InfoLogic Ltd
Policies

Responsible for oversight and document
M Eldridge
customerservices@infologic.biz

Revision Control
21st August 2019 updated cookie policy - M Eldridge
16th OCT 17 (agent, contractor and employee policies added) - M Eldridge

Treating Customers Fairly (TCF) (agents / contractors / employees)

The Directors, Senior Management and Employees of InfoLogic Ltd as well as Consultants working for InfoLogic Ltd are committed to ensure that the Financial Services Authority's principles of treating customers fairly (TCF) is applied in all areas of our day to day business activities.

In adopting the TCF principle we recognise that fair treatment of our customers is about adding value to the service we offer by aiming to:

- protect the interests of our customers at each stage of the product life cycle, from promotion right through to after sales service
- meet as best we can the unique needs of each customer by offering a transparent, efficient and professional service, and constantly reviewing our service to identify areas for improvement

In practical terms for the different areas of our business this means:

- ensuring that promotional material is clear, compliant, jargon free and appropriately targeted
- ensuring that sales staff (both on and off-site) have thorough training on all products they advise on or sell, understand who they are and aren't suitable for, and are encouraged to challenge product providers where they spot inconsistencies, ambiguities or potential unfairness in the product literature or product features
- operating sales remuneration systems which assure fairness to the customer as well as customer satisfaction, rather than only rewarding sales volumes
- finding ways to encourage non sales staff to implement TCF in their day to day business activities
- keeping detailed records of customer instructions and profile/attitude to risk, and of the advice and options given before, during and after a sale – to help ensure we treat customers fairly and can deal with any complaints that may arise swiftly and fairly
- encouraging after sales contact with clients where appropriate to correct or improve on the service already offered
- ensuring that customer complaints are assessed fairly, promptly and impartially, and in line with FSA deadlines and rules
- encouraging staff to recommend improvements to service following customer complaints – and monitoring the outcome

- ensuring that staff are kept up to date with relevant training in relation to competence, data protection and other matters directly affecting the quality of service offered to customers
- offering regular training in the principle of TCF at all levels of the business
- regularly monitoring and reporting on all of the above TCF activities as part of the company's monthly statistics/MI, in order to assess TCF performance across the business and recommend changes where appropriate
- ensuring that TCF values, which are set and communicated by Senior Management, are supported by all staff and understood in the same way

Information Security (including Cyber)

OBJECTIVE

The purpose and objective of this Information Security (including Cyber Information) Policy is to protect the company's information assets (note 1) from all threats, whether internal or external, deliberate or accidental, to ensure business continuity, minimise business damage and maximise return on investments and business opportunities.

POLICY

- The Company's Directors have approved this Information Security Policy.
- It is our policy to ensure that:

    a. Information will be protected from a loss of: confidentiality (note 2), integrity (note 3) and availability (note 4).
    b. Regulatory and legislative requirements will be met (note 5).
    c. Business continuity plans will be produced, maintained and tested (note 6).
    d. Information security training will be available to all staff.
    e. All breaches of information security, actual or suspected, will be reported to, and investigated by, the Information Security Manager.

- Guidance and procedures will be produced to support this policy. These may/will include risk assessment, information classification, data protection, credit card handling (PCI), incident handling, information backup, system access, third party services (supplier due diligence), malware controls, mobile device security & remote working, passwords and encryption.
- The role and responsibility of the designated Information Security Manager (note 7) is to manage information security and to provide advice and guidance on implementation of the Information Security Policy.
- The designated owner of the Information Security Policy [name] has direct responsibility for maintaining and reviewing the Information Security Policy.
- All managers are directly responsible for implementing the Information Security Policy within their business areas.
- It is the responsibility of each employee to adhere to the Information Security Policy.

NOTES

1. Information takes many forms and includes data printed or written on paper, stored electronically, transmitted by post or using electronic means, stored on tape or video, spoken in conversation.
2. Confidentiality: ensuring that information is accessible only to authorised individuals.
3. Integrity: safeguarding the accuracy and completeness of information and processing methods.

4. Availability: ensuring that authorised users have access to relevant information when required.
5. This includes the requirements of legislation such as the Companies Act, the Data Protection Act, the Computer Misuse Act and the Copyright, Design and Patents Act.
6. This will ensure that information and vital services are available to users whenever they need them.
7. Depending on the size and nature of the business this may be a part or full-time role for the nominated person.

Health & Safety

We are committed to ensuring the highest practicable standards of health and safety. In particular, we acknowledge our duties under the Health and Safety at Work Act 1974 and secondary health and safety legislation.

Accordingly, we are committed to ensuring the health and safety of our employees, sub-contractors and members of the public who may be affected by our work as much as is reasonably practicable, and will assess and alter our work conditions, systems and equipment where necessary.

We genuinely care for our staff and others affected by our work, and we design our systems accordingly. In addition, we actively encourage all our staff and contractors to engage and cooperate on workplace matters, in particular health and safety.

Statement of general policy

More particularly, we are committed to:

- Managing health and safety risks and thereby preventing accidents and work-related ill health. In particular, we have conducted a risk assessment (including fire risk assessment) and will review it when appropriate.
- Providing first aid where necessary and recording/reporting accidents when necessary.
- Communicating and providing training to employees on health and safety matters.
- Engaging and consulting with employees on health and safety matters as appropriate.
- Implementing emergency procedures and evacuation plans as appropriate.
- Complete accident/incident recording and reporting procedures as appropriate.
- Maintaining safe and healthy working conditions as appropriate.
- Ensure work equipment is suitable, safe and maintained appropriately as appropriate.

