Commercial Data Protection Policy

1. Introduction

1.1. TBT Marketing Ltd, ("**we/us**") is the Data Controller, and in some instances, we are the Data Processor, for the purposes of the EU General Data Protection Regulation and the Data Protection Act 2018.

1.2. We collect and use certain types of personal information about the following categories of individuals:

1.2.1. employees;

1.2.2. shareholders;

1.2.3. service users;

1.2.4. clients;

1.2.5. client's business partners & distributors

1.2.6. directors and other officers;

1.2.7. suppliers;

and other individuals who come into contact with us.

1.3. We will process this personal information in the following ways:

1.3.1. Refer to Appendix 1

1.3.2. to comply with statutory and contractual obligations relating to employment;

1.3.3. to comply with statutory and other legal obligations relating to safeguarding, of any individual at TBT Marketing Limited that comes into contact with children as part of his or her duties.

1.4. This policy is intended to ensure that personal information is dealt with properly and securely and in accordance with the EU General Data Protection Regulation (**GDPR**) and other related legislation. It will apply to information regardless of the way it is used or recorded and applies for as long as the information is held.

1.5. The GDPR applies to all computerised data and manual files if they come within the definition of a filing system. Broadly speaking, a filing system is one where the data is structured in some way that it is searchable on the basis of specific criteria (so you would be able to use something like the individual's name to find their information), and if this is the case, it does not matter whether the information is located in a different physical location.

1.6. This policy will be updated as necessary to reflect best practice, or amendments made to the GDPR or other relevant legislation and shall be reviewed every two years.

2. Personal Data

2.1. 'Personal data' is information that identifies an individual and includes information that would identify an individual to the person to whom it is disclosed because of any special knowledge that they have or can obtain· A sub-set of personal data is known as 'special categories of personal data'. This special category data is information that relates to:

2.1.1. race or ethnic origin;

2.1.2. political opinions;

2.1.3. religious or philosophical beliefs;

2.1.4. trade union membership;

2.1.5. physical or mental health;

2.1.6. an individual's sex life or sexual orientation;

2.1.7. genetic or biometric data for the purpose of uniquely identifying a natural person.

2.2. Special category data is given special protection, and additional safeguards apply if this information is to be collected and used.

2.3. Information relating to criminal convictions shall only be held and processed where there is legal authority to do so.

3. The Data Protection Principles

3.1. The six data protection principles as laid down in the GDPR must be followed at all times:

3.1.1. personal data shall be processed fairly, lawfully and in a transparent manner, and processing shall not be lawful unless one of the processing conditions (see paragraph 4) can be met;

3.1.2. personal data shall be collected for specific, explicit, and legitimate purposes, and shall not be further processed in a manner incompatible with those purposes;

3.1.3. personal data shall be adequate, relevant, and limited to what is necessary for the purpose(s) for which they are being processed;

3.1.4. personal data shall be accurate and, where necessary, kept up to date;

3.1.5. personal data processed for any purpose(s) shall not be kept for longer than is necessary for that/those purpose(s);

3.1.6. personal data shall be processed in such a way that ensures appropriate security of the data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

3.2. In addition to this, we are committed to ensuring that, at all times, anyone dealing with personal data shall be mindful of the individual's rights under the law (as explained in more detail in paragraphs 7 and 8 below).

3.3. We are committed to complying with the principles in paragraph 3.1 at all times. This means that we will:

3.3.1. inform individuals as to the purpose of collecting any information from them, as and when we ask for it;

3.3.2. be responsible for checking the quality and accuracy of the information;

3.3.3. regularly review the records held to ensure that information is not held longer than is necessary, and that it has been held in accordance with our Records Retention Policy;

3.3.4. ensure that when information is authorised for disposal it is done appropriately;

3.3.5. ensure appropriate security measures to safeguard personal information, whether it is held in paper files or on our computer system, and follow the relevant security policy requirements at all times;

3.3.6. share personal information with others only when it is necessary and legally appropriate to do so;

3.3.7. set out clear procedures for responding to requests for access to personal information, known as subject access requests;

3.3.8. report any breaches of the GDPR in accordance with the procedure in paragraph 0 below.

