DATA PROTECTION POLICY

V2.0

Abstract

The General Data Protection Regulation 2016 replaces the EU Data Protection Directive of 1995 and supersedes the laws of individual Member States that were developed in compliance with the Data Protection Directive 95/46/EC.

BESA Group is committed to compliance with the GDPR and collects/processes personal data in accordance with this policy.

Registered Office: Old Mansion House, Eamont Bridge, Penrith, Cumbria, CA10 2BX

Table of Contents

1. INTRODUCTION

Background

The General Data Protection Regulation 2016 replaces the EU Data Protection Directive of 1995 and supersedes the laws of individual Member States that were developed in compliance with the Data Protection Directive 95/46/EC.

Its purpose is to protect the “rights and freedoms” of natural persons (i.e. living individuals) and to ensure that personal data is not processed without their knowledge, and, wherever possible, that it is processed with their consent.

Definitions

Material scope (Article 2) **–** the GDPR applies to the processing of personal data wholly or partly by automated means (i.e. by computer) and to the processing other than by automated means of personal data (i.e. paper records) that form part of a filing system or are intended to form part of a filing system.

Territorial scope (Article 3) **–** the GDPR will apply to all controllers that are established in the EU (European Union) who process the personal data of data subjects, in the context of that establishment. It will also apply to controllers outside of the EU that process personal data in order to offer goods and services, or monitor the behaviour of data subjects who are resident in the EU.

Establishment – the main establishment of the controller in the EU will be the place in which the controller makes the main decisions as to the purpose and means of its data processing activities. The main establishment of a processor in the EU will be its administrative centre. If a controller is based outside the EU, it will have to appoint a representative in the jurisdiction in which the controller operates to act on behalf of the controller and deal with supervisory authorities.

Personal data – any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Special categories of personal data – personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Data controller – the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Data subject – any living individual who is the subject of personal data held by an organisation.

Processing – any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Profiling **–** is any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person, or to analyse or predict that person's performance at work, economic situation, location, health, personal preferences, reliability, or behaviour. This definition is linked to the right of the data subject to object to profiling and a right to be informed about the existence of profiling, of measures based on profiling and the envisaged effects of profiling on the individual.

Personal data breach **–** 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. There is an obligation on the controller to report personal data breaches to the supervisory authority and where the breach is likely to adversely affect the personal data or privacy of the data subject.

Data subject consent **-** means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data.

Child **–** the GDPR defines a child as anyone under the age of 16 years old, although this may be lowered to 13 by Member State law. The processing of personal data of a child is only lawful if parental or custodian consent has been obtained. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child.

Third party – a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

Filing system – any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

2. POLICY STATEMENT

BESA Group are committed to compliance with the GDPR and processes personal data in accordance with this policy. Compliance with the GDPR is described by this policy and other related policies, processes and procedures.

This policy applies to all of BESA Group's personal data processing functions, including those performed on customers', clients', employees', suppliers' and partners' personal data, and any other personal data the organisation processes from any source.

The GDPR Owner is responsible for reviewing data mapping and associated risk assessments annually, in light of any changes to BESA Group's activities and any additional requirements identified by means of data protection impact assessments. These records need to be available to the supervisory authority on request.

This policy applies to all Employees/Staff of BESA Group. Any breach of the GDPR will be dealt with under BESA Group's disciplinary policy and may also be a criminal offence, in which case the matter will be reported as soon as possible to the appropriate authorities.

Partners and any third parties working with or for BESA Group, and who have or may have access to personal data, will be expected to comply with this policy. The consequences of breaching this policy are set out in contracts and agreements with third parties.

No third party may access personal data held by BESA Group without having first entered into a confidentiality agreement, which imposes on the third party obligations no less onerous than those to which BESA Group is committed, and which gives BESA Group the right to audit compliance with the agreement.

In determining its scope for compliance with the GDPR, BESA Group considers:

- any external and internal issues that are relevant;
- specific needs and expectations of interested parties;
- organisational objectives and obligations;
- the organisations acceptable level of risk; and
- any applicable statutory, regulatory or contractual obligations.

BESA Group's objectives for compliance with the GDPR:

- are consistent with this policy;
- are measurable;
- take into account the results from risk assessments and risk mitigation.

