DOCUMENT DETAIL

Document Title	AET Data Protection Policy	
Document Version / Date	Rev. No: 2.0	Rev. Date: 21/06/2024
Document Status	Approved	
Process Owner	General Counsel & Chief Integrity Officer	
Document Id/ Reference	Legal-LAI-AET Data Protection Policy	

DOCUMENT CLASSIFICATION

DOCUMENT SECURITY	
Secret	
Confidential	
Internal use	X
Open	

DOCUMENT STRUCTURE	
Level 1: Policy	
Level 2: Standards / Guidelines / Framework	X
Level 3: Manuals / Procedures / Work Instructions	
Level 4: Records	

DOCUMENT REVISION HISTORY

REV NO.	DATE	REVISION DETAILS	AUTHOR
0.0	25/05/2018	New Document	Global Director, Legal
1.0	31/07/2020	Inclusion of the sentence 'In the event of a conflict between this policy and local laws, local laws will prevail.'	Global Director, Legal
2.0	21/06/2024	• Streamlined document format with MGMF. • Changed the document process owner title due to business realignment. • Update Division reference to reflect current organisation structure. • Section 4: Scope - amend sentence of "In the event of a conflict between this policy and local laws, local laws will prevail." to "In the event of a conflict between this policy and local law, contact The Legal & Integrity department of AET immediately. As a general rule, AET will apply whichever is stricter and always on the basis that AET remains in full compliance with applicable laws."	General Counsel & Chief Integrity Officer

Table Of Contents

1.0 Terms & definitions

Table 1: Terms and definitions

Term	Definition
Automated Processing	is any form of automated processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of Automated Processing.
Data Controller	the person or organisation that determines when, why and how to process Personal Data. It is responsible for establishing practices and policies in line with the relevant global legislation. AET are the Data Controller of all Personal Data relating to our business and Personal Data used in our business for our own commercial purposes.
Data Subject	a living, identified or identifiable individual about whom we hold Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data.
EEA	the 28 countries in the EU, and Iceland, Liechtenstein and Norway.
General Data Protection Regulation	the General Data Protection Regulation ((EU) 2016/679), being legislation enacted under the laws of the European Union. Personal Data is subject to the legal safeguards specified in the GDPR.
Personal Data	any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other

Term	Definition
	identifiers we possess or can reasonably access. Personal Data includes Sensitive Personal Data and Pseudonymised Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.
Personal Data Breach	any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach.
Privacy by Design	implementing appropriate technical and organisational measures in an effective manner to ensure compliance with relevant legislation.
Privacy Impact Assessment	tools and assessments used to identify and reduce risks of a data processing activity. DPIA can be carried out as part of Privacy by Design and should be conducted for all major system or business change programs involving the Processing of Personal Data.
Privacy Notices (also referred to as Fair Processing Notices) or Privacy Policies	separate notices setting out information that may be provided to Data Subjects when the Company collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals (for example, employee privacy notices or the website privacy policy) or they may be stand-alone, one time privacy statements covering Processing related to a specific purpose.

Term	Definition
Processing or Process	any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties.
Pseudonymisation or Pseudonymised	replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure.
Related Policies	the Company's policies, operating procedures or processes related to Policy including AET's Data Protection Procedure.
Sensitive Personal Data	information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and Personal Data relating to criminal offences and convictions.

1.1 Abbreviations

Table 1.1: Abbreviations

Abbreviation	Term
EEA	European Economic Area
GDPR	General Data Protection Regulation
PIA	Privacy Impact Assessment

2.0 Language Convention

In this document, the use of:

- The word "shall" indicate a course of action that is required or mandatory. The English language equivalent or interchangeable term for "shall" is "must",
- The word “should” indicate a preferred course of action,
- The word "may" indicate a possible course of action.

3.0 Objective

AET is committed to all aspects of data protection and takes seriously its duties, and the duties of its employees, under Data Protection legislation throughout the world. This policy sets out how AET deals with personal data of our Employees, customers, suppliers and third parties including personnel files and data subject access requests, and employees' obligations in relation to personal data.

This policy applies to all Personal Data regardless of the media on which that data is stored or whether it relates to past or present Employees, customers, clients, suppliers, shareholders, website users or any other person on whom Data is processed.

4.0 Scope

This Policy covers all individuals working on shore and off shore at all levels and grades on behalf of any Company within the AET Group in any capacity whatsoever, including without limitation, the senior management team, employees, consultants, contractors, trainees, homeworkers, part-time and fixed-term employees, casual and agency staff, and volunteers (collectively referred to as “Employees” throughout this Policy).

