

DATA PROTECTION POLICY

The Organisation needs to collect and use certain types of information about staff, clients and other individuals who come into contact with the company in order to operate. In addition, it may be required by law to collect and use certain types of information to comply with statutory obligations of Local Authorities, government agencies and other bodies.

This personal information must be dealt with properly, however, it is collected, recorded and used – whether on paper, in a computer, or recorded on other material - and there are safeguards to ensure this is within the EU General Data Protection Regulation and the Data Protection Act 2018.

We regard the lawful and correct treatment of personal information as very important to successful operations, and to maintaining confidence between those with whom we deal and ourselves. We ensure that our Organisation treats personal information lawfully and correctly.

Most businesses hold personal data on their customers, employees and partners. The explosion in the use of the Internet, electronic communication and computerisation of business data has led to an increase in the importance of privacy. Breaches of computerised data security have prompted the introduction of legislation on a national and European level.

These include:

- Human Rights Act 1998
- Freedom of Information Act 2000
- Privacy and Electronic Communications Regulations 2003
- Regulation of Investigatory Powers Act 2000
- Telecommunications (Lawful Business Practice) Interception of Communications Regulations 2000
- Data Protection Act 2018
- Computer Misuse Act 1990.
- European Union General Data Protection Regulation 2016 (EU GDPR).

The General Data Protection Regulation 2016 replaces the EU Data Protection Directive of 1995 and supersedes the laws of individual Member States that were developed in compliance with the Data Protection Directive 95/46/EC. Its purpose is to protect the “rights and freedoms” of living individuals, and to ensure that personal data is not processed without their knowledge, and, wherever possible, that it is processed with their consent.

The top management of the Organisation are strongly committed to the rights of individuals whose data they collect and process and will comply with UK and EU laws related to personal information in line with the EU General Data Protection Regulation (GDPR).

The top management of the Organisation ensures that it meet its requirements under EU GDPR for the management of personal information, that the objectives of the Organisation and obligations under the law are met, and ensures that controls are in place that reflect the level of risk that the Organisation is willing to accept.

In addition, steps are taken to ensure that the Organisation is able to meet all the regulatory, statutory and contractual obligations that are applicable, including the protection of the interests of individuals and all other relevant stakeholders.

To comply with the requirements of GDPR, the Organisation will:

- Process personal information only where this is strictly necessary for legitimate organisational purposes
- Collect only the minimum personal information required for these purposes and not process excessive amounts of personal information

- Provide clear information to individuals about how their personal information will be used and who will be using the information
- Only process relevant and adequate personal information
- Process personal information fairly and lawfully
- Keep all personal information secure
- Maintain an inventory of the categories of personal information that is processed
- Ensure they keep personal information accurate and up to date
- Retain personal information only for as long as is necessary for legal or regulatory reasons or, for legitimate organisational purposes
- Respect individuals' rights in relation to their personal information as defined in the GDPR
- Only transfer personal information outside the EU Member States in circumstances where it can be adequately protected and aligned with EU GDPR Regulations
- Only apply exemptions permitted by data protection legislation
- Identify internal and external stakeholders and the degree to which these stakeholders are involved in the governance of the Organisation's stored or processed personal information
- Identify staff with specific responsibility and accountability for the ongoing maintenance and support of the requirements of the GDPR.

Notification to the Information Commissioner's Office (ICO)

the Organisation has notified the Information Commissioner that it is a data controller and/or processor and that it processes personal data. the Organisation has identified and recorded all the personal data that it processes in the Data Register.

A record of notification to the ICO is retained by the DPO (*Data Protection Officer*) and the ICO Notification Handbook is used as the authoritative guidance for notification. This notification is reviewed annually and update notifications are issued accordingly.

The DPO is responsible for reviewing the details of notification to ensure that any changes to the way that the Organisation processes or controls personal data is (as determined by changes to the Data Register and following management review) referred back to the ICO. Additional requirements for notification may also arise from Personal Data Impact Assessments.