In order to achieve these objectives, BESA Group has determined:

- what will be done;
- what resources will be required;
- who will be responsible;
- when it will be completed;
- how the results will be evaluated.

3. ROLES AND RESPONSIBILITIES UNDER GDPR

For its customer-facing services, BESA Group is an independent data controller and in some circumstances, may be a joint-controller role with another party. Within BESA Group, support services are centralised and intra-group working is defined by a service level agreement or similar.

BESA Group management team are responsible for developing and encouraging good information handling practices; responsibilities are referenced in individual job descriptions.

The Director of People maintains a record of specific GDPR roles and responsibilities as follows:

ROLE TYPE	TO	WHO
Senior Manager or Group	Be accountable to the Board for: • Management of personal data within the Group • Compliance with DP legislation • Demonstrate good practice	TBC
Legal (GDPR Owner)	• development and review of the data protection policy; • approval of procedures where personal data is processed, such as: ○ review privacy notices; • provision of expert advice and guidance on legislative and regulatory data protection matters • the interpretation and application of the various exemptions applicable to the processing of personal data • advise and inform on the data protection impact assessment and monitor performance against the requirements of the EU GDPR;	Head of Legal
IT (GDPR Owner)	• liaison with those responsible for risk management and security issues within the BESA Group; • provision of advice in relation to data sharing projects (including security issues when data are off site) • approval of procedures where personal data is processed, such as: ○ the communication of privacy notices;	Head of IT

People (GDPR Owner)	• training and ongoing awareness as required by the data protection policy;
	• approval of procedures where personal data is processed, such as:
	  ○ the handling of requests from individuals, including requests for access, rectification, erasure, etc.;
	  ○ complaints handling;
	• Ownership of DPO mailbox – forwarding emails as appropriate
		Head of People and Culture

Department Level (GDPR Rep) *(GDPR Owners also responsible for these activities within their own departments)*	• Ensuring implementation of the data protection policy represent departments or systems that are recognised as high-risk in relation to the management of personal data;
	• Assist the GDPR Owner(s) with day-to-day responsibility for compliance with the data protection policy, for example: data inventory, staff training and staff access, privacy notices, etc.
	• Complete data protection impact assessments on all departmental change activities
	• approval of procedures where personal data is processed, such as:
	  ○ the management of security incidents
	  ○ the collection and handling of personal data;
	  ○ outsourcing and off-shoring
		GDPR Working Group Members

All Above	• be member of the information governance committee (review over time – initial monthly meetings – as embedded quarterly (minimum) – with option for additional if required)	As above

The GDPR Owner is accountable to Board of Directors of BESA Group for the management of personal data and for ensuring that compliance with data protection legislation and good practice can be demonstrated. This accountability includes:

- development and implementation of the GDPR as required by this policy; and
- security and risk management in relation to compliance with the policy.

The GDPR Owner, who the Board of Directors considers to be suitably qualified and experienced, has been appointed to take responsibility for BESA Group's compliance with this policy on a day-to-day basis and, in particular, has direct responsibility for ensuring that BESA Group complies with the GDPR, as do all managers in respect of data processing that takes place within their area of responsibility.

The GDPR Owner has specific responsibilities in respect of procedures such as the Subject Access Request and are the first point of call for Employees/Staff seeking clarification on any aspect of data protection compliance.

Compliance with data protection legislation is the responsibility of all Employees/Staff of BESA Group who process personal data. BESA Group provides relevant GDPR training to fulfil requirements in relation to specific roles and Employees/Staff of BESA Group generally.

Employees/Staff of BESA Group are responsible for ensuring that any personal data about them and supplied by them to BESA Group is accurate and up-to-date.

4. DATA PROTECTION PRINCIPLES

All processing of personal data must be conducted in accordance with the data protection principles as set out in Article 5 of the GDPR. BESA Group's policies and procedures are designed to ensure compliance with the principles.

The data protection principles can be summarised as:

- Data must be processed **lawfully, fairly and in a transparent manner**.
- Data must be obtained **for specified, explicit and legitimate purposes**.
- Data processing is **adequate, relevant and limited** to what is necessary.
- Data is **accurate** and, where necessary, **kept up to date**.
- Data is **not kept for longer than is necessary** for the purpose.
- Appropriate technical and organisational **measures are in place to protect data**.

These principles are explained in more detail below.