4. Conditions For Processing In The First Data Protection Principle

4.1. The individual has given consent that is specific to the particular type of processing activity, and that consent is informed, unambiguous and freely given;

4.2. The processing is necessary for the performance of a contract, to which the individual is a party, or is necessary for the purpose of taking steps with regard to entering into a contract with the individual, at their request;

4.3. The processing is necessary for the performance of a legal obligation to which we are subject;

4.4. The processing is necessary to protect the vital interests of the individual or another;

4.5. 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 us;

4.6. The processing is necessary for our legitimate interests or those of a third party, except where this interest is overridden by the rights and freedoms of the individual concerned. More details of this are given in the Privacy Notice.

5. Disclosure Of Personal Data

5.1. The following list includes the most usual reasons that we will authorise disclosure of personal data to a third party:

5.1.1. to give a confidential reference relating to a current or former employee;

5.1.2. for the prevention or detection of crime;

5.1.3. for the assessment of any tax or duty;

5.1.4. where it is necessary to exercise a right or obligation conferred or imposed by law upon us (other than an obligation imposed by contract) e.g. regulatory obligations under the Money Laundering Regulations;

5.1.5. for the purpose of, or in connection with, legal proceedings (including prospective legal proceedings);

5.1.6. for the purpose of obtaining legal advice;

5.1.7. for research, historical and statistical purposes (so long as this neither supports decisions in relation to individuals, nor causes substantial damage or distress);

5.2. We may receive requests from third parties (i.e. those other than the data subject, us, and our employees) to disclose personal data we hold about

individuals. This information will not generally be disclosed unless one of the specific exemptions under the GDPR which allow disclosure applies, or where disclosure is necessary for the legitimate interests of us or the third party concerned.

5.3. All requests for the disclosure of personal data must be sent to Human Resources, who will review and decide whether to make the disclosure, ensuring that reasonable steps are taken to verify the identity of the requesting third party before making any disclosure.

6. Security Of Personal Data

6.1. We will take reasonable steps to ensure that members of staff will only have access to personal data where it is necessary for them to carry out their duties. All staff will be made aware of this Policy and their duties under the GDPR. We will take all reasonable steps to ensure that all personal information is held securely and is not accessible to unauthorised persons.

6.2. For further details as regards security of IT systems, please refer to the ICT Policy.

7. Subject Access Requests

7.1. Anybody who makes a request to see any personal information held about them by us is making a subject access request. All information relating to the individual, including that held in electronic or manual files should be considered for disclosure, provided that they constitute a "filing system" (see paragraph 1.5).

7.2. All requests should be sent to Human Resources within three working days of receipt and must be dealt with in full without delay and at the latest within one month of receipt.

7.3. Where a child or young person does not have sufficient understanding to make his or her own request (usually those under the age of twelve, or over twelve but with a special educational need which makes understanding their information rights more difficult), a person with parental responsibility can make a request on their behalf. Human Resources must, however, be satisfied that:

7.3.1. the child or young person lacks sufficient understanding; and

7.3.2. the request made on behalf of the child or young person is in their interests.

7.4. Any individual, including a child or young person with ownership of their own information rights, may appoint another person to request access to their records. In such circumstances, we must have written evidence that the individual has authorised the person to make the application and Human Resources must be

confident of the identity of the individual making the request and of the authorisation of the individual to whom the request relates.

7.5. Access to records will be refused in instances where an exemption applies, for example, information sharing may place the individual at risk of significant harm or jeopardise police investigations into any alleged offence(s).

7.6. A subject access request must be made in writing. We may ask for any further information reasonably required to locate the information.

7.7. An individual only has the automatic right to access information about themselves, and care needs to be taken not to disclose the personal data of third parties where consent has not been given, or where seeking consent would not be reasonable, and it would not be appropriate to release the information. Particular care must be taken in the case of any complaint or dispute to ensure confidentiality is protected.

