Data Protection Policy

Version: 1.12

Date: 1st June 2020

1. Data Protection Policy

What is this policy for?

tiQtoQ Limited Data Protection Policy for employees, clients and others who we work with. We take issues relating to personal data seriously. This policy is to explain more to you about how we handle your personal data. We will always be clear about why we need the details we ask for and ensure your personal information or that belonging to any third party you give to us is kept as secure as possible.

It is important that you read this privacy policy together with any other privacy notice or fair processing 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 Policy supplements the other notice and is not intended to override them.

Controller

tiQtoQ Limited is the controller and responsible for your personal data (in the case of individual clients) or your employees' personal data (in the case of employers) (collectively referred to in this policy as "we", "us" or "our")

We have appointed a data protection officer (DPO) who is responsible for overseeing questions in relation to this Policy. You should not hesitate to contact Paul Gitsham

Email address: paul.gitsham@tiqtoq.co.uk

Postal address: Mornington Bungalow, Drope Road, St George's-Super-Ely, Cardiff, CF5 6EP

Telephone number: 07970 825433

This version was last updated on 1st June 2020

It is important that the personal data we hold about you is accurate and current. Please keep us informed if your personal data changes during your relationship with us.

If you provide us with an email address that you share with another person (such as a partner), you can expect them to see any emails that we send to you.

Third-Party Links

Our website may include links to other websites. Clicking on those links 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.

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.

Data Retention

HOW LONG WILL YOU USE MY PERSONAL DATA FOR?

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 clients (including Contact, Identity, Financial, Advice and Transaction Data) for seven years after they cease being customers for tax, insurance and regulatory purposes.

In some circumstances you can ask us to delete your data: see Request erasure 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.

Your Legal Rights

Under certain circumstances, you have rights under data protection laws in relation to your personal data. These are:

- Request access to your personal data.
- Request correction of your personal data.
- Request erasure of your personal data.
- Object to processing of your personal data.
- Request restriction of processing your personal data.
- Request transfer of your personal data.
- Right to withdraw consent.

If you wish to exercise any of the rights set out above, please contact us.

You have the right to:

Request access to your personal data (commonly known as a "data subject access request"). This enables you to receive a copy of the personal data we hold about you that you have given to us and to check that we are lawfully processing it.

Request correction of the personal data that we hold about you. This enables you to have any incomplete or inaccurate data we hold about you corrected, though we may need to verify the accuracy of the new data you provide to us.

Request erasure of your personal data. This enables you to ask us to delete or remove personal data where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal data where you have successfully exercised your right to object to processing (see below), where we may have processed your information unlawfully or where we are required to erase your personal data to comply with local law. Note, however, that we may not always be able to comply

with your request of erasure for specific legal reasons which will be notified to you, if applicable, at the time of your request.

Object to processing of your personal data where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground as you feel it impacts on your fundamental rights and freedoms. You also have the right to object where we are processing your personal data for direct marketing purposes. In some cases, we may demonstrate that we have compelling legitimate grounds to process your information which override your rights and freedoms.

Request restriction of processing of your personal data. This enables you to ask us to suspend the processing of your personal data in the following scenarios: (a) if you want us to establish the data's accuracy; (b) where our use of the data is unlawful but you do not want us to erase it; (c) where you need us to hold the data even if we no longer require it as you need it to establish, exercise or defend legal claims; or (d) you have objected to our use of your data but we need to verify whether we have overriding legitimate grounds to use it.

Request the transfer of your personal data to you or to a third party. We will provide to you, or a third party you have chosen, your personal data in a structured, commonly used, machine-readable format. Note that this right only applies to automated information which you initially provided consent for us to use or where we used the information to perform a contract with you.

Withdraw consent at any time where we are relying on consent to process your personal data. However, this will not affect the lawfulness of any processing carried out before you withdraw your consent. If you withdraw your consent, we may not be able to provide certain products or services to you. We will advise you if this is the case at the time you withdraw your consent.

No Fee

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 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 several requests. In this case, we will notify you and keep you updated.

Glossary

Lawful Basis

Legitimate Interest means the interest of our business in conducting and managing our business to enable us to give you the best service/product and the best and 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). You can obtain further information about how we assess our legitimate interests against any potential impact on you in respect of specific activities by contacting us.

Performance of Contract 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.