Personal data must be processed lawfully, fairly and transparently.

Lawful – identify a lawful basis before you can process personal data. These are often referred to as the "conditions for processing", for example contract, legal obligation or legitimate interest.

Fairly – in order for processing to be fair, the data controller has to make certain information available to the data subjects as practicable. This applies whether the personal data was obtained directly from the data subjects or from other sources.

Transparently – the GDPR includes rules on giving privacy information to data subjects. This must be communicated to the data subject using clear and plain language, preferably in the form of a Privacy Notice.

The specific information that must be made available to the data subject must include:

- the identity and the contact details of the controller and, if any, of the controller's representative;
- the contact details of the GDPR Owner;
- the purposes of the processing as the legal basis for the processing;
- the period for which the personal data will be stored;
- the existence of the data subject rights;
- the categories of personal data concerned;
- the recipients or categories of recipients of the personal data, where applicable;
- where applicable, information relating to the transfer of personal data to a third country;
- any further information necessary to guarantee fair processing.

For more detail, also see BESA Group's Privacy Notice Procedure.

Personal data can only be collected for specific, explicit and legitimate purposes.

Data obtained for specified purposes must not be used for a purpose that differs from those formally notified to the supervisory authority as part of BESA Group's GDPR register of processing.

Personal data must be adequate, relevant and limited to what is necessary for processing.

The GDPR Owner is responsible for ensuring that BESA Group does not collect information that is not strictly necessary for the purpose for which it is obtained.

All data collection forms (electronic or paper-based) must include a fair processing statement or link to the relevant online privacy policy.

The GDPR Owner will ensure that, on at least an annual basis all data collection methods are reviewed to ensure that collected data continues to be adequate, relevant and not excessive (see Data Protection Impact Assessment Procedure).

Personal data must be accurate and kept up to date and modified where required without delay.

Data that is stored must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that it is accurate.

The GDPR Owner is responsible for ensuring that all staff are trained in the importance of collecting accurate data and maintaining it.

It is also the responsibility of the data subject to ensure that data held by BESA Group is accurate and up to date. Completion of a registration or application form by a data subject will include a statement that the data contained therein is accurate at the date of submission.

Employees/Staff are required to notify BESA Group of any changes to their personal circumstances, to enable personal records to be updated accordingly. It is the responsibility of BESA Group to ensure that any notification regarding change of circumstances is recorded and acted upon.

The GDPR Owner is responsible for ensuring that appropriate procedures and policies are in place to keep personal data accurate and up to date, taking into account the volume of data collected, the speed with which it might change and any other relevant factors.

On at least an annual basis, the GDPR Owner will review the retention dates of all the personal data processed by BESA Group and will identify any data that is no longer required in the context of the registered purpose. This data will be securely deleted/destroyed.

The GDPR Owner is responsible for responding to requests for rectification from data subjects within one month (see Subject Access Request Procedure). This can be extended to a further two months for complex requests. If BESA Group decides not to comply with the request, the GDPR Owner must respond to the data subject within one month to explain its reasoning and inform them of their right to complain to the supervisory authority and seek judicial remedy.

Where third-party organisations may have been passed inaccurate or out-of-date personal data, the GDPR Owner must inform them that the information is inaccurate and not to be used to inform decisions about the individuals concerned, and for passing any corrections to the third party where this is required.

Personal data must be kept in a form such that the data subject can be identified only as long as is necessary for processing.

If personal data is retained beyond the processing date, it will either be amended sufficiently in order to protect the identity of the data subject in the event of a data breach, otherwise securely destroyed.

The GDPR Owner must specifically approve any data retention that exceeds the pre-defined retention periods and must ensure that the justification is clearly identified and in line with the

requirements of the data protection legislation.

Personal data must be processed in a manner that ensures the appropriate security

The GDPR Owner will carry out a risk assessment, taking into account all the circumstances of BESA Group's controlling or processing operations.

In determining appropriateness, the GDPR Owner should also consider the extent of possible damage or loss that might be caused to individuals (e.g. staff or customers) if a security breach occurs, the effect of any security breach on BESA Group itself, and any likely reputational damage including the possible loss of customer trust.

