It is the policy of HORIBA MIRA Ltd (hereafter 'MIRA') that it shall at all times adhere to data protection law and respect the privacy of individuals by processing personal data only for legitimate and lawful purposes and in strict adherence to current data protection legislation. Set out below is our Data Privacy Policy which makes clear how we meet our obligations to everyone whose personal data we process and to the Information Commissioner's Office (ICO).

HORIBA MIRA Ltd is for all data processing purposes a **Data Controller**. Our contact details are:

HORIBA MIRA Ltd
Watling Street
Nuneaton
Warwickshire
CV10 0TU
www.horiba-mira.com

+44 (0)24 7635 5000

The Data Protection Officer

The Data Protection Officer for HORIBA MIRA Ltd can be contacted at dataprotection@horiba-mira.com
+44 (0) 24 7635 5175

Supervising Authority

The Supervising Authority for data privacy matters in the UK is the Information Commissioner's Office (ICO):

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Tel: 0303 123 1113 (local rate) or 01625 545 745 (national rate)

Definitions

"Personal Data" means any information relating to an identified or identifiable natural person (the 'Data Subject'). An identifiable natural person is one who can be identified, directly or indirectly by reference to any other identifier.

"Data Controller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

"Data Protection Law" means in the United Kingdom Regulation (EU) 2016/679 (General Data Protection Regulation), any successor thereof and any legislation in force from time to time in any jurisdiction which supplements it, including the Data Protection Act 2018 or any successor thereof and any other applicable national privacy legislation or regulations, guidance or codes of practice issued in respect of such legislation by the Information Commissioner's Office (ICO).

"Data Subject" means a natural person to whom the Personal Data applies directly or indirectly.

"Shared Personal Data" means any Personal Data collected or received by one Party in respect of which another Party is a Controller; or where the Data Subject from whom the Personal Data is obtained has provided the Personal Data in the context of its relationship with the other Party.

"Processing" means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"Consent" of the Data Subject means any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of Personal Data relating to him or her.

"Data Processor" means a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Controller.

"International Organisation" is defined as an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries.

"Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.

Data Protection Principles

- *Data will be processed fairly, lawfully and in a transparent manner*
- *Data will be collected for specified, explicit and legitimate purposes*
- *Data will be adequate, relevant and limited to what is necessary*
- *Data will be accurate and kept up to date*
- *Data will be retained only for as long as necessary*
- *Data will processed in a manner to maintain security*

Lawful Basis for Processing

MIRA will obtain, hold, use and disclose personal information either with specific Data Subject consent, for our legitimate business purposes, for the fulfilment of legal obligations or as part of contractual or pre-contractual arrangements. Processing of personal data be for the purposes of:

- Staff administration including occupational health, welfare and performance management
- Management of public relations, advertising and media
- Management of finance and accounts
- Training and personal development
- Property, asset and insurance management
- Vehicle and transport management
- Payroll and benefits management
- Management of complaints
- Vetting and security including CCTV images
- Management of information and communication technology systems
- Legal services
- Licensing and registration where applicable
- Pensions administration
- Research
- Sports and recreation
- Procurement and contract management
- Health and safety management
- Performance of a business contract
- Obligations under the law to statutory authorities
- Business development and planning
- Customer relationship management

The lawful basis for processing personal data is in all cases strictly in accordance with one or more of the following:

- The explicit consent of the individual; or
- The performance of a contract (or for the purposes of entering in to a contract at the request of the individual); or
- A legal obligation upon us e.g. tax affairs; or
- In the vital interests of an individual; or
- In the public interest; or
- For our legitimate business interests specifically to the extent that the Data Protection Principles allow and where these are not overridden by the privacy rights of the Data Subject

All personal information processed by us is done so fairly, lawfully and with appropriate justification. We ensure that any personal information used by us or on our behalf is of the highest quality in terms of accuracy, relevance, adequacy and limitation. It will be kept up-to-date, be protected appropriately and securely destroyed when no longer required.

