Policy Overview

Many countries have enacted data protection laws, which regulate the way Personal Data (as defined below) is handled and processed. This Data Protection Policy ('**Policy'**) sets out information on the processing of Personal Data, which originates in the European Union ('**EU**'), by Makor Group (together, "**Makor**", "**we**" or "**us**").

Makor is committed to complying with applicable laws and regulations wherever we conduct business. Makor conducts business on a global basis and is therefore required to comply with various laws and regulations relating to data protection including the EU General Data Protection Regulation (2016/679) ("**GDPR**"). Data protection laws vary widely from country to country.
In the European Economic Area ("**EEA**"), a breach of the GDPR can lead to fines of up to 4% of total annual worldwide turnover, or €20 million, whichever is higher. If Personal Data is not properly processed and protected, it may also present a risk to the data protection rights of individuals. This might also cause adverse publicity for Makor's use of Personal Data and result in damage to our reputation, including a loss of trust from our customers. This Policy sets out the minimum requirements that Personnel are to apply to the collection and processing of Personal Data.

Scope

This Policy applies to all Makor's Personnel (as defined below). In the course of its regular business activities, Makor collects data (whether on paper, on a computer, or on any other medium) about individuals it interacts with, including: individual consumers, corporate customer representatives, Personnel and suppliers or vendors. When this data can be used to directly or indirectly identify a living individual, it is called Personal Data.

Processed or processing (defined below) is broadly defined under EU data protection laws. It basically means any activity that involves use of the data. This Policy governs the processing of any Personal Data by Makor.

For operations outside of the EEA, this Policy governs the processing of Personal Data that is transferred from a Makor company located within the EEA to any other Makor company located outside of the EEA.

Local, national or regional laws and regulations in countries with data protection laws may require that further protections beyond those identified within this Policy; if so, all Makor's Personnel are expected to follow such stricter standards or requirements in addition to the principles set out in this Policy.

Separate Makor policies also apply and supplement this Policy, and further mandate the controls applicable to Personal Data, details of which can be found at Section H (Related Policies) of this Policy.

Key obligation

All Personnel having access to, and working with, Personal Data have an obligation to maintain the confidentiality of the Personal Data they process. Personnel must only process Personal Data as necessary to fulfil their legitimate job functions and must observe at all times this Policy and any related policies and procedures.

Responsibility

Compliance Officer has primary responsibility for ensuring Personnel's compliance with this Policy. They may develop supplemental policies and procedures to offer more detailed guidance and ensure the effective implementation of this Policy.

Policy at a glance

A. Handling Personal Data - General Rules. Sets out the key data protection principles.

B. Transferring data. Sets out the principles around transferring Personal Data, both within the Makor group and externally.

C. International Transfers of Personal Data to countries outside of the EEA. Specifically addresses the transfer of Personal Data outside of the EEA.

D. Rights of Individuals. Sets out the key rights of individuals in respect of the information Makor holds about them.

E. Data Protection Impact Assessment ('DPIA'). Explains the requirement to complete a DPIA when embarking upon a new project which involves the processing of Personal Data which is likely to result in a high risk to the rights and freedoms of individuals.

F. Data Protection by Design and by Default. Explains the obligation to consider technical and organisational measures to be implemented to protect Personal Data, from the beginning to the end of a project.

G. Violations. Sets out the process and actions we might take in response to any violations of this Policy.

H. Related Policies. Includes any additional and related policies.

I. **Monitoring and ongoing compliance**. Sets out how ongoing compliance will be effected through internal and external audits.

Policy definitions

"**Personal Data**" means any information relating to an identified or identifiable person. An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to that person's physical, physiological, genetic, mental, economic, cultural, or social identity of that person.

"**Personnel**" means current, past and prospective employees, officers, directors and other personnel, such as temporary workers or contractors of Makor.

"**Process**", "**processing**" or "**processed**" means any operation or set of operations performed upon Personal Data, whether or not by automatic 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.

"**Special Categories of Personal Data**" (or "**Sensitive Data**") is a subset of Personal Data which may contain information relating to a person's race or ethnic origin, political opinions, religious or philosophical beliefs, genetic data, biometric data for the purpose of uniquely identifying an individual, data concerning health or data concerning an individual's sex life or orientation. Data protection legislation in certain countries requires additional safeguards for the processing of Sensitive Data.

A. Handling Personal Data — General Rules

Data Protection Principles

As part of your job function with Makor, you may have access to or, where appropriate, be required to process Personal Data. Personnel are required to process Personal Data in a fair and lawful manner and in accordance with the principles of good data protection practice set out below.