The policy applies to all Employees and Processors of the Organisation such as outsourced suppliers. Any breach of the GDPR will be considered as a breach of the disciplinary policy and could also be considered a criminal offence, potentially resulting in prosecution.

All third parties working with or for the Organisation, and who have or may have access to personal information, will be expected to comply with this policy. All third parties who require access to personal data will be required to sign a confidentiality agreement before access is permitted. This agreement will ensure that the third party has the same legal obligations as the Organisation. This will also include an agreement that the Organisation can audit compliance with the agreement.

GDPR will apply to all controllers that are established in the EU (European Union) who process the personal data of data subjects, in the context of that establishment. It will also apply to controllers outside of the EU that process personal data in order to offer goods and services, or monitor the behaviour of data subjects who are resident in the EU.

The location, for the purposes of GDPR, of any data controller located in the EU will be the place where the controller makes the key decisions related to the data processing purpose. This is likely to be the Organisation's HQ.

Any data controller that is not located within the EU will be required to appoint a representative in a location that is under the jurisdiction that applies to the data that is being used in order to act on behalf of the controller and engage with the appropriate supervisory authorities for that location.

Company Responsibilities

The Organisation is a data controller and/or data processor (*Client to delete inapplicable title upon acceptance of the Policy from QMS*) as defined under the GDPR.

Senior Management and all those in managerial or supervisory roles throughout the Organisation are responsible for developing and encouraging good information handling practices within the Organisation; responsibilities are set out in individual job descriptions.

A DPO, a member of the senior management team, is accountable to the top management of the Organisation for the management of personal information within the Organisation and for ensuring that compliance with data protection legislation and good practice can be demonstrated. This accountability includes the development and implementation of security and risk management to ensure compliance.

The Organisation has appointed a suitably qualified and experienced DPO who is responsible for day-to-day compliance with this policy. The DPO is responsible for ensuring that the Organisation complies with the GDPR in relation to all aspects of data processing. The DPO has direct responsibility for policy and procedures, including Subject Access Requests. The DPO is also the person to whom all staff will go to seek guidance regarding GDPR compliance.

It should be noted that compliance with GDPR requirements remains the responsibility of all staff who process or control personal information for the Organisation. All members of staff employed by the Organisation are also responsible for ensuring that any personal data that is about them that is supplied by them to the Organisation is accurate and up to date.

The Training Policy defines specifically what training is required for all staff, including specific roles.

Risk Assessment in relation to GDPR

The Organisation needs to ensure that it is aware of any risks associated with the processing of all types of personal information. A Risk Assessment procedure has been implemented and is used by the Organisation to assess any risk to individuals during processing of their personal information. Assessments will also be completed by the Organisation for any processing that is undertaken on their behalf by any third party organisation. The Organisation will also, through the application of the Risk Assessment procedure, ensure that any identified risks are managed appropriately to reduce the risk of non-compliance.

Where processing of personal information may result in a high risk to the "rights and freedoms" of natural persons, the Organisation shall complete a data protection impact assessment, prior to conducting the processing, to ensure the personal information is protected. This assessment may also be used to apply to a number of similar processing scenarios with a similar level of risk.

Where, as a result of a Data Protection Impact Assessment, it is clear that the Organisation will process personal information in a manner that may cause damage and/or distress to the data subjects, the DPO must review the process before the Organisation proceeds to process the information. If the DPO decides that there are significant risks to the data subject they will escalate to the ICO for final guidance. The organisation shall apply selected controls for the ISO 27001 Annex A to reduce risk. This should also reference the Organisation's risk acceptance criteria and the requirements of the GDPR.

Principles of Data Protection

Any processing of personal data must be conducted in accordance with the following data protection principles of the Regulation, and the Organisation's policies and procedures will ensure compliance.

Personal data must be processed lawfully, fairly and transparently. The Organisation's Fair Processing Procedure details how this is achieved.