This Policy does not form part of any Employee's contract of employment and AET may amend it at any time.

In the event of a conflict between this policy and local law, contact The Legal & Integrity department of AET immediately. As a general rule, AET will apply whichever is stricter and always on the basis that AET remains in full compliance with applicable laws.

5.0 What is AET's data protection Policy?

AET is committed to complying with the applicable data privacy and security requirements in the countries in which it and its subsidiaries operate. Because of differences among these jurisdictions, AET has adopted a Data Protection Policy which creates a common core of values, policies and procedures based on the most stringent law globally (predominantly the GDPR) and intended to achieve compliance across our global offices.

Protecting the confidentiality and integrity of Personal Data is a critical responsibility that AET must take seriously at all times. AET is exposed to potential fines of up to EUR20 million (approximately US$25 million) or 4% of total worldwide annual turnover, whichever is higher and depending on the breach, for failure to comply with the provisions of the GDPR.

This Policy supplements but does not supersede nor replace any data protection obligations set out in an Employee's terms and conditions of employment, any consent for processing which the Employees may have previously provided to AET nor does it affect any right that AET may have at law in connection with the collection, use, disclosure, retention and/ or transfer of the Personal Data.

6.0 The Data Protection Officer

The AET Data Protection Officer (DPO) is responsible for overseeing this Policy and, as applicable, developing related procedures. Employees may consult the Legal Department to determine who the current DPO is.

Please contact the DPO with any questions about the operation of this Policy, the supporting procedures, or if you have any concerns that this Policy is not being or has not been followed.

7.0 What is “Personal data”

This Policy applies only to information that constitutes "Personal Data". Personal Data means data related to an individual (known as a ‘Data Subject’):

- who can be *identified* from the data in the possession of the Data Controller (or from such data which together with other information in the possession of, or likely to come into the possession of); and

- which affects that person's *privacy* (whether in his/her personal or family life, business or professional capacity) in the sense that the information has the person as its focus or is otherwise *biographical* in nature.

Any automated and computerised personal information held about a Data Subject or information stored physically (for example, on paper) which is held in a "relevant filing system" is covered by this Policy.

8.0 What is “Sensitive personal data”

"Sensitive personal data" is information about a Data Subject's:

- racial or ethnic origin;

- political opinions;

- religious beliefs or other beliefs of a similar nature;

- trade union membership;

- physical or mental health or condition (including sickness and injury records);

- sexual history or orientation;
- commission or alleged commission of any criminal offence; and
- proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings.

In accordance with our obligations under global legislation, AET maintains strict guidelines on how and why Sensitive Personal Data can be processed.

9.0 What is Processing?

This Policy applies to Personal Data that is "processed". Processing covers a wide variety of operations including:

- obtaining personal information
- retaining and using personal information
- allowing personal information to be accessed
- disclosing personal information
- disposing of personal information

10.0 AET's data protection principles

AET has adopted eight data protection principles (which align with the GDPR) which are to be followed when handling Personal Data. These principles require that Personal Data must:

1. only be processed fairly and lawfully;

2. only be obtained for specified, explicit and legitimate purposes and shall not be processed in any manner incompatible with those purposes;

3. be adequate, relevant and not excessive in relation to the purpose for which it is collected or processed;

4. be accurate, complete and up to date;

5. not be kept longer than is necessary;

6. be secure;

7. not be transferred to countries without adequate protection; and

8. be processed in accordance with individuals' rights.

The information below sets out in more detail each of AET's data protection principles:

First	Processing and the use of Personal Data	This Policy is not intended to prevent the processing of Personal Data, but to ensure that it is done fairly, in accordance with the law of the relevant jurisdiction and without adversely affecting the rights of the individual about whom the data relates to. The law (including GDPR) allows Processing for specific purposes. The main purposes which AET rely on are set out below: a. the Data Subject has given his or her Consent; b. the Processing is necessary for the performance of a contract with the Data Subject;

		c. to meet AET's legal compliance obligations; d. to protect the Data Subject's vital interests; or e. to pursue our legitimate interests for purposes where they are not overridden because the Processing prejudices the interests or fundamental rights and freedoms of Data Subjects. The purposes for which we process Personal Data for legitimate interests need to be set out in applicable Privacy Notices or Fair Processing Notices. Before processing Personal Data, Employees should satisfy themselves that the Processing they intend to carry out is covered by one of the Purposes set out above. In the event of doubt, please seek guidance from the Data Protection Office. Data Subjects must be easily able to withdraw Consent to Processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if you intend to Process Personal Data for a different and incompatible purpose which was not disclosed when the Data Subject first consented. Where explicit consent is required, it should be obtained in accordance with the procedure set out in the Data Protection Procedure. It is the policy of AET to rely on other legal basis for Processing, instead of consent, wherever possible. In general, AET will not unreasonably retain or process Sensitive Personal Data without the explicit consent of the Data Subject. However, there are