Comply with a legal or regulatory obligation means processing your personal data where it is necessary for compliance with a legal or regulatory obligation that we are subject to.

Third Parties

EXTERNAL THIRD PARTIES

- Service providers based in the UK who provide IT and system administration services: generally, they are accessing our systems for the legitimate interest of diagnosing and dealing with IT related problems rather than accessing personal data. We are satisfied that our contractual relationships with those providers (Lawware a Legal Software supplier) contains provisions dealing and with the security of all data and that Lawware take appropriate measures to prevent unlawful access to the data).
- Professional advisers including lawyers, bankers, auditors and insurers based in the UK who provide consultancy, banking, legal, insurance and accounting services to the company. Generally, they are not accessing personal data when providing us with advice and support but if they are likely to have access to such data
- Debt-collectors, based in the UK acting as joint controllers who will have access to Financial Data and Identity Data in order to enforce the debts you us.
- Our freelance PA acting as a processor who offers admin support services. We have in place with her a contract which requires her to take the same steps we would take to protect your privacy and data and she has been trained in data security.
- In the case of individual clients: You may require us to share your Identity data with a third party such as an outplacement consultant. We will only do this with your express written consent.
- In the case of employer clients: You may require us to appoint a third-party provider to assist you with investigations, hearings or appeals in which case we will only share data with that third-party with your permission. Where the third-party contracts with us rather than directly with you, we only use third parties we have entered into contractual arrangements with where we are satisfied that have put in place measures to protect your employee's privacy and data.

2. Data Protection Policy

Policy for data processing, security and protocols in line with data protection and GDPR regulations.

Policy statement

tiQtoQ Limited is committed to a policy of protecting the rights and privacy of individuals in accordance with the data protection legislation in force.

To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully.

This policy applies to all staff and contractors any breach of either the Data Protection Legislation or this policy is considered to be an offence and the company's disciplinary procedures will apply/it may result in a contract coming to an end.

This policy helps to protect the Company from some very real data security risks and regulatory breaches, including:

- Breaches of confidentiality (For instance, information being given out inappropriately).
- Reputational damage. (For instance, the company could suffer if hackers successfully gained access to sensitive data)

Purpose of the Data Protection Legislation

Its purpose is to protect the rights and privacy of living individuals and to ensure that personal data is not processed without their knowledge, and that processing of data is done so lawfully.

Definitions (Data Protection Act 2018)

Data Protection Legislation: the General Data Protection Regulation 2016/679; the UK Data Protection Act 2018 and all relevant EU and UK data protection legislation.

Personal Data

This is data relating to a living individual who can be identified from it or from that data and other information in the possession of the Company and it includes, amongst other things, name, address, email, telephone number and any unique information such as passport or driving licence details. Information about companies or public authorities is not personal data.

Information about individuals acting as sole traders, employees, partners and company directors where they are individually identifiable and the information relates to them as an individual may constitute personal data.

Information about a deceased person does not constitute personal data and therefore is not subject to this policy.

Sensitive/Special categories of Data

This is data which relates to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation, the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person and criminal convictions or offences. This type of data is subject to much stricter conditions of processing. Given what we do we are likely to hold this kind of data.

Data Controller

In this policy this is the Company because it makes decisions with regard to particular personal data, including decisions regarding the purposes for which personal data are processed and the way in which personal is processed.

Data Subject

Any individual who is the subject of personal data held by the Company.

Processing

Any operation related to the organisation, retrieval, disclosure and deletion of data including:

- Obtaining and recording data, accessing, altering, adding to, merging, deleting, data retrieval, consultation or use of data, disclosure or otherwise making data available.
- Relevant Filing System - this is any paper filing system or other manual filing system which is structured, so that information about an individual is readily accessible. Our client files will form part of a Relevant Filing System.

