General Data Protection Regulations (GDPR)

MRI New Zealand Holdings Limited's ("MRI") approach has always been with a strong commitment to privacy, security, compliance and transparency. This approach includes our customers' compliance with EU data protection requirements, including those set out in the General Data Protection Regulation ("GDPR"), which was enforceable from May 25, 2018.

Please note as part of our GDPR program we apply GDPR security and privacy principles to all data not just EU personal data. That way, You will be well positioned with data protection regulatory frameworks around the world.

Definitions

There are several definitions You must be aware of in relation to MRI's compliance with GDPR. The most important is the difference between a 'Data Controller' and a 'Data Processor'. Below we provide You with clarity on both, along with other definitions, as this is extremely important to avoid some ambiguity about responsibilities.

Data Controller

The Data Controller is an individual or legal entity that determines (controls) the purposes and the means of the processing of personal data about a Data Subject (a

visitor, employee, or contractor). This determination can be done alone or jointly with others.

If You are a user of our visitor, contractor, employee, or evacuation management services, You, our customer, will be the ‘Data Controller’ and MRI will be acting on our customer’s behalf and will therefore be acting as our customer’s “Data Processor”.

MRI is also a Data Controller as it collects and processes its customers data for sales, service delivery, invoicing, customer relationship management and direct marketing.

Data Processor

A Data Processor is responsible for processing personal data on behalf of a Data Controller. In the context of our Customers use of our MRI OnLocation services Data Processor means Us, MRI.

As the Data Processor our details are:

MRI New Zealand Holdings Limited
Level 2, 181 Vivian Street
Te Aro
Wellington 6011
New Zealand

Legal Registration Identifiers:

- Company Number: 8161227

  NZBN Number: 9429049034622

Contact Details

- Australia: 1300 106 541
- Canada: (800)-501-1761
- New Zealand +64 (04) 891 0886

- United Kingdom: 0808 189 1412
- United States: (800)-501-1761
- Global: +64 4 891 0886
- Email: support@whosonlocation.com

Data Subject

A Data Subject means the ‘visitor’, or contractor, or employee who has data about them collected and controlled by the Data Controller; (Name, organisation, email, mobile, etc.). The Data Controller may capture data from a Data Subject directly, or the Data Subject may submit data to the Data Controller; but in both cases the Data is captured using our application service.

Personal Data

The GDPR applies to ‘personal data’ meaning any information relating to an identifiable person (Data Subject) who can be directly or indirectly identified in particular by reference to that personal data.

We define the scope of Personal Data, both non-sensitive and sensitive, in relation to its capture and use by the Data Controller below.

In-scope Personal Data (non-sensitive)

The following personal data information from Data Subjects (visitor, employees and contractors) are processed by MRI on behalf of the Data Controller:

- Full Name
- Email address
- Cell Phone (Mobile)
- Phone
- Title/Position
- Department
- Organisation
- Host (who are they visiting)
- Purpose of visit
- Car parking information (vehicle registration, car park space)
- Records of qualifications and certificates
- ID Verification (ID card type, reference etc.)

- Date and time a visitor, employee, or contractor entered and departed at the site
- Location data

In-Scope Personal Data (sensitive)

- Photo Capture (could identify the ethnicity or religious association of the Data Subject)
- Need Assistance (identifies whether a Data Subject has a disability)

Note: Custom questionnaires can be enabled by the data controller (Customer) to capture any additional information required. Additional personal information may be collected depending on what the data controller requires in these customer questionnaires.

The rights of the Data Subject when You, our Customer, are the Data Controller

MRI has documented and will follow its procedure for responding to GDPR requests to support its Data Controller in the event an individual exercises their Data Subject rights:

Data Subject Right	**Description**	**How MRI Supports this right**
The right of access	Data Subjects have the right to obtain confirmation that their personal data is being processed, access to their personal data and information on the processing.	Data Controllers have access to captured data about any Data Subject via the application's reporting tools. Data can be exported and shared with the Data Subject on request.
The right to erasure;	Personal data shall be erased without undue delay if: • the personal data is no longer necessary to achieve the purposes for which it was collected or otherwise processed; • the Data Subject withdraws consent; • the individual objects to the processing and there is no overriding legitimate interest	Data controllers (or MRI on the data controllers behalf) will be able to delete specific records from their live instance either in bulk or record by record. There is a setting to enable "auto removal of records after x number of days" to automatically remove all visitor information after a certain length of time has passed. Once a record is removed from their live instance, it will no longer be available to be reported on or be visible to anyone with access to their MRI account.

