Data Policy

It is the responsibility of all APEM Group employees to comply with this policy and to report concerns. APEM Group prohibits any form of retaliation for the reporting of such matters.

All staff will be made aware of this statement as part of their induction on appointment and subsequent on-going training. This policy is communicated and published on the company website for all interested parties.

Reference	Version	Date released	Approved by
T1-GP-007	2	01/08/2023	Leah McGimpsey - APEM Group Chief Executive Officer
This policy is communicated and published on the company website for all interested parties.			
This policy is subject to periodic review and change to ensure it remains valid. The policy may be reviewed when prompted by context, such as developments in legislation, industry practice, or the organisation. The live version of this policy can be found on The Source and is the only version that is controlled. Any other versions either printed or embedded into other documents or web pages should be viewed as uncontrolled and as such may not necessarily contain the latest updates, amendments or linkages to other documents. This Policy has been Equality Impact Assessed and no adverse impact has been identified.			

Contents

1. Definitions

Company name: APEM Group Limited, Riverview A17 Embankment Business Park, Vale Road, Heaton Mersey, Stockport, England, SK4 3GN, Company Number 11768489.

Company Personnel: all employees, workers, contractors, agency workers, consultants, directors, members and others.

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 UK and EU GDPR. We are the Controller of all Personal Data relating to our Company Personnel 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.

Data Privacy Impact Assessment (DPIA): 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 programmes involving the Processing of Personal Data.

Data Protection Officer (DPO): the person required to be appointed in specific circumstances under the UK and EU GDPR. Where a mandatory DPO has not been appointed, this term means a data privacy manager or other voluntary appointment of a DPO or refers to the Company data privacy team with responsibility for data protection compliance.

UK and EU GDPR: the retained EU law version of the General Data Protection Regulation (*(EU) 2016/679*). Personal Data is subject to the legal safeguards specified in the GDPR.

Group Company: APEM Group Limited, its subsidiaries or holding companies from time to time and any subsidiary of any holding company from time to time.

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 identifiers we possess or can reasonably access. Personal Data includes Special Categories of 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 the GDPR.

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.

Special Categories of 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.

2. Introduction

This Data Privacy Policy sets out how APEM Group Limited and its Group Companies ("we", "our", "us", "the Company") handle the Personal Data of our customers, suppliers, employees, workers and other third parties.

This Data Privacy Policy applies to all Personal Data we Process regardless of the media on which that data is stored or whether it relates to past or present employees, workers, customers, clients or supplier contacts, shareholders, website users or any other Data Subject.

This Data Privacy Policy is an internal document and cannot be shared with third parties, clients or regulators without prior authorisation from APEM's DPO.

We recognise that the correct and lawful treatment of Personal Data will maintain confidence in the Company and will provide for successful business operations. Protecting the confidentiality and integrity of Personal Data is a critical responsibility that we take seriously at all times. The Company is exposed to potential fines of up to £17.5 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 UK and EU GDPR.

All Company Personnel are responsible for ensuring compliance with this Data Privacy Policy and need to implement appropriate practices, processes, controls and training to ensure that compliance.

APEM is not a public authority or body whose core activities involve processing personal data on a large scale and therefore does not need to appoint or register with the ICO a Data Protection Officer. However, APEM does have an internal staff member who oversees compliance with data protection regulations who will work alongside APEM's Data Protection Team and monitor internal compliance with the GDPR and our own data protection policies.

The Data Protection Team is responsible for overseeing this Data Privacy Policy and can be contacted at: data.protection@apemltd.co.uk.

Please contact the DPO or the Data Protection Team with any questions about the operation of this Data Privacy Policy or the GDPR or if you have any concerns that this Data Privacy Policy is not being or has not been followed. In particular, you must always contact the DPO and the Data Protection Team in the following circumstances:

a) if you are unsure about what security or other measures you need to implement to protect Personal Data;
b) if there has been a Personal Data Breach;
c) if you are unsure on what basis to transfer Personal Data outside the UK;
d) if you need any assistance dealing with any rights invoked by a Data Subject;
e) whenever you are engaging in a significant new, or change in, Processing activity which is likely to require a DPIA or plan to use Personal Data for purposes other than what it was collected for;
f) if you need help complying with applicable law when carrying out direct marketing activities; or
g) if you need help with any contracts or other areas in relation to sharing Personal Data with third parties (including our customers and suppliers).

3. Personal data protection principles

We adhere to the principles relating to Processing of Personal Data set out in the GDPR which require Personal Data to be:

a) Processed lawfully, fairly and in a transparent manner (Lawfulness, Fairness and Transparency);
b) collected only for specified, explicit and legitimate purposes (Purpose Limitation);
c) adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (Data Minimisation);
d) accurate and where necessary kept up to date (Accuracy);
e) not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is Processed (Storage Limitation);
f) Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage (Security, Integrity and Confidentiality);
g) not transferred to another country without appropriate safeguards being in place (Transfer Limitation); and
h) made available to Data Subjects and allow Data Subjects to exercise certain rights in relation to their Personal Data (Data Subject's Rights and Requests).
i) We are responsible for and must be able to demonstrate compliance with the data protection principles listed above.

4. Data held by APEM

We hold data about customers, potential customers, our employees and from our website as follows:

4.1 Client and potential client data

- Company name;
- Contact name;
- Contact address;
- Contact telephone number (mobile and landline);
- Contact email address;
- Contract details (where appropriate);
- Customer owned data which is related to a project.