Responsibilities under the Data Protection Act

- The Company is the Data Controller. The directors are ultimately responsible for ensuring that it meets its legal obligations.
- Compliance with Data Protection Legislation is the responsibility of all members of the Company who process personal data which will mean this policy is the responsibility of all staff/contractors.
- The Company is not required to appoint a Data Protection Officer and has not done so, however, it has appointed a director Peter Jones with special responsibility for:
    - Keeping the staff updated about data protection responsibilities, risks and issues.
    - Reviewing all data protection procedures and related policies, in line with an agreed schedule.
    - Arranging data protection training and advice for the people covered by this policy.
    - Handling data protection questions from staff and anyone else covered by this policy.
    - Dealing with requests from individuals to see the data the Company holds about them (also called 'subject access requests').
    - Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.
    - Ensuring all systems, services and equipment used for storing data meet acceptable security standards through effective Risk Management.
    - Performing regular checks and scans to ensure security hardware and software is functioning properly.
    - Evaluating any third-party services, the company is considering using to store or process data. For instance, cloud computing services.
    - Approving any data protection statements attached to communications such as emails and letters.
    - Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

Data Protection Principles

The Company complies with the data protection principles set out below. When processing personal data, it ensures that:

- it is processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency')
- it is collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ('purpose limitation')
- it is all adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')
- it is all accurate and, where necessary, kept up to date and that reasonable steps will be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy')

- it is kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed ('storage limitation')
- it is processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')

All processing of data must be done in accordance with the seven data protection principles:

Principle 1 Personal data shall be processed fairly, lawfully and in a transparent manner
Those responsible for processing personal data must make reasonable efforts to ensure that data subjects are informed of the identity of the data controller, the purpose(s) of the processing, any disclosures to third parties that are envisaged and an indication of the period for which the data will be kept.

Principle 2. Personal data shall be obtained for specific and lawful purposes and not processed in a manner incompatible with those purposes.
It is the responsibility of the partners to notify anyone whose data the Company processes of the purposes for which the data will be processed. This is done via a Privacy Notice. Anyone who is, or intends processing data for purposes not included in the Company's Privacy Notices should seek advice from the director. Data obtained for a specific purpose must not be used for a different purpose, without the data subject's consent or other lawful purpose.

Principle 3. Personal data shall be adequate, relevant and not excessive in relation to the purpose for which it is held.
Information which is not strictly necessary for the purpose(s) for which it is obtained should not be collected. If data is given or obtained which is excessive for the purpose, it should be immediately deleted or destroyed.

Principle 4. Personal data shall be accurate and, where necessary, kept up to date.
Data kept for a long time must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that it is accurate and up to date. Completion of any form giving personal or business details will be taken as an indication that the data contained in them is accurate.

Principle 5. Personal data shall be kept only for as long as necessary.
This is connected to principles 1 and 2 and why we are processing the data (the purposes for doing so).

Principle 6. Appropriate technical and organisational measures shall be taken for the security of personal data and protect against unauthorised or unlawful processing of personal data and against accidental loss or destruction of data.

Principle 7. Responsible for and able to demonstrate compliance with the data protection regime and these principles.

Further details can be found here https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/

Individual (Data Subject) Rights

Data subjects have the following rights regarding processing data, and the data that are recorded about them:

- The right to be informed
  Individuals have the right to be informed about the collection and use of their personal data.
- The right of access
  Individuals have the right to access their personal data (subject access request).
- The right to rectification
  The right for individuals to have inaccurate personal data rectified, or completed if it is incomplete
- The right to erasure
  The right to erasure is also known as 'the right to be forgotten'
- The right to restrict processing
  The right to request the restriction or suppression of their personal data
- The right to data portability
  The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services.
- The right to object
  The right to object to the processing of their personal data in certain circumstances.

Further details can be found here https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/

Lawful basis for processing

At least one of these must apply whenever you process personal data:

- Consent: the individual has given clear consent for us to process their personal data for a specific purpose.
- Contract: the processing is necessary for a contract we have with the individual, or because they have asked us to take specific steps before entering into a contract e.g. agreement for lease.
- Legal obligation: the processing is necessary for us to comply with the law (not including contractual obligations) e.g. Anti-Money Laundering regulations.
- Vital interests: the processing is necessary to protect someone's life.
- Public task: the processing is necessary for us to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
- Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

Points to consider when acting for clients:

- Obtaining information to fulfil data regulations is a legal obligation
- Consent is needed when releasing information for a client to another third party
- Providing details of the client to fulfil their instructions is a lawful basis

Wherever possible, personal data or sensitive data should not be obtained, held, used or disclosed unless the individual has given consent or there is a lawful basis for processing. We advise clients of the way in which we use their data when we send out our terms of business and if after receipt of these the client continues to instruct us, then the client is deemed to have accepted the way in which we process data.

For sensitive data, explicit written consent of data subjects must be obtained unless an alternative legitimate basis for processing exists.

