRI Platform https://ambrey.maps.arcgis.com/ or any other Ambrey platforms, the pages that you look at, and a short text file called a cookie, are downloaded to your computer. A cookie is used to store small amounts of information. This information is collected for traffic analysis only. The cookie does not contain personal details. Depending on the browser that you use, you can set your preferences to block/ refuse cookies, and/ or notify you before they are placed.

We do not use your data for market research or advertising purposes.

9. Storing data

All electronic data is kept securely on Ambrey local and cloud platforms.

Our IT management team follow our compliance policies regarding data processing at a minimum in the following IT environments, where applicable:

  - Live
  - Development
- All Ambrey staff follow strict security policies for system access and data storing
- All Ambrey stakeholders have the relevant access and visibility of our systems
- Our chosen suppliers have controlled access to maintain and upgrade our systems to ensure security and maintenance patches are regularly applied. As required, Ambrey share the minimum personal data with these stakeholders in order for them to support and assist us to provide the Ambrey Group with an effective and secure IT Service.
- Ambrey ensure the IT stakeholders give their employees appropriate access to our systems and follow strict access termination procedures if required.
- Ambrey servers are located within the UK and abide by EU Data processing and GDPR regulations. Examples of servers and locations below:
  - Microsoft servers (SharePoint, Outlook & Sonar7/Databases) - Cardiff or London.
  - Microsoft backup servers – Cardiff or London.
  - PeopleHR (HR management system) - London.
  - Mimecast (archive emails) - London
- Any data deemed to require removal or following request to withdraw consent from Ambrey systems will be by the Legal, HR, Compliance and IT teams
- In the instance that data recovery from our encrypted backups is ever required it will be cross-referenced by the IT team to ensure any removal requests / withdrawal of consents are actioned appropriately and immediately purged as required upon restoration.
- All non electronic data is kept securely and routinely disposed of by a professional paper shredding company certified in the secure removal of sensitive documents.

    - All personnel are responsible for their own hard copy records at all times. Appropriate storage of these is managed by individuals. Lockable desk drawers and filing cabinets are available. Hard copy records should not be left on desks, in unattended areas or shared inappropriately with other.
- Appropriate environmental controls are in place to prevent excessive paper storage. For example two sided printing, adequate electronic storage space

10. Sharing Data

- Data is not shared for marketing purposes
- It is often necessary for Ambrey to share personal information with companies we are working with for clarity purposes – for example employment history, background checks.
- There is clear accountability for the member of staff sharing the information
- Training and policies are in place to ensure guidance is provided to all staff that clearly set out when it is appropriate for them to share or disclose data.
- Only information necessary for us to fulfil contractual obligations, meet legal, employment, regulatory requirements or flag state approval and for company security purposes will be shared.
- Ambrey SOPs are released to relevant personnel at release along with a read and understood receipt request and permission to share relevant data. Ensuring all individuals are aware of any information that may be shared about them and their express permission for this to happen has been received.

11.Removal and Disposal of Data

- Ambrey staff are responsible for the continuous cleansing of data
- Records that are out of data or no longer needed are identified during regular annual reviews and anything out of date or unnecessary is deleted from the system. An annual process of removing archive data to a 'Deep Archive' secure electronic vault with restricted access is maintained. Deep Archive is then reviewed / cleansed of out of date or unnecessary data.
- Ambrey has a confidential waste disposal scheme ensuring all sensitive data is shredded and disposed of safely.
- Employee data will be deleted after the appropriate length of time according to GDPR

12. Transfers of personal data outside of the EU/EEA

Your personal data will be processed within our global IT systems and by staff primarily within the EU/EEA. Ambrey are continually upgrading to the latest technologies & processes to ensure all electronic data shared externally is secure & controlled.

Ambrey's third party supply chain will be required to hold data for specific processes for a specific timeframe in and outside the EU/EEA. For example, flag states, medical management response teams, commercial client entities, shipping agents.

