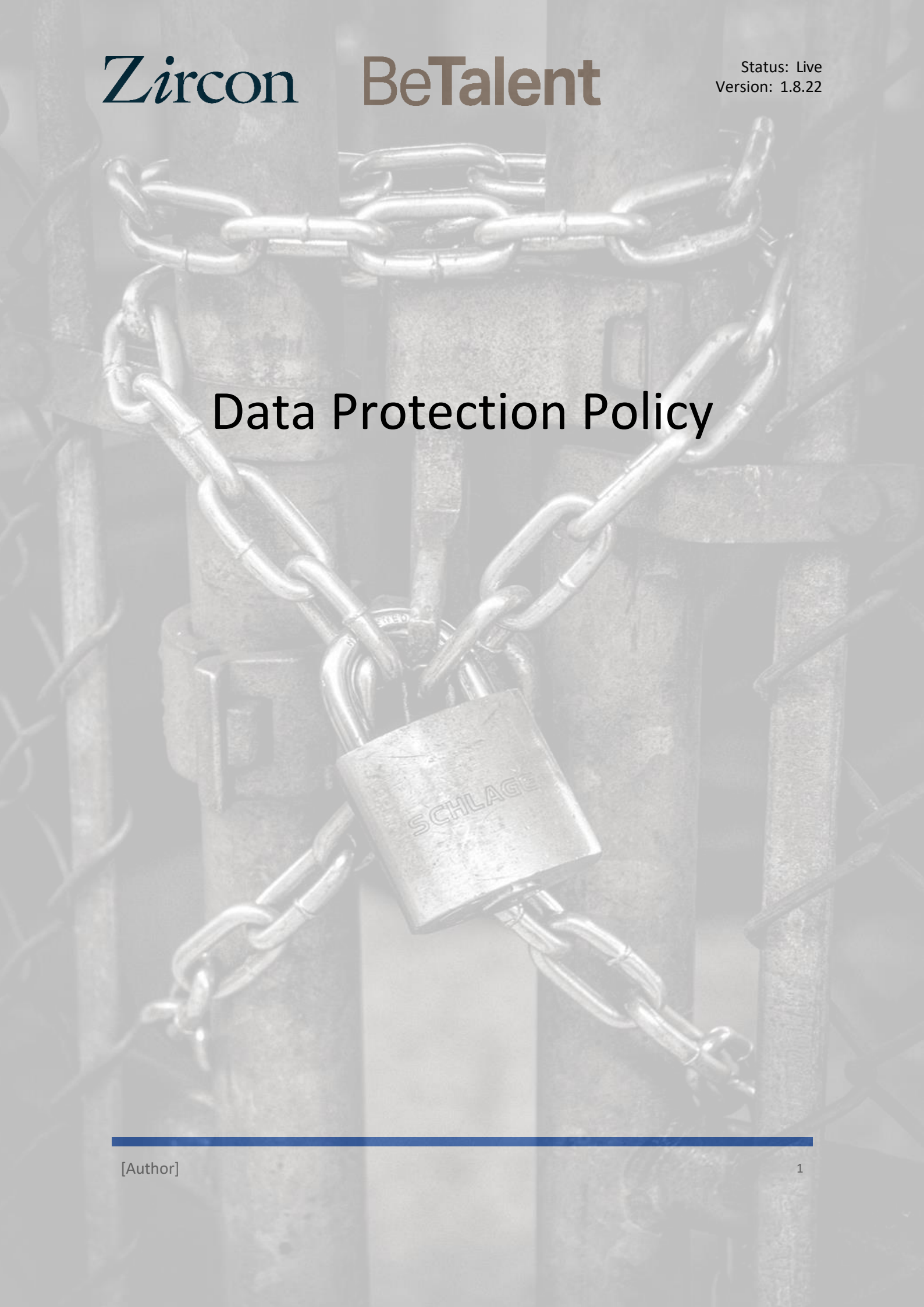
Zircon BeTalent

Status: Live
Version: 1.8.22



Data Protection Policy

Table of Contents

1. Introduction

Zircon and BeTalent (collectively referred to as 'ZBeT', 'we', 'us', 'our'), is a Data Controller for the purposes of the General Data Protection Regulation ("GDPR") and the Data Protection Act 2018 ("DPA 2018").