Data Protection (agents / contractors / employees)

Introduction

In the course of your work with our Company you are likely to collect, use, transfer or store personal information about employees, clients, customers and suppliers, for example their names and home addresses. The UK's data protection legislation, including the General Data Protection Regulations (GDPR) contains strict principles and legal conditions which must be followed before and during any processing of any personal information.

The purpose of this policy is to ensure that you are aware that everyone has a responsibility to comply with the principles and legal conditions provided by the data protection legislation, including the GDPR and failure to meet those responsibilities are likely to lead to serious consequences. Firstly, a serious breach of data protection is likely to be a disciplinary offence and will be dealt with under the Company's disciplinary procedure. If you access another employee's personnel records or any sensitive personal information without authority, this will constitute a gross misconduct offence and could lead to your summary dismissal. Additionally, if you knowingly or recklessly disclose personal data in breach of the data protection legislation, including the GDPR you may be held personally criminally accountable for any such breach.

Breach of the data protection legislation, including the GDPR rules can cause distress to the individuals affected by the breach and is likely to leave the Company at risk of serious financial consequences.

If you are in any doubt about what you can or cannot disclose and to whom, do not disclose the personal information until you have sought further advice from the Company's Data Protection Officer OR a Company Director.

This policy does not form part of a contract of employment. However, it is mandatory that all employees, workers or contractors must read, understand and comply with the content of this policy and you must attend associated training relating to its content and operation. Failure to adhere to this policy is likely to be regarded as a serious disciplinary matter and will be dealt with under the Company's disciplinary rules and procedures.

Definitions

Data Subject: a living individual.

Data Controller: the person or organisation that determines the means and the purpose of processing the personal data.

Data Protection Legislation: includes (i) the Data Protection Act 2018, (ii) the General Data Protection Regulation ((EU) 2016/679) **(**GDPR**)** and any national implementing laws, regulations and secondary legislation, for so long as the GDPR is effective in the UK, and (iii) any successor and supplemental legislation to the Data Protection Act 1998 and the GDPR, in particular the Data Protection Bill 2017-2019 and the E-Privacy Directive (and its proposed replacement), once it becomes law.

Personal data: is any information that identifies a living individual (data subject) either directly or indirectly. This also includes special categories of personal data. Personal data does not include data which is entirely anonymous, or the identity has been permanently removed making it impossible to link back to the data subject.

Processing: is any activity relating to personal data which can include collecting, recording, storing, amending, disclosing, transferring, retrieving, using or destruction.

Special categories of personal data: this includes any personal data which reveals a data subject's, ethnic origin, political opinions, religious and philosophical beliefs, trade union membership, genetic, biometric or health data, sex life and sexual orientation.

Criminal records data: means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

What are the GDPR principles?

We are a data controller. This means that we are required by law to ensure that everyone who processes personal data and special categories of personal data during the course of their work with us does so in accordance with the data protection legislation, including the GDPR principles. In brief, the principles say that:

- Personal data must be processed in a lawful, fair and transparent way.
- The purpose for which the personal information is collected must be specific, explicit and legitimate.
- The collected personal data must be adequate and relevant to meet the identified purpose.
- The information must be accurate and kept up to date.
- The personal data should not be kept in a form which permits identification of a data subject for longer than is necessary for the purposes for which it is used.
- The personal data must be kept confidential and secure and only processed by authorised personnel.

Other rules under the GDPR state that:

- The transfer of personal data to a country or organisation outside the EEA should only take place if appropriate measures are in place to protect the security of that data.
- The data subject must be permitted to exercise their rights in relation to their personal data.

The Company and all employees must comply with these principles and rules at all times in their information-handling practices. We are committed to ensuring that these principles and rules are followed, as we take the security and protection of data very seriously.

You must inform us immediately if you become aware that any of these principles or rules have been breached or are likely to be breached.

What are the lawful reasons under which we would expect you to process personal data?

Whilst carrying out your work activities you are likely to process personal data. The Company will only expect you to process personal data where the business has a lawful basis (or bases) to process that information. The lawful basis may be any one of the following reasons or a combination of:

a) Consent has been obtained the data subject to process their personal data for specified purposes.
b) Where we need to perform the contract, we have entered into with the data subject either for employment or commercial purposes.
c) Where we need to comply with a legal obligation.
d) Where it is necessary for our legitimate interests (or those of a third party) and the interests and fundamental rights of the data subject do not override those interests.

There are other rare occasions where you may need to process the data subject's personal information, these include:

e) Where we need to protect the data subject's interests (or someone else's interests).
f) Where it is needed in the public interest [or for official purposes].

You must always ensure that you keep a documentary inventory of the legal basis (or bases) which is being relied on in respect of each processing activity which you perform.

Privacy Notices

- Personal data must be processed in a lawful, fair and transparent way.

Before you begin collecting or processing personal data directly from a data subject you must ensure that an appropriate privacy notice has been issued to the data subject. Different notices are used for employment and commercial purposes. The content of the privacy notice must provide accurate, transparent and unambiguous details of the lawful and fair reason for why we are processing the data. It must also explain how, when and for how long we propose to process the data subject's personal information. We need to include information around the data subjects' rights and most importantly, the notice should also explain how we will keep the information secure and protected against unauthorised use.

Where you intend to collect data indirectly from a third party or a public source (i.e. electoral register), you must ensure that a privacy notice is issued to the data subject within a reasonable of period of obtaining the personal data and no later than one month; if the data is used to communicate with the individual, at the latest, when the first communication takes place; or if disclosure to someone else is envisaged, at the latest, when the data is disclosed.