	for continuing the processing; • it was unlawfully processed (i.e. otherwise in breach of the GDPR); • it has to be erased in order to comply with a legal obligation; or • it is processed in relation to the offer of information society services to a child	
The right to object;	Data Subjects have the right to object to the processing of personal data on grounds of the Data Subject's situation.	• MRI, as the Data Processor, only perform very high-level metrics on visitor information such as total numbers processed over what time period. Personal data is not processed and used for profiling, direct marketing or research and statistic purposes. • However, if a data subject wishes to exercise its right to object, MRI or its data controllers can perform the "Right to Erasure" process above to permanently delete the personal data so it won't be further processed. • Data Controllers can also show a waiver (optionally with signature required) to visitors who You require consent from.
The right to rectification;	The Data Subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her.	Data Controllers (customers) can rectify personal data stored within the application.
The right to restrict processing;		Allowing site administrators to enable an option for visitors to "Do not remember me" during the sign in process. This will prevent the returning visitor feature for this visitor's subsequent visits.
The right to data portability;	The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have	Data Controllers have access to captured data about any Data Subject via the application's reporting tools. Data can be exported and shared with the Data Subject on request.

	the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided.	
The right not to be subject to automated decision-making including profiling.	The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.	MRI as a data processor does not perform automated decision-making including profiling but data controllers can set up rules that consists of conditions that when met can trigger an action based on the rule being met. There is a reliance on the data controller to ensure any automated individual decision making they perform are in accordance to the GDPR's requirements.

Lawfulness processing and Consent

GDPR specifies the need to have consent obtained before using personal information for specific purposes.

MRI does not collect personal information directly from the Data Subjects. It only processes information on behalf of the data controller. The requirement of gaining consent is the responsibility of the data controller. The data controller must ask for the Data Subject's consent prior to collecting any personal information.

MRI's customers (data controllers) decide under what circumstances require a waiver (or Privacy Statement) to be acknowledged prior to signing into a location. Once signed in, if a Data Subject (visitor, contractor, or employee) has signed a waiver, the waiver can be shared with that Data Subject if the Data Controller applies 'sharing' settings. The Data Controller can also access a report on specific Data Subject and provide this information to the Data Subject on request.

Processing of special categories of personal data

MRI (as the Data Processor) does not process personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, genetic data, health data, sexual orientation data, or trade union membership, for the purpose of uniquely identifying a natural person. However we may process biometric data if the Data

Controller captures it as part of their use of the application but only where the Data Subject has given explicit approval prior to such data being captured and processed or any other circumstance permitting such processing under Article 9 of the GDPR.

Personal Data Breach Notification

The GDPR requires the data processor to notify the personal data breach to the data controller without undue delay and to the supervisory authority not later than 72 hours after having become aware of the personal data breach unless it is unlikely to result in a risk to the rights and freedoms of natural persons.

MRI's Information Security and Privacy Incident Management process has been updated to ensure that in an event of a data breach, the data controller and supervisory authority are notified within the required period.

The notification will contain relevant information including the nature of the personal data breach and likely consequences of the personal data breach, etc.

Transfer of Personal Data to a third country

International transfers and processing of personal information must fulfil requirements laid down in the GDPR. Data transfers to countries whose privacy arrangements (laws, regulations, official compliance mechanisms) are compliant with GDPR do not require official authorisation or specific additional safeguards.

MRI's server regions are in United States, United Kingdom, Australia, Canada, Germany and New Zealand.

The European Commission has recognised Canada (commercial organisations), New Zealand, the US (limited to the Privacy Shield framework) as providing adequate protection.

The UK government has committed itself to 'maintaining the stability of data transfer between the EU Member States and the UK' after Brexit, in its White paper.

Data Protection by design and by default

The GDPR specifies the requirement to implement appropriate technical and organisational measures to ensure compliance with GDPR and protect the rights of the Data Subjects.