We will comply with all Data Subject Rights under existing data protection law.

Where personal data is held purely by virtue of the consent of the individual, that consent will be explicitly given, recorded and may be withdrawn at any time without penalty.

'Legitimate Interest'

Legitimate interest is one of the lawful bases that allows the processing of personal data. It may also apply to the legitimate interest of a third party receiving the data. It is the most flexible of the six lawful bases. It is not focused on a particular purpose and therefore gives us more scope to potentially rely on it in different circumstances. The legitimate interest basis is likely to be most useful where there is either a minimal impact on the individual and/or a compelling justification for the processing. It does not require the consent of the data subject.

When considering whether we have a legitimate interest to process personal data consider 3 factors, known as the 3 part test:

- The PURPOSE for which we are processing the data
- The NECESSITY for processing the data and whether alternatives are available
- The BALANCE between our interests and the privacy rights of the individual. Our interests cannot override individual rights

Legitimate interest is most likely to apply when processing employee or client data, direct marketing (as long as is carried out in compliance with Privacy and Electronic Communications Regulations), Intra-group administrative transfers, or for the purposes of fraud prevention, network and information security and indicating possible criminal acts or threats to public security.

A legitimate interest most likely exists where there is a 'relevant and appropriate relationship' between us and the individual e.g. if the individual is our client, business partner or employee. It is more likely to apply because we are more likely to have a clear legitimate purpose for using this data and the nature of our relationship means the processing is less likely to be unexpected or unwanted.

Data Subject Protection Rights

As the person to whom personal data relates, you have certain rights regarding how your data is held, used, processed or shared by us. These are explained below:

- **The right to be informed** – You have the right to insist on transparency over how we use your personal data and to be provided with 'fair processing' information.

- **The right of access** – You have the right to access your personal data and any other supplementary information within one month. You can request this free of charge.

- **The right to rectification** – You are entitled to have data rectified if it is inaccurate or incomplete.

- **The right to erasure** – You may request the deletion or removal of personal data if you believe that there is no longer any lawful basis for which MIRA can process it.

- **The right to restrict processing** – You have the right to request restriction of the processing of your data if you contest its accuracy or object to its processing for any reason. In such cases MIRA is entitled to store your data but not further process it until an investigation is complete and your complaint is verified.

- **The right to data portability** – You have the right to request your personal data be given to you in a machine readable format to be used for your own purposes and to transfer it easily from one IT environment to another. This only applies to information that you have given us and where the processing is carried out by automated means. We may not be able to provide you with this information if it prejudices the rights of another person.

- **The right to object** – You have the right to object to the processing of your data where the processing is based on the legitimate interests of MIRA with regard to direct marketing or where it is being used for statistical purposes.

- **The right to object to automated decision making and profiling** – There is a right not to be subject to a decision based solely on automated processing, including profiling (i.e. decisions made without human intervention). This right does not apply however if the processing is necessary for entering into, or performance of, a contract between you and MIRA (e.g. employment contract) or where the data is processed with your explicit consent.

Types of Personal Data Processed

In the legitimate course of our business we may obtain, hold, use and disclose personal information relating to or consisting of any of the following:

- Personal details such as name, address and biographical details
- Family and social circumstances
- Education and training details
- Employment details
- Professional qualifications and experiences
- Financial details
- Goods or services provided
- Racial or ethnic origin
- Trade union membership
- Physical or mental health
- Criminal offences, outcomes and sentences
- Sound and visual images
- Licenses or permits held

- Information relating to health and safety
- Complaints and correspondence
- Incident and accident details
- Performance management information
- Copies of correspondence to or from us
- Data derived from IT systems such as IP addresses or location information
- Information that may be required for the performance of a contract

We will only obtain, hold, use or disclose appropriate personal information necessary to fulfil a lawful purpose. Personal information may be held in computer format or in structured paper files. It can also include other types of electronically held information such as location data, CCTV images or audio recordings.