You must only use data collected indirectly if you have evidence that it has been collected in accordance with the GDPR principles.

In all circumstances you must check that you are using an up to date version of the Company's privacy notice and it is being used in accordance with the Company's guidelines.

Purpose Limitation

- The purpose for which the personal information is collected must be specific, explicit and legitimate.

When you collect personal information, you will set out in the privacy notice how that information will be used. If it becomes necessary to use that information for a reason other than the reason which you have previously identified, you must usually stop processing that information. However, in limited circumstances you can continue to process the information provided that your new reason for processing the personal information remains compatible with your original lawful purpose (unless your original lawful basis was consent).

Adequate and relevant

- The collected personal data must be adequate and relevant to meet the identified purpose.

You must only process personal data where you have been authorised to do so because it relates to your work or you have been delegated temporary responsibility to process the information. You must not collect, store or use unnecessary personal data and you must

ensure that personal data is deleted, erased or removed within the Company's retention guidelines. You must not process or use personal data for non-work related purposes.

The Company will review its records and in particular employees' personnel files on a regular basis to ensure they do not contain a backlog of out-of-date or irrelevant information and to check there are lawful reasons requiring information to continue to be held.

Accurate and kept up to date

- The information must be accurate and kept up to date.

If your personal information changes, for example you change address, or you get married and change your surname, you must inform your line manager as soon as practicable so that the Company's records can be updated. The Company will not be responsible for any inaccurate personal data held on its systems where you have failed to notify it of the relevant change in circumstances.

Kept for longer than is necessary

- The personal data should not be kept in a form which permits identification of a data subject for longer than is necessary for the purposes for which it is used.

Different categories of personal data will be retained for different periods of time, depending on legal, operational and financial requirements. Any data which the Company decides it does not need to hold for a particular period of time will be destroyed in accordance with its retention of data policy.

Kept confidential and secure

- The personal data must be kept confidential and secure and only processed by authorised personnel.

To achieve this you must follow these steps:

- The Company has in place appropriate technical and organisational measures to protect against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to data. These procedures must always be adhered to and not overridden or ignored.
- Where the Company provides you with code words or passwords to be used before releasing personal information, for example by telephone, you must strictly follow the Company's requirements in this regard.

- Only transmit personal information between locations by fax or e-mail if a secure network is in place, for example, a confidential fax machine or encryption is used for e-mail.
- Ensure that any personal data which you hold is kept securely, either in a locked filing cabinet or, if it is computerised, it is password protected so that it is protected from unintended destruction or change and is not seen by unauthorised persons.
- Do not access another employee's records without authority as this will be treated as gross misconduct and it is also a criminal offence.
- Do not write down (in electronic or hard copy form) opinions or facts concerning a data subject which would be inappropriate to share with that data subject.
- Do not remove personal information from the workplace with the intention of processing it elsewhere unless this is necessary to enable you to carry out your job duties and has been authorised by your line manager.
- Ensure that when working on personal information as part of your job duties when away from your workplace and with the authorisation of your line manager, you continue to observe the terms of this policy and the data protection legislation, in particular in matters of data security.
- Ensure that hard copy personal information is disposed of securely, for example cross-shredded.
- Manual personnel files and data subject files are confidential. Only authorised employees have access to these files. For a list of authorised employees, please contact the Company's Data Protection Officer OR Company Director. These will not be removed from their normal place of storage without good reason.
- Data stored on memory sticks, discs, portable hard drives or other removable storage media is kept on an encrypted server.
- The Company has network back-up procedures to ensure that data on computers cannot be accidentally lost or destroyed.

Transfer to another country

- Transfer of personal data to countries or organisations outside of the EEA is not permitted.

The data subject rights

- The data subject must be permitted to exercise their rights in relation to their personal data.

Under the GDPR, subject to certain legal limitations, data subjects have available a number of legal rights regarding how their personal data is processed. At any time a data subject can request that the Company should take any of the following actions, subject to certain legal limitations, with regard to their personal data:

- Allow access to the personal data
- Request corrections to be made to data
- Request erasure of data
- Object to the processing of data
- Request that processing restrictions be put in place
- Request a transfer of personal data
- Object to automated decision making
- Right to be notified of a data security breach

There are different rules and timeframes that apply to each of these rights. You must follow the Company's policies and procedures whenever you process or receive a request in relation to any of the above rights.

How should you respond to a data subject request?

You must follow the Company's data subject access procedure which details how to deal with requests and it describes the circumstances where a fee may be charged. The procedure includes the following:

- Always verify the identity of the person making a data subject request and the legitimacy of the request.

- If you are unsure as to whether you are authorised to action the request check the privacy notice to ascertain who is authorised to deal with data subject requests. If you are still unsure how to handle the enquiry, you should forward this to [the Data Protection Officer] OR contact [INSERT DETAILS, our Data Representative].

- If you are authorised to deal with the request do not give out confidential personal information unless you have received the appropriate consent from the data subject. Seek explicit written consent to process the data subject request and ensure that you keep a clear audit trail of the request and your response.

- Do not share personal information with a third party, unless the data subject has given their explicit prior consent to the sharing of their information. A third party is anyone who is not the actual data subject and can include a family member of the data subject.

- Take great care not to accidentally share information with an unauthorised third party.

Be aware that those seeking information sometimes use deception in order to gain access to it.