The GDPR introduces the requirement for transparency whereby the controller has transparent and easily accessible policies relating to the processing of personal data and the exercise of individuals' 'rights and freedoms'.

Information must be communicated to the data subject in an intelligible form using clear and plain language.

The specific information that must be provided to the data subject must as a minimum include:

- The identity and the contact details of the controller and, if any, of the controller's representative
- The contact details of the DPO, where applicable
- The purposes of the processing for which the personal data are intended as well as the legal basis for the processing
- The period for which the personal data will be stored
- The existence of the rights to request access, rectification, erasure or to object to the processing
- The categories of personal data concerned
- The recipients or categories of recipients of the personal data, where applicable
- Where applicable, that the controller intends to transfer personal data to a recipient in a third country and the level of protection afforded to the data
- Any further information necessary to guarantee fair processing.

Personal data can only be collected for specified, explicit and legitimate purposes. Data obtained for specified purposes must not be used for a purpose that differs from those formally notified to the Information Commissioner as part of the Organisation's GDPR registration.

Personal data must be adequate, relevant and limited to what is necessary for processing. The DPO is responsible for ensuring that information, which is not strictly necessary for the purpose for which it is obtained, is not collected.

All data collection methods (electronic or paper-based), including data collection requirements in new information systems, must be approved by the DPO and approval recorded.

The DPO will ensure that all data collection methods are reviewed annually by internal audit or external experts to ensure that collection continues to be adequate, relevant and not excessive.

The DPO is responsible for ensuring that any data that is shown to have been obtained excessively, or is not specifically required by the Organisation, is securely deleted or destroyed (see A.8.3.2 and A.11.2.7 of the Statement of Applicability).

Other Considerations

Personal data must be accurate and kept up to date.

Data that is kept for a long time must be reviewed and updated as necessary. Any data that is considered to be inaccurate or likely to be inaccurate must be removed.

Top management is responsible for ensuring that all staff are trained in the importance of collecting accurate data and maintaining it.

All individuals are responsible for ensuring that any data held by the Organisation is accurate and up to date. Any data submitted by an individual to a company, such as via a registration form, will be considered to be accurate at the time of receipt.

Employees or other individuals should notify the Organisation of any changes in personal information to ensure personal information is kept up to date. It is the responsibility of the Organisation to ensure that any notification of changes to personal information is implemented.

The DPO is responsible for ensuring that all necessary actions are taken to ensure personal information is accurate and up to date. This should also take into account the volume of data collected, the speed with which it might change and any other relevant factors.

The DPO will review, at least once a year, all the personal data processed by the Organisation, held in the Data Register. The DPO will note any data that is no longer required in the context of the registered purpose and will ensure that it is appropriately removed and securely disposed of (see A.8.3.2 and A.11.2.7 of the Statement of Applicability).

If a third party organisation has provided inaccurate or out-of-date personal information, the DPO is responsible for informing them that the personal information is inaccurate and/or out-of-date and will advise them that the information should no longer be used. The DPO should also ensure that any correction to the personal information is passed on to the third party.

Personal Data Considerations

Personal data must be kept in a form such that the data subject can be identified only as long as is necessary for processing.

Where personal data is retained beyond the processing date, it will be encrypted in order to protect the identity of the data subject in the event of a data breach.

Personal data will be retained in line with the retention of records procedure and, once its retention date is passed, it must be securely destroyed as set out in the Retention of Records Procedure.

The DPO must specifically approve any data retention that exceeds the retention periods defined in the Retention of Records procedure and must ensure that the justification is clearly identified and in line with the requirements of the data protection legislation. This approval must be written.

Personal data must be processed in a manner that ensures its security.

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. These controls have been selected on the basis of identified risks to personal data, and the potential for damage or distress to individuals whose data is being processed. Security controls will be subject to audit and review.

The Organisation's compliance with this principle is contained in its Information Security Management System (ISMS), which has been developed in line with ISO/IEC 27001 : 2013 and the Security Policy set out in the ISMS.