		circumstances which allow AET to collect, process and disclose Sensitive Personal Data without explicit consent. These include for the purpose of carrying out AET's obligations and rights relating to the employment of the Data Subject; in order to establish, exercise or defend legal claims; or for preventive or occupation health.
Second	Purpose Limitation	Employees cannot use Personal Data for new, different or incompatible purposes from that disclosed when it was first obtained unless they have informed the Data Subject of the new purposes and they have Consented where necessary.
Third	Data Minimisation	Employees may only Process Personal Data if it is required for the true performance of their job duties and should not collect excessive data. Employees cannot Process Personal Data for any reason unrelated to their job duties. Employees must ensure that when Personal Data is no longer needed for specified purposes, it is deleted or anonymised in accordance with AET's Data Protection Procedure.
Fourth	Accuracy	Personal Data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate. Employees are expected to check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards in accordance with the AET's Data Protection Procedure.
Fifth	Storage Limitation	Employees must not keep Personal Data in a form which permits the identification of the Data Subject for longer than needed for the legitimate business purpose or purposes for which AET originally

		collected it including for the purpose of satisfying any legal, accounting or reporting requirements. Employees should avoid storing their own personal data on company property including their laptops. Examples of documents likely to contain personal data include personal emails, bank statements, payslips, passports, tenancy agreements, passwords, CVs and insurance policies. AET reserves the right to permanently delete personal documents from any company property without notice to the Employee. Employees must following the procedures on data retention set out in the AET's Data Protection Procedure.
Sixth	Security Integrity And Confidentiality	Personal Data must be secured by appropriate technical and organisational measures against unauthorised or unlawful Processing, and against accidental loss, destruction or damage. AET will develop, implement and maintain safeguards appropriate to our size, scope and business, our available resources, the amount of Personal Data that we own or maintain on behalf of others and identified risks. Employees must follow all procedures and technologies AET puts in place to maintain the security of all Personal Data from the point of collection to the point of destruction. Employees must comply with and not attempt to circumvent the administrative, physical and technical safeguards AET implements and maintains and relevant standards to protect Personal Data.

		Employees must exercise particular care in protecting Sensitive Personal Data from loss and unauthorised access, use or disclosure.
Seventh	Transfer Limitation	The law restricts data transfers to different countries, and particularly from countries within to outside the European Economic Area (EEA), in order to ensure that the level of data protection afforded to individuals is not undermined. Employees must follow the procedures set out in AET's Data Protection Procedure when they transmit, send, view or access data originating in one country in a different country.
Eight	Data Subject's Rights And Requests	Data Subjects have rights when it comes to how we handle their Personal Data. These include rights to: a. withdraw Consent to Processing at any time; b. receive certain information about how AET is processing their data c. request access to their Personal Data that AET hold (see Subject Access Request below); d. prevent AET's use of their Personal Data for direct marketing purposes; e. ask AET to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or Processed or to rectify inaccurate data or to complete incomplete data; f. restrict or challenge Processing in specific circumstances;

		g. request a copy of an agreement under which Personal Data is transferred outside of the EEA; h. object to decisions based solely on Automated Processing, including profiling (ADM); i. prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else; j. be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms; and k. make a complaint to the supervisory authority; Employees must immediately forward any Data Subject request you receive to the DPO and should exercise extreme caution to ensure that the identification of the individual submitting the request has been verified.

11.0 Reporting A Personal Data Breach

AET is required to notify any Personal Data Breach to the applicable regulator and, in certain instances, the Data Subject.

AET have put in place procedures to deal with any suspected Personal Data Breach and will notify Data Subjects or any applicable regulator where we are legally required to do so.

There are extremely short timescales for notification which AET must comply with and thus, if an Employee knows or suspects that a Personal Data Breach has occurred, they must notify the DPO or Legal Department ***immediately***. Employees should preserve all evidence relating to the potential Personal Data Breach and should not attempt to investigate the matter themselves.

12.0 Privacy By Design and Privacy Impact Assessments (PIA)

AET have an obligation to ensure appropriate Privacy by Design measures have been considered and implemented for all projects, programs, systems and processes.