When assessing appropriate technical measures, the GDPR Owner will consider the following:

- Password policy
- Automatic locking of idle terminals;
- Removal of access rights or encryption for USB and other memory media.
- Virus checking software and firewalls.
- Role-based access rights including those assigned to temporary staff.
- Encryption of devices that leave the organisations premises such as laptops.
- Security of local and wide area networks.
- Privacy enhancing technologies such as pseudonymisation and anonymisation;
- Identifying appropriate international security standards relevant to BESA Group.

When assessing appropriate organisational measures the GDPR Owner will consider the following:

- The appropriate training levels throughout BESA Group;
- Measures that consider the reliability of employees (such as references etc.);
- The inclusion of reference to data protection in employment contracts;
- Identification of disciplinary action measures for data breaches;
- Monitoring of staff for compliance with relevant security standards;
- Physical access controls to electronic and paper based records;
- Adoption of a clear desk policy;
- Storing of paper-based data in lockable fire-proof cabinets;
- Restricting the use of portable electronic devices outside of the workplace;
- Restricting the use of employee's own personal devices being used in the workplace;
- Adopting clear rules about passwords;
- Making regular backups of personal data and storing the media off-site;
- The imposition of contractual obligations on the importing organisations to take appropriate security measures when transferring data outside the EEA.

These controls have been selected on the basis of identified risks to personal data, and the potential for damage or distress to individuals whose data is being processed.

The controller must be able to demonstrate compliance with the GDPR's other principles

The GDPR includes provisions that promote accountability and governance. These complement the GDPR's transparency requirements. The accountability principle in Article 5(2) requires you to demonstrate that you comply with the principles and states explicitly that this is your responsibility.

BESA Group will demonstrate compliance with the data protection principles by implementing data protection policies, training, adhering to codes of conduct, implementing technical and organisational measures, as well as adopting techniques such as data protection by design, DPIAs, breach notification procedures and incident response plans.

Data subjects' rights

Data subjects have the following rights regarding their data and associated processing:

- The right to **be informed**.
  To be told about how personal data is being processed.
  To make subject access requests regarding the nature of information held and processed.

- The right of **access**.
  To get access to a copy of the personal data.

- The right to **rectification**.
  To take action to rectify inaccurate data.

- The right to **erase**.
  To take action to erase or destroy inaccurate data, including a right to be forgotten.
  This right is not absolute and only applies in certain circumstances.

- The right to **restrict processing**.
  To restrict or limit how personal data is used and processed.
  This right is not absolute and only applies in certain circumstances.

- The right to **data portability**.
  To have the data they have provided transferred to another controller.
  To have their data provided to them in a structured, commonly used and machine-readable format

- The right to **object**.
  To prevent processing for purposes of direct marketing.
  To prevent processing likely to cause damage or distress.

- The right to know and object to **automated decision making / profiling**.
  To be informed about the mechanics of automated decision-taking process that will affect them.
  To object to any automated profiling that is occurring without consent.
  To not have significant decisions that will affect them taken solely by automated process.
  This right may not apply when processing is required to fulfil a contractual obligation.

- To request the supervisory authority to assess whether the GDPR has been contravened.
- To sue for compensation if they suffer damage by any contravention of the GDPR.

BESA Group ensures that data subjects may exercise these rights:

- Data subjects may make subject access requests as described in Subject Access Request Procedure. This procedure also describes how BESA Group will ensure that its response to the data access request complies with the requirements of the GDPR.

- Data subjects have the right to complain to BESA Group related to the processing of their personal data, the handling of a request from a data subject and appeals from a data subject on how complaints have been handled.

5. CONSENT

In most circumstances, consent to process personal and sensitive data is obtained by the BESA Group using standard documents, for example when a new client completes an enquiry form, signs a service contract or agreement.

Most processing of personal data across the BESA Group is justified using the following legal basis:

- Contractual. Processing is being done to establish or deliver a contracted service.
- Legal Obligation. Processing is being done because of a legal requirement to do so.
- Legitimate Interest. Processing is being done because it is necessary to provide the service or is relevant to the service being provided.

There are some circumstances where data subjects might need to provide explicit consent for processing of their personal data, for example in support of direct marketing. Where consent is being used as the legal basis for data processing, BESA Group must be able to demonstrate that consent was obtained for the processing operation.

BESA Group understands 'consent' to mean approval that has been explicitly and freely given. This will be a specific, informed and unambiguous indication of the data subject's wishes that signifies agreement to the processing of their personal data.

