



Data Protection Policy

Cutlass Group Limited (Cutlass) processes the personal data of living individuals such as its staff, contractors, and customers. This processing is regulated by the Data Protection Act 2018 (DPA) and the General Data Protection Regulation (GDPR). The UK's regulator for the DPA and GDPR is the Information Commissioner's Office (ICO).

Cutlass is registered as a Data Controller with the ICO and is responsible for compliance with the GDPR and DPA.

You can view our registration with the ICO by typing Cutlass Security Group into the search function accessible via the following link: <https://ico.org.uk/about-the-ico/what-we-do/register-of-datacontrollers/>

1.1 Key Definitions

This DPA and GDPR contain several key definitions which are referenced in this policy such as 'Personal Data', 'Processing' and 'Data Controller'. Those definitions are set out in **Annex A**.

1.2 Purpose and Objectives of Policy

This policy sets out Cutlass's commitment to comply with the Data Protection Act 2018 ('DPA'), and the General Data Protection Regulation ('the GDPR').

1.3 Scope and Status of the Policy

This policy applies to all Cutlass staff, and others who use or process any Personal Data. This policy applies regardless of where Personal Data is held and or the equipment used if the Processing is for Cutlass's purposes. Further, the policy applies to all Personal Data (including Sensitive Personal Data) held in any form whether manual paper records or electronic records.

2. Roles and Responsibilities

2.1 Board of Directors

The Board of Directors are responsible for approval of the Policy.

Cutlass Board of Directors

Cutlass Board of Directors is responsible for strategic level implementation of the policy, oversight of compliance with the policy and reporting identified risks to the **Group Chairman Humayun Shahzad**.



Information Asset Owners

Cutlass will appoint Information Asset Owners (IAOs) with local responsibility for data protection compliance for Personal Data processed in their area.

Information Asset Managers

Cutlass Information Asset Manager **Pavan Sesham** who will hold local responsibility for data protection compliance processed within their teams. A list of the IAOs and IAMs can be accessed for audit purposes upon request.

Data Protection Officer

Cutlass's Data Protection Officer (DPO) **Group Chairman Humayun Shahzad** is primarily responsible for advising on and assessing Cutlass's compliance with the DPA and GDPR and making recommendations to improve practice in this area. Further, the DPO acts as Cutlass's primary point of contact for DPA and GDPR matters.

Legal Services

Legal Services are responsible for providing advice, support, and guidance in relation to day-to-day data protection matters.

All Head Office Staff

All staff, including permanent staff, fixed term contractors and temporary workers must comply with this Policy, the DPA and the GDPR whenever Processing Personal Data held by Cutlass or on behalf of Cutlass.

All Employees

All Employees are responsible for compliance with the rules and policies made by Cutlass.

Employees must comply with this policy were collecting and Processing Personal Data as part of their duties.

Contractors and Consultants

Third parties such as consultants, contractors, or agents, undertaking work on behalf of Cutlass involving Personal Data, must adhere to Cutlass's Data Protection Policy and comply with the DPA and the GDPR. Provision will be made in contracts with external providers to ensure compliance with this Policy, the DPA and GDPR.



3. Compliance with the DPA and GDPR

3.1 Awareness & Capability

Cutlass will implement, and monitor annual completion of, mandatory Data Protection training for all staff. The content of that training will be reviewed annually.

3.2 Privacy by Design

Cutlass will implement a Privacy by Design Approach to Processing Personal Data through integrating Privacy Impact Assessments into business processes and projects.

3.3 Lawful, Fair & Transparent Processing

Cutlass will provide appropriate information to individuals when collecting their Personal Data by means of privacy notices. Cutlass will also ensure at least one lawful basis is available before Processing Personal Data.

3.4 Purpose Limitation

Cutlass will clearly set out purposes for Processing Personal Data. Cutlass will only process Personal Data for purposes notified to individuals and where the new purpose is compatible with an existing purpose.

3.5 Data Minimisation

Cutlass will only collect as much information as is necessary to meet the purposes that have been identified. Personal Data must be adequate, relevant, and not excessive.

3.6 Accuracy

Cutlass will ensure that Personal Data processed is accurate and where necessary kept up to date.

3.7 Security

Cutlass will protect the security of Personal Data by maintaining, and monitoring compliance with Cutlass's Information Security Policy, CUT-133-CCP-ISM

3.8 Record Keeping & Retention

Cutlass will maintain a Records Retention and Disposal Schedule setting the periods for which records containing Personal Data are to be retained.



3.9 External Contractors and International Transfers

Cutlass will enter legally binding written contracts with external bodies where those bodies are engaged to process Personal Data on our behalf. Cutlass will not transfer any information outside of the United Kingdom.

3.10 Lawful, Fair & Transparent Processing

Cutlass will provide appropriate information to individuals when collecting their Personal Data by means of privacy notices. Cutlass will also ensure at least one lawful basis is available before Processing Personal Data.

3.11 Purpose Limitation

Cutlass will clearly set out purposes for Processing Personal Data. Cutlass will only process Personal Data for purposes notified to individuals and where the new purpose is compatible with an existing purpose.

3.12 Data Minimisation

Cutlass will only collect as much information as is necessary to meet the purposes that have been identified. Personal Data must be adequate, relevant, and not excessive.

3.13 Accuracy

Cutlass will ensure that Personal Data processed is accurate and where necessary kept up to date.

