Data Protection Policy

1. Introduction

This Policy sets out the obligations of Built Environment Communications Group Ltd, a company registered in England under number 03096503, whose registered office is at The Pump House, Garnier Road, Winchester SO23 9QG ("BECG") regarding data protection and the rights of members of the public, elected officials, government and local authority employees, business owners, shoppers, users of public and private services, business contacts ("data subjects") in respect of their personal data under EU Regulation 2016/679 General Data Protection Regulation ("GDPR").

The GDPR defines "personal data" as any information relating to an identified or identifiable natural person (a "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.

This Policy sets BECG's obligations regarding the collection, processing, transfer, storage, and disposal of personal data. The procedures and principles set out herein must be followed at all times by BECG, its employees, agents, contractors, or other parties working on behalf of BECG.

BECG is committed not only to the letter of the law, but also to the spirit of the law and places high importance on the correct, lawful, and fair handling of all personal data, respecting the legal rights, privacy, and trust of all individuals with whom it deals.

2. The Data Protection Principles

This Policy aims to ensure compliance with the GDPR. The GDPR sets out the following principles with which any party handling personal data must comply. All personal data must be: 2.1 Processed lawfully, fairly, and in a transparent manner in relation to the data subject.

2.2 Collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.

2.3 Adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.

2.4 Accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased, or rectified without delay.

2.5 Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of the data subject.

2.6 Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

3. The Rights of Data Subjects

The GDPR sets out the following rights applicable to data subjects (please refer to the parts of this policy indicated for further details): 3.1 The right to be informed (Part 12).

3.2 The right of access (Part 13);

3.3 The right to rectification (Part 14);

3.4 The right to erasure (also known as the 'right to be forgotten') (Part 15);

3.5 The right to restrict processing (Part 16);

3.6 The right to data portability (Part 17);

3.7 The right to object (Part 18); and

3.8 Rights with respect to automated decision-making and profiling (Parts 19 and 20).

4. Lawful, Fair, and Transparent Data Processing

4.1 The GDPR seeks to ensure that personal data are processed lawfully, fairly, and transparently, without adversely affecting the rights of the data subject. The GDPR states that processing of personal data shall be lawful if at least one of the following applies:

4.1.1 The data subject has given consent to the processing of their personal data for one or more specific purposes;

4.1.2 The processing is necessary for the performance of a contract to which the data subject is a party, or in order to take steps at the request of the data subject prior to entering into a contract with them;

4.1.3 The processing is necessary for compliance with a legal obligation to which the data controller is subject;

4.1.4 The processing is necessary to protect the vital interests of the data subject or of another natural person;

4.1.5 The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller; or

4.1.6 The processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

4.2 If the personal data in question are "special category data" (also known as "sensitive personal data") (for example, data concerning the data subject's race, ethnicity, politics, religion, trade union membership, genetics, biometrics (if used for ID purposes), health, sex life, or sexual orientation), at least one of the following conditions must be met:

4.2.1 The data subject has given their explicit consent to the processing of such data for one or more specified purposes (unless EU or EU Member State law prohibits them from doing so);

4.2.2 The processing is necessary for the purpose of carrying out the obligations and exercising specific rights of the data controller or of the data subject in the field of employment, social security, and social protection law (insofar as it is authorised by EU or EU Member State law or a collective agreement pursuant to EU Member State law which provides for appropriate safeguards for the fundamental rights and interests of the data subject);

4.2.3 The processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

4.2.4 The processing relates to personal data which are clearly made public by the data subject;

4.2.5 The processing is necessary for the conduct of legal claims or whenever courts are acting in their judicial capacity;

4.2.6 The processing is necessary for substantial public interest reasons, on the basis of EU or EU Member State law which shall be proportionate to the aim pursued, shall respect the essence of the right to data protection, and shall provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject;

4.2.7 The processing is necessary for the purposes of preventative or occupational medicine, for the assessment of the working capacity of an employee, for medical diagnosis, for the provision of health or social care or treatment, or the management of health or social care systems or services on the basis of EU or EU Member State law or pursuant to a contract with a health professional, subject to the conditions and safeguards referred to in Article 9(3) of the GDPR;