If an individual instructing us as an individual does not consent to certain types of processing (e.g. direct marketing), appropriate action must be taken to ensure that the processing does not take place.

Security of Data

- All staff are responsible for ensuring that any personal data which they hold is kept securely and that it is not disclosed to any unauthorised third party.
- Computer passwords must be kept confidential.
- Devices must lock when not in use.
- Encryption must be used on laptops and USB sticks.
- Manual records – including print outs from the computer databases containing personal data must be disposed of as confidential waste and placed in shredding boxes supplied for this purpose.
- No paper or files are to be left around the office – a clear desk policy is employed.
- Hard drives on redundant PCs must be wiped clean before disposal.
- This policy also applies to staff that process personal data "off-site". Staff should take particular care when processing personal data at home or out of the office.
- Laptops should never be left unattended/in cars.
- Cloud storage must be secure

Rights of Access to Data – Subject Access Requests

The Company will facilitate any request from a data subject who wishes to exercise their rights under data protection law as appropriate, always communicating in a concise, transparent, intelligible and easily accessible form and without undue delay.

Such rights relate to accessing any personal data which is/are held by the Company in electronic format and manual records which form part of a 'relevant filing system'. They do not have the right to access information relating to other people (unless the information is also about them or they are acting on behalf of someone). Therefore, it is important that you establish whether the information requested falls within the definition of personal data.

It is important to not only respond to the subject access request but to do so complying with the terms of the Data Protection Legislation and this policy as set out here:

How we deal with Subject Access requests

Upon receipt of a Subject Access Request (SAR) the Company will:

(a) Verify whether it is the controller of the data subject's personal data. If it is not a controller, but merely a processor, We will inform the data subject and refer them to the actual controller.

(b) Verify the identity of the data subject. If needed, we will request further evidence on the identity of the data subject.

(c) Verity the access request. we will establish if the request is sufficiently substantiated and determine whether the SAR is clear regarding what personal data is requested. If we are uncertain of what data is required, it will request additional information from the data subject.

(d) Verify whether requests are unfounded or excessive. If so, we may refuse to act on the request or charge a reasonable fee.

(e) Promptly acknowledge receipt of the SAR and inform the data subject of any costs involved in the processing of the SAR.

(f) Verify whether we process the data requested. If we do not process any data it will inform the data subject accordingly. We will, at all times ensure the internal SAR policy is followed and progress is monitored.

(g) Ensure data is not changed as a result of the SAR. However, routine changes as part of the processing activities concerned are permitted.

(h) Verify whether the data requested also involves data on other data subjects and will make sure this data is filtered before the requested data is supplied to the data subject. If data cannot be filtered, we will ensure that other data subjects have consented to the supply of their data as part of the SAR.

Responding to a SAR

(a) We will respond to an SAR within one month after receipt of the request, however:

(i) if more time is needed to respond to complex requests an extension of another two months is permissible. We will communicate this to the data subject as soon as possible after the need for an extension of time becomes apparent, but within the first month;

(ii) if we cannot provide the information requested, it will inform the data subject on this decision without delay and at the latest within one month of receipt of the request.

(b) If an SAR is submitted electronically, we will aim to respond using the same means.

(c) Where data on the data subject is processed, RL will provide the following information in the SAR response:

(i) the purposes of the processing;

(ii) the categories of personal data concerned;

(iii) the recipients or categories of recipients to whom personal data has been or will be disclosed;

(iv) where possible, the envisaged period for which personal data will be stored, or, if not possible, the criteria used to determine that period;

(v) the existence of the right to request rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;

(vi) the right to lodge a complaint with the Information Commissioner's Office ("ICO");

(vii) if the data has not been collected from the data subject, the source of such data;

On receipt of a Subject Access Request or if you are not sure something is a SAR please notify a director.

Disclosure of Data

The Company must ensure that personal data is not disclosed to unauthorised third parties which includes other family members, connected third parties and government bodies. All staff should

exercise caution when asked to disclose personal data held on another individual to a third party. If there is any doubt as to whether or not the information should be disclosed contact a director.