Personal data shall not be transferred to a country or territory outside the European Union Member States unless that country or territory ensures an adequate level of protection for the 'rights and freedoms' of data subjects in relation to the processing of personal data.

The transfer of personal data outside of the EU Member States is prohibited unless one or more of the specified safeguards or exceptions apply.

Safeguards

An assessment of the adequacy by the data controller taking into account the following factors:

- The nature of the information being transferred
- The country or territory of the origin, and final destination, of the information
- How the information will be used and for how long
- The laws and practices of the country of the transferee, including relevant codes of practice and international obligations and
- The security measures that are to be taken as regards the data in the overseas location (this is a UK-specific option).

Binding Corporate Rules

The Organisation may adopt approved Binding Corporate Rules for the transfer of data outside the EU Member States. This requires submission to the relevant Supervisory Authority for approval of the rules that the Organisation is seeking to rely upon.

Model Contract Clauses

The Organisation may adopt approved model contract clauses for the transfer of data outside of the EU Member States. If the Organisation adopts the model contract clauses approved by the relevant Supervisory Authority, there is an automatic recognition of adequacy.

Exceptions

In the absence of an adequacy decision, including binding corporate rules, for the transfer of personal data to a third country, or an international organisation, it shall take place only on one of the following conditions:

- The data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards
- The transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request
- The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person
- The transfer is necessary for important reasons of public interest
- The transfer is necessary for the establishment, exercise or defence of legal claims
- The transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent
- The transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down in Union or Member State law for consultation are fulfilled in the particular case.

A list of countries that satisfy the adequacy requirements of the Commission is published in the Official Journal of the European Union and in the GDPR 2016.

Accountability

The GDPR states that the controller is not only responsible for ensuring compliance but for demonstrating that each processing operation complies with the requirements of the GDPR. As a result, controllers are required to keep all necessary documentation of all processing operations, and implement appropriate security measures. They are also responsible for completing Data Processing Impact Assessments (DPIAs), complying with requirements for prior notifications, or approval from supervisory authorities and ensuring a DPO is appointed if required.

Data Subjects' Rights

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

- To make subject access requests regarding the nature of information held and to whom it has been disclosed
- To prevent processing likely to cause damage or distress
- To prevent processing for purposes of direct marketing

- To be informed about the mechanics of automated decision-taking process that will significantly affect them
- Not to have significant decisions that will affect them taken solely by automated process
- To sue for compensation if they suffer damage by any contravention of the GDPR
- To take action to rectify, block, erase, including the right to be forgotten, or destroy inaccurate data
- To request the ICO to assess whether any provision of the GDPR has been contravened
- The right for personal data to be provided to them in a structured, commonly used and machine-readable format, and the right to have that data transmitted to another controller
- The right to object to any automated profiling without consent.

Data subjects may make data access requests as described in the Subject Access Requests procedure. This procedure also describes how the Organisation will ensure that its response to the data access request complies with the requirements of the Regulation.

Complaints

A Data Subject has the right to complain at any time to the Organisation if they have concerns about how their information is used. If they wish to lodge a complaint, this should be directed to the DPO following the complaints procedure using a complaint form supplied by the Organisation. *[A complaints form and procedure must be implemented to include a GDPR complaints section. This would normally be provided through the 'Contact Us' section of the company website. It is also important to display a Fair Processing Notice at this point.]*

A Data Subject also has the option to complain directly to the Information Commissioner's Office. Details of the options for lodging a complaint should be provided by the Organisation, usually within the 'Contact Us' section on the company website.

Consent

The Organisation understands 'consent' to mean that it has been explicitly and freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she by statement, or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. The consent of the data subject can be withdrawn at any time.

In addition, the Organisation understands 'consent' to mean that the data subject has been fully informed of the intended processing and has signified their agreement, while in a fit state of mind to do so and without pressure being exerted upon them. Consent obtained under duress or on the basis of misleading information will not be a valid basis for processing. There must be some active communication between the parties which demonstrate active consent. Consent cannot be inferred from non-response to a communication. For sensitive data, explicit written consent of data subjects must be obtained unless an alternative legitimate basis for processing exists.

