Privacy Policy

BBS Privacy Policy V3 December 2020

1. Policy objectives

1.1. To protect all Personal Information that BBS is the Controller of or processes on behalf of another Controller.

1.2. To protect the rights and freedoms of the Information Subjects whose Personal Information BBS is the Controller of or processes on behalf of another Controller.

1.3. To ensure appropriate controls are implemented that provide protection for Personal Information and are proportionate to their value and the threats to which they are exposed.

1.4. To ensure that BBS complies with and can demonstrate compliance with all relevant legal, customer and other third-party requirements relating to the processing of Personal Information in particular the Data Protection Act 2018 "DPA 2018" and the General Data Protection Regulations (EU 2016/679) "GDPR"

2. Scope

2.1. This policy applies to the processing of Personal Information by any employees or suppliers of BBS

3. Responsibilities

3.1. It is the responsibility of the Data Protection Team to ensure that this policy is implemented and that any resources required are made available.

3.2. It is the responsibility of the Data Protection Team to monitor the effectiveness of this policy and report the results at management reviews.

3.3. It is the responsibility of Data Protection Team to ensure that a Personal Information Processing Register is maintained.

3.4. It is the responsibility of all employees, to adhere to this policy and report to the Data Protection Team any issues they may be aware of that breach any of its contents.

3.5. BBS has appointed a Data Protection Team that will:

● Report directly to the Company Board of Directors;

● Be involved properly and in a timely manner, in all issues which relate to the protection of Personal Information;

● Have the full support of the Board of Directors in performing their tasks;

● Be provided with all resources necessary to carry out the tasks required by the DPA 2018 and the GDPR;

● Be provided with all the resources necessary to maintain their expert knowledge;

● Have unlimited access to Personal Information processing operations;

● Not receive any instructions from Senior Management regarding the exercise of the tasks required by the DPA 2018 and the GDPR;

● Not be dismissed or penalised by the Senior Management for performing tasks and duties required of them by the DPA 2018 and the GDPR;

● Not undertake any other tasks and duties that result in a conflict of interest.

3.6. It is the responsibility of the Data Protection Team to:

● Inform and advise Senior Management, employees and any suppliers who undertake processing of Personal Information on behalf of BBS, of their obligations in regards to this policy and the requirements of the DPA 2018 and the GDPR;

● Monitor BBS's compliance with this policy, the DPA 2018 and the GDPR;

● Ensure all employees have appropriate training with regards to processing of Personal Information;

● Act as a contact point for the Information Commissioner's Office on issues relating to the processing of Personal Information.

4. Definitions

Within this policy, the following definitions apply.

4.1. Asset: Any physical entity that can affect the confidentiality, availability and integrity of Personal Information.

4.2. Availability: The accessibility and usability of Personal Information upon demand by an authorised individual.

4.3. Automated decision-making: Processing of information that results in decisions being made about Information Subjects without any review of the information being made by an individual.

4.4. Beyond use: Controls placed on Personal Information that it is no longer necessary for BBS to keep where it is not reasonably feasible to delete the information. These controls must comply with guidance from the Information Commissioner's Office (see Information Commissioner's Office Guidance on GDPR Compliance).

4.5. Confidentiality: The restrictions placed on the access or disclosure of Personal Information

4.6. Controller: A 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 a set of Personal Information.

4.7. High risk processing: Processing of Personal Information (in particular using new technologies) that is likely to result in a high risk to the rights and freedoms of Information Subjects (see Information Commissioner's Office Guidance on GDPR Compliance).

4.8. Identifiable Natural Person: A natural person who can be identified directly or indirectly, in particular with 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 person.

4.9. Information subject: An Identifiable Natural Person who has Personal Information that BBS is the Controller of or is a Processor of on behalf of a Controller.

4.10. Integrity: The accuracy and completeness of Personal Information.

4.11. Personal information: Any information relating to an Identifiable Natural Person.

4.12. Personal information protection principles: Principles that shall be applied in relation to all Personal Information as laid down in the DPA 2018, the GDPR and any subsequent amendments.

4.13. Processor: A natural or legal person, public authority, agency or other body which processes Personal information on behalf of a Controller.

4.14. Security incident: Any event that has a potentially negative impact on the confidentiality and/or integrity and/or availability of Personal Information or restrict the rights and freedoms of Information Subjects.

5. Associated documents

5.1. All associated documents referred to in this policy are highlighted in bold and underlined.

6. Policy

6.1. Application of the Personal Information protection principles

● The following principles must be applied and compliance with them demonstrated in relation to all Personal Information that is accessed, stored or processed by employees, and employees or suppliers, while they are accessing or processing the BBS's information assets and any Personal Information that BBS is the Controller of or processing on behalf of another Controller:

● Personal information shall be processed lawfully, fairly and in a transparent manner;

● Personal information shall be collected for specified, explicit and legitimate purposes and not processed in a manner that is incompatible with those purposes;

● Any Personal Information collected shall be adequate, relevant and and limited to what is necessary in relation to the purposes for which it is processed;

● Any Personal information processed shall be accurate, kept up-to-date (where necessary) and every reasonable step is taken to ensure that Personal Information that is inaccurate with regards to the purposes for which it is processed is erased or rectified without delay;

● Personal information shall not be kept in form that permits identification of Information Subjects for longer than is necessary for purposes for the which the personal information is processed (Personal Information may be put Beyond Use where deletion is not reasonably feasible);

● Appropriate technical and organisational measures shall be taken to ensure appropriate security of the Personal Information, including protection against unauthorised or unlawful processing and accidental loss, destruction or damage;

● All processes and operations that involve the processing of Personal Information must be designed to ensure that these principles can be achieved and are applied. Where any changes are required to BBS's Assets that impact on the processing of Personal Information, a review of the Control Measures applied must be completed.