4.2.8 The processing is necessary for public interest reasons in the area of public health, for example, protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of EU or EU Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject (in particular, professional secrecy); or

4.2.9 The processing is necessary for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes in accordance with Article 89(1) of the GDPR based on EU or EU Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection, and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

5. Specified, Explicit, and Legitimate Purposes

5.1 BECG collects and processes the personal data set out in Part 19 of this Policy. This includes:

5.1.1 Personal data collected directly from data subjects; and

5.1.2 Personal data obtained from third parties.

5.2 BECG only collects, processes, and holds personal data for the specific purposes set out in Part 19 of this Policy (or for other purposes expressly permitted by the GDPR).

5.3 Data subjects are kept informed at all times of the purpose or purposes for which BECG uses their personal data. Please refer to Part 12 for more information on keeping data subjects informed.

6. Adequate, Relevant, and Limited Data Processing

BECG will only collect and process personal data for and to the extent necessary for the specific purpose or purposes of which data subjects have been informed (or will be informed) as under Part 5, above, and as set out in Part 19, below.

7. Accuracy of Data and Keeping Data Up-to-Date

7.1 BECG shall ensure that all personal data collected, processed, and held by it are kept accurate and up-to-date. This includes, but is not limited to, the rectification of personal data at the request of a data subject, as set out in Part 14, below.

7.2 The accuracy of personal data shall be checked when they are collected and at regular 12month intervals thereafter, if the project for which the data have been collected is still running. If any personal data are found to be inaccurate or out-of-date, all reasonable steps will be taken without delay to amend or erase those data, as appropriate.

8. Data Retention

8.1 BECG shall not keep personal data for any longer than is necessary in light of the purpose or purposes for which those personal data were originally collected, held, and processed.

8.2 When personal data are no longer required, all reasonable steps will be taken to erase or otherwise dispose of it without delay.

8.3 For full details of BECG's approach to data retention, including retention periods for specific personal data types held by BECG, please refer to our Data Retention Policy.

9. Secure Processing

BECG shall ensure that all personal data collected, held, and processed are kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction, or damage. Further details of the technical and organisational measures which shall be taken are provided in Parts 22 to 27 of this Policy.

10. Accountability and Record-Keeping

10.1 BECG's Company Data Protection Representative is Maddie Jones, dataprotection@becg.com, telephone 01962 893 893.

10.2 The Company Data Protection Representative shall be responsible for overseeing the implementation of this Policy and for monitoring compliance with this Policy, BECG's other data protection-related policies, and with the GDPR and other applicable data protection legislation.

10.3 In addition, BECG will appoint a number of Data Protection Controllers who will be responsible for overseeing the implementation of this Policy and for monitoring compliance with this Policy, BECG's other data protection-related policies, and with the GDPR and other applicable data protection legislation at its satellite offices and within service disciplines. These Data Protection Controllers will report to the Company Data Protection Representative.

10.4 BECG shall keep written internal records of all personal data collection, holding, and processing, which shall incorporate the following information:

10.4.1 The name and details of BECG, its Company Data Protection Representative, and any applicable thirdparty data processors;

10.4.2 The purposes for which BECG collects, holds, and processes personal data;

10.4.3 Details of the categories of personal data collected, held, and processed by BECG, and the categories of data subject to which those personal data relate;

10.4.4 Details of any transfers of personal data to non-EEA countries including all mechanisms and security safeguards;

10.4.5 Details of how long personal data will be retained by BECG (please refer to BECG's Data Retention Policy); and

10.4.6 Detailed descriptions of all technical and organisational measures taken by BECG to ensure the security of personal data.

11. **Data Protection Impact Assessments**

11.1 BECG shall carry out Data Protection Impact Assessments for any and all new projects and/or new uses of personal data which involve the use of new technologies and the processing involved is likely to result in a high risk to the rights and freedoms of data subjects under the GDPR.