This policy determines that personal data may be legitimately disclosed where one of the following conditions applies:

1. The individual has given their consent (e.g. the client has consented to us speaking to their adviser or other named third party and we have this in writing from them);
2. Where the disclosure is in the legitimate interests of the client and the practice (e.g. disclosure of information to other staff members or parties involved in the transaction to be able to proceed as instructed);

Legitimate interest

If anyone is unsure of the legitimate interest test as it has a wide scope then the three-part question test can be used:

1) Purpose test – is there a legitimate interest behind the processing?
2) Necessity test – is the processing necessary for that purpose?
3) Balancing test – is the legitimate interest overridden by the individual's interests, rights or freedoms?

3. Where the practice is legally required to disclose the data (e.g. money laundering legislation);

For further examples please refer to our Privacy Notice for clients where we have informed them of the legitimate purposes for which their data may be processed.

Retention and Disposal of Data

The Company will not retain personal data for longer than necessary. The data retention periods are documented in our Privacy Notice.

Clients

Data for clients is generally retained for 7 years to comply with legal and regulatory requirements.

Staff

All employees have signed a Staff Data Processing Notice setting out the Company's lawful purposes for processing data and the retention guidelines for that data.

- Recruitment Records
  A record and information of the names of applicants who have been short listed and/or interviewed or unsuccessful applicants will be kept only by RL for 3 months from the interview date to aid in the management of the recruitment process. CVs will be deleted for our records after the 3 months.

- Disposal of Records
  All personal data must be disposed of in a way that protects the rights and privacy of the data subjects (e.g. by way of shredding, disposal of confidential waste or secure electronic deletion).

Documentation

The Company has the following documentation in place regarding data protection;-

- Privacy Policy
  - Explaining to clients what personal data we need, why we need it, how we collect it, who has access, how we protect it, how long we will keep it and their rights.

- Report a data breach template
- Breach register
- Internal guidance - data protection breach assessment
- Service Level Agreements with suppliers that process data for us. Each Agreement has outlined their GDPR obligations to the Company to keep the data secure and confidential.

Direct Marketing

Before any direct Marketing to individuals is undertaken, it must be clear that the people to be contacted have consented to receiving such marketing and they must be given the opportunity to object to the use of their data for direct marketing purposes (e.g. an opt out box). Email marketing is governed by The Privacy and Electronic Communications (EC Directive) Regulations 2003.

Cookies

The practice complies with the requirements of The Privacy and Electronic Communications (EC Directive) Regulations 2003 in relation to the use of cookies and other similar technologies for storing information.

Review of systems and operations for processing data (privacy by design)

The following will be kept under review with an annual review of systems:

- Retention of data timescales and storage for clients data
- Staff data
- Processing any third party data excluding clients
- Encryption, IT assets, mobile devices and data processing IT systems are reviewed under IT handbook
- Supplier agreements and offsite storage
- Procedures around subject access rights
- Breach reporting procedures
- All privacy notices
- Our records of processing activities

Data protection impact assessments (DPIA)

The Company will need to consider if a DPIA is needed when working on high risk projects (for the purpose of data protection and personal data).

The areas we would need to consider most relevant to our work are:

- Processing on large scale
- Systematic monitoring
- Innovative technological or organisational solutions

In these circumstances we will consider whether we need to carry out a DPIA and any reason for not carrying one out will be documented.

DPIA checklist

- We describe the nature, scope, context and purposes of the processing

- Identify whether any high risks are involved and what they are including how to mitigate them if possible. Describe source of risk and nature of potential impact on individuals.
- Information we will provide or any consultancy with stakeholders or any individuals before processing the data
- Explain the measures and protocols adopted to keep data secure without any detriment to relevant parties
- Sign off and recorded outcomes of the DPIA with any follow up actions required

The DPIA template from the ICO website will be used when completing a DPIA.

Personal data breach and reporting

The Company will take the responsibility to identify potential data breaches and the procedure for reporting these breaches.

When do we have to report a breach?

We have to report a notifiable breach without undue delay and within 72 hours of when we become aware of it. Any breach must be reported to Paul Gitsham or Peter Jones.

What is the processing for reporting a breach?

Step 1 – report internally immediately to a director

Step 2 – identify whether it is a personal data breach

Step 3 – consider if the breach is considered 'high risk' and detriment to subject/client – all breaches will be recorded in the Company's breach register

Step 4 – complete the personal data breach form

Step 5 – consider any additional measures to avoid repeat of breach and to cascade learning throughout the Company

Is it a data breach?

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration or unauthorised disclosure of personal data.