At ZBeT we recognise that the personal information we handle in our business activities is held by us in a position of trust. We respect its confidential nature and accept our responsibility to keep it secure. In the course of our business activities some of us will hold or have access to personal information (being any information which makes an individual identifiable) about colleagues, customers, suppliers, consumers and other individuals. It is essential that we respect and protect this information and ensure we meet the requirements of the Data Protection Legislation in effect where we do business. Any personal information which we hold, or which others collect, hold or process for us, or to which we have access must only be used for legitimate ZBeT business purposes.

Sensitive data is a sub-category of personal information that needs to be handled with particular care. This is information typically relating to an individual's health, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, sexual life and sexual orientation and any genetic data and biometric data processed to uniquely identify a person.

This policy outlines how ZBeT will comply with its responsibilities under the GDPR and DPA 2018.

2. Scope

This policy applies to all personal data we process regardless of the location where that personal data is stored (e.g. on an employee's own device) and regardless of the data subject.

All staff and others processing personal data on ZBeT's behalf must read it. A failure to comply with this policy may result in disciplinary action.

All managers are responsible for ensuring that all staff within their area of responsibility comply with this policy and should implement appropriate practices, processes, controls and training to ensure that compliance.

The Chief Operating Office, Sarah Linton is responsible for overseeing this policy, as is also the designated Data Protection Officer (DPO). She can be reached at sarah.linton@zircon-mc.co.uk.

3. Policy objectives

ZBeT holds written (offline) and electronic (online) personal information about our employees, customers, suppliers, consumers and other individuals. As an employer we process personal information about our employees (and, in limited circumstances, their family members) for employment administration purposes, from recruitment and reference checks through to performance, payroll and pension administration.

We also handle personal information of customers, suppliers, consumers and other individuals for a variety of other business purposes, including customer and supplier administration, credit checking, consumer research, marketing and promotion of our products and crime prevention or detection.

This information may be held in paper format (notebooks) or electronically within computers, mobile devices, email systems, HR systems, other applications (including communications and sharing applications and marketing databases some of which may be owned and operated by third parties. Where we engage with such third parties, they are required to protect personal information.

This policy therefore seeks to ensure that we:

- Are clear about how personal data must be processed and ZBeT's expectations for all those who process personal data on its behalf.
- Comply with the data protection laws and with good practice.
- Protect ZBeT's reputation by ensuring the personal data entrusted to us is processed in accordance with data subjects' rights.
- Protect ZBeT from risks of personal data breaches and other breaches of data protection law.

4. Definitions

Personal Data – data/information that relates to a living individual who can be identified from the data or from any other information that is in the possession of, or likely to come into the possession of the data controller. It includes any expression of opinion and any indication of the intentions of the data controller (or any other person) in respect of the individual.

Special Categories of Personal Data – specific categories of personal data which reveal the racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic, biometric and health data of data subjects, and information relating to a data subject's sex life or sexual orientation. These categories are subject to additional processing restrictions.

Data Controller – the person or organisation who determines the purposes for which and the manner in which any personal data are, or are to be, processed. ZBeT is the data controller in respect of all personal information that relates to our business.

Data Subject – is the identified or identifiable person to whom the personal data relates.

Processing – is defined very broadly and encompasses collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction (that is, the marking of stored data with the aim of limiting its processing in the future, erasure and destruction. In effect, any activity involving personal data falls within the scope of the GDPR.

Data Processor – the person or organisation who processes personal data on behalf of a data controller.

5. Data protection principles

ZBeT has an obligation to comply with the following Data Protection principles when processing personal data.

- **Fairly, Lawfully and Transparently**: We should process personal information fairly, lawfully and transparently.
- **Purpose Limitation**: We should collect personal information only for specified, explicit and legitimate purposes and only use it only in this way unless other uses are permitted by law, the individual has consented or it is within their reasonable expectation.
- **Minimisation**: The personal information we handle should be enough and limited to what is relevant and necessary for the purpose.
- **Accuracy**: Personal information should be accurate and where necessary kept up to date.
- **Storage Limitation**: Personal information should be in a form which does not allow the identification of individuals for longer than is necessary for the handling purpose.
- **Confidentiality and Integrity**: Processed with appropriate confidentiality and integrity.
- **Accountability**: ZBeT must also be able to demonstrate its compliance.

5.1. Fairly, lawfully and transparently

We should ensure that personal information is processed fairly, lawfully and transparently. This means we need to check what legal basis we have to process personal information and inform individuals what categories of personal information we have collected, or will collect, and explain the purpose(s) for which their personal information will be used.