11.2 Data Protection Impact Assessments shall be overseen by the Company Data Protection Representative and shall address the following:

11.2.1 The type(s) of personal data that will be collected, held, and processed;

11.2.2 The purpose(s) for which personal data are to be used;

11.2.3 BECG's objectives;

11.2.4 How personal data are to be used;

11.2.5 The parties (internal and/or external) who are to be consulted;

11.2.6 The necessity and proportionality of the data processing with respect to the purpose(s) for which they are being processed;

11.2.7 Risks posed to data subjects;

11.2.8 Risks posed both within and to BECG; and

11.2.9 Proposed measures to minimise and handle identified risks.

12. **Keeping Data Subjects Informed**

12.1 BECG shall provide the information set out in Part 12.2 to every data subject:

12.1.1 Where personal data are collected directly from data subjects, those data subjects will be informed of its purpose at the time of collection; and

12.1.2 Where personal data are obtained from a third party, the relevant data subjects will be informed of its purpose:

a) if the personal data are used to communicate with the data subject, when the first communication is made; or

b) if the personal data are to be transferred to another party, before that transfer is made; or

c) as soon as reasonably possible and in any event not more than one month after the personal data are obtained.

12.2 The following information shall be provided:

12.2.1 Details of BECG including, but not limited to, the identity of its Company Data Protection Representative;

12.2.2 The purpose(s) for which the personal data are being collected and will be processed (as detailed in Part 19 of this Policy) and the legal basis justifying that collection and processing;

12.2.3 Where applicable, the legitimate interests upon which BECG is justifying its collection and processing of the personal data;

12.2.4 Where the personal data are not obtained directly from the data subject, the categories of personal data collected and processed;

12.2.5 Where the personal data are to be transferred to one or more third parties, details of those parties;

12.2.6 Where the personal data are to be transferred to a third party that is located outside of the European Economic Area (the "EEA"), details of that transfer, including but not limited to the safeguards in place (see Part 26 of this Policy for further details);

12.2.7 Details of data retention;

12.2.8 Details of the data subject's rights under the GDPR;

12.2.9 Details of the data subject's right to withdraw their consent to BECG's processing of their personal data at any time;

12.2.10 Details of the data subject's right to complain to the Information Commissioner's Office (the "supervisory authority" under the GDPR);

12.2.11 Where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of the personal data and details of any consequences of failing to provide it; and

12.2.12 Details of any automated decision-making or profiling that will take place using the personal data, including information on how decisions will be made, the significance of those decisions, and any consequences.

13. Data Subject Access

13.1 Data subjects may make subject access requests ("SARs") at any time to find out more about the personal data which BECG holds about them, what it is doing with those personal data, and why.

13.2 Responses to SARs shall normally be made within one month of receipt, however this may be extended by up to two months if the SAR is complex and/or numerous requests are made. If such additional time is required, the data subject shall be informed.

13.3 All SARs received shall be handled by BECG's Company Data Protection Representative.

13.4 BECG does not charge a fee for the handling of normal SARs. BECG reserves the right to charge reasonable fees for additional copies of information that has already been supplied to a data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

14. Rectification of Personal Data

14.1 Data subjects have the right to require BECG to rectify any of their personal data that are inaccurate or incomplete.

14.2 BECG shall rectify the personal data in question, and inform the data subject of that rectification, within one month of the data subject informing BECG of the issue. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.

14.3 In the event that any affected personal data have been disclosed to third parties, those parties shall be informed of any rectification that must be made to those personal data.

15. **Erasure of Personal Data**

15.1 Data subjects have the right to request that BECG erases the personal data it holds about them in the following circumstances:

15.1.1 It is no longer necessary for BECG to hold those personal data with respect to the purpose(s) for which they were originally collected or processed;

15.1.2 The data subject wishes to withdraw their consent to BECG holding and processing their personal data;

15.1.3 The data subject objects to BECG holding and processing their personal data (and there is no overriding legitimate interest to allow BECG to continue doing so) (see Part 17 of this Policy for further details concerning the right to object);

15.1.4 The personal data have been processed unlawfully;

15.1.5 The personal data need to be erased in order for BECG to comply with a particular legal obligation.

15.2 Unless BECG has reasonable grounds to refuse to erase personal data, all requests for erasure shall be complied with, and the data subject informed of the erasure, within one month of receipt of the data subject's request. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.