13. Updates to our Privacy Policy

We will make changes to this Privacy Policy as required. This policy has been written to the guidelines of the new European data protection legislation which came into force on 25 May 2018 (the "General Data Protection Regulation").

Ambrey commit to:

- Routinely reviewing all policy and procedure annually and interim reviews as per exception and requirement.

If you have questions in relation to your personal data, how it is stored or would like to submit a request for an extract from the register, data portability, correction, deletion, objection, restriction or withdrawal of consent, contact us at privacy@ambrey.com

Jan 2021 Additional Section:

The UK has left the EU.

Receiving personal data from the EU/EEA and already adequate third countries

The EU-UK Trade and Cooperation Agreement contains a bridging mechanism that allows the continued free flow of personal data from the EU/EEA to the UK after the transition period until adequacy decisions come into effect, for up to 6 months. EU adequacy decisions for the UK would allow for the ongoing free flow of data from the EEA to the UK.

As a sensible precaution, during the bridging mechanism, it is recommended that you work with EU/EEA organisations who transfer personal data to you to put in place alternative transfer mechanisms to safeguard against any interruption to the free flow of EU to UK personal data.

For most organisations, the most relevant of these will be Standard Contractual Clauses (SCCs). The ICO also provides more detailed guidance on what actions might be necessary and an interactive tool that allows you to build SCCs.

11 of the 12 third countries deemed adequate by the EU are maintaining unrestricted personal data flows with the UK. Further information can be found on the ICO's website.

EU-UK Trade and Cooperation Agreement interim bridging mechanism for personal data

The UK regained full autonomy over its data protection rules from 1 January 2021. The EU-UK Trade and Cooperation Agreement bridging mechanism for personal data (Part Seven, Article FINPROV.10A) operates on the basis of UK law, as it stands on 1 January, and with some restrictions on the UK's use of international data transfer powers.

The provision includes mechanisms to enable the UK to make changes to its data protection regime or exercise international transfer powers, subject to mutual agreement, without affecting the bridging mechanism. The EU does not have the power to block changes to its framework or use of its powers. If the EU objects to changes, and the UK anyway makes them, the bridge will end.

For personal data flows from the UK

There are currently no changes to the way you send personal data to the EU/EEA, Gibraltar and other countries deemed adequate by the EU. If this situation changes, information will be updated.

For international data transfers from the UK to other jurisdictions, further information can be found on the ICO's website.

Associated Annexes:

- Cookie Policy
- Data Compliance Statement
- Data Breach Policy
- Data Breach Process
- Data Masking Policy
- Data Retention Ploicy

Associated Documents:

- Group Information Security Policy and ISMS (Information Security Management System)

Appendix 1 [July 2022].
Microsoft Teams Meetings.

Recording of Meetings.

We sometimes record meetings that we hold within Microsoft Teams, to provide a record of discussions and agreements held within the meeting.
You will be informed (normally verbally) in the meeting that the session will be recorded prior to any recording taking place.
The recording could contain:

- Your video stream (including images of yourself), if you choose to enable your video device during the meeting
    - Anything or anyone else that may be in the background could be recorded. You can choose to put up a background in Microsoft Teams meetings to stop any additional pictures of your home being recorded.

- Your audio stream, if you choose to enable your audio device during the meeting
    - This could include any opinions you contribute and anything you say about yourself.

- Sometimes, chat within the meeting could also be captured in the meeting recording
    - Therefore, anyone attending the recorded meeting may have aspects of their personal data recorded, if they actively participate or not.

We use meeting recordings to produce:

- Informal notes of any discussions in the recorded meeting
- Formal records of any discussions, actions, agreements, or decisions in the recorded meeting

These formal and informal records will take the form of written, digital content.
Meeting recordings can be viewed by authorised people in Ambrey. A meeting recording may also be viewed by meeting invitees who were unable to attend.
The legal basis for processing will be related to the topic and data in any agreed meeting recording, the most likely being, but not limited to:

- Explicit consent is given by participants
- Processing necessary to ensure compliance with a legal obligation
- Processing necessary for the performance of a contract to which the data subject is a party
- Processing relating to a task carried out in the public interest

Disclosing your information

We may pass on your personal information if we have a legal obligation to do so, or if we have to enforce or apply our terms of use and other agreements. This includes exchanging information with other government departments for legal reasons.
We won't share your information with any other organisations for marketing, market research or commercial purposes.