7.8. All files must be reviewed by Human Resources before any disclosure takes place. Access will not be granted before this review has taken place.

7.9. Where all the data in a document cannot be disclosed, a permanent copy should be made and the data obscured or retyped if this is more sensible. A copy of the full document and the altered document should be retained, with the reason why the document was altered.

8. Exemptions To Access By Data Subjects

Where a claim to legal professional privilege could be maintained in legal proceedings, the information is likely to be exempt from disclosure unless the privilege is waived.

9. Other Rights Of Individuals

9.1. We have an obligation to comply with the rights of individuals under the law and take these rights seriously. The following section sets out how we will comply with the right to:

9.1.1. object to processing;

9.1.2. rectification;

9.1.3. erasure; and

9.1.4. data portability.

10. Right To Object To Processing

10.1. An individual has the right to object to the processing of their personal data on the grounds of pursuit of a public interest or legitimate interest (grounds 4.5 and 4.6 above) where they do not believe that those grounds are made out.

10.2. Where such an objection is made, it must be sent to Human Resources within two working days of receipt, and Human Resources will assess whether there are compelling legitimate grounds to continue processing which override the interests, rights and freedoms of the individuals, or whether the information is required for the establishment, exercise or defence of legal proceedings.

10.3. Human Resources shall be responsible for notifying the individual of the outcome of their assessment within 10 working days of receipt of the objection.

10.4. Where personal data is being processed for direct marketing purposes, an individual has the right to object at any time to processing of personal data concerning him or her for such marketing (which includes profiling to the extent that it is related to such direct marketing) and his or her personal data shall no longer be processed by us for direct marketing purposes.

11. Right to Rectification

11.1. An individual has the right to request the rectification of inaccurate data without undue delay. Where any request for rectification is received, it should be sent to Human Resources within two working days of receipt, and where adequate proof of inaccuracy is given, the data shall be amended as soon as reasonably practicable, and the individual notified.

11.2. Where there is a dispute as to the accuracy of the data, the request and reasons for refusal shall be noted alongside the data and communicated to the individual. The individual shall be given the option of a review under the complaints procedure, or an appeal direct to the Information Commissioner.

11.3. An individual also has a right to have incomplete information completed by providing the missing data, and any information submitted in this way shall be updated without undue delay.

12. Right to Erasure

12.1. Individuals have a right, in certain circumstances, to have data permanently erased without undue delay. This right arises in the following circumstances:

12.1.1. where the personal data is no longer necessary for the purpose or purposes for which it was collected and processed;

12.1.2. where consent is withdrawn and there is no other legal basis for the processing;

12.1.3. where an objection has been raised under the right to object, and found to be legitimate;

12.1.4. where personal data is being unlawfully processed (usually where one of the conditions for processing cannot be met);

12.1.5. where there is a legal obligation on us to delete.

12.2. Human Resources will make a decision regarding any application for erasure of personal data and will balance the request against the exemptions provided for in the law. Where a decision is made to erase the data, and this data has been passed to other controllers, and/or has been made public, reasonable attempts to inform those controllers of the request shall be made.

13. Right To Restrict Processing

13.1. In the following circumstances, processing of an individual's personal data may be restricted:

13.1.1. where the accuracy of data has been contested, during the period when we are attempting to verify the accuracy of the data;

13.1.2. where processing has been found to be unlawful, and the individual has asked that there be a restriction on processing rather than erasure;

13.1.3. where data would normally be deleted, but the individual has requested that their information be kept for the purpose of the establishment, exercise or defence of a legal claim;

13.1.4. where there has been an objection made under paragraph 8.2, pending the outcome of any decision.

14. Right To Portability

If an individual wants to send his or her personal data to another organisation, he or she has a right to request that you provide his/her information in a structured, commonly used, and machine- readable format. If a request for this is made, it should be forwarded to Human Resources within two working days of receipt, and Human Resources will review and revert as necessary.