Categories of information

During the course of your employment you may be required to process personal data which falls into different categories, general personal data and special categories of personal data. All data should be processed in accordance with the privacy notice and at all times in a confidential manner. However, where that data is classed as a special category extra care should be taken to ensure the privacy and security of that data. This means that you should maintain a high level of security and you should only share this data with those who are also authorised to process that data. In the context of employee relations, the scenarios when you may be required to process special categories information may arise for one or more of the following reasons:

- In order to comply with employment and other laws when processing and managing situations connected with absences arising in relation to sickness or family/ dependant related leave.

- To ensure health and safety obligations and other employment related obligations are met you may be required to process information about the physical or mental health or disability status of an employee in order to assess their capability to perform a role. You may also be required to monitor and manage sickness absence, recommend appropriate workplace adjustments and administer health related benefits.

- Where it is needed in the public interest, for example for equal opportunity monitoring and reporting.

- And any other reasons which we advise you of under a separate policy or notice.

We may also require you to process special categories of information in connection with customers and other third parties.

There may also be circumstances where we ask you to process this type of information in relation to assisting the Company with legal claims or to protect a data subjects' interests (or someone else's).
You may be asked to process information in relation to criminal convictions. This should be processed with the highest degree of confidentiality and in accordance with any data protection legislation and privacy notices that are in force in our business.

When will you need to seek consent?

In limited circumstances during your work you may need consent from a data subject in order to process personal data or special categories of data. You will be provided with training and details of which circumstances consent is needed and the type of consent that should be sought.

However, in limited circumstances, you may find it necessary to request a data subject to provide written consent to allow the processing of special categories of personal data. You will be provided with training and details of which circumstances consent is needed and the type of consent that should be sought. For example, in an employment context you should request the data subject's written consent to instruct a medical practitioner to prepare a medical report. If it becomes necessary to request consent to process special categories of personal data, you must provide the data subject with details of the information that will be required and why it is needed, so that they can make an informed decision as to whether they wish to provide consent.

You must not compel a data subject to provide written consent. Giving consent will always be a decision made by freewill and choice and is not a contractual condition. Consent can be withdrawn at any time without any reason provided. You must not subject a data subject to a sanction or detriment as a consequence of withdrawing consent. This would be viewed a serious disciplinary issue.

Exemptions

In limited circumstance there are certain categories of personal data which are exempt from the GDPR regime. In an employment for example:

- Confidential references that are given, but not those received by the Company from third parties. Only designated line managers can give Company references. Confidential references will not be provided unless the Company is sure this is the employee's wish.
- Management forecasts and management planning (including documents setting out management plans for an employee's future development and progress).
- Data which is required by law to be publicly available.
- Documents subject to legal professional privilege.

Action to be taken in the event of a data protection breach

A personal data breach will arise whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on a data subject.

In the event of a security incident or breach, do not try to handle this yourself.

You must follow the Company's Data Breach Policy which includes immediately informing [the Data Protection Officer] OR [the Data Representative] so that steps can be taken to:

- Contain the breach;
- Assess the potential adverse consequences for individuals, based on how serious or substantial these are, and how likely they are to happen; and
- To limit the scope of the breach by taking steps to mitigate the effects of the breach.

The Data Protection Officer OR Company Director will determine within 72 hours the seriousness of the breach and if the Information Commissioner's Office (ICO) and/or data subjects need to be notified of the breach.

Record keeping

- As we have fewer than 250 employees, we only need to document processing activities that:
    - are not occasional; or
    - could result in a risk to the rights and freedoms of individuals; or
    - involve the processing of special categories of data or criminal conviction and offence data.]

OR

Training

All employees that handle personal information of individuals must have a basic understanding of the data protection legislation, including the GDPR. Staff with duties such as computer and internet security, marketing and database management may need specialist training to make them aware of particular data protection requirements in their work area.

We will provide you with continuous training and updates on how to process personal data in a secure and confidential manner and in accordance with the spirit of the data protection legislation, including the GDPR. You will be required to attend all training and to keep yourself informed and aware of any changes made to privacy notices, consent procedures and any other policies and procedures associated with our internal processing of personal data.

You must regularly review all your data processing activities and ensure that you are acting in

accordance with the most current best practice and legal obligations in relation to data security and confidentiality.

Automated processing and decision making

From time to time we may use computer programmes to process data and make automated decisions. We will provide you with a separate notice explaining when and how this happens. Where automated processing or decision making does take place and the effect of that processing impacts on the freedoms and legitimate interests of the data subject, then in certain circumstances the data subject can request for human intervention. This means that they can ask for a human to review the machine made outcome/decision.

Sharing personal data

We may share personal data internally as is necessary. You must always ensure that personal data is only shared with authorised persons and is shared in accordance with the purposes stated in any privacy notice or consents. Extra care and security must be taken when sharing special categories of data or transferring data outside of the Company to a third party.

Direct Marketing

We are subject to specific rules under the GDPR in relation to marketing our services. Data subjects have the right to reject direct marketing and we must ensure that data subjects are given this option at first point of contact. When a data subject exercises their right to reject marketing you must desist immediately from sending further communications.

Complaints

If you believe that this policy has been breached by a colleague or to exercise all relevant rights, queries or complaints please in the first instance contact our Data Protection Officer or a Company Director via email.

Changes to this policy

We reserve the right to change this policy at any time so please always check this document regularly to ensure you are following the correct procedures.

Compliance with GDPR is everyone's responsibility.

Privacy Policy

We respect your privacy and are determined to protect your personal data. The purpose of this privacy notice is to inform you as to how we look after your personal data when you visit our website (regardless of where you visit it from). We'll also tell you about your privacy rights and how the data protection law protects you.