4.2 Employee and potential Employee Data

- Employee / candidate name;
- Employee / candidate address;
- Employee / candidate contact details (email / phone numbers etc);
- Employee / candidate National Insurance Number;
- Employee bank details;
- Employee emergency contact and next of kin details;
- Employee medical records if relevant;
- Employee sickness information;
- Employee Nationality;
- Employee D&I information;
- Employee Marital status;
- Employee driving license details;
- Employee grey fleet details if driving own car for work purposes;
- Data for company insurance policy.

4.3 Website Data

- Internet Protocol (IP) Address;
- Cookie data;
- CV data sent through via the website;
- Data supplied by website users via the online enquiries form.

5. What we use the data for

5.1 Client and potential client data

- Contact name to address clients, or potential clients directly;
- Contact address to address clients, or potential clients directly;
- Contact telephone number (mobile and landline) to address clients, or potential clients directly;
- Contact email address to address clients, or potential clients directly;

- Contract details (where appropriate) to provide the appropriate services to our clients;
- Project details (where appropriate) to provide support applicable to the client contract;
- Customer owned data, which is related to a project, to resolve a specific support issue.

Under the banner of legitimate interest in the UK, client data is also used for marketing, including email marketing under The Privacy and Electronic Communications Regulations (PECR). Clients can unsubscribe from receiving email marketing at any time.

All email communications undertaken by the APEM Group's marketing team operate under marketing best practice and will not include data that has been:

- 'Scraped' from a website, even if it is in the public domain
- Provided to the team without proof of providence or licence

The Marketing team also obtain consent via an opt in mechanism on the APEM Ltd, APEM Inc and APEM Ireland websites. The inclusion of this mechanism will be included on other APEM Group entity websites as and when they are redeveloped.

5.2 Employee data

All employee data is held for the purposes of employment, insurance, payment and compliance with tax and pension payments. It is kept on the secure cloud servers and access to this information is strictly limited.

5.3 Website Data

- We do not send customers information based on their IP addresses. If they have a query, we ask them to fill out a short form with their email address so we can get back to them directly.
- Cookie data. We collect data about visitors to our website and browsing patterns. For more details see our Cookie Policy.

6. Storage of data

Personal Data must be secured by appropriate technical and organisational measures against unauthorised or unlawful Processing, and against accidental loss, destruction or damage.

We 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 (including use of encryption and Pseudonymisation where applicable). We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our Processing of Personal Data.

APEM's physical servers are located in a secure server room at company Headquarters.

APEM's cloud servers are hosted within Microsoft Azure. This is a cloud-based server solution hosted

in Microsoft data centres in the UK. These data centres are maintained and protected by Microsoft, in-line with industry standard legislation.

Data gathered via the Company website is held on secure servers by our website service provider.

Data stored locally is held on APEM owned equipment. Security of that data complies to the Government backed Cyber Essentials Scheme which includes:

- Secure boundary controls between APEM and the internet.
- Controls on access to the data. Access is restricted to only those persons authorised to see the data.
- Up to date antimalware protection to reduce the risk of data being damaged by malicious software.
- Regular patching of our software and operating systems to further reduce the risks of a malicious software attack.
- Secure configuration of our devices removing any known weaknesses.

7. Reporting a Personal Data Breach

The UK and EU GDPR requires Controllers to notify any Personal Data Breach to the Information Commissioner and, in certain instances, the Data Subject.
We 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 (see Data Breach Procedure Policy).

8. Sharing of data

APEM will only share data in the following situations, with the employee's permission:

- When required for performance of a contract.
- When required for optional employee benefits such as the pension scheme.

Other than for the purposes highlighted above APEM will not share your details with any other third parties.

8.1 Transportation of Data

When APEM transfer data, it is done with secure connections. Any personal data held by APEM does not leave the UK without explicit consent.

9. Data retention

9.1 Client and potential client data

All client data is securely destroyed seven years after our last contact with the client company, or for as long as the contract stipulates where this exceeds seven years.

9.2 Employee and potential data

To stay in line with the various regulations covering payroll, pension, contract and employee data and, to maintain a system that is not overly burdensome to manage, APEM will keep all employee data for seven years after the employee leaves the organisation. Data collected during the application process will be deleted after a year if the candidate is unsuccessful.

9.3 Client data used in projects

Where possible, APEM will avoid copying any client data. However, in situations where this is not possible, the data will be destroyed or returned to the customer on closure of the project.

10. Communicating with you

APEM will communicate with you via email to:

- Inform you of new or improved services offered by APEM
- Business updates and trading information

Customers may opt out of the communications at any time by following the unsubscribe link in the specific message.

11. Correction of Data and Subject Access Requests

If the data we hold about you is incorrect, please contact: dataprotection@apemltd.co.uk stating what the problem is and what correction is required. It would aid our investigation if you could provide a screen shot of the issue.
Customers and potential customers have the right to receive a copy of their data held by us. Please send an email to dataprotection@apemltd.co.uk to make your request.

If a Data and Subject Access Request is received as a result of marketing activity, the Marketing team will respond within 28 days, advising where the data was obtained from, and confirmation of action requested.

12. Issues or comments on this Privacy Statement

If you have any issues or concerns with this Privacy Statement, or the way APEM handles data, please contact: dataprotection@apemltd.co.uk