There must be some active communication between the parties to demonstrate active consent. Consent cannot be inferred from non-response to a communication. The data subject has been fully informed of the intended processing and has signified their agreement, while in a fit state of mind to do so and without pressure being exerted upon them.

Consent obtained under duress or on the basis of misleading information will not be a valid basis for processing. The data subject can withdraw their consent at any time.

For special categories of data (sensitive personal data), explicit written consent of data subjects must be obtained, unless an alternative legal basis for processing exists.

Where BESA Group provides online services to children, parental or custodial authorisation must be obtained. This requirement applies to children under the age of 13 (thirteen).

6. SECURITY OF DATA

All Employees/Staff are responsible for ensuring that any personal data that BESA Group holds and for which they are responsible, is kept securely and is not under any conditions disclosed to any third party unless that third party has been specifically authorised by BESA Group to receive that information and has entered into a confidentiality agreement.

All personal data should only be accessible to those who need to use it and access may only be granted in line with the access control procedures.

Measures must be taken to protect personal data, in line with the level of risk associated with the category, format, quantity and location of the personal data being stored. By default, all personal data should be protected with the highest security and must be kept:

- in a lockable room with controlled access; or
- in a locked drawer or filing cabinet.
- if computerised, password protected in line with corporate requirements in the access control procedures.
- stored on (removable) computer media which are encrypted.

Care must be taken to ensure that PC screens and terminals are not visible except to authorised Employees/Staff of BESA Group. All Employees/Staff are required to enter into an acceptable use agreement before they are given access to organisational information of any sort.

Manual records may not be left where they can be accessed by unauthorised personnel and may not be removed from business premises without explicit authorisation. As soon as manual records are no longer required for day-to-day client support, they must be archived securely.

Manual records that have reached their retention date are to be shredded and disposed of as ‘confidential waste’. Redundant PCs and data storage media should be returned to the IT function, where they will be disposed of securely.

Processing of personal data ‘off-site’ presents a potentially greater risk of loss, theft or damage to personal data. Staff must be specifically authorised to process data off-site.

7. DISCLOSURE OF DATA

BESA Group must ensure that personal data is not disclosed to unauthorised third parties which includes family members, friends, government bodies, and in certain circumstances, the police.

All Employees/Staff should exercise caution when asked to disclose personal data held on another individual to a third-party. It is important to bear in mind whether or not disclosure of the information is relevant to, and necessary for, the conduct of BESA Group's business. All requests to provide data for one of these reasons must be supported by appropriate paperwork and all such disclosures must be specifically authorised by the GDPR Owner.

All Employees/Staff should also exercise caution in situations where personal data could be inadvertently shared with third-parties, for example when using online collaboration tools (e.g. Skype, Instant Messaging), or through verbal communication and face-to-face meetings.

8. RETENTION AND DISPOSAL OF DATA

BESA Group shall not keep personal data in a form that permits identification of data subjects for longer a period than is necessary, in relation to the purpose(s) for which the data was originally collected.

BESA Group may store data for longer, only if the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the implementation of appropriate technical and organisational measures to safeguard the rights and freedoms of the data subject.

The retention period for each set of personal data will be set out in the relevant Privacy Notice and internally within a Record Retention Register.

Personal data must be disposed of securely in accordance with the sixth principle of the GDPR – processed in an appropriate manner to maintain security, thereby protecting the "rights and freedoms" of data subjects.

9. DATA TRANSFERS

All exports of data from within the European Economic Area (EEA) to non-European Economic Area countries (referred to in the GDPR as 'third countries') are unlawful unless there is an appropriate "level of protection for the fundamental rights of the data subjects".

The transfer of personal data outside of the EEA is prohibited unless one or more of the specified safeguards, or exceptions, apply:

- An adequacy decision – a list of pre-approved countries.
- Privacy Shield – covers EU/US transfers.
- Binding corporate rules – specific arrangements approved by the supervisory authority.
- Model contract clauses – protection through pre-approved contract clauses.
- Exceptions – some specific circumstances where it can be done.

These are explained in more detail below.

An adequacy decision
The European Commission can and does assess third countries, a territory and/or specific sectors within third countries to assess whether there is an appropriate level of protection for the rights and freedoms of natural persons. In these instances no authorisation is required.

Countries that are members of the European Economic Area (EEA) but not of the EU are accepted as having met the conditions for an adequacy decision.

A list of countries that currently satisfy the adequacy requirements of the Commission are published in the *Official Journal of the European Union.* *http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm*

Privacy Shield
If BESA Group wishes to transfer personal data from the EU to an organisation in the United States it should check that the organisation is signed up with the Privacy Shield framework at the U.S. Department of Commerce. The obligation applying to companies under the Privacy Shield are contained in the "Privacy Principles".

The US DoC is responsible for managing and administering the Privacy Shield and ensuring that companies live up to their commitments. In order to be able to certify, companies must have a privacy policy in line with the Privacy Principles e.g. use, store and further transfer the personal data according to a strong set of data protection rules and safeguards.

The protection given to the personal data applies regardless of whether the personal data is related to an EU resident or not. Organisations must renew their "membership" to the Privacy Shield on an annual basis. If they do not, they can no longer receive and use personal data from the EU under that framework.

Assessment of adequacy by the data controller

In making an assessment of adequacy, the UK based exporting controller should take account of the following factors:

- the nature of the information being transferred;
- the country or territory of the origin, and final destination, of the information;
- how the information will be used and for how long;
- the laws and practices of the country of the transferee, including relevant codes of practice and international obligations; and
- the security measures that are to be taken as regards the data in the overseas location.

Checks on adequacy should be repeated on an annual basis.

Binding corporate rules
BESA Group may adopt approved binding corporate rules for the transfer of data outside the EU. This requires submission to the relevant supervisory authority for approval of the rules that BESA Group is seeking to rely upon.

Model contract clauses
BESA Group may adopt approved model contract clauses for the transfer of data outside of the EEA. If BESA Group adopts model contract clauses approved by the relevant supervisory authority, there is an automatic recognition of adequacy.

Exceptions
In the absence of an adequacy decision, Privacy Shield membership, binding corporate rules and/or model contract clauses, a transfer of personal data to a third country or international organisation shall only take place on one of the following conditions:

- the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;
- the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;
- the transfer is necessary for important reasons of public interest;
- the transfer is necessary for the establishment, exercise or defence of legal claims; and/or
- the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent.

10. DATA MAPPING AND RISK ASSESSMENT (PRIVACY REGISTER)

BESA Group has established a data mapping and risk assessment process as part of its approach to address risks and opportunities throughout its GDPR compliance project. BESA Group's data mapping determines:

- business processes that use personal data;
- source of personal data;
- volume of data subjects;
- processing activity;
- maintains the inventory of data categories of personal data processed;
- documents the purpose(s) for which each category of personal data is used;
- recipients, and potential recipients, of the personal data;
- key systems and repositories; and
- any data transfers.

BESA Group is aware of any risks associated with the processing of particular types of personal data.

BESA Group assesses the level of risk to individuals associated with the processing of their personal data. Data Protection Impact Assessments (DPIAs) are carried out in relation to the processing of personal data by BESA Group, and in relation to processing undertaken by other organisations on behalf of BESA Group.

BESA Group shall manage any risks identified by the risk assessment in order to reduce the likelihood of a non-conformance with this policy.

Where there is a proposed change to processing activity that is likely to result in a high risk to the rights and freedoms of natural persons, BESA Group shall carry out a Data Protection Impact Assessment to evaluate the impact of the envisaged processing operations on the protection of personal data.

Where, as a result of a DPIA it is clear that BESA Group is about to commence processing of personal data that could cause damage and/or distress to the data subjects, the decision as to whether or not BESA Group may proceed must be escalated for review to the management team.

The management team and/or the GDPR Owner shall, if there are significant concerns, either as to the potential damage or distress, or the quantity of data concerned, escalate the matter to the supervisory authority.

APPENDIX 1 – RELATED PROCEDURES

These procedures are designed as corporate procedures to be undertaken by the nominated GDPR Owners.

General awareness for all BESA staff, with operational signposting to line managers and GDPR Owners will be done through the GDPR FAQ section of the intranet (Work In Progress).

Privacy Notice Procedure	How to inform data subjects about processing.
Subject Access Request Procedure	How to deal with requests from data subjects.
Personal Data Breach Procedure	How to handle a data breach.
Data Protection Impact Assessment Procedure	How to complete an impact assessment.