3.14 Security

Cutlass will protect the security of Personal Data by maintaining, and monitoring compliance with Cutlass's Information Security Policy, CUT-133-CCP-ISM

3.15 Record Keeping & Retention

Cutlass will maintain a Records Retention and Disposal Schedule setting the periods for which records containing Personal Data are to be retained.

3.16 External Contractors and International Transfers

Cutlass will enter legally binding written contracts with external bodies where those bodies are engaged to process Personal Data on our behalf. Cutlass will not transfer any information outside of the United Kingdom.



3.17 Other Third-Party Access

Cutlass will only disclose Personal Data to third parties such as the police, central government, and other legal bodies such as The Security Industry Authority and HSE where there is a lawful basis for doing so and appropriate arrangements are in place with those parties.

3.18 Internal Sharing

Cutlass will seek to ensure that Personal Data is only shared across different teams, divisions, or departments where those areas have a business need for accessing that data.

4. Data Subjects Rights

Cutlass will comply with requests from an individual to exercise their rights under the DPA, and the GDPR. All individuals have the right to be informed what information Cutlass holds about them and to request copies of that information. This is known as a Subject Access Request. Any individual wishing to submit a Subject Access Request should contact HR in the first instance.

Under the DPA and GDPR, individuals also have the following rights in relation to their Personal Data:

- The right to request their Personal Data is rectified if inaccurate
- The right to request erasure of their Personal Data
- The right to request that the Processing of their Personal Data is restricted
- The right of portability in relation to their Personal Data
- The right to object to the Processing of their Personal Data
- The right to object to Processing which involves automated decision making or profiling.

Individuals who wish to exercise the above rights should contact Cutlass's Data Protection Officer at:

Shaz@cutlassgroup.co.uk

It is recommended that Individuals submit their request in writing and specify exactly what Personal Data and/or processing they are referring to and which right they wish to exercise. If you are seeking access to your Personal Data (i.e., making a 'Subject Access Request') then you may find it helpful to review our guidance available on the documents section of Timegate, accessible via your employee portal.

Any staff member who receives a request from an individual to exercise the above rights under the DPA and GDPR must forward it to HR immediately: HR@cutlassgroup.co.uk

All staff are responsible for cooperating with Legal Services to ensure that Cutlass can comply with an individual's request under the DPA and GDPR within the statutory timescales.

5. Own Personal Data

All staff are responsible for checking that information they provide to Cutlass in connection with their employment or studies is accurate and up to date. Any changes to Personal Data provided (e.g., change of address) must be promptly notified, in writing, to Cutlass (via the SMS employee App).

Cutlass cannot be held responsible for errors unless the member of staff has properly informed Cutlass about them.

6. Personal Data Breaches

Cutlass will respond promptly to any identified Personal Data Breaches and thoroughly investigate those incidents to ascertain whether:

- The breach should or must be reported to the ICO
- Data subjects should or must be made aware of the breach; and
- It is necessary to amend processes or introduce new measures to mitigate against any further breaches.

Any staff member who knows or suspects that an actual or potential Personal Data Breach has occurred must immediately notify the information security officer: shaz@cutlassgroup.co.uk

All staff are responsible for fully engaging and cooperating with the company in relation to their investigation of a Personal Data Breach.

7. Compliance

Compliance with this Policy, the DPA and the GDPR is the responsibility of all members of staff. Employees must comply with the rules and procedures made by Cutlass. It is a condition of being an employee that all Cutlass rules and policies are fully complied with.

Any breach of the policy by a member of staff may result in disciplinary action or access to the companies' facilities being withdrawn. Serious or deliberate breaches of the DPA can result in a criminal prosecution.

Any breach of the GDPR by Cutlass may result in a substantial fine or actions imposed upon Cutlass by the ICO.

8. FURTHER INFORMATION

Questions about the interpretation or operation of this policy should be taken up in the first instance with the Data Protection Officer: shaz@cutlassgroup.co.uk

Any individual who considers that the Policy has not been followed in respect of Personal Data about themselves should also raise the matter with Cutlass's Data Protection Officer.



Further information about the DPA and the GDPR can be found on the Information Commissioner's Office ([ICO website](#)).

Please see the policy section of the Cutlass shared drive for related policies.

Annex A Key Definitions

1. 'Personal Data' means data which relate to a living individual who can be identified from those data or from those data and other information, which is in the possession of, or is likely to come into the possession of, the Data Controller and includes any expression of opinion about the individual and any indication of the intentions of the Data Controller or any other person in respect of the individual. Under the GDPR, the definition of Personal Data will explicitly extend to IP addresses.
2. 'Sensitive Personal Data' means information:
 - a. about an individual's Special Category Data; and
 - b. the commission or alleged commission by an individual of any criminal offence or any proceedings for any offence committed or alleged to have been committed by her or him, the disposal of such proceedings or the sentence of any court in such proceedings.
3. 'Special Category Data' means any Personal Data about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and their genetic or biometric data.
4. 'Processing' means any operations or set of operations which is performed on Personal Data whether or not by automated means such as collection, use, disclosure or storage of Personal Data etc.
5. 'Data Controller' means the organisation which, either alone or jointly with another organisation, determines the manner and purpose of the Processing of Personal Data. The Data Controller is responsible for compliance with the DPA and GDPR.
6. 'Personal Data Breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored, or otherwise processed.

Signed: _____



Review Date: 12.08.2027

Name: Humayun Shahzad Group Chairman

Date: 13.08.2026