Examples of a data breach

- Emails going to wrong recipient
- Losing laptop or memory stick (if not encrypted)
- Sending clients passport to third party without their consent
- Cyber-attack leading to unauthorised access to legal documents or clients personal data
- Losing a physical document
- A sensitive letter sent to wrong address

Questions to consider

1. Was personal data involved?
2. How many individuals did it affect?
3. Was data processed or sent without consent (when it required it)?
4. Is there risk or any detriment to the data subject (i.e. the client)? What are the likely consequences?
5. Has the data subject complained?

6. Has there been a breach in client confidentiality?
7. What measures have you have taken or propose to take to address the breach including, where appropriate, measures to mitigate its effects?
8. Has this type of breach happened before (i.e. forms part of a trend/pattern)?

General Staff Guidelines

- The only people able to access data covered by this policy should be those who need it for their work.
- Data should not be shared informally.
- we will provide training to all employees to help them understand their responsibilities when handling data.
- Employees should keep all data secure, by taking sensible precautions and following the guidelines given in the Firms policies.
- In particular, strong passwords must be used and they should never be shared.
- Personal data should not be disclosed to unauthorised people, either within the company or externally.
- Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Employees should request help if they are unsure about any aspect of data protection.
- When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it.
- Data printouts should be shredded and disposed of securely when no longer required.
- When working with personal data, employees should ensure the screens of their computers are always locked when left unattended.
- Personal data should not be shared informally. In particular, it should never be sent by email, as this form of communication is not secure.
- Data must be encrypted before being transferred electronically. The IT manager can explain how to send data to authorised external contacts.
- Employees should not save copies of personal data to their own computers. Always access and update the central copy of any data.

Data Processing Notice

Data fairness processing notice for employees, workers and contractors of tiQtoQ Ltd.

What is the purpose of this document?

We are committed to protecting the privacy and security of your personal information.

This privacy notice describes how we collect and use personal information about you during and after your working relationship with us, in accordance with the General Data Protection Regulation (GDPR) and other UK Data Protection legislation.

It applies to all employees, workers and contractors.

tiQtoQ Ltd is a "data controller". This means that we are responsible for deciding how we hold and use personal information about you. We are required under data protection legislation to notify you of the information contained in this privacy notice.

This notice applies to current and former employees, workers and contractors. This notice does not form part of any contract of employment or other contract to provide services. We may update this notice at any time.

It is important that you read this notice, together with any other privacy notice we may provide on specific occasions when we are collecting or processing personal information about you, so that you are aware of how and why we are using such information.

Data protection principles

We will comply with data protection law. This says that the personal information we hold about you must be:

1. Used lawfully, fairly and in a transparent way.
2. Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
3. Relevant to the purposes we have told you about and limited only to those purposes.
4. Accurate and kept up to date.
5. Kept only as long as necessary for the purposes we have told you about.
6. Kept securely.

What kind of information do we hold about you?

Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data).

There are "special categories" of more sensitive personal data which require a higher level of protection.

We may collect, store, and use the following categories of personal information about you:

- Personal contact details such as name, title, addresses, telephone numbers, and personal email addresses.

- Date of birth
- Gender
- Marital status and dependants
- Next of kin and emergency contact information
- National Insurance number
- Bank account details, payroll records and tax status information
- Salary, annual leave, pension and benefits information
- Start date
- Location of employment or workplace
- Copy of driving licence (for applicable employees)
- Recruitment information (including copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process).
- Employment records (including job titles, work history, working hours, training records and professional memberships)
- Compensation history
- Performance information
- Disciplinary and grievance information
- Information about your use of our information and communications systems
- Photographs
- Information about qualifications you hold

We may also collect, store and use the following "special categories" of more sensitive personal information:

- Information about your race or ethnicity, religious beliefs, sexual orientation and political opinions
- Trade union membership
- Information about your health, including any medical condition, health and sickness records
- Information about criminal convictions and offences such as for driving.

How is your personal information collected?

We typically collect personal information about employees, workers and contactors through the application and recruitment process, either directly from candidates or sometimes from an employment agency or background check provider. We may sometimes collect additional

information from third parties including former employers, credit reference agencies or other background check agencies.

We will collect additional personal information in the course of job-related activities throughout the period of you working for us.

How we will use information about you?

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

1. Where we need to perform the contract we have entered into with you.
2. Where we need to comply with a legal obligation.
3. Where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests.