5.2. Purpose limitation

We should collect personal information only for specified, explicit and legitimate purposes and only use it in this way unless other uses are permitted by law, the individual has consented or it is within their reasonable expectations. This ensures that there are 'no surprises' for the individual regarding how we use their personal information. Usually ZBeT will provide this information to individuals through the use of a Privacy Notice or Privacy Policy.

Please ask Sarah Linton for any support you need preparing a Privacy Notice. Sensitive personal information needs to be handled with particular care. We should try not to collect or use sensitive personal information at all unless the individual has made the information public themselves (e.g. political beliefs) or the person explicitly consents to ZBeT using it for a specific purpose (e.g. to receive occupational health services) or, in exceptional circumstances, as permitted or required by law. We should apply the data minimisation principle and comply with the Information Handling Standard to protect sensitive data.

We are committed to keeping data confidential. The data supplied to us may differ depending upon whether from a client or a candidate. We process information for the purpose of providing

consulting services to our clients, which may include the carrying out of Questionnaires of personal characteristics, performance and workplace, and generating analysis, research, comment and reports in relation to such Questionnaires. We may also process personal information for the purposes of using and refining Questionnaire tools, research, analysis, accounting, billing and audit, credit or other payment card verification, security, administration, enforcing and defending legal rights, systems testing, maintenance and product development, customer relations, performing our obligations to individuals and our clients whether under contract or otherwise, and to help us in future dealings with you. The Questionnaire reports and services we provide to our clients may be used by them for purposes which may include the selection and development of individuals in an employment or human resources context.

If you are an existing client, we may email you with information about further questionnaires, reports and services similar to those which were the subject of a previous contact with you.

5.3. Data Minimisation

We should only handle personal information that is adequate, relevant, and limited to what is necessary for the purpose it was collected. For example, we should strip out irrelevant data fields when collecting personal information from individuals and when disclosing information to a third party (e.g. to a service provider) we should only provide the minimum amount of personal information the third-party needs.

5.4. Data Accuracy

We should ensure that personal information is accurate and allow individuals to update their personal information taking all reasonable steps to amend or delete inaccurate or irrelevant data.

5.5. Data storage limitation

We should securely destroy or delete redundant or excessive data (or suppress in the case of consumer data) in line with applicable retention schedules. Where practical, we should consider whether to anonymise personal information or use an alias which replaces personal identifiers in a data set with other values (pseudonyms). For personal information to be truly anonymous it needs to fulfil certain legal requirements. Please check with Sarah Linton if in doubt.

5.6. Data confidentiality and integrity

We should handle personal information with appropriate confidentiality and ensure data integrity.

5.7. Data Accountability

The accountability principle covers the range of requirements for organisations to demonstrate data protection compliance. Other requirements explained in this section cover High Risk Processing and when a Privacy Impact assessment is needed; Security; Individual Rights; Third Party Data Handling and International Data Transfer.

5.7.1.High risk processing and privacy impact assessment

Data Protection Legislation in some countries requires that a privacy impact assessment (PIA) should be carried out when the processing of personal information is likely to result in a high risk to individuals (e.g. this includes material damage or any harm to them). For example, if you are engaging in an innovative marketing activity or a new third-party service provider, new technology, product or service or any monitoring activity we should assess the risk posed to individuals and if that risk is likely to be high then a PIA should be conducted. You must consult with Sarah Linton on the need to complete a PIA. "Privacy by design" needs to be demonstrated in many countries. The PIA should be carried out early to ensure any new processing activity, tool or functionality involved in the handling of personal information is designed and built in a way that allows it to comply with the Data Protection Principles listed at the start of this Policy.

If you are involved in any new digital marketing activities and /or profiling involving personal information you must comply with our Digital Code and consult Sarah Linton early on to ensure that the legal requirements are met. In some markets such as the EU and the UK there are potentially significant restrictions on direct marketing and profiling and you may need to complete a PIA and check whether you need consumer consent or adaptions to your transparency notice for direct marketing activities.

5.7.2.Security

We should store personal information securely and follow applicable security policies and guidance. All systems that hold personal information should have clear well-managed and documented organisational access controls and protocols (which are appropriate to the sensitivity of the personal information) and ensure any bulk personal information removed from the system is appropriately secure at all times.

5.7.3.Individual Rights

Individuals may ask us to access, correct, obtain a copy of or delete personal information that we hold about them. Immediately Sarah Linton if an individual makes a request. Statutory time periods within which we must respond could apply and may be as short as 14 or 30 days so it is important to contact with Sarah Linton promptly. Individuals also have the right to object to our using their personal information for certain purposes, such as direct marketing. Individuals may also have the right to file a formal complaint in relation to the collection and processing of their personal information to the relevant supervisory authority (e.g. the Information Commissioner's Office in the UK or the Data Protection Commissioner in Ireland).