1. Limitation on Purpose

You must only process Personal Data for the specified, explicit and legitimate purpose for which such Personal Data were collected, i.e. the purposes that were communicated to the individual. This means that Personal Data must not be collected for one purpose and then used for another. If it becomes necessary to change the purpose for which the Personal Data are processed, you must contact the Compliance Officer because, depending on the location of the individual, legislation may require Makor to provide individuals with additional information on these changes as to how their Personal Data is processed and, where applicable, obtain their consent to the additional processing purposes.

2. Adequate, Relevant and Non-excessive Processing

You must only process Personal Data that is strictly necessary for its defined business purposes. This means a 'must have' and not 'nice to have' approach must be taken before any Personal Data are collected. Personal Data that are not necessary for that intended business purpose should not be collected or processed. Personal Data should only be handled by designated and/or authorised employees on a 'need-to-know' basis.

3. Accuracy of Information

You must take steps to check that any Personal Data you have collected, or are processing on behalf of Makor, is accurate, complete, reliable and kept up-to-date as necessary for the purposes for which the Personal Data are held and used. Such steps must be taken at the time the Personal Data are first collected and at regular intervals thereafter.

4. Retention of Personal Data

You must ensure that Makor does not keep any Personal Data in a form that permits identification (data which has not been anonymised) for longer than is necessary for the purpose(s) for which it was collected. Any Personal Data that no longer serves a legitimate, identified business purpose should be deleted or destroyed in accordance with Makor's applicable records management and retention policy. If you have any questions around the retention of Personal Data, you must consult with the Compliance Offer.

5. Security of Personal Data

Makor is required to take appropriate technical, physical and organisational measures to keep Personal Data secure to prevent unlawful or unauthorised processing or accidental loss of, destruction or damage to, Personal Data. The measures and security controls which Makor has taken to protect Personal Data are detailed in our information security policy. If you become aware of an incident which involves Personal Data, you must refer to our Personal Data Breach procedure for handling such breaches.

Special Categories of Personal Data (or Sensitive Data)

Special Categories of Personal Data requires heightened protection under certain laws. Special Categories of Personal Data may only be collected and processed in limited circumstances, for example where an individual has provided their explicit consent. Where consent is required, the information provided must detail the reasons and circumstances required for the collection and processing of such Sensitive Data.

If you seek to collect or process any Special Categories of Personal Data, you must not do so without first contacting the Compliance Officer and seeking guidance. If you are unsure as to whether something qualifies as Special Categories of Personal Data, you must consult with the Compliance Officer before collecting or processing such information.

B. Transferring data

Transfers to other Makor group entities

Makor aims to ensure a consistent and adequate level of protection for all Personal Data that are processed and/or transferred between Makor group entities. A transfer of Personal Data to another Makor entity is considered a transfer between two different entities, which means that even in such "intra-group" cases, a data transfer shall be carried out only if:

- the transfer is based on a clear business need;
- the receiving entity provides appropriate security for the data; and
- the receiving entity ensures compliance with this Policy for the transfer and any subsequent processing.

To the extent Personal Data is transferred to a Makor entity located in a country outside of the EEA, please refer to Section C below.

Transfers to third parties

Personal Data may be transferred to select third parties outside of the Makor group to perform services on Makor's behalf.

Makor may also be required to disclose certain Personal Data to other third parties:

- as a matter of law (e.g., to tax, social security and financial regulatory authorities);
- to protect its legal rights (e.g., to defend a legal claim); or
- in an emergency where the health or security of an employee is endangered.

Please note that any data transfers to third parties must only be carried out if adequate legal safeguards are in place. Personnel who plan to transfer Personal Data to a third party which has not previously been confirmed as a legal recipient of Personal Data must first consult with the Compliance Officer to confirm that the transfer is permitted under all applicable laws.

To the extent Personal Data is transferred to a third party in a country outside of the EEA, please refer also to Section C below.

C. International Transfers of Personal Data to third countries outside of the EEA

All Makor group entities and third-party service providers that process Personal Data on Makor's behalf will be required to comply with this Policy or to guarantee equivalent levels of protection when processing Personal Data.

On occasion, Personal Data may be transferred to and stored in a country whose laws do not provide equivalent protection to that which applies within the EEA. In such circumstances, Makor will implement contractual or other measures to ensure an adequate level of protection for such Personal Data. If you are transferring data to a third party based in a country outside of the EEA, or which has operations outside the EEA, please speak with the Compliance Officer for further information.