1. WHO WE ARE AND IMPORTANT INFORMATION

What is the purpose of this privacy notice? This privacy notice aims to give you information on how we collect and process your personal data through your use of this website, including any data you may provide through this website when you purchase a product or sign up to our newsletter.

This website is not intended for children and we do not knowingly collect data relating to children.

You must read this privacy notice together with any other privacy notice we may provide on specific occasions when we are collecting or processing personal data about you so that you are fully aware of how and why we are using your data. This privacy notice supplements the other notices and is not intended to override them.

Data controller: InfoLogic Ltd is the controller and responsible for your personal data (collectively referred to as "InfoLogic", "we", "us" or "our" in this privacy notice). Our contact details are Norton House, New Street, Chipping Norton, Oxfordshire, OX7 5LJ; email customerservices@infologic.biz. For all data matters contact our Data Protection Officer.

Third-party links outside of our control: This website may include links to third-party websites, plug-ins and applications in order to process your orders with us. Clicking on those links or enabling those connections may allow third parties to collect or share data about you. We do not control these third-party websites and are not responsible for their privacy statements. When you leave our website, we encourage you to read the privacy notice of every website you visit.

2. THE PERSONAL DATA WE COLLECT ABOUT YOU

Personal data, or personal information, means any information about an individual from which that person can be identified. You can find out more about personal data from the Information Commissioners Office.

We may collect, use, store and transfer different kinds of personal data about you which we have grouped together as follows:

- Identity Data includes First Name, Last Name, Title and Username.
- Contact Data includes Billing Address, Delivery Address, Email address and telephone numbers.

We also collect, use and share aggregated data such as statistical or demographic data for any purpose. Aggregated data may be derived from your personal data but is not considered personal data in law as this data does not directly or indirectly reveal your identity. For example, we may aggregate your usage data to calculate the percentage of users accessing a specific website feature. However, if we combine or connect aggregated data with your personal data so that it can directly or indirectly identify you, we treat the combined data as personal data which will be used in accordance with this privacy notice.

We do not collect any Special Categories of Personal Data about you (this includes details about your race or ethnicity, religious or philosophical beliefs, sex life, sexual orientation, political opinions, trade union membership, information about your health and genetic and biometric data). Nor do we collect any information about criminal convictions and offences.

If you fail to provide personal data where we need to collect your personal data by law, or under the terms of a contract we have with you and you fail to provide that data when requested, we may not be able to perform the contract we have or are trying to enter into with you (for example, to provide you with goods or services). In this case, we may have to cancel a product or service you have with us but we will notify you if this is the case at the time.

3. HOW WE COLLECT YOUR PERSONAL DATA

We use different methods to collect data from and about you including through:

- You may give us your identity, contact and financial data by filling in forms or by corresponding with us by post, phone, email or otherwise. This includes personal data you provide when you:
- Purchase our products or services;
- Create an account on our website;
- Subscribe to our email newsletter;
- Request marketing to be sent to you.

4. HOW WE USE YOUR PERSONAL DATA

We will only use your personal data when the law allows us to. Most commonly, we will use your personal data in the following circumstances:

- Performance of Contract this means processing your data where it is necessary for the performance of a contract to which you are a party or to take steps at your request before entering into such a contract.
- Legitimate Interest this means the interest of our business in conducting and managing our business to enable us to give you the best service/product and the most secure experience. We make sure we consider and balance any potential impact on you (both positive and negative) and your rights before we process your personal data for our legitimate interests. We do not use your personal data for activities where our interests are overridden by the impact on you (unless we have your consent or are otherwise required or permitted to by law).
- Comply with a legal or regulatory obligation this means processing your personal data where it is necessary for compliance with a legal or regulatory obligation that we are subject to.

PURPOSES FOR WHICH WE WILL USE YOUR PERSONAL DATA

We have set out below, in a table format, a description of all the ways we plan to use your personal data, with the legal bases we rely on to do so. Note that we may process your personal data for more than one lawful ground depending on the specific purpose for which we are using your data.

PURPOSE/ACTIVITY
To register you as a new customer
To process and deliver your order including: (a) Manage payments, fees and charges (b) Collect and recover money owed to us
To manage our relationship with you which will include: (a) Notifying you about changes to our terms, products or privacy policy (b) Asking you to leave a review or take a survey
To administer and protect our business and this website (including troubleshooting, data analysis, testing, system maintenance, support, reporting and hosting of data)
To deliver relevant website content and advertisements to you and measure or understand the effectiveness of the advertising we serve to you
To use data analytics to improve our website, products/services, marketing, customer relationships and experiences
To make suggestions and recommendations to you about goods or services that may be of interest to you

Marketing
We will get your express opt-in consent before we use or share your personal data. We strive to provide you with choices regarding certain personal data uses, particularly around marketing and advertising. We have established the following personal data control mechanisms:

Promotional offers from us
We will get your express opt-in consent before we use or share your personal data. We may use your Identity, Contact, Technical, Usage and Profile Data to form a view on what we think you may want or need, or what may be of interest to you. This is how we decide which products, services and offers may be relevant for you. You will receive marketing communications from us if you have requested information from us or purchased goods or services from us or if you provided us with your details when you entered a competition or registered for a promotion and, in each case, you have not opted out of receiving that marketing.

Opting out
You can ask us to stop sending you marketing messages at any time by following the opt-out links on any marketing message sent to you or by sending an email to customerservices@infologic.biz at any time.

Change of purpose
We will only use your personal data for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal data for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so. Please note that we may process your personal data without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

5. WHO WE SHARE YOUR PERSONAL DATA WITH

We will sometimes share your data with the parties set out below.