15.3 In the event that any personal data that are to be erased in response to a data subject's request have been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

16. **Restriction of Personal Data Processing**

16.1 Data subjects may request that BECG ceases processing the personal data it holds about them. If a data subject makes such a request, BECG shall retain only the amount of personal data concerning that data subject (if any) that are necessary to ensure that the personal data in question are not processed further.

16.2 In the event that any affected personal data have been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing them (unless it is impossible or would require disproportionate effort to do so).

17. **Objections to Personal Data Processing**

17.1 Data subjects have the right to object to BECG processing their personal data based on legitimate interests, direct marketing (including profiling), and processing for scientific and/or historical research and statistics purposes.

17.2 Where a data subject objects to BECG processing their personal data based on its legitimate interests, BECG shall cease such processing immediately, unless it can be demonstrated that BECG's legitimate grounds for such processing override the data subject's interests, rights, and freedoms, or that the processing is necessary for the conduct of legal claims.

17.3 Where a data subject objects to BECG processing their personal data for direct marketing purposes, BECG shall cease such processing immediately.

17.4 Where a data subject objects to BECG processing their personal data for scientific and/or historical research and statistics purposes, the data subject must, under the GDPR, "demonstrate grounds relating to his or her particular situation". BECG is not required to

comply if the research is necessary for the performance of a task carried out for reasons of public interest.

18. **Profiling**

18.1 BECG uses personal data for profiling purposes. The profiling is done to ensure that public consultation programmes and activities have taken into account the demographic make-up of a particular consultation area. In general, the profiling will be anonymised, that is with no reference to specific data subjects, however, in some instances it may be necessary to profile individual data subjects.

18.2 When personal data are used for profiling purposes, the following shall apply:

18.2.1 Clear information explaining the profiling shall be provided to data subjects, including the significance and likely consequences of the profiling;

18.2.2 Appropriate mathematical or statistical procedures shall be used;

18.2.3 Technical and organisational measures shall be implemented to minimise the risk of errors. If errors occur, such measures must enable them to be easily corrected; and

18.2.4 All personal data processed for profiling purposes shall be secured in order to prevent discriminatory effects arising out of profiling (see Parts 22 to 26 of this Policy for more details on data security).

19. **Personal Data Collected, Held and Processed**

The following personal data are collected, held, and processed by BECG (for details of data retention, please refer to BECG's Data Retention Policy):

Data Ref.	Type of Data	Purpose of Data
Name	Name	To enable us to identify a data subject who: a) Is participating in a public consultation process. b) Is taking part in market research activities. Is participating in a marketing or PR campaign.
Address	Postal address	To enable us to contact data subjects to discuss: a) The project on which a public consultation is being held. b) Market research activities. c) Various products and services promoted by us on behalf of our clients.
Telephone	Mobile and landline numbers	To enable us to contact data subjects to discuss: a) The project on which a public consultation is being held. b) Market research activities. c) Various products and services promoted by us on behalf of our clients.

E-mail	E-mail address	To enable us to contact data subjects to discuss: a) The project on which a public consultation is being held. b) Market research activities. c) Various products and services promoted by us on behalf of our clients.

Data Ref.	**Type of Data**	**Purpose of Data**
Gender	Gender	a) To enable us to ensure that public consultation programmes and activities have taken into account the demographic makeup of a particular geography (or group of service-users). b) To ensure that market research activity is targeted at the correct audiences. c) To enable us to correctly target the promotion of various products and services on behalf of our clients.
Sexual orientation	Sexual Orientation	a) To enable us to ensure that public consultation programmes and activities have taken into account the demographic makeup of a particular geography (or group of service-users). b) To ensure that market research activity is targeted at the correct audiences. c) To enable us to correctly target the promotion of various products and services on behalf of our clients.
Date of Birth	Date of Birth	a) To enable us to ensure that public consultation programmes and activities have taken into account the demographic makeup of a particular geography (or group of service-users). b) To ensure that market research activity is targeted at the correct audiences. c) To enable us to correctly target the promotion of various products and services on behalf of our clients. d) To ensure that we are not collecting data from anyone under the age of 16.
Age Group	Age Group	a) To enable us to ensure that public consultation programmes and activities have taken into account the demographic makeup of a particular geography (or group of service-users). b) To ensure that market research activity is targeted at the correct audiences. c) To enable us to correctly target the promotion of various products and services on behalf of our clients. d) To ensure that we are not collecting data from anyone under the age of 16.