6.2. Registration with the Information Commissioner

● It is the responsibility of the Data Protection Team to ensure that the appropriate registration is maintained with the Information Commissioner.

6.3. Personal Information Processing Register

● A Personal Information Processing Register must be maintained that contains information on:

● All Personal Information that BBS is the Controller of regardless of whether it is processed by BBS or by a Processor engaged by BBS;

● All Personal Information that BBS is a Processor of on behalf a Controller or other Processor;

● The types of Information Subjects that the Personal Information relates to, the limit of the information collected and the source that it is obtained from;

● The reason the processing is undertaken and the the legal grounds for doing so;

● The types of processing employed and the methods and technologies used;

● The details of any Processors used (where BBS is the Controller) or direct Sub-Processors used (where BBS is the Processor);

● The country or region where the Personal Information is processed and stored;

● All recipients of the Personal Information;

● The period for which the Personal Information is retained and the justification for doing so;

● Whether any Automated Processing is undertaken;

● Whether the Personal Information falls into a Special Category and if so the processing justification offered by Article 9 of the GDPR that applies.

● Whether the Personal Information is transferred in any way outside of the EEA and if so the countries/territories/organisations it is transferred to.

6.4. Consent to process Personal Information

● Where BBS is a Controller of Personal Information and it undertakes processing of Personal Information requiring the consent of the Information Subject, a record of the consent must be

obtained from the Information Subjects using a Personal Information Processing Consent Form, unless consent can be demonstrated by some other statement or a clear affirmative action.

● The Personal Information Processing Consent Form will be based on the Privacy Notice + Consent Opt-in template. in all other circumstances;

6.5. When processing Personal Information obtained from an Information Subject

● Where BBS has collected personal data directly from an Information Subject, they must be provided with a Privacy Notice at that contains at least the following information who consent to the processing of their Personal information of:

● The contact details of the Data Protection Team at support@bbsltd.co.uk;

● The scope and legal justification of processing that will be undertaken with the information they provide;

● Where the legal justification for processing the Personal Information is the Controller's legitimate interest, details of the legitimate interest;

● Where the legal justification for Processing the Personal Information is that the Information Subject has consented to the processing, the existence of a right to withdraw consent at any time, without affecting the lawfulness of the processing carried out prior to the withdrawal;

● The categories of recipients who will have access to their Personal Information;

● The time period for which their information will be stored or the criteria that will be applied to determine the time period;

● Any planned transfers of their information to a third country or international organisation and information on the safeguards being applied and the means by which the Information Subject can obtain a copy of them or where they are available;

● Whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;

● Whether any automated decision-making will be applied to their information and if so the logic that will be applied and the envisaged consequences for them;

● Whether BBS is a joint Controller of the information and if so and overview of the agreement in place with other joint Controllers;

● Their rights to:

● request access to their information

● request corrections be made to their information

● request their information be deleted

● request that processing of their information is restricted

● request their information be transferred to another Controller

● lodge a complaint with the Information Commissioner

● and the means by which they can notify BBS to exercise one or more of these rights.

6.6. Processing of Personal Information obtained from third parties

● Where BBS is a Controller of Personal Information and it undertakes processing of Personal Information obtained from a third party (i.e. not directly from the Information Subjects it relates to) then unless:

● The Information Subject already has the information that BBS has obtained; or

● The collection or disclosure of the information is authorised or required by EU or UK law; or

● The disclosure of the information is restricted by due to the obligation of a professional body that has provided it or a requirement of EU or UK law;

● It would require a disproportionate effort to provide the information.

● BBS will provide the following information to Information Subjects about whom the Personal Information relates to:

● The name and contact details of BBS's Data Protection Team;

● The scope and legal justification of processing that will be undertaken with the information they provide;

● The categories of information that will be processed;

● The categories of recipients who will have access to their Personal Information;

● The source of the Personal Information and whether that source was publicly available;

● The time period for which their information will be stored or the criteria that will be applied to determine the time period;

● Where the legal justification for processing the Personal Information is the Controller's legitimate interest, details of the legitimate interest;

● Where the legal justification for Processing the Personal Information is that the Information Subject has consented to the processing, the existence of a right to withdraw consent at any time, without affecting the lawfulness of the processing carried out prior to the withdrawal;

● Any planned transfers of their information to a third country or international organisation and information on the safeguards being applied and the means by which the Information Subject can obtain a copy of them or where they are available;

● Whether any automated decision-making will the applied to their information and if so the logic that will be applied and the envisaged consequences for them;

● Whether BBS is a joint Controller of the information and if so and overview of the agreement in place with other joint Controllers;

● Their rights to:

● request access to their information

● request corrections be made to their information

● request their information be deleted

● request that processing of their information is restricted

● request their information be transferred to another Controller

● request to not be subject to a decision based solely on Automated Processing.