- Personal Data shared with Royal Mail based in the United Kingdom who require reports of customer details who have licensed their data products.
- Anonymised data shared with Google Analytics to help us understand how our customers use the Site -- you can read more about how Google uses your Personal Information here: https://www.google.com/intl/en/policies/privacy/. You can also opt-out of Google Analytics here: https://tools.google.com/dlpage/gaoptout.
- HM Revenue & Customs based in the United Kingdom who require reporting of activities in certain circumstances.
- Consultants and solutions providers hired directly by us to perform a specific one of task (a freelancer developing our website)
- Payment solutions providers when you purchase a product
- Shopping Cart solutions providers when you purchase a product

We require all third parties to respect the security of your personal data and to treat it in accordance with the law. We do not allow our third-party service providers to use your personal data for their own purposes and only permit them to process your personal data for specified purposes and in accordance with our instructions and your consent where it is required by law.

6. INTERNATIONAL TRANSFERS

Some of our external third parties are based outside the European Economic Area (EEA) so their processing of your personal data will involve a transfer of data outside the EEA. Whenever we transfer your personal data out of the EEA, we ensure a similar degree of protection is afforded to it by implementing safeguards.

7. DATA SECURITY

We have put in place appropriate security measures to prevent your personal data from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal data to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal data on our instructions, and they are subject to a duty of confidentiality.
We have put in place procedures to deal with any suspected personal data breach and will notify you and any applicable regulator of a breach where we are legally required to do so.

8. DATA RETENTION

We will only retain your personal data for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements.

To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

By law we have to keep basic information about our customers (including contact, identity, financial and transaction data) for six years after they cease being customers for tax purposes.

In some circumstances you can ask us to delete your data: see Your legal rights below for further information. In some circumstances we may anonymise your personal data (so that it can no longer be associated with you) for research or statistical purposes in which case we may use this information indefinitely without further notice to you.

9. YOUR LEGAL RIGHTS

Unless subject to an exemption under the data protection laws, you have the following rights with respect to your personal data:

- The right to request a copy of the personal data which we hold about you;
- The right to request that we correct any personal data if it is found to be inaccurate or out of date;
- The right to request your personal data is erased where it is no longer necessary to retain such data;
- The right to withdraw your consent to the processing at any time, where consent was the lawful basis for processing your data;
- The right to request that we provide you with your personal data and where possible, to transmit that data directly to another data controller, (known as the right to data portability), where applicable 9i.e. where our processing is based on consent or is necessary for the performance of our contract with you or where we process your data by automated means);
- The right, where there is a dispute in relation to the accuracy or processing of your personal data, to request a restriction is placed on further processing;
- The right to object to our processing of personal data, where applicable i.e. where processing is based on our legitimate interests (or in performance of a task in the public interest/exercise of official authority); direct marketing or processing for the purposes of scientific/historical research and statistics).

No fee required – with some exceptions
You will not have to pay a fee to access your personal data (or to exercise any of the other rights). However, we may charge a reasonable admin fee if your request is clearly unfounded, repetitive or excessive. Alternatively, we may refuse to comply with your request in these circumstances.

What we may need from you
We may need to request specific information from you to help us confirm your identity and ensure your right to access your personal data (or to exercise any of your other rights). This is a security measure to ensure that personal data is not disclosed to any person who has no right to receive it. We may also contact you to ask you for further information in relation to your request to speed up our response.

Time limit to respond
We try to respond to all legitimate requests within one month. Occasionally it may take us longer than a month if your request is particularly complex or you have made a number of requests. In this case, we will notify you and keep you updated.

10. CHANGES TO THIS NOTICE AND YOUR DUTY TO INFORM US OF CHANGES

This version was last updated on 16th August 2019 and historic versions can be obtained by contacting us. Please keep us informed if your personal data changes during your

relationship with us. It is important that the personal data we hold about you is accurate and current.

11. QUERIES, REQUESTS OR CONCERNS

To exercise all relevant rights, queries or complaints in relation to this policy or any other data protection matter between you and us, please in the first instance contact our Data Protection Officer by emailing customerservices@infologic.biz or calling the telephone number on our website. If this does not resolve your complaint to your satisfaction, you have the right to lodge a complaint with the Information Commissioners Office on 03031231113 or at the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF, England, UK

Cookie Policy

We use cookies on this website to ensure our website works correctly whilst you use it. Primarily to ensure the menu items you select take you to the correct product page and that the shopping cart works as it should and doesn't get confused with another shoppers cart.

1. About cookies

A cookie is a tiny text file that a website stores on your machine (including any computer, mobile phone or tablet) and reads when you visit the site. They are widely used in order to make websites work, or work more efficiently, as well as to provide information to website owners. It allows the website to identify you and for example, remember your log in details the next time you visit.

2. The types of cookies we use

2.1 Strictly necessary technical cookies
These are cookies that are essential, e.g. to load the website and fulfil actions requested by you, e.g. browsing the website, adding items to your shopping cart, or allowing you to pay for items you want to buy from our site. They also include Session Cookies, which are stored in your computer or device's memory during your browsing session and are automatically deleted from your computer when you leave a website. These cookies usually store a session ID, allowing you to move from page to page without having to log-in repeatedly.

2.2 Performance cookies
These are cookies used to improve a website, for example, for analytics that let companies see how their site is used and where to make improvements.

2.3 Persistent cookies
These cookies are stored on your computer or device after you visit and are not deleted when your browser is closed. Persistent cookies can be used to retain your preferences for a particular website, allowing those preferences to be used in future browsing sessions. Persistent cookies usually assign a unique ID to your browser and they are usually configured to identify you for a prolonged period of time, from days to months or even years.