15. Breach Of Any Requirement Of The Gdpr

15.1. Any breach of the GDPR, including a breach of any of the data protection principles of the Data Protection Act 1998 (as amended or replaced from time to

time) shall be reported as soon as it is discovered, to Human Resources.

15.2. Once notified, the Human Resources shall assess:

15.2.1. the extent of the breach;

15.2.2. the risks to the data subjects as a consequence of the breach;

15.2.3. any security measures in place that will protect the information;

15.2.4. any measures that can be taken immediately to mitigate the risk to the individuals.

15.3. Unless Human Resources concludes that there is unlikely to be any risk to individuals from the breach, it must be notified to the Information Commissioner's Office within seventy-two hours of the breach having come to our attention, unless a delay can be justified.

15.4. The Information Commissioner shall be told:

15.4.1. details of the breach, including the volume of data at risk, and the number and categories of data subjects;

15.4.2. the contact point for any enquiries (which shall usually be Human Resources);

15.4.3. the likely consequences of the breach;

15.4.4. measures proposed or already taken to address the breach.

15.5. If the breach is likely to result in a high risk to the rights and freedoms of the affected individuals, Human Resources shall notify affected data subjects of the breach without undue delay, unless the data would be unintelligible to those not authorised to access it, or measures have been taken to mitigate any risk to the affected individuals.

15.6. Data subjects shall be told:

15.6.1. the nature of the breach;

15.6.2. who to contact with any questions; and

15.6.3. measures taken to mitigate any risks.

15.7. Human Resources shall be responsible for instigating an investigation into the breach, including how it happened, and whether it could have been prevented. Any recommendations for further training or a change in procedure shall be reviewed by the Board and a decision made about implementation of those recommendations.

16. CONTACT

If anyone has any concerns or questions in relation to this policy they should contact Human Resources.

APPENDIX 1

What personal information we might need and why

- **Your name**
- **Your Job Title**
- **Contact information (eg address, telephone numbers, email addresses)**
- **Information about your age, ethnicity, gender, nationality, disability status**
- **ID documentation**
- **Photographs**
- **Biographical data**
- **Your bank details**
- **Your occupation**
- **Your place of work**
- **Information about your education and qualifications**
- **Information about your skills and expertise**
- **Information relevant to our HR function**
- **Marketing & communications data (includes your preferences in receiving marketing from us, our clients and your communication preference)**
- **Transaction data (includes details of services we have provided to you)**

We may use/process this information to:

- **Carry out our statutory functions**
- **Recognise awarding organisations**
- **Handle complaints**
- **Conduct investigations**
- **Conduct research**
- **Understand people's views and opinions (eg through consultations)**
- **Improve our services**
- **Carry out administrative functions (eg HR)**
- **Share it with third parties for the purpose of obtaining advice and in complying with our contractual obligations**
- **Comply with our legal and regulatory obligations**
- **Enable payment to suppliers**
- **Enable payment to employees**
- **Arrange travel on your behalf**
- **Proof of right to work**
- **Organise travel insurance cover**
- **To register you as a new client**
- **To deliver relevant website content to you and measure or understand the effectiveness of the marketing we serve to you**
- **To make suggestions and recommendations to you about goods or services that may be of interest**

APPENDIX 2

Data Breach Incident Response Plan

The flow of actions following a Data Breach is classified in four main phases, following the guidelines
of the Information Commissioner's Office (ICO):

1. Containment and recovery
2. Assessment of ongoing risk
3. Notification of breach
4. Evaluation and response

1. Containment and recovery

- Data breaches and weaknesses which could lead to breaches need to be reported as soon as detected to Human Resources, who will lead the investigation.
- Following notification, Human Resources will open an incident log and make an initial assessment of the breach's severity. This step will involve Netitude Limited (TBT Marketing Limited's outsourced IT provider), who will help identify the most effective course of action to contain the situation and, where possible, recover any losses.
- Once the first two steps are completed, Human Resources will inform a Legal TBT Director and assess whether any other contacts outside the organisation need to be made aware of the breach, (in case directly involved), informing them of what TBT is going to do to assist in the containment exercise.