● lodge a complaint with the Information Commissioner

and the means by which they can notify BBS to exercise one or more of these rights;

● This information will be provided to Information Subjects either within one month of BBS obtaining the information or at the time of first communicating with the Information Subject (whichever is the soonest).

6.7. Accessing, processing and storage of Personal Information

● The Data Protection Team must ensure that appropriate physical and technical controls are in place to:

● Protect to confidentiality, integrity and availability of all Personal Information;

● Prevent unlawful processing of Personal Information.

● Personal information should be accessed, processed and stored only to:

● Fulfil the needs of customers;

● Comply with legal requirements;

● Enable the effective implementation of the organisation's ISMS.

● Access to Personal Information must be provided in only where is necessary for individuals to undertake tasks assigned to them that require access.

6.8. Requests by Information Subjects to exercise their rights and freedoms

● For all Personal Information that BBS is the Controller of:

● All requests by Information Subjects whose Personal Information is processed by BBS, to exercise their rights and freedoms under the DPA 2018 and the GDPR will be managed in accordance with the Handling of Personal Information Requests Procedure.

● Any information that needs to be provided to Information Subjects who submit requests will be provided in a concise, transparent, intelligent and easily accessible form, using clear and plain language.

● Any information requested by Information Subjects in the relation to any of their Personal Information processed by BBS that BBS is legally obliged to provide, will be provided free of charge unless the request if manifestly unfounded or excessive, in which case BBS may change a reasonable fee for providing the information of refuse to act on the request.

● Where the request covers the deletion of information that has been made public then BBS will take all reasonable steps possible to inform other Controllers who are processing the information to delete any copy of the information that they hold or any links they have to the information.

6.9. Transferring Personal Information

● Any transfer of personal information to a third party must be carried out under a written agreement, setting out the scope and limits of the sharing.

● In the event that BBS needs to transfer Personal Information to a non-EU country or an international organisation then:

● The relevant Privacy Notices need to identify this;

● The Information Subjects affected must be informed before the transfer takes place and provided with information regarding the safeguards that BBS will ensure are in place.

6.10. Compliance and Controls Assessments

● To ensure that:

● All controls employed to protect Personal Information is controlled or processed by BBS are maintained and effective;

● BBS complies with the DPA 2018 and the GDPR

● Audits will be completed annually as part of the company's Interna Audit programme.

6.11. Arrangements with Joint Controllers

● Where BBS is a joint Controller of any Personal Information then a Joint Controller Agreement (or an equivalent agreement) will be implemented with any joint Controllers;

6.12. Arrangements with Controllers

● Where BBS undertakes processing on behalf of a Controller:

● A Personal Information Processing Agreement (or an equivalent agreement) will be implemented with any Processors,

● No processing of information provided by the Controller will be undertaken without an explicit instruction from them.

6.13. Arrangements with Processors

● Where BBS uses a supplier to undertake processing on its behalf:

● A Personal Information Processing Agreement (or an equivalent agreement) will be implemented with any Processors;

● A Personal Information Processor Assessment will be completed to assess whether they can provide sufficient guarantees to implement appropriate control measures that will ensure the processing they undertake complies with the DPA 2018 and the GDPR and protects the rights and freedoms on the Information Subjects whose information they process on behalf of BBS.

● An audit of a supplier's compliance with the DPA 2018 and the GDPR will be undertaken where:

● The information obtained from a Personal Information Processor Assessment raises doubts as to the adequacy of the guarantees provided by a Processor; or

● The supplier is undertaking High Risk Processing; or

● A Personal Information Breach occurs that has a significant impact on the confidentiality or integrity or availability of any Personal Information and following an investigation of the root cause of the incident, the controls and processes employed by the supplier are identified as having been a contributing factor.

● The audit will be completed using a Personal Information Processing Compliance Assessment Form.

6.14. High Risk Processing

● A data impact assessment must be completed for any High Risk Processing of Personal Information that BBS is a Controller of before any such processing is started.

● The results of the data impact assessment must be recorded in the Personal Information Processing Register.

● If a data impact assessment indicates that the processing would result in a high risk to the rights and freedoms of the Information Subjects whose Personal Information is being processed, then Data Protection Team must consult with the Information Commissioner's office before any processing is started

6.15. Personal Information Breaches

● In the event of a Security Incident that compromises the confidentiality, integrity of availability of any Personal Information actions shall be taken and records maintained in accordance with the Security Incident Management Procedure.

7. Policy Review

This policy shall be reviewed at least annually or if significant changes occur that might affect its continuing suitability, adequacy and effectiveness.

8. Policy Authorisation

Signed on behalf of BBS:

Position: Director Date: 21/12/2020