Ethnicity	Ethnicity	a) To enable us to ensure that public consultation programmes and activities have taken into account the demographic makeup of a particular geography (or group of service-users). b) To ensure that market research activity is targeted at the correct audiences. c) To enable us to correctly target the promotion of various products and services on behalf of our clients.

Data Ref.	**Type of Data**	**Purpose of Data**
Employment	Employment details	a) To enable us to ensure that public consultation programmes and activities have taken into account the demographic makeup of a particular geography (or group of service-users). b) To ensure that market research activity is targeted at the correct audiences. To enable us to correctly target the promotion of various products and services on behalf of our clients.
Shopping Habits	Information on where people shop and what they buy	To enable us to carry out work on behalf of clients to: a) Profile areas for potential development opportunities. b) Understand the shopping habits of different demographic groups, so that our clients can refine and develop new products and services and marketing activity.
Income	Income group	a) To enable us to ensure that public consultation programmes and activities have taken into account the demographic makeup of a particular geography (or group of service-users). b) To ensure that market research activity is targeted at the correct audiences. c) To enable us to correctly target the promotion of various products and services on behalf of our clients.
Feedback	Opinions	a) Opinions of data subjects as part of statutory and non-statutory public consultation exercises, including information on: • Views on proposed residential, commercial, retail, transport, energy, waste and general developments • Views on past residential, commercial, retail, transport, energy, waste and general developments • Views on residential, commercial, retail, transport, energy, waste and developments as well as these types of developments in general • Political opinions b) Opinions about the provision of both existing and proposed public and private sector service. Understand the shopping habits of different demographic groups, so that our clients can refine and develop new products and services and marketing activity.

Politics	Affiliations, memberships, voting intentions	To enable us to analyse feedback in respect of: a) Public consultation programmes and activities in the context of people's affiliations, memberships and voting intentions. b) Carry out work on behalf of clients to profile areas for potential development opportunities.
Data Ref.	**Type of Data**	**Purpose of Data**
Socio Demographic	Socio Demographic	To enable us to: a) Ensure that public consultation programmes and activities have taken into account the demographic make-up of a particular geography (or group of service-users). b) Carry out work on behalf of clients to profile areas for potential development opportunities. c) Understand the accommodation arrangements of different demographic groups, so that our clients can refine and develop new products and services and marketing activity.
Social Media	Social media names and profiles	To enable us to monitor people's opinions on developments made in public forums.
Housing	Information on home ownership. Tenure, type and size of housing	To enable us to: a) Ensure that public consultation programmes and activities have taken into account the demographic make-up of a particular geography (or group of service-users). b) Carry out work on behalf of clients to profile areas for potential development opportunities. c) Understand the accommodation arrangements of different demographic groups, so that our clients can refine and develop new products and services and marketing activity.
Disability	Disability	a) To enable us to ensure that public consultation programmes and activities have taken into account the demographic makeup of a particular geography (or group of service-users). b) To ensure that market research activity is targeted at the correct audiences. c) To enable us to provide services on behalf of clients in healthcare including the following: • Medical device and pharmaceutical development • The provision of health services by the public and private sectors • Public consultation activities around the provision of public and private sector healthcare.

Medical information	Information about current and past medical history	To enable us to provide services on behalf of clients in healthcare including the following: • Medical device and pharmaceutical development • The provision of health services by the public and private sectors • Public consultation activities around the provision of public and private sector healthcare.