Keeping your information secure

Meeting recordings will typically be deleted after 30 days if there is no further need to retain them.
Recordings are securely stored within the EU and will be appropriately and securely deleted when no longer required.

Who views this information?

These Microsoft Teams recordings will be made available to other staff within Ambrey to support their practice.
Therefore, anyone who works for Ambrey or who has been co-opted or contracted to work for Ambrey, may view the recordings.

Process summary:

- Inform participants the meeting is recorded
  - A banner is also visible on screen
- Once the meeting is complete, the recording will be shared with all participants in the chat window. You will also see all your recording available in your online OneDrive folder; to get there from the Ambrey home page click on the App menu, OneDrive, then under My Files open the Recordings folder to see them listed.
- File retention and expiration
  - the default retention period for recorded meetings is 30 days; after this time the file will be deleted. If required, you can extend the expiration date of each file in the file's details menu.

Appendix 2 [July 2022].
Stakeholder Screening.

Stakeholders (or interested parties) are companies or individuals (or vessels) the Ambrey Group works with externally.

Screening processes established for the following:

- Sanctions (Trade & Financial)
- Anti-Money Laundering (AML)
- Politically Exposed Persons (PEPs)

We screen to:

- Ensure financial, corporate & reputational integrity & best practice.
- To minimise financial, corporate & reputational risk to the Group.
  - We are obligated to work IAW UK sanctions & embargoes.
  - We are obligated to work IAW relevant International sanctions & embargoes.

We are obligated to screen:

- Initially on first contact
- On a routine basis

External Stakeholders	Contracted Operational Personnel	Shore Based Personnel
Clients	All Ambrey contractors	All Ambrey personnel
Suppliers	Guards	
Partners	Crew	Shore based personnel are responsible for initial screening of new stakeholders and are responsible for providing stakeholder information to the Compliance team for on going screening.
Vessel Owners Vessels	Contractor screening in place: (c/o the Personnel Team) • Qualifications	The Compliance team are responsible for on going screening of Ambrey Group stakeholders and feeding the

	• Health • Training	results back to the shore based personnel responsible for the stakeholder.
Certification Bodies Authorising Bodies Financial Providers Insurance Underwriters	Screening in place: (Compliance Team / Personnel Team) • Sanctions & Terrorism	

All Ambrey personnel who manage Stakeholders are responsible for screening the stakeholders they manage.
1. 100% of NEW stakeholders MUST be screened & records filed.

2. Routine (on going) screening will also be completed for EXISTING Stakeholders.
This is completed by the Compliance/Legal team based on information supplied by all personnel & outcomes fed back to Stakeholder Managers.

- Reports containing alerts are escalated to the Compliance & Legal Teams for review & decisions.
  - Escalation to Group owners as required.

All stakeholders are assigned an Ambrey Stakeholder Identification Number.

The Stakeholder screening Management System is located: 21. Compliance/ Stakeholder Screening

Appendix 3 [Jan 2023].
Data Control Cttee, Ambrey Group.

Establishment of a cross group committee with the purpose of monthly meetings to review:

- Policy changes
- Procedure / process changes
- Incidents (incl breaches)
- Root Cause
- Complaints (incl data access requests – DSAR/)
- Privileged Access Review (General Staff/IT Administrators)
- Planning
- ISMS review and maintenance
- Status of comms privacy@ambrey.com

The committee file records of meetings and members are the Technology & Innovation and Compliance Teams. The cttee will liaise with teams across the Ambrey Group.

21. Compliance / InfoSec & Privacy/Data Cttee

Footnote:

- Microsoft Privacy Statement
- https://privacy.microsoft.com/en-GB/privacystatement#mainnoticetoendusersmodule