3. Why we use cookies

We use cookies:
to ensure you are properly logged in, where this is necessary to use the site
to store personal registration information so that you do not have to provide it to us again
to track your progress through the site so we can make improvements to the service we offer you, and/or to remember any preferences which the site may allow you to set.

4. Managing and deleting cookies

The General Data Protection Regulation ('GDPR') 2018 requires website users to be told about cookies used on the site and how to opt into accepting cookies, or to be able to opt out of certain cookies that are not essential to the basic functioning of the website.
We only use cookies that are essential to the basic functioning of the website and do not use cookies for other purposes.

Using your browser controls to control your cookie settings. Most web browsers (including Chrome, Internet Explorer, Firefox and Safari) allow you to control your cookie settings and to delete any cookies already stored on your computer or other device. You can control the use of cookies on your device, including deleting and blocking the cookies we and other sites use, through the browser settings on your device, but please note that any changes you make may affect some functionality of this Site.

5. Changes to our cookies statement

We may change the content of our Site or services without notice, and consequently our Privacy Policy and/or Cookies Statement may change at any time in the future. We therefore encourage you to review it from time to time to stay informed of how we are using personal information.

6. Redirects to third party sites

Our website will re-direct you to a contracted third-party site including our bankers and card processing agents but only when you make a purchase. As these websites are operated by third parties, we have no control over their use of cookies.

7. Learn more about cookies

To find out more about the way cookies work, how to see what cookies have been set and how to manage and delete them, visit aboutcookies.org or allaboutcookies.org

Anti-Corruption & Bribery (employees / agents / contractors)

Introduction

One of the Company's core values is to uphold sound, responsible and fair business operations. It is committed to promoting and maintaining the highest possible ethical standards in relation to all of its business activities. The Company's reputation for maintaining lawful business practices is of paramount importance to it and this policy is designed to preserve these values. The Company therefore has a zero-tolerance policy towards bribery and corruption and is committed to acting fairly and with integrity in all of its business dealings and relationships wherever it operates and implementing and enforcing effective systems to counter bribery.

Purpose and scope

This policy sets out the Company's position on any form of bribery and corruption and provides guidelines aimed at:

- Ensuring compliance with anti-bribery laws, rules and regulations, not just within the UK, but also in any other country within which the Company may carry out its business or in relation to which its business may be connected.
- Enabling employees and persons associated with the Company to understand risks associated with unlawful conduct and to enable and encourage them to be vigilant and to effectively recognise, prevent, avoid and report any wrongdoing, whether by themselves or others.
- Providing suitable and secure reporting and communication channels and ensuring that any information that is reported is properly and effectively dealt with.
- Creating and maintaining a rigorous and effective framework for dealing with any suspected instances of bribery or other unethical conduct.

This policy applies to all permanent and temporary employees of the Company (including any of its intermediaries, subsidiaries or associated companies). It also applies to any individual or corporate entity associated with the Company or who performs functions in relation to, or for and on behalf of, the Company, including, but not limited to, directors, agency workers, casual workers, contractors, consultants, seconded staff, agents, suppliers and sponsors ("associated persons").

All employees and associated persons are expected to adhere to the principles set out in this policy.

Legal obligations

The key UK legislation on which this policy is based is the Bribery Act 2010 and it applies to the Company's conduct both in the UK and abroad.

A bribe is an inducement or reward offered, promised or provided in order to gain any commercial, contractual, regulatory or personal advantage.

It is an offence in the UK to:

- Offer, promise or give a financial or other advantage to another person (i.e. bribe a person) whether within the UK or abroad, with the intention of inducing or rewarding improper conduct.
- Request, agree to receive or accept a financial or other advantage (i.e. receive a bribe) for or in relation to improper conduct.
- Bribe a foreign public official.

You can be held personally liable for any such offence.

It is also an offence in the UK for an employee or an associated person to bribe another person in the course of doing business intending either to obtain or retain business, or to obtain or retain an advantage in the conduct of business, for the Company. The Company can be liable for this offence where it has failed to prevent such bribery by associated persons. As well as an unlimited fine, it could also suffer substantial reputational damage in connection with this offence.

Policy

All employees and associated persons are required to:

- Comply with any anti-bribery and anti-corruption legislation that applies in any jurisdiction in any part of the world in which they might be expected to conduct business.
- Act honestly, responsibly and with integrity.
- Safeguard and uphold the Company's core values by operating in an ethical, professional and lawful manner at all times.

Bribery of any kind is prohibited. Under no circumstances should any provision be made, money set aside or accounts created for the purposes of facilitating the payment or receipt of a bribe.

The Company recognises that industry practices may vary from country to country or from culture to culture. What is considered unacceptable in one place may be normal or usual practice in another. Nevertheless, a strict adherence to the guidelines set out in this policy is expected of all employees and associated persons at all times.

If in doubt as to what might amount to bribery or other unethical conduct or might constitute a breach of this policy, you should refer the matter to a line manager or a Company Director immediately via email.

For the Company's rules and procedures in relation to the receipt of business gifts from third parties such as clients, customers, contractors and suppliers and corporate hospitality offered to or received from such third parties, please refer to the Company's Receipt of Gifts Policy and Corporate Hospitality Policy. These policies form part of the Company's zero tolerance policy towards any form of bribery and should be read in conjunction with this policy.