Consent to process personal and sensitive data is obtained routinely by the Organisation using standard consent documents. This may be through a contract of employment or during induction.

Where the Organisation provides online services to children, parental, or custodial authorisation must be obtained. This requirement applies to children under the age of 16 (unless the Member State has made provision for a lower age limit – which may be no lower than 13).

Data Security

All the Organisation Staff that are responsible for any personal data which the Organisation holds must keep it securely and ensure that it is not disclosed under any conditions to any third party unless that third party has been specifically authorised by the Organisation to receive that information and has entered into a confidentiality agreement.

All personal data should be accessible only to those who need to use it, and access may only be granted in line with the Access Control Policy. You should form a judgment based upon the sensitivity and value of the information in question, but personal data must be kept:

- In a lockable room with controlled access; and/or
- In a locked drawer or filing cabinet; and/or
- If computerised, it must be password protected in line with the Access Control Policy
- Cryptographic Controls Policy.

Care must be taken to ensure that PC screens and terminals are not visible except to authorised Staff of the Organisation's E-mail & Internet Acceptable Usage Policy.

Manual records may not be left where they can be accessed by unauthorised personnel and may not be removed from business premises without explicit [written] authorisation. As soon as manual records are no longer required for day-to-day client support, they must be removed from secure archiving in line with [procedure reference].

Personal data may only be deleted or disposed of in line with the Retention of Records procedure. Manual records that have reached their retention date are to be shredded and disposed of as 'confidential waste'. Hard drives of redundant PCs are to be removed and immediately destroyed (see A.8.3.2 and A.11.2.7). Because of the increased risk, all Staff must be specifically authorised to process data off-site.

Rights of Access to Data

Data subjects have the right to access any personal data (i.e. data about them) which is held by the Organisation in electronic format and manual records which form part of a relevant filing system. This includes the right to inspect confidential personal references received by the Organisation, and information obtained from third party organisations about that person. Subject Access Requests are dealt with as described in the Subject Access Request Procedure.

Disclosure of Data

The Organisation must ensure that personal data is not disclosed to unauthorised third parties which includes family members, friends, government bodies, and in certain circumstances, the Police. All Employees/Staff should exercise caution when asked to disclose personal data held on another individual to a third party [and will be required to attend specific training that enables them to deal effectively with any such risk]. It is important to bear in mind whether or not disclosure of the information is relevant to, and necessary for, the conduct of the Organisation's business.

GDPR permits a number of exemptions where certain disclosure without consent is permitted, as long as the information is requested for one or more of the following purposes:

- To safeguard national security
- Prevention or detection of crime including the apprehension or prosecution of offenders
- Assessment or collection of tax duty
- Discharge of regulatory functions (includes health, safety and welfare of persons at work)
- To prevent serious harm to a third party
- To protect the vital interests of the individual - this refers to life and death situations.

All requests to provide data for one of these reasons must be supported by appropriate paperwork and all such disclosures must be specifically authorised by the DPO.

Retention and Disposal of Data


Personal data may not be retained for longer than it is required. Once a member of staff has left the Organisation, it may not be necessary to retain all the information held on them. Some data

will be kept for longer periods than others. The Organisation's data retention and data disposal procedures will apply in all cases.

Disposal of Records

Personal data must be disposed of in a way that protects the "rights and freedoms" of data subjects (e.g. shredding, disposal as confidential waste, secure electronic deletion) (see A.8.3.2 and A.11.2.7).

Policy Sign-off

Date of Issue:	16/11/2020
Date of Next Review:	15.11.2021
Name:	Thiru Sundaresan
Signed:	

Amendment History

Version	Modified On	Modified By	Comments
1.0	16/11/2020	Thiru Sundaresan	