Source and Origins of Personal Data

We may obtain personal information from a wide variety of sources, including the following:

- HM Revenue and Customs
- Law enforcement agencies and regulatory or licensing authorities
- Legal representatives
- Business partners who share a legitimate business contract with us
- Prospective business partners
- External auditors
- Central or local government, government agencies and departments
- Emergency services
- Individuals themselves
- Relatives, guardians or other persons associated with the individual
- Current, past or prospective employers of the individual
- Healthcare, social and welfare practitioners
- Education, training establishments and examining bodies
- Business associates and professional advisors
- Employees and agents of MIRA
- Suppliers and providers of goods or services
- Persons making an enquiry or complaint
- Financial organisations and advisors
- Credit reference agencies
- Survey and research organisations
- Trade, employer associations and professional bodies
- Data Processors working on behalf of MIRA
- Our parent organisation and its subsidiaries
- CCTV systems
- Recruitment agencies

Personal Data Processed

We may obtain, use and disclose personal information relating to a wide variety of individuals including the following:

- Staff including volunteers, contractors, agency staff including temporary and casual workers
- Suppliers and service providers
- Business partners
- Complainants, correspondents and enquirers
- Relatives and associates of the individual concerned
- Advisers, consultants and other professional experts
- Former and potential members of staff
- Pensioners and beneficiaries

- Customers and prospective customers
- Tenants
- Visitors
- Social contacts i.e. those who attend MIRA social events

Retention of Personal Data

We keep personal data for as long as, but no longer than is necessary for the lawful purposes for which it was collected or for any period that might be required by law. Where there is no further requirement to use, hold or store personal data and the law does not require us to do so, we shall remove it from our records and systems or it may be archived and no longer processed. Our retention of personal data is strictly on the basis of the clear and justifiable existence of a lawful basis for processing and MIRA has a separate Data Retention Policy as required by law.

The overriding rule is that the 'storage limitation' Data Protection Principle will apply in all cases: "*Data shall be 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"*

Where Personal Data is Held

Personal data relating to any individual may be held, used and processed on a number of systems and in a variety of formats. Personal data will be held in machine readable format on computers, servers (whether ours or hosted by a business partner), on mobile devices or in structured paper files. These will include:

- HR systems
- Finance systems
- Customer databases
- Recruitment systems
- Managers' individual filing systems – electronic and hard copy
- Project management systems
- Emails and correspondence
- Bespoke Management Information Systems

Who We Share Information With

We may disclose personal information to a wide variety of recipients in any part of the world, including those from who personal information is obtained. Disclosure of personal information will be made strictly on the grounds of the following and with suitable controls in place:

- The explicit consent of the individual; or
- The performance of a contract or prior to a contract; or
- A legal obligation upon us; or
- In the vital interests of an individual; or
- The public interest; or
- For our legitimate business interests

Where processing is to be carried out on behalf of MIRA by a Data Processor, MIRA shall use only processors by means of contractual clauses sufficient to guarantee appropriate technical and organisational measures that meet the requirements of the law and ensure the protection of the rights of the data subject. The processor shall not engage another processor without the prior specific written authorisation of MIRA. We may also share data with 3rd Party Data Controllers who are Controllers in their own right and therefore separately have also to be compliant to data protection law. In such cases safeguards are provided through a Data Processing Addendum to any Principal Agreement with them. We do not act as Joint Controllers with any other organisation. We are not a Data Processor for any other organisation. We may share personal information with any of the following:

- Law enforcement agencies and regulatory or licensing authorities
- Legal representatives
- Business (and prospective) partners who share a legitimate business contract with us
- External auditors
- Central or local government, government agencies and departments
- Emergency services
- Current, past or prospective employers of the individual
- Healthcare, social and welfare practitioners
- Education, training establishments and examining bodies
- Business associates and professional advisors
- Managers within the HORIBA Group of companies
- Suppliers and providers of goods or services
- Financial organisations and advisors
- Credit reference agencies
- Survey and research organisations
- Trade, employer associations and professional bodies
- Recruitment agencies

Overseas Transfers of Personal Data

MIRA as part of its business operation will under certain conditions share personal data within the HORIBA Group overseas and also to other overseas organisations. Some organisations that MIRA disclose personal information to are outside of the European Economic Area. We ensure that all personal data shared with any overseas organisation is adequately protected.