The giving of business gifts to clients, customers, contractors and suppliers is not prohibited provided the following requirements are met:

- The gift is not made with the intention of influencing a third party to obtain or retain business or a business advantage, or to reward the provision or retention of business or a business advantage.
- It complies with local laws.
- It is given in the Company's name, not in the giver's personal name.
- It does not include cash or a cash equivalent (such as gift vouchers).
- It is of an appropriate and reasonable type and value and given at an appropriate time.
- It is given openly, not secretly.
- It is approved in advance by a Director of the Company.

Essentially, it is not acceptable to give, promise to give, or offer, a payment, gift or hospitality with the expectation or hope that a business advantage will be received, or to reward a business advantage already given, or to accept a payment, gift or hospitality from a third party that you know or suspect is offered or provided with the expectation that it will obtain a business advantage for them.

For the avoidance of doubt, any payment or gift to a public official or other person to secure or accelerate the prompt or proper performance of a routine government procedure or process, otherwise known as a "facilitation payment", is also strictly prohibited. Facilitation payments are not commonly paid in the UK but they are common in some other jurisdictions.

Responsibilities and reporting procedure

It is the contractual duty and responsibility of all employees and associated persons to take whatever reasonable steps are necessary to ensure compliance with this policy and to prevent, detect and report any suspected bribery or corruption in accordance with the procedure set out in the Company's Public Interest Disclosure Policy. You must immediately disclose to the Company any knowledge or suspicion you may have that you, or any other employee or associated person, has plans to offer, promise or give a bribe or to request, agree to receive or accept a bribe in connection with the business of the Company. For the avoidance of doubt, this includes reporting your own wrongdoing.

The duty to prevent, detect and report any incident of bribery and any potential risks rests not only with the Directors of the Company but applies equally to all employees and associated persons.

The Company encourages all employees and associated persons to be vigilant and to report any inappropriate or unlawful conduct, suspicions or concerns promptly and without undue delay so that investigation may proceed and any action can be taken expeditiously. For example, if a client or potential client offers you something to gain a business advantage with the Company or indicates to you that a gift or payment is required to secure their business.

In the event that you wish to report an instance or suspected instance of bribery, you should follow the steps set out in the Company's Public Interest Disclosure Policy. Confidentiality will be maintained during the investigation to the extent that this is practical and appropriate in the circumstances. The Company is committed to taking appropriate action against bribery or other unethical conduct. This could include either reporting the matter to an appropriate external government department, regulatory agency or the police and/or taking internal disciplinary action against relevant employees and/or terminating contracts with associated persons.

The Company will support anyone who raises genuine concerns in good faith under this policy, even if they turn out to be mistaken. It is also committed to ensuring nobody suffers any detrimental treatment as a result of refusing to take part in bribery or corruption, or because of reporting in good faith their suspicion that an actual or potential bribery or corruption offence has taken place or may take place in the future.

All employees and associated persons must ensure that any contract or agreement entered into by them for or on behalf of the Company contains an appropriate clause aimed at ensuring that any third party to the contract is aware of and agrees to adhere to the contents of this policy and further, that the contract expressly sets out the consequences of non-compliance including, where appropriate, clear provision for terminating the contract in the event of non-compliance or the commission of any relevant bribery offence.

Record-keeping

All accounts, receipts, invoices and other documents and records relating to dealings with third parties must be prepared and maintained with strict accuracy and completeness. No accounts must be kept "off the record" to facilitate or conceal improper payments.

Sanctions for breach

Breach of any of the provisions of this policy will constitute a disciplinary offence and will be dealt with in accordance with the Company's disciplinary procedure. Depending on the gravity of the offence, it may be treated as gross misconduct and could render the employee liable to summary dismissal.

As far as associated persons are concerned, breach of this policy could lead to the suspension or termination of any relevant contract, sub-contract or other agreement with the associated person.

Data Protection

When processing information in connection with a report made in pursuance of this policy or when processing any records or documents relating to dealings with third parties which relates to personal data, the Company will process this in accordance with its data protection policy and any internal privacy notices in force at the relevant time.

Inappropriate access or disclosure of this data will constitute a data breach and should be reported immediately to the Company's Data Protection Officer, a Supervisor or Company Director by email as is in accordance with the Company's data protection policy. Reported data breaches will be investigated and may lead to sanctions under the Company's disciplinary procedure.

Monitoring compliance

The Company's Anti-Corruption Officer has lead responsibility for ensuring compliance with this policy and will review its contents on a regular basis. They will be responsible for monitoring its effectiveness and will provide regular reports in this regard to the Directors of the Company who have overall responsibility for ensuring this policy complies with the Company's legal and ethical obligations.

Training

The Company will provide training to all employees to help them understand their duties and responsibilities under this policy.

The Company's zero tolerance approach to bribery will also be communicated to all business partners at the outset of the business relationship with them and as appropriate thereafter.

Examples of potential risks

The following is a non-exhaustive list of possible issues which may raise bribery concerns and which you should report in accordance with the reporting procedure set out above:

- A third party insists on receiving a commission or fee before committing to signing a contract with the Company, or carrying out a government function or process for the Company.
- A third party requests payment in cash, or refuses to sign a formal commission or fee agreement, or to provide an invoice or receipt for a payment made.
- A third party requests an unexpected additional commission or fee to facilitate a service.
- A third party demands lavish, extraordinary or excessive gifts or hospitality before commencing or continuing contractual negotiations or provision of services.
- You are offered an unusually lavish, extraordinary or excessive gift or hospitality by a third party.
- You receive an invoice from a third party that appears to be non-standard or extraordinary.
- The Company is invoiced for a commission or fee payment that appears large given the service stated to have been provided.