- MRI adheres to security guidelines and standards defined under OWASP and Sarbanes-Oxley Act (SOX).
- 3rd Party Penetration tests and vulnerability scans are routinely run by both MRI customers and an independent third party on behalf of MRI.
- For physical data hosting, MRI chooses data hosts who have ISO 27001 certification.

The GDPR specifies the requirement to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, considering the nature, scope, context, purposes of processing and the risk to the rights of freedoms of natural persons.

MRI takes technical and organisational security measures such as, but not limited to:

- Secure Application Development in accordance with OWASP guidelines
- 3rd Party Penetration tests and vulnerability scans
- Controls Audit
- Physical Security
- Security awareness training for all MRI staff.
- Access Controls
- Password Management System
- Information Security Policies
- Encryption of Data in Transit
- Information Security and Privacy Incident Management
- Staff Vetting
- Human Resource Security
- Event Logging, Alerting, and Auditing
- Media Engagement Strategy
- Contractual Agreements and SLAs
- Hardening of Systems, Network Devices and Applications
- Backup and Restore
- Media Sanitisation and Disposal

MRI has been ISO 27001 information security management system (ISMS) certified since December 2019.

Data Protection Officer (DPO)

The GDPR requires that you appoint a representative in the EU.

MRI has appointed a DPO who will be responsible for setting up policies, reviewing Data Protection Impact Assessment reports, monitoring compliance with the GDPR, and all tasks listed in Article 39.

Contact:

The Data Protection Officer
MRI Software, LLC
Email: dataprivacypractitioner@mrisoftware.com

Data Protection Representative (EU)

The GDPR specifies under Article 27 that an organisation with no establishment in the European Union (EU), but which processes the personal data of data subjects inside the EU, must appoint a Data Protection Representative in the EU to allow data subjects and local data protection authorities to have a relevant contact.

MRI, which processes the personal data of individuals in the European Union, in either the role of ‘data controller’ or ‘data processor’, has therefore appointed MRI Software Ireland Limited as its EU Data Protection Representative for the purposes of GDPR.

The contact details are:

MRI Software Ireland Limited
The Diamond
Donegal Town
Co. Donegal

Donegal
Ireland

If you want to raise a data protection query, or otherwise exercise your rights in respect of your personal data, to our Data Protection Representative, you may do so by:

- sending an email to dataprivacypractitioner@mrisoftware.com quoting “MRI OnLocation” in the subject line; or
- by mailing your inquiry to the above address for the attention of “MRI Data Privacy Practitioner”.

On receiving your correspondence, MRI is likely to request evidence of your identity to ensure that we are permitted to discuss and disclose information to you.

When mailing inquiries, it is essential that your mark your letters for ‘MRI Software Ireland Limited’ or your inquiry may not reach us. Please refer clearly to MRI OnLocation in your correspondence.

On receiving your correspondence, MRI is likely to request evidence of your identity, to ensure your personal data and information connected with it is not provided to anyone other than you.

If you have any concerns over how MRI Software Ireland Limited will handle the personal data that we will require to undertake our services, please contact dataprivacypractitioner@mrisoftware.com

Third Party Subprocessors and Subcontractors

MRI New Zealand Holdings Limited (“MRI”) uses certain subprocessors, subcontractors and content delivery networks to assist it in providing the MRI OnLocation Services as described in the Master Subscription Agreement (“MSA”).

WhosOnLocation maintains an up-to-date list of the names and locations of all sub-processors used for hosting or other processing of Service Data, which is available

to our Customers. The list also may be obtained by contacting dataprivacypractitioner@mrisoftware.com.

How MRI OnLocation helps You meet your GDPR Compliance

MRI OnLocation offers several settings to help your organisation meet its GDPR (General Data Protection Regulation) compliance. We have given you the tools to meet these standards through a combination of existing and new features.

Learn more in our Helpdesk.

Our Commitment to Security and Privacy

Fulfilling our privacy and data security commitments is important to us. We are committed to:

- Continuing to invest in our security management program
- Making sure we have the appropriate contractual terms in place
- Product offerings that include new tools for data portability and data management

We'll update customers on any changes to our Privacy Policy.

For more information or any questions please email dataprivacypractitioner@mrisoftware.com