We may also use your personal information in the following situations, which are likely to be rare:

1. Where we need to protect your interests (or someone else's interests).
2. Where it is needed in the public interest or for official purposes.

Situations in which we will use your personal information

We need all the categories of information in the list above (see *The kind of information we hold about you*) primarily to allow us to perform our contract with you and to enable us to comply with legal obligations. In some cases we may use your personal information to pursue legitimate interests of our own or those of third parties, provided your interests and fundamental rights do not override those interests. The situations in which we will process your personal information are listed below.

- Making a decision about your recruitment or appointment
- Determining the terms on which you work for us.
- Checking you are legally entitled to work in the UK.
- Paying you and, if you are an employee or non-executive director, deducting tax and National Insurance contributions.
- Providing the following benefits to you: [private medical insurance, life assurance, gym membership].
- Liaising with your pension provider.
- Administering the contract we have entered into with you.
- Business management and planning, including accounting and auditing.
- Conducting performance reviews, managing performance and determining performance requirements.
- Making decisions about salary reviews and compensation.
- Assessing qualifications for a particular job or task, including decisions about promotions.

- Gathering evidence for possible grievance or disciplinary hearings including dealing with complaints made about you to us
- Making decisions about your continued employment or engagement.
- Making arrangements for the termination of our working relationship.
- Education, training and development requirements.
- Dealing with legal disputes involving you, or other employees, workers and contractors, including accidents at work.
- Ascertaining your fitness to work
- Managing sickness absence.
- Complying with health and safety obligations.
- To prevent fraud and other crime.
- To monitor your use of our information and communication systems to ensure compliance with our IT policies.
- To ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution.
- To conduct data analytics studies to review and better understand employee retention and attrition rates and other metrics within the business.
- Equal opportunities monitoring.
- Where it is necessary to do so for the purposes of bringing, defending and carrying out litigation.

Some of the above grounds for processing will overlap and there may be several grounds which justify our use of your personal information.

What if you fail to provide personal information?

If you fail to provide certain information when requested, we may not be able to perform the contract we have entered into with you (such as paying you or providing a benefit), or we may be prevented from complying with our legal obligations (such as to ensure the health and safety of our workers).

What if there is a change of purpose?

We will only use your personal information 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 information 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 information without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

How do we use particularly sensitive personal information?

"Special categories" of particularly sensitive personal information require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal information. We may process special categories of personal information in the following circumstances:

1. In limited circumstances, with your explicit written consent.
2. Where we need to carry out our legal obligations and in line with our data protection policy.
3. Where it is needed in the public interest, such as for equal opportunities monitoring, and in line with our data protection policy.
4. Where it is needed to assess your working capacity on health grounds, subject to appropriate confidentiality safeguards.

Less commonly, we may process this type of information where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public. We may also process such information about employees or former employees in the course of legitimate business activities with the appropriate safeguards.

What are our obligations as an employer?

We will use your particularly sensitive personal information in the following ways:

- We will use information relating to leaves of absence, which may include sickness absence or family related leaves, to comply with employment and other laws.
- We will use information about your physical or mental health, or disability status, to ensure your health and safety in the workplace and to assess your fitness to work, to provide appropriate workplace adjustments, to monitor and manage sickness absence and to administer benefits.
- We will use information about your race or national or ethnic origin, religious, philosophical or moral beliefs, or your sexual life or sexual orientation, to ensure meaningful equal opportunity monitoring and reporting.

Do we need your consent?

We do not need your consent if we use special categories of your personal information in accordance with our written policy to carry out our legal obligations or exercise specific rights in the field of employment law.

In limited circumstances, we may approach you for your written consent to allow us to process certain particularly sensitive data. If we do so, we will provide you with full details of the information that we would like and the reason we need it, so that you can carefully consider whether you wish to consent. You should be aware that it is not a condition of your contract with us that you agree to any request for consent from us.

Information about criminal convictions

We may only use information relating to criminal convictions where the law allows us to do so. This will usually be where such processing is necessary to carry out our obligations and provided we do so in line with our data protection policy.

Less commonly, we may use information relating to criminal convictions where it is necessary in relation to legal claims, where it is necessary to protect your interests (or someone else's

interests) and you are not capable of giving your consent, or where you have already made the information public.

We envisage that we will hold information about criminal convictions.