20. **Data Security – Transferring Personal Data and Communications**

BECG shall ensure that the following measures are taken with respect to all communications and other transfers involving personal data:

20.1 All emails containing personal data must be encrypted using TLS and Bitlocker on Server Side;

20.2 All emails containing personal data must be marked "confidential";

20.3 Personal data may be transmitted over secure networks only; transmission over unsecured networks is not permitted in any circumstances;

20.4 Personal data may not be transmitted over a wireless network if there is a wired alternative that is reasonably practicable;

20.5 Personal data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely. The email itself should be deleted. All temporary files associated therewith should also be deleted**.** Once an email has been deleted and enters into the "Deleted Items" folder. Unless the user immediately empties the "Deleted Items" folder the data will be retained for a maximum of 30 days. On reaching the 30-day limit the "Deleted Items" folder will automatically purge the aged emails. The emails remain on the Exchange server hosted by Microsoft for another 30 days. On reaching the 30day limit the aged emails will be permanently deleted. During this time all data are fully encrypted using Bit Locker encryption on the hosted Microsoft servers;

20.6 Where personal data are to be sent by facsimile transmission the recipient should be informed in advance of the transmission and should be waiting by the fax machine to receive the data;

20.7 Where personal data are to be transferred in hardcopy form it should be passed directly to the recipient or sent using Royal Mail Recorded or a secure courier service; and

20.8 All personal data to be transferred physically, whether in hardcopy form or on removable electronic media shall be transferred in a suitable container marked "confidential".

21. **Data Security – Storage**

BECG shall ensure that the following measures are taken with respect to the storage of personal data:

21.1 All electronic copies of personal data should be stored securely using passwords and TLS and Bitlocker on Server-Side data encryption;

21.2 All hardcopies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet, or similar;

21.3 All personal data stored electronically should be backed up daily with backups stored offsite. All backups should be encrypted using TLS and Bitlocker on Server Side;

21.4 No personal data should be stored on any mobile device (including, but not limited to, laptops, tablets, and smartphones), whether such device belongs to BECG or otherwise without the

formal written approval of Julian Isaacson, Managing Director and, in the event of such approval, strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is absolutely necessary; and

21.5 No personal data should be transferred to any device personally belonging to an employee and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of BECG where the party in question has agreed to comply fully with the letter and spirit of this Policy and of the GDPR (which may include demonstrating to BECG that all suitable technical and organisational measures have been taken).

22. **Data Security – Disposal**

When any personal data are to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of. For further information on the deletion and disposal of personal data, please refer to BECG's Data Retention Policy.

23. **Data Security – Use of Personal Data**

BECG shall ensure that the following measures are taken with respect to the use of personal data:

23.1 No personal data may be shared informally and if an employee, agent, sub-contractor, or other party working on behalf of BECG requires access to any personal data that they do not already have access to, such access should be formally requested from Julian Isaacson, Managing Director;

23.2 No personal data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of BECG or not, without the authorisation of Julian Isaacson, Managing Director;

23.3 Personal data must be handled with care at all times and should not be left unattended or on view to unauthorised employees, agents, sub-contractors, or other parties at any time;

23.4 If personal data are being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it; and

23.5 Where personal data held by BECG are used for marketing purposes, it shall be the responsibility of the Marketing Manager to ensure that the appropriate consent is obtained and that no data subjects have opted out, whether directly or via a third-party service such as the TPS.

24. **Data Security – IT Security**

BECG shall ensure that the following measures are taken with respect to IT and information security:

24.1 All passwords used to protect personal data should be changed regularly and should not use words or phrases that can be easily guessed or otherwise compromised. All passwords must contain a combination of uppercase and lowercase letters, numbers, and symbols. All software used by BECG is designed to require such passwords.;

24.2 Under no circumstances should any passwords be written down or shared between any employees, agents, contractors, or other parties working on behalf of BECG, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method. IT staff do not have access to passwords;

24.3 All software (including, but not limited to, applications and operating systems) shall be kept up-to-date. BECG's IT staff shall be responsible for installing any and all security-related updates

not more than three months after the updates are made available by the publisher or manufacturer, unless there are valid technical reasons not to do so; and

24.4 No software may be installed on any Company-owned computer or device without the prior approval of the IT Manager.

24.5 BECG will maintain the Cyber Essentials Plus standard and will be audited annually to test the security of its IT network and data.