D. Rights of Individuals

Individuals located in the EEA for whom Makor holds Personal Data (including individual consumers, corporate customer representatives, Personnel and supplier or vendor representatives) and/or individuals whose Personal Data are processed by a Makor company located in the EEA (such as, in Paris or London) may be able to exercise certain 'individual rights' in relation to their Personal Data. Similar rights may apply to other individuals (who are based in non-EEA countries and whose information is not subject to the GDPR), and Makor will respond to any such individual rights request pursuant to local law requirements.

Requests can be communicated to Makor in any way, including via email, fax, letter, telephone, website request, customer services or via a third-party. Any Personnel who receives a request in relation to Personal Data should forward it immediately to the Compliance Officer and should not make any representations to the individual in relation to how the request will be dealt with.

Individuals located within the EEA may be able to exercise the following rights:

Right of Access: individuals may have the right to request access to Personal Data that Makor holds about them.

Right to Rectification: individuals have the right to request that any incorrect or inaccurate Personal Data relating to them is corrected and/or amended. If required to do so, Makor must comply with such requests. Makor will use reasonable endeavours to maintain the accuracy of Personal Data and keep it up-to-date. Personnel should, however, notify local Human Resources department promptly of any changes to their Personal Data

Right to Erasure: individuals are entitled to request for their Personal Data to be deleted and Makor must comply under certain circumstances.

Right to Restriction of Processing: if an individual requests for the processing of their Personal Data to be restricted, Makor is to cease processing of it where: (i) the accuracy of it is contested by the individual; (ii) the processing is unlawful but erasure has not been requested; (iii) the processing is no longer necessary; or (iv) the individual has objected to the processing and Makor determines that three are no overriding legitimate grounds to continue processing.

Right to Data Portability: individuals have the right to request to receive their Personal Data in a structured, commonly used and machine-readable format and, where requested and technically feasible, transmit them to another organisation.

Right to Object: individuals have the right to object to processing of their Personal Data based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling); direct marketing (including profiling); and processing for purposes of scientific or historical research and statistics.

Rights against Automated Decision-making, including Profiling: individuals have the right not to be subject to a decision when it is based on automated processing and it produces a legal effect or a similarly significant effect on the individual. Makor must ensure that individuals are able to: obtain human intervention; express their point of view; and obtain an explanation of the decision and challenge it.

E. Data Protection Impact Assessment

It may be necessary to carry out a Data Protection Impact Assessment ("**DPIA**") when planning a new project, process or product that makes use of new technologies, or is otherwise likely to result in a high risk to the rights of individuals with respect to their Personal Data. A DPIA is a systematic process for reviewing processing operations, which will help to identify the safeguards and security measures that should be put in place to mitigate risks.

The Compliance Officer must be informed of any new DPIA that is carried out, and will be available to provide advice in relation to its process. The Compliance Officer will be responsible for monitoring compliance with the DPIA and, where necessary, carrying out reviews of the DPIA at specific intervals.

F. Data Protection by Design and by Default

Makor is under an obligation to consider the technical and organisational measures that should be implemented to protect Personal Data from the time that a project or process is planned through to its conclusion. This assessment must take into account available technology, the cost of its implementation, the scope of processing, and weigh this against the risk presented to individuals. For further information, please contact the Compliance Officer.

G. Violations

If you encounter a possible violation of this Policy, you should report it to the Compliance Officer. Violations of this Policy will not be condoned or tolerated. The type of discipline for violations of this Policy will depend upon the nature, severity and/or frequency of the violation, and may result in one or more of the following sanctions: verbal warning, retraining, written warning, reprimand, demotion, restitution, probation, suspension and discharge.

The processes described in this Policy supplements any other remedies and dispute resolution processes which may be provided by Makor and/or which may be available under applicable local laws.

H. Related Policies

The following policies provide additional guidance on the handling of Personal Data:

- Information Security Policy
- Personal Data Breach Procedure
- Records Retention Policy

Please contact your local Human Resources Team to obtain copies of any local policies covering records management and handling of Personal Data.

I. Monitoring and ongoing compliance

This Policy will be governed by and its effectiveness will be measured using the following methods:

- Internal audit
- External audit
- Management review

The results from these processes will enable the Makor to review the effectiveness of the controls and continuous development of the Policy.

Management review and approval of this Policy and requirements will be performed as a minimum every 12 months or following any material change in business and legislative requirements.