We will only collect information about criminal convictions if it is appropriate given the nature of the role and where we are legally able to do so. Where appropriate, we will collect information about criminal convictions as part of the recruitment process or we may be notified of such information directly by you or third parties in the course of you working for us, such as road traffic offences. We will use information about criminal convictions and offences in the following ways:

- determining who we recruit;
- determining whether it is legal for you to carry out your duties such as driving; and
- whether any action should be taken to terminate your employment.

We are allowed to use your personal information in this way to carry out our obligations.

What about automated decision-making?

Automated decision-making takes place when an electronic system uses personal information to make a decision without human intervention. We are allowed to use automated decision-making in the following circumstances:

1. Where we have notified you of the decision and given you 21 days to request a reconsideration.
2. Where it is necessary to perform the contract with you and appropriate measures are in place to safeguard your rights.
3. In limited circumstances, with your explicit written consent and where appropriate measures are in place to safeguard your rights.

If we make an automated decision on the basis of any particularly sensitive personal information, we must have either your explicit written consent or it must be justified in the public interest, and we must also put in place appropriate measures to safeguard your rights.

You will not be subject to decisions that will have a significant impact on you based solely on automated decision-making, unless we have a lawful basis for doing so and we have notified you.

We do not envisage that any decisions will be taken about you using automated means, however we will notify you in writing if this position changes.

What about data sharing?

We may have to share your data with third parties, including third-party service providers and other entities in the group if the company grows in the future.
We require third parties to respect the security of your data and to treat it in accordance with the law.
We may transfer your personal information outside the EU.
If we do, you can expect a similar degree of protection in respect of your personal information.

Why might you share my personal information with third parties?

We may share your personal information with third parties where required by law, where it is necessary to administer the working relationship with you or where we have another legitimate interest in doing so.

Which third-party service providers process my personal information?

"Third parties" includes third-party service providers (including contractors and designated agents) and other entities within our group. The following activities are carried out by third-party service providers: [pension administration, benefits provision and administration, IT services].

How secure is my information with third-party service providers and other entities in our group?

All our third-party service providers and other entities in the group are required to take appropriate security measures to protect your personal information in line with our policies. We do not allow our third-party service providers to use your personal data for their own purposes. We only permit them to process your personal data for specified purposes and in accordance with our instructions. They have to return data to us when they cease processing it.

When might you share my personal information with other entities in the group?

We will share anonymized data with other entities in our group as part of our regular reporting activities on company performance but we do not share your personal data with Israel without it being anonymised.

What about other third parties?

We may share your personal information with other third parties, for example in the context of the possible sale or restructuring of the business or in relation to investment into the business by relevant investors. We may also need to share your personal information with a regulator or to otherwise comply with the law eg:- the Health and Safety Executive.

What about Transferring information outside the EU?

We do not share your data outside the EU.

What about data security?

We have put in place measures to protect the security of your information. Details of these measures are available upon request.

Third parties will only process your personal information on our instructions and where they have agreed to treat the information confidentially and to keep it secure.

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

What about data retention? How long will you use my information for?

We will only retain your personal information 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. Our policy on data retention is available from the Managing Director.

In some circumstances we may anonymise your personal information so that it can no longer be associated with you, in which case we may use such information without further notice to you. Once you are no longer an employee, worker or contractor of the company we will retain and securely destroy your personal information in accordance with applicable laws and regulations.

Rights of access, correction, erasure, and restriction

Your duty to inform us of changes

It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your working relationship with us.

Your rights in connection with personal information

Under certain circumstances, by law you have the right to:

- Request access to your personal information (commonly known as a "data subject access request"). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it.
- Request correction of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.
- Request the erasure of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to stop processing personal information where we are relying on a legitimate interest and there is something about your particular situation which makes you want to object to processing on this ground.
- Request the restriction of processing of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.
- Request the transfer of your personal information to another party.

If you want to review, verify, correct or request erasure of your personal information, object to the processing of your personal data, or request that we transfer a copy of your personal information to another party, please contact the General Manager in writing.

No fee usually required

You will not have to pay a fee to access your personal information (or to exercise any of the other rights). However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in such 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 the information (or to exercise any of your other rights). This is another

appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

Right to withdraw consent

In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact the General Manager. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

Changes to this privacy notice

We reserve the right to update this privacy notice at any time, and we will provide you with a new privacy notice when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal information.