Data Protection Policy

Mitutoyo UK Ltd., is referred to herein as the 'Company'.

Mitutoyo is committed to working in accordance with the General Data Protection Regulation (GDPR) as implemented by the Data Protection Act 2018 to ensure the highest standards of ethical conduct.

This policy outlines the rules, behaviours and standards required of the organisation, employees, workers and third parties working on behalf of the Company in relation to the collection, retention, transfer, disclosure, use and destruction of any personal data, this includes data received from third parties (such as our clients) for which Mitutoyo is acting as Data Processor. Employees are expected to:

- Ensure documents containing any employee personal data of a physical or electronic nature are not publicly available and securely stored out of view.
- Ensure that Personal and Company devices as used for work purposes, such as laptops, telephones, memory sticks remain at all times, when working in or out of the office, securely stored and out of view or harm's way or theft when not in use. Mobile devices e.g. laptops, mobile phones must remain securely in the employee's possession or stored in a safe place for retrieval when required such as in boot of car, locked drawer/cupboard.
- Protect any personal/sensitive data by password and encrypt any sensitive personal information before sending on to approved recipients.
- Use a password protected screen saver that activates when away from the device.
- Never discuss confidential matters relating to either Mitutoyo or our clients in a public place, such as on public transport or social media.
- Use passwords containing a mix of upper and lower-case letters and numbers. Never share passwords and change them regularly. Access will be cancelled if an employee leaves or is absent from the business for longer than 4 consecutive weeks.
- Protect personal data if posted by using recorded delivery to ensure safe delivery.
- Ensure that when entering into written correspondence with clients on employee issues, that data should be anonymised and actual names/data avoided, unless absolutely essential.
- Ensure all clients are aware of this policy and remind them as and when necessary.
- Not to store any files or data on your computer desktop or allow any downloaded documents to be saved on to your personal devices e.g. phones, tablets. If these are accidentally downloaded/saved, they should be deleted as soon as possible.
- Report any breaches or near misses of information security/data protection e.g. fraud, information leaks, laptop thefts as soon possible to your Manager.

Data Protection Principles

The Organisation is committed to adhering to the Data Protection Principles which state:

- Data must be processed lawfully, fairly and in a transparent manner.
- Data must be obtained for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- Data processed must be adequate, relevant and limited to what is necessary.
- Data must be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure data that are inaccurate, are erased or rectified without delay.
- Data must not be kept for longer than is necessary for the purposes for which the data are processed.
- Data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing, accidental loss, destruction or damage, using appropriate technical or organisational measures.

Information is kept and processed about individuals for legal purposes (such as for payroll), for administration purposes and for the purposes of day-to-day people-management. The Company is aware that in order to process personal data, or sensitive personal data, the Company must rely on the data being:

- necessary for the performance of a contract, or;
- in preparation for a contract, or;
- to comply with our legal obligations, or;
- for our legitimate business interests or;
- to perform a task carried out in the public interest or in the exercise of an official authority.

If the organisation wishes to hold and process data which does not fall within conditions listed above, then it will seek to obtain the consent of the individual.

Personal Data

The Organisation collects and processes the following personal data (this is not an exhaustive list):

- Mitutoyo employee/worker data, such as: names, job titles, addresses, contact details, bank details, NI numbers, date of birth, health/medical information, next of kin details, psychometric profile data and so on.
- Personal data from Data Controllers (such as clients) for whom we are acting as Data Processor, such as; employee names, addresses, data related to remuneration, NI numbers, date of birth, psychometric profile data, health/medical information and so on.
- Personal data from third parties as individuals for the purposes of direct marketing, including names, job titles, addresses, contact details etc.

Rights of Data Subjects

The Company will recognise that individuals have the following rights under data protection legislation:

- the right to be informed, which encompasses the obligation on employers to provide transparency as to how personal data will be used;
- the right of access;
- the right to rectification of data that is inaccurate or incomplete;
- the right to be forgotten under certain circumstances;
- the right to block or suppress processing of personal data; and
- the new right to data portability which allows employees to obtain and reuse their personal data for their own purposes across different services under certain circumstances.

Right of Access

Individuals have the right to access the information stored about them and can ask for access to their own personal details held electronically or held manually. Individuals who wish to see their records should give notice electronically, in writing, using a Subject Access Request Form which is available upon request. The Company has up to 1 month to provide the information following the subject access request, which it will usually do in electronic format.

In complex cases, or where there are numerous related requests, the Company will liaise with the individual to inform them of progress of their request(s), and if it is not possible to complete this within 1 month, the Company will inform the individual of the delay, the reasons for the delay and reserves the right to extend the timescale for completion by up to a further 2 months.

In the event that data is retained with third parties, the Company will ensure that the request is communicated and actioned by the third party in line with the timescales outlined above, unless impossible or if it would require disproportionate effort.

The Company reserves the right to charge a fee or to refuse to respond to a request if it is manifestly unfounded or excessive. Similarly, the Company reserves the right to withhold personal data if disclosing it would adversely affect the rights and freedoms of others.