5.7.4.Third party data processing

Whenever personal information is processed by a third party for our business purposes you should consult Sarah Linton to identify any contractual protections or steps required such as the completion of a PIA. In the EU and UK, for instance, the GDPR requires processing clauses to be included in contracts which involve handling personal information.

Generally, the disclosure and/or transfer of personal information to third parties should not occur unless an agreement exists confirming that they will give the data the appropriate level of protection and ensure that appropriate security measures are in place. ZBeT should not disclose an individual's personal information to third parties unless they have agreed to this or it is otherwise permitted or required by law. Sometimes, ZBeT may be legally obliged to make disclosures or there may be a legitimate business requirement to disclose the data which does not prejudice the interests of individuals or breach local privacy laws.

All requests for disclosure of personal information to third parties should be referred to Sarah Linton unless we know how to deal with the request in line with applicable Data Protection Legislation and this Policy. Personal information of individuals within the UK and EU may not be shared with any with government bodies outside the EU without prior consultation with Sarah Linton on any EU clearances needed (e.g. in the context of an investigation or litigation).

5.7.5.International transfer

If you are transferring personal information to another country, Data Protection Legislation may require us to put certain safeguards in place before the transfer happens.

6. Data subjects' rights

Data subjects have rights in relation to the way we handle their personal data. These include the following rights:

1. Where the legal basis of our processing is consent, to withdraw that consent at any time.
2. To ask for access to the personal data that we hold.
3. To prevent our use of the personal data for direct marketing purposes.
4. To object to our processing of personal data in limited circumstances.
5. To ask us to erase personal data without delay:
    a. If it is no longer necessary in relation to the purposes for which it was collected or otherwise processed.
    b. If the only legal basis of processing is Consent and that Consent has been withdrawn and there is no other legal basis on which we can process that personal data.
    c. If the data subject objects to our processing where the legal basis is the pursuit of a legitimate interest or the public interest and we can show no overriding legitimate grounds or interest.
    d. If the data subject has objected to our processing for direct marketing purposes.
    e. If the processing is unlawful.
6. To ask us to rectify inaccurate data or to complete incomplete data.
7. To restrict processing in specific circumstances e.g. where there is a complaint about accuracy.
8. To ask us for a copy of the safeguards under which personal data is transferred outside of the EU.

9. The right not to be subject to decisions based solely on automated processing, including profiling, except where necessary for entering into, or performing, a contract, with ZBeT; it is based on the data subject's explicit consent and is subject to safeguards; or is authorised by law and is also subject to safeguards.
10. To prevent processing that is likely to cause damage or distress to the data subject or anyone else.
11. To be notified of a personal data breach which is likely to result in high risk to their rights and freedoms.
12. To make a complaint to the ICO.
13. In limited circumstances, receive or ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format.

In addition, an individual is entitled to receive further information about ZBeT's processing of their personal data as follows:

1. The purposes
2. The categories of personal data being processed
3. Recipients/categories of recipient
4. Retention periods
5. Information about their rights
6. The right to complain to the ICO,
7. Details of the relevant safeguards where personal data is transferred outside the EEA
8. Any third-party source of the personal data

You should not allow third parties to persuade you into disclosing personal data without proper authorisation. For example, clients' contractors do not have an automatic right to gain access to clients' data.

The entitlement is not to documents per se (which may however be accessible by means of the Freedom of Information Act, subject to any exemptions and the public interest), but to such personal data as is contained in the document. The right relates to personal data held electronically and to limited manual records.

You must verify the identity of an individual requesting data under any of the rights listed
Requests must be complied with, usually within one month of receipt.

You must immediately forward any Data Subject Access Request you receive to Sarah Linton. You should not alter, conceal, block or destroy personal data once a request for access has been made. You should contact Sarah Linton before any changes are made to personal data which is the subject of an access request.

A charge can be made for dealing with requests relating to these rights only if the request is excessive

or burdensome.

7. Information disclosure

Information is disclosed to our clients in the context of the provision of services and reports to them in connection with the Questionnaires that have been performed. We do not control the further dissemination or use of this information by our clients.

To facilitate the questionnaire process, information may also be passed to other companies within the ZBeT and its agents from time to time. We may also pass data containing information in an anonymised and/or statistically aggregated form to our approved agents, current or future potential clients or research institutions. We may from time to time appoint third parties to process data containing information on our behalf as a data processor. We research responses to our tests and questionnaires in the light of areas such as gender, age and ethnic origin over the longer term; this is considered best practice and allows us to monitor our tools for fairness in use.