All transfers of data overseas are governed strictly as follows:

- Within the HORIBA Group – As allowed by a Framework Agreement approved by the European Commission.

- Outside of the HORIBA Group and outside of the EEA - By EC Model Data Protection Clause agreements approved by the European Commission.

- Outside of the HORIBA Group and within the EEA (and to countries approved by the EC as having adequate data protection standards) – Using Standard Contract Clauses.

- With the US – Using companies approved with EU/US Privacy Shield arrangements.

There are circumstances where the adequacy mechanisms above do not need to apply. These are where the transfer of data is:

- Made with the individual's informed consent;
- Necessary for the performance of a contract between the individual and the organisation or for pre-contractual steps taken at the individual's request;
- Necessary for the performance of a contract made in the interests of the individual between the controller and another person;
- Necessary for important reasons of public interest;
- Necessary for the establishment, exercise or defence of legal claims;
- Necessary to protect the vital interests of the data subject or other persons where the data subject is physically or legally incapable of giving consent

Automated Decision Making and Profiling

Automated decision making and profiling occurs where a computer system generates an output relating to an individual without any human intervention, upon which a decision is made. MIRA may in limited circumstances use such systems and these are likely to be:

- Systems used by credit reference agencies
- Psychometric or capability evaluations systems used in the recruitment process

There is a right not to be subject to a decision based solely on automated processing, including profiling (i.e. decisions made without human intervention). This right does not apply however if the processing is necessary for entering into, or performance of, a contract between the Data Subject and MIRA (e.g. employment contract) or where the data is processed with explicit consent.

Data Security

MIRA takes information security very seriously. Our IT systems are accredited by HM Government using the Cyber Essentials Plus scheme. All staff receive training in data protection, IT security and acceptable computer use. MIRA has robust policies with regard to IT Security, Information Security Management Systems, confidentiality of information, acceptable Internet use, handling of personal data, software and data control, Data Privacy Impact Assessments, and data breach incident management.

Special Category Data

Previously 'Sensitive Personal Data' has now been designated as Special Category Data. Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data or biometric data for the purpose of uniquely identifying a person, data concerning health or a person's sex life or sexual orientation can only be processed under specific conditions. MIRA will in the course of business hold and process data relating to:

- Employee health records
- Employee race and ethnicity
- Employee Trade Union membership (where union subscriptions are deducted from payroll)
- Criminal record checks are carried out where the individual will come in to contact with HM Government classified information as part of their job role.

All Special Category Data is held strictly on the basis of the consent of the data subject and is afforded the highest degree of protection.

Data Privacy Impact Assessments

In order to comply with Data Protection law there is a requirement on MIRA to carry out Data Privacy Impact Assessments (DPIA) where data processing activities pose potentially a high risk of compromise to the rights or freedoms of individuals. DPIAs will be carried out either by the project manager directly responsible for the processing activity and/or by the MIRA Data Protection Officer. An effective DPIA will be initiated and maintained throughout the development and implementation of a project or system. DPIAs will be applied at a time when it is still possible to have an impact on the project. The DPIA process is integrated with existing project management processes.

Complaints or Queries

You have the right to make a complaint about the manner in which your personal data is stored, used, processed or shared by us; or if you feel that any of your Data Protection Rights have been violated.

You can direct all personal data queries or complaints to us by contacting our Data Protection Officer at dataprotection@horiba-mira.com

Or you can complain directly to the Information Commissioner's Office (ICO) at https://ico.org.uk/concerns

You can also call the ICO Helpline on 0303 123 1113. The ICO is the UK's independent body set up to uphold information rights.

Amendment No.	Amended By	Section(s) Affected	Date
02	Chris Hoad	Updated revision of document whole	11.7.2018