Rectification of Data

The Company is committed to keeping data that is accurate and up to date. Data will be checked for accuracy where possible, and any data that is in accurate, out of date or unnecessary will be corrected or erased as appropriate.

Where an individual identifies that their personal data is incorrect or incomplete, or where they are aware that their personal data has changed, they must inform the organisation as soon as possible. The organisation will then take steps to rectify any inaccuracies as soon as possible, and at the latest within 1 month.

In complex cases, or where there are numerous cases, the Company will liaise with the individual to inform them of progress of their request, and if it is not possible to complete this within 1 month, the Company will inform the individual of the delay and the reasons for the delay and reserves the right to extend the timescale for completion by up to a further 2 months.

In the event that data has been disclosed to third parties, the Company will ensure that the request for rectification is communicated and actioned by the third party in line with the timescales outlined above, unless this is impossible or if it would involve disproportionate effort.

The Right to be Forgotten

Also known as 'the right to erasure', the right to be forgotten doesn't provide an absolute right to be forgotten, but individuals have a right to have personal data erased and to prevent processing in some circumstances i.e.

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.
- When the individual withdraws consent.
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.
- The personal data was unlawfully processed.
- The personal data has to be erased in order to comply with a legal obligation.
- The personal data is processed in relation to the offer of information society services to a child.

If an individual wants to ask for their own personal data to be partially/fully erased and no longer processed, please write to the Director responsible for HR with full details of your request. The Company has up to 1 month to respond to you and either delete the data or explain why it is unable to comply with your request. Circumstances where the Company may be unable to comply include where it is required to retain the information by law, or if the data is needed in connection with legal proceedings.

In complex cases, or where there are numerous related requests, the Company will liaise with the individual to inform them of progress, and if it is not possible to respond to this within 1 month, the Company will inform the individual of the delay, the reasons for the delay and reserves the right to extend the timescale for completion by up to a further 2 months, if necessary.

In the event that data is retained with third parties, the Company will ensure that the request is communicated and if appropriate actioned by the third party in line with the timescales outlined above.

Security of Data

The Company is committed to taking steps to ensure that personal data is protected, and to prevent any unauthorised access, accidental loss, destruction, unlawful processing, equipment

failure or human error, and will do this through the continual monitoring of our security systems and by regular training and awareness raising.

Any data breaches will be managed according to the procedures documented in our Data Protection Breach Reporting Policy and Procedure.

Data Breaches

All staff are responsible for data protection and should be alert to any actual, suspected, threatened or potential data protection breaches. As soon as a data protection breach has been discovered, where possible, the member of staff should complete a Data Protection Breach Reporting Form (to the fullest extent possible at that time), which provides full details concerning the breach. This form should then be passed to the Director responsible for HR as soon as possible and within 24 hours of the discovery of the breach. If you need help completing the form, or are unable to complete the form, then any delay should be avoided and instead the matter should be reported immediately at least within 24 hours, either verbally or using electronic means, such as email.

For more information regarding managing data protection breaches, please refer to the Data Protection Breach Reporting Policy and Procedure.

Objections to Personal Data Processing

You have the right to object to data processing when Mitutoyo is:

- processing information based on its legitimate business interests, or the performance of a task in the public interest/exercise of official authority (including profiling)
- direct marketing
- processing for the purposes of scientific/historical research and statistics.

If you wish to object to processing, you should write to the Director responsible for HR, outlining the grounds relating to your particular situation and the Company will stop the processing unless it has compelling legitimate grounds for the processing which override your interests, rights and freedoms, or the processing is in relation to legal claims. If the Company is unable to agree to your request, you will be written to and the reason why will be explained, along with your right to complain to the ICO.

Data Protection Measures

Mitutoyo is committed to ensuring the security of your data and to processing it in line with the Data Protection rules. As such, Mitutoyo will:

- Ensure that all staff are aware of their responsibilities and Mitutoyo's obligations and responsibilities in relation to data protection.
- Ensure that all staff are aware of and adhere to Mitutoyo's Information Security Guidelines.

- Ensure that all staff who handle data on behalf of Mitutoyo are appropriately trained and receive refresher training on a regular basis.
- Ensure that all staff and Data Processors who handle data on our behalf are regularly monitored, assessed and reviewed.
- Ensure that all of the Data Processors working on behalf of Mitutoyo who handle data on our behalf are carrying out data processing in line with the Data Protection rules.
- Regularly audit and work to continuously improve Mitutoyo's methods of data collection, handling, processing and storage.

Data Retention

Mitutoyo is committed to managing and handling personal data in line with best practice and data protection principles. As such this Policy details the procedures to use to ensure timely and secure disposal of documents and records that are no longer required for business purposes.

Mitutoyo holds a wide variety of personal data, from employees, workers and contractors, as well as financial data, client data, which may include client employee data. This data is held in various formats including, letters, emails, contracts, forms, software systems in both hard copy and electronic form.

It is essential that this policy is adhered to, as premature destruction of documents could result in an inability to defend claims, business difficulties and failure to comply with data protection legislation, whilst appropriate destruction and disposal will ensure that the storage space is maximised and we are not keeping documents for an unnecessarily long period of time which would breach the data protection legislation.