25. Organisational Measures

BECG shall ensure that the following measures are taken with respect to the collection, holding, and processing of personal data:

25.1 All employees, agents, contractors, or other parties working on behalf of BECG shall be made fully aware of both their individual responsibilities and BECG's responsibilities under the GDPR and under this Policy, and shall be provided with a copy of this Policy;

25.2 Only employees, agents, sub-contractors, or other parties working on behalf of BECG that need access to, and use of, personal data in order to carry out their assigned duties correctly shall have access to personal data held by BECG;

25.3 All employees, agents, contractors, or other parties working on behalf of BECG handling personal data will be appropriately trained to do so;

25.4 All employees, agents, contractors, or other parties working on behalf of BECG handling personal data will be appropriately supervised;

25.5 All employees, agents, contractors, or other parties working on behalf of BECG handling personal data shall be required and encouraged to exercise care, caution, and discretion when discussing work-related matters that relate to personal data, whether in the workplace or otherwise;

25.6 Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed;

25.7 All personal data held by BECG shall be reviewed periodically, as set out in BECG's Data Retention Policy;

25.8 The performance of those employees, agents, contractors, or other parties working on behalf of BECG handling personal data shall be regularly evaluated and reviewed;

25.9 All employees, agents, contractors, or other parties working on behalf of BECG handling personal data will be bound to do so in accordance with the principles of the GDPR and this Policy by contract;

25.10 All agents, contractors, or other parties working on behalf of BECG handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of BECG arising out of this Policy and the GDPR; and

25.11 Where any agent, contractor or other party working on behalf of BECG handling personal data fails in their obligations under this Policy that party shall indemnify and hold harmless BECG against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

26. Transferring Personal Data to a Country Outside the EEA

26.1 BECG may from time to time transfer ('transfer' includes making available remotely) personal data to countries outside of the EEA.

26.2 The transfer of personal data to a country outside of the EEA shall take place only if one or more of the following applies:

26.2.1 The transfer is to a country, territory, or one or more specific sectors in that country (or an international organisation), that the European Commission has determined ensures an adequate level of protection for personal data;

26.2.2 The transfer is to a country (or international organisation) which provides appropriate safeguards in the form of a legally binding agreement between public authorities or bodies; binding corporate rules; standard data protection clauses

adopted by the European Commission; compliance with an approved code of conduct approved by a supervisory authority (e.g. the Information Commissioner's Office); certification under an approved certification mechanism (as provided for in the GDPR); contractual clauses agreed and authorised by the competent supervisory authority; or provisions inserted into administrative arrangements between public authorities or bodies authorised by the competent supervisory authority;

26.2.3 The transfer is made with the informed consent of the relevant data subject(s);

26.2.4 The transfer is necessary for the performance of a contract between the data subject and BECG (or for pre-contractual steps taken at the request of the data subject);

26.2.5 The transfer is necessary for important public interest reasons;

26.2.6 The transfer is necessary for the conduct of legal claims;

26.2.7 The transfer is necessary to protect the vital interests of the data subject or other individuals where the data subject is physically or legally unable to give their consent; or

26.2.8 The transfer is made from a register that, under UK or EU law, is intended to provide information to the public and which is open for access by the public in general or otherwise to those who are able to show a legitimate interest in accessing the register.

27. Data Breach Notification

27.1 All personal data breaches must be reported immediately to BECG's Company Data Protection Representative.

27.2 If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the Company Data Protection Representative must ensure that the Information Commissioner's Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.

27.3 In the event that a personal data breach is likely to result in a high risk (that is, a higher risk than that described under Part 27.2) to the rights and freedoms of data subjects, the Company Data Protection Representative must ensure that all affected data subjects are informed of the breach directly and without undue delay.

27.4 Data breach notifications shall include the following information:

27.4.1 The categories and approximate number of data subjects concerned;

27.4.2 The categories and approximate number of personal data records concerned;

27.4.3 The name and contact details of BECG's Company Data Protection Representative (or other contact point where more information can be obtained);

27.4.4 The likely consequences of the breach;

27.4.5 Details of the measures taken, or proposed to be taken, by BECG to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

28. **Implementation of Policy**

This Policy shall be deemed effective as of 25 May 2018. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

This Policy has been approved and authorised by:

Name:	Julian Isaacson
Position:	Managing Director
Date:	16 May 2018
Due for Review by:	15 May 2019
Signature: