BESA’s Data Protection Policy

All of BESA’s staff processing personal data should ensure that the data are secure: appropriate measures must be taken to prevent unauthorised access, disclosure and loss.

It is rarely necessary to store electronic personal data on USB flash drives, portable hard drives, CDs, DVDs, or any computer not owned by BESA. In the case of electronic data, to minimise the risk of loss or disclosure, a secure remote connection to BESA should be used wherever possible.

Downloading personal data on to portable devices or taking manual personal data offsite must be authorised in writing by the Data Owner, who must explain and justify the operational need in relation to the volume and sensitivity of the data.

The data must be strongly encrypted. Users should only store the data necessary for their immediate needs and should remove the data as soon as possible. To avoid loss of encrypted data, or in case of failure of the encryption software, an unencrypted copy of the data must be held in a secure environment.

Personal data should be securely destroyed when no longer required, with consideration for the format of the data.

Personal data must not be disclosed unlawfully to any third party. Transfers of personal data to third parties must be authorised in writing by the data owner and protected by adequate contractual provisions or data processor agreements, agree with BESA’s notification and must use safe transport mechanisms.

All losses of personal data must be reported to BESA’s Communications and Website Manager. Negligent loss or unauthorised disclosure of personal data, or failure to report such events, may be treated as a disciplinary matter and could be considered gross misconduct.

BESA will make public as much corporate information as possible. The following types of personal information will usually be published prominently on BESA’s website:

1. Names of members of the Executive Council and the BESA Secretariat.
2. Staff contact details, including telephone number and BESA email address.

Data subjects have a right of access to their personal data, including some unstructured manual personal data. Subject access requests must be made in writing, or otherwise and sent to the Communications and Website Manager. Data subjects must prove their identity.

Copies will be provided in permanent form promptly and in any event within 40 days.

Some personal data are exempt from the right of subject access, including confidential references provided by BESA.

BESA does not charge a fee for subject access requests.

Although the DPA applies only to living individuals, data about deceased persons who at the time of processing would be under 100 years old should be treated as personal data, unless the information is the subject of a valid request under Freedom of Information legislation.

It is sometimes necessary for BESA to monitor information and communications. This may include personal data. The circumstances in which monitoring may be carried out, and procedures for doing so, are described in the BESA Staff Handbook.

In certain circumstances, the DPA provides for disclosure of personal data, without the consent of the data subject, to certain organisations. Requests for such disclosures from third parties, such as the police, UK Border Agency, local authorities or sponsors, should be made in writing and handled by the Communications and Website Manager. This will ensure the validity of the request and any warrants or orders of court can be checked. Staff disclosing personal data may not be protected by an invalid warrant.

Records in all formats containing personal data must be created, stored and disposed of in accordance with BESA’s Records Management Policy and any associated procedures and codes of practice. They must be authentic, reliable and usable and capable of speedy and efficient retrieval.

THE DATA PROTECTION PRINCIPLES

It is the duty of data controllers and data processors to comply with all the data protection principles. These are set out in Schedule 1 of the Data Protection Act 1998, from which the following extract is taken:

1) Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless—

(a) at least one of the conditions in Schedule 2 is met, and

(b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

2) Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3) Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4) Personal data shall be accurate and, where necessary, kept up to date.

5) Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6) Personal data shall be processed in accordance with the rights of data subjects under this Act.

7) Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8) Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of persona.

**Last updated: May 2018**