This policy applies to all the information held by Mitutoyo and also any personal data that may be held by data processors (service providers) where they are processing information on the Company's behalf.

All employees are responsible for ensuring that the records that they create/maintain are accurate, maintained and disposed of in accordance with this policy. It is recognised that the documentation created and maintained by the Company will change over time and therefore this policy should be viewed as a living document and it will be reviewed on an annual basis, or as necessary, if sooner.

This policy should be read in conjunction with the Data Protection Policy and the Data Protection Breach Reporting Policy.

Destruction/Disposal

Hard copies of confidential documents or personal data should be disposed of using the confidential waste bins and sacks. Under no circumstances should any personal or confidential data be disposed of in any other manner, as this would potentially breach data protection legislation.

Disposal of documents which do not contain personal data or confidential information can be disposed of in any bin, or by recycling or by electronic deletion in the case of electronic documents.

Records of disposal should be maintained, recording the document disposed of, date and the individual responsible for authorising the disposal.

Data Protection Breach Policy and Procedure

Mitutoyo is committed to handling personal data in line with best practice and as such this policy details the procedures to use when dealing with and responding to data protection breaches. This is to ensure that incidents are responded to promptly, risks are minimised, learnings identified and remedial actions are implemented.

These procedures apply to all staff, suppliers, contractors, agency workers, volunteers, clients, data processors or anyone else who may handle or have an interest in personal data on behalf of Mitutoyo.

Data Protection Breaches

A data protection breach occurs when personal data (which includes any information that allows an individual to be identified), is processed without authorisation, and which may result in its security being compromised. For the purposes of this policy, data protection breaches included both confirmed and suspected breaches.

This procedure is concerned with the management of such data protection breaches, which involves the detection and reporting of breaches as well as learning from the breach and implementing appropriate remedial actions.

Most commonly, data protection breaches occur as a result of human error, theft, unauthorised access, equipment failure, hacking or loss i.e. of a memory stick or confidential papers left on public transport etc. When a data protection breach has been discovered, whatever the reason for the breach, the following procedure will be implemented: -

Discovery

All individuals, or organisations (including Data Processors) working on behalf of Mitutoyo are responsible for data protection and should be alert to any actual, suspected, threatened or potential data protection breaches. As soon as a data protection breach has been discovered, where possible, a Data Protection Breach Reporting Form should be completed (to the fullest extent possible at that time), which provides full details concerning the breach. This form should then be passed to Data Protection Officer as soon as possible and within 24 hours of the discovery of the breach. If you need help completing the form, or are unable to complete the form, then any delay should be avoided and instead the matter should be reported immediately, either verbally or using electronic means, such as email.

Once a data protection breach has been reported, an initial assessment will be made by a senior manager within Mitutoyo concerning the content, quality of data involved and the potential impact and risk of the breach.

Reporting

Following a discovery of a breach and the receipt of such a report, consideration will be made regarding whether the matter needs to be reported to the Information Commissioner's Office (ICO) and whether individuals who are potentially affected need to be informed.

Current legislation states that any data protection breaches that are likely to result in a risk to the rights and freedoms of the individuals concerned (irrespective of their severity) must be reported to the ICO as soon as possible and no later than 72 hours after their discovery.

In addition to this, the individuals affected by the breach must be informed if the breach is likely to pose a high risk to them. The individuals must be informed of the nature of the data breach and the steps that Mitutoyo is taking to protect their data. The incident will also be logged in the Data Protection Breach Register.

Containment and Recovery

As soon as possible after the discovery of an actual or suspected data protection breach, consideration will be given to: -

- whether the breach has been contained as far as possible and whether any further steps can be taken to contain the data from further loss;
- whether any steps can be taken to mitigate the impact and risk of the loss;
- whether anything can be done to recover the data.

Investigation

Following the initial discovery/reporting of an incident, an investigation will be initiated to understand the full facts regarding the data protection breach. The extent of the investigation will be a matter for Mitutoyo to decide and may simply involve the collation of documents, or may be involve interviewing staff involved in the breach/collecting witness statements, CCTV etc.

Remedial Actions

Once the full facts have been ascertained, and the investigation has been concluded, consideration will be given to the learnings from the breach and most importantly, what remedial actions Mitutoyo needs to take to prevent a recurrence of the incident, this may include any appropriate disciplinary action for individuals implicated in the breach, or termination of relationships with third parties who are involved.

Actions will be documented on an action plan, which is reviewed on a regular basis thereafter to ensure that the actions have been carried out.

During and/or at the end of the completion of the investigation the Data Protection Breach Reporting Form and the Data Protection Breach Register will be updated to ensure that all the details of the events have been properly documented.

Any employees who act in breach of this policy or who do not implement it, may be subject to formal disciplinary proceedings, which may involve dismissal depending on the relevant circumstances. Any third parties or workers who act in breach of this policy or fail to implement it may have their relationships with the Company terminated with immediate effect.