Due to the international nature of internet-based questionnaire services, the persons to whom we may disclose this information may be located in countries outside of the European Economic Area ("EEA"). These countries may not have data protection laws equivalent to those which are in force in the EEA to protect your information. Where data is transferred to third parties, these parties are bound by the terms of the ZBeT Privacy Policy contained on the ZBeT website and other data sharing agreements.

By submitting personal data, it is agreed to this transfer, storing or processing. We will take all steps reasonably necessary to ensure that your data is treated securely and in accordance with this privacy policy. All information you provide to us is stored on our secure servers and the backup data is encrypted.
We may disclose your personal information to third parties:

- In the event that we sell any part of our business or assets of our business, in which case we may disclose your personal data to the prospective buyer of the business or assets. We may also disclose your personal data to a vendor of another business or assets that we are acquiring or to a joint venture or merger partner.
- If ZBeT assets are acquired by a third party, personal data held by it about its customers will be one of the transferred assets.
- If we are under a duty to disclose or share personal data in order to comply with any legal obligation, or in order to enforce or apply our Terms of Use or our applicable Standard Terms and Conditions and other agreements; or to protect the rights, property, or safety of ZBeT, our customers, or others. This includes exchanging information with other companies and organisations for the purposes of fraud protection and credit risk reduction.

8. Reporting a data breach

The GDPR requires that we report to the Information Commissioner's Office (ICO) any personal data breach where there is a risk to the rights and freedoms of the data subject. Where the Personal data breach results in a high risk to the data subject, he/she also has to be notified unless subsequent steps have been taken to ensure that the risk is unlikely to materialise, security measures were applied to render the personal data unintelligible (e.g. encryption) or it would amount to disproportionate effort to inform the data subject directly. In the latter circumstances, a public communication must be made or an equally effective alternative measure must be adopted to inform data subjects, so that they themselves can take any remedial action.

We have put in place procedures to deal with any suspected personal data breach and will notify data subjects or the ICO where we are legally required to do so.

If you know or suspect that a personal data breach has occurred, you should immediately contact Sarah Linton at sarah.linton@zircon-mc.co.uk, and follow the instructions in the Data Breach Policy.

You must retain all evidence relating to personal data breaches in particular to enable ZBeT to maintain a record of such breaches, as required by the GDPR.

9. Record Keeping

The GDPR requires us to keep full and accurate records of all our data processing activities. You must keep and maintain accurate corporate records reflecting our processing, including records of data subjects' Consents and procedures for obtaining Consents, where Consent is the legal basis of processing.

These records should include, at a minimum, the name and contact details of ZBeT as Data Controller and the DPO, clear descriptions of the personal data types, data subject types, processing activities, processing purposes, third-party recipients of the personal data, personal data storage locations, personal data transfers, the personal data's retention period and a description of the security measures in place.

Records of personal data breaches must also be kept, setting out:

1. the facts surrounding the breach.
2. its effects; and
3. the remedial action taken.

10.Document history

10.1. Revision history

This document is subject to Change Control and as such any amendments must be carried out through the Document Change Management process and all Approvers must agree to the amendments. This document will update as and when required, and in any case, on an annual basis

Date of this revision 01/08/2022 Date of next review 01/08/2023

Version Number	Revision Date	Change History	Changes Marked	Updated By
V1.1	Nov 2020			SCL
V1.8.21	02/08/2021	Update version number, distribution list and formatting.	n/a	Sarah Linton
V1.8.22	01/08/2022	Amended version name and number. Re-formatted. Content amended to reflect best industry practices.	yes	Sarah Linton, Talal Malik

10.2. Reviewers

This document requires to be reviewed by the following reviewers.

Name	Title	Review date
Sarah Linton, Stu Scott Davies, Rhys Connolly	COO, IT Director, Strategic Client Partner.	02/08/2021
Sarah Linton, Stu Scott Davies	COO, IT Director	15/08/2022

10.3. Approvers

This document requires the following approvals.

Name	Title	Approved date
Sarah Linton	Director.	30/10/2020
Sarah Linton, Stu Scott Davies, Rhys Connolly	COO, IT Director, Strategic Client Partner.	02/08/2021
Sarah Linton, Stu Scott Davies	COO, IT Director	15/08/2022

10.4. Distribution list

Once complete, this document will be distributed to:

All interested parties.