2. Assessing the risks

- After the initial assessment of the breach's severity, Human Resources, Netitude Limited and a Legal TBT Director will assess the risks which may be associated with the breach. The purpose of this is to identify potential adverse consequences for individuals, how serious and substantial these are and how likely they are to reoccur.
- Once the scope of the breach has been ascertained, there may be a need to obtain additional information about how and why this happened, the assets affected, the type of incident, its category and priority before putting together a dedicated team to manage the incident, (if appropriate).
- The above is achieved by interviewing the key personnel involved in the breach and their Line Managers, collecting all available information to help determine how the breach occurred, what actions have to be taken, whether outside parties are involved and whether the data subjects have been notified.

3. Notification of breaches

- The objective of any breach investigation is to identify what actions the organisation needs to take to first prevent a recurrence of the incident and second to determine whether the incident needs to be reported to appropriate regulatory bodies. The purpose of the report is to document the circumstances of the breach, what actions have been and will be taken, what recommendations have been made and whether the disciplinary procedure needs to

  be followed. Not all data protection breaches will result in formal action – this will be assessed on a case-by-case basis.
- In case a large number of people are affected or there are very serious consequences relating to a personal data breach, the ICO will be informed within 72 hours from detection.
- When notifying individuals, TBT will give specific and clear advice on the additional steps they can take to protect themselves, also providing all necessary information to ensure that they can contact TBT for any further information that might be needed.

4. Evaluation and response

- Key to preventing further incidents is ensuring the organisation learns from it. Following an incident, all stakeholders involved in investigating a data breach will attend a dedicated meeting chaired by Human Resources to evaluate the effectiveness of the response to it.
- Regular review meetings chaired by Human Resources will also take place to discuss "what if" scenarios, put forward recommendations, review and possibly update policies in the light of experience. These recurrent meetings will be attended by key stakeholders across the organisation and outsourced IT provider to consider trends and identify opportunities for improvement.
- Human Resources will be in charge to monitor staff awareness of security issues and look to fill any gaps through dedicated training or tailored advice.

APPENDIX 3

Outline Procedure for Data Breach Incidents

Once a breach has been reported the following actions must be followed by Human Resources, as soon as possible:

1. Create an entry in the Incident Log using the information provided by the Reporter
2. Create a folder under Data Breaches in TBT – Docs
3. Start an investigation report and save it in this folder together with any emails/documents relating to the breach
4. Prepare report for Breach Review meeting if required
5. If required, notification to the ICO must take place
6. An initial report for the ICO should also be prepared
7. Consideration must be given to notifying the individual(s) affected by the breach.

Factors to be considered include:

- Sensitivity of Information
- Volume of Information
- Likelihood of unauthorised use
- Impact on individual(s)
- Feasibility of contacting individual(s)

8. Any notification must be agreed by stakeholders connected with the breach, including Legal TBT Directors

9. Begin investigation and complete report as soon as possible

Recommendations

Regardless of the type and severity of incidents, there will always be recommendations to be made even if it is only to reinforce existing procedures. There are two categories of recommendation that can be made:

- Local – these apply purely to a department affected by the incident and will usually reflect measures that need to be taken to restrict the chances of the same type of incident occurring

- Corporate – some incidents will be caused by factors that are not unique to one department but can be found right across the organisation. Issues such as training, information handling and physical security affect all departments and it is essential that the organisation identifies such risks and puts in place measures to prevent the incident occurring elsewhere.

All recommendations will be assigned an owner and have a timescale by when they should be implemented which has a dual purpose. The first is to ensure that the organisation puts in place whatever measures have been identified and that there is an individual that can report back on progress. The second is that where incidents are reported to the ICO, TBT can demonstrate that the measures have either put in place or that there is a documented plan to do so.

This is a recurrent theme of ICO enforcement and it's important that the organisation's procedures reflect this. Identifying recommendations is more than just damage control – the knowledge of what has happened together with the impact is a fundamental part of learning which can then be disseminated throughout the organisation.