Where it is determined that the processing which is being carried out is considered 'high risk' or when implementing major system or business change programs involving the Processing of Personal Data, AET must carry out a PIA. Employees are required to notify the DPO if they become aware of any processing which is or may become 'high risk'. Employees should follow the procedure for completing a PIA as set out in AET's Data Protection Procedure.

13.0 Automated Processing (including Profiling) And Automated Decision-Making

It is AET's policy not to undertake any Automated Processing or Automated Decision Making.

If an Employee, on behalf of AET, becomes aware that Automated Processing or Automated Decision Making is taking place or is about to be commenced they must consult the DPO as soon as possible.

A PIA must be carried out before any Automated Processing (including profiling) or ADM activities are undertaken.

14.0 Direct Marketing

AET are subject to certain rules and privacy laws when marketing to our customers.

It is AET's policy not to undertake any Direct Marketing to our customers. If Employees would like to commence any Direct Marketing activities, they must contact the DPO and the Communications Department in advance.

15.0 Data Subject Access Requests

Employees are entitled to make a formal request in writing for Personal Data AET holds about them, including personnel files, sickness records, disciplinary or training records, appraisal or performance review notes, emails in which the Employee is the focus of the email and documents that are about the Employee. The Human Resources Department is responsible for dealing with data subject access requests.

AET will not charge for allowing Employees access to information about them. Following receipt of a legitimate written request from an Employee, AET will respond to any data subject access according to the law of the relevant jurisdiction and within the period set out by the law.

AET may ask the Employee to provide additional details in order to assist AET to locate the data requested. AET will allow the Employee access to hard copies of any personal information, however if this involves a disproportionate effort on the part of AET, the Employee shall be invited to view the information on-screen or inspect the original documentation at a place and time to be agreed by AET.

AET may reserve its right to withhold the Employee's right to access or delete data where any relevant statutory exemptions apply. AET reserves the right to deny unfounded, excessive, abusively burdensome or repetitive requests from Employees.

16.0 Correction, updating and deletion of Employee data

AET has an electronic system in place that enables Employees to check their personal information on a regular basis so that they can correct, delete or update any data. If an Employee becomes aware that AET holds any inaccurate, irrelevant or out-of-date information about them, they must notify the Human Resources Department immediately and provide any necessary corrections and/or updates to the information.

17.0 Employee's obligations regarding personal information

Employees must observe the data protection requirements according to the law of the relevant jurisdiction. If it is not necessary for them to retain that information, Employees should arrange for it to be transferred to and handled by the appropriate individual within AET and subsequently delete their copy of such information.
If an Employee is in any doubt about what he/she may or may not do with personal information, they should seek advice from Human Resource Department or the Legal Department.

18.0 Disclosure and sharing of personal information

AET may share Personal Data we hold with any member of the AET Group, which includes subsidiaries and AET's ultimate holding company and its subsidiaries.

It is AET's policy not to share Personal Data with third parties unless and until certain safeguards and contractual arrangements have been put in place.

AET may disclose personal data we hold to selected third parties:

- In the event that AET sell or buy any business or assets, in which case we may disclose personal data AET holds to the prospective seller or buyer of such business or assets but only to the extent necessary to conduct negotiations and then only after obtaining an appropriate non-disclosure agreement.

- If AET or substantially all of AET's assets are acquired by a third party, in which case personal data AET hold will be one of the transferred assets.

- If AET are under a duty to disclose or share Employee's personal data in order to comply with any legal obligation, or in order to enforce or apply any contract with the Employee or other agreements; or to protect our rights, property, or safety of our Employees, or others. This includes third parties such as payroll providers and manning agents.

19.0 Record Keeping

Under AET's legal obligations globally, AET are required to keep full and accurate records of all our data Processing activities by using the Internal Data Protection Register. In order to assist AET in fulfilling that requirement, Employees must keep and maintain accurate corporate records reflecting Processing which they complete on AET's behalf. This includes records of Data Subjects' Consents and procedures for obtaining Consents.

20.0 Review of procedures and training

AET will provide mandatory training to all Employees on data protection matters on induction and on a regular basis thereafter.

If an Employee considers that they would benefit from refresher training, they should contact the Human Resource Department.

21.0 Limited Effect of Policy

This Policy shall not be interpreted or construed as giving the Employee rights greater than those which such person would be entitled to under applicable laws and other binding agreements.

22.0 Consequences of non-compliance

Breach of any part of this Policy may result in disciplinary action, up to and including dismissal, in accordance with our Disciplinary Procedure. Failure to observe the data protection principles within this Policy may result in an Employee incurring personal criminal liability.

Any member of staff suspected of committing a breach of this Policy will be required to co-operate with AET's investigation, which may involve handing over relevant passwords and login details.