Privacy Policy

29 December 2023

Mastek Legal Function

Division: Mastek Legal

1. GENERAL

MASTEK Group Companies* ("Mastek") are committed to international compliance with data protection laws and respects the rights and freedoms of individuals in relation to the control, protection and safeguarding of their personal information. This is so whether such information originates from its customers, its own organization, its agents, consultants, employees, sub-contractors, partners, suppliers, prospective customers, visitors to its website or otherwise.

This Privacy Policy is part of the wider Mastek Data Protection Framework and identifies the type of personal information collected by Mastek, how and why it is used, and the mechanisms Mastek employs to safeguard such information in accordance with the Data Protection Legislation.

The contact for all corporate Data Protection matters at Mastek is the Data Protection Officer ("DPO"), Dianna Anthony at Dianna.Anthony@mastek.com. In addition, you could also write to data.protection@mastek.com to receive a response from the DPO about your data protection queries.

*Mastek Group Companies ("Mastek"): Includes the following list of Mastek businesses: Mastek Enterprise Solutions Private Limited (formerly known as Trans American Information Systems Private Limited), Evolutionary Systems Corp & Newbury Cloud Inc., Mastek Digital Inc. Evolutionary Systems Canada Limited, Mastek Arabia FZ LLC, Evolutionary Systems Consultancy LLC, Evolutionary Systems Egypt LLC, Evolutionary Systems Saudi LLC, Evolutionary Systems Bahrain WLL, Evosys Kuwait WLL, Evolutionary Systems Qatar WLL, Evolutionary Systems Singapore Pte Ltd., Evosys Consultancy Services (Malaysia) Sdn Bhd., Mastek Systems Pty Ltd., Evolutionary Systems B.V. – Netherlands, Evolutionary Systems B.V. – Romania Branch

2. SCOPE AND APPLICATION

Compliance with this Policy is mandatory in connection with: (1) the processing by Mastek of the personal data information of the European Economic Area (EEA) and United Kingdom (UK) residents; and (2) the processing by Mastek of personal data information of individuals based anywhere in the world regardless of whether or not Mastek is based in the EU.

This Privacy Policy aims to summarise the principles contained in the following laws:

1. The General Data Protection Regulation (EU) 2016/679;
2. The UK Data Protection Act 2018 (DPA '18); and
3. The UK Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR).

It is applicable to Mastek Limited and its subsidiaries, their employees, associated consultants, contractors and third party service providers, worldwide, without exception. Employees should note that failure to comply with this Policy may lead to disciplinary or court action, including, termination of employment or contract with Mastek.

This Privacy Policy comprises the internationally accepted data privacy principles without replacing existing national laws. It supplements national data privacy laws. The relevant national law will take precedence in the event that it conflicts with this Privacy Policy, or it has stricter requirements than this Privacy Policy.

At Mastek, Line managers, and functional and project leads shall work with their respective local legal and compliance advisers and the Head of Legal, UK to ensure their business division, project and function complies with this Policy. Where applicable, any local policies and processes governing the processing of personal information shall comply with this Policy, except as may otherwise be required by local law, and shall be created in agreement with Head of Legal, UK.

This Policy applies to third parties who have dealings with Mastek. As such, line managers and functional leads shall ensure their employees and individual contractors, consultants, agents and suppliers working for on or behalf of Mastek safeguard personal information from loss, destruction, misuse, and unlawful disclosure in accordance with this Privacy Policy, Mastek contractual obligations, applicable procedures and the Data Protection Laws. Additional guidance for managers, if required, may be obtained by contacting Mastek Head of Legal, UK in the first instance at data.protection@mastek.com.

Mastek will at all times uphold and practice the data protection principles described in Art 5(1) of the GDPR when processing personal information. Mastek shall:

- Process such data lawfully, fairly and in a transparent manner;
- Collect such information for specified, explicit and legitimate purposes only;
- Ensure 'data minimisation applies' and that such information is adequate, relevant and limited to that which is necessary for the identified purposes only;
- Ensure such information is accurate and kept up to date;
- Ensure the information is kept for no longer than is necessary;
- Use such technical and operational means to ensure the information is processed with appropriate levels of security to guard against unauthorised and unlawful processing, loss, destruction or damage.

3. **RESPONSIBILITIES**

a) Record keeping/inventory

The GDPR (Article 30) requires companies to ensure that an appropriate record is maintained of all activities (performed by, for, or on behalf of the company) which constitute processing of personal information.

Mastek Line Managers and/or function leads within departments where personal data processing activities are being carried out shall ensure that a record of processing activities are inputted on an inventory record.

b) Contracts

All contracts under which Mastek processes personal information, or under which a third party processes personal information for or on behalf of Mastek, need to contain certain information about (amongst other things) the processing activity and type of personal information being processed under the contract, in addition to mandatory contract terms as required by Article 28 of the GDPR.

Mastek staff should be vigilant for scenarios where Mastek acts as, or may be considered, a joint controller and shall report all such circumstances to Mastek Legal.

New and renewed contracts

Mastek Legal has prepared certain template documents (available for use on the Legal site of MastekNet) which, where applicable, contain the mandatory terms and provide guidance and pro-forma information to project leads to ensure that the necessary information is captured in the contract. Project leads should ensure that they seek to use Mastek templates as the basis for any new or renewed contract where possible.

Where third party terms must form the basis for any new contract, project leads shall ensure that Mastek Legal is engaged at an early stage to review the data protection clauses contained within such contracts to ensure they conform to the mandatory requirements.

Existing contracts

Mastek is undertaking a contract 're-papering' exercise to ensure that all existing contracts with customers and suppliers under which personal data is processed by, for, or on behalf of Mastek are retrospectively amended to include the necessary information and terms, as mandated by Article 28 GDPR.

Mastek Legal will be in contact with any Mastek employees who are required to assist with this exercise. This is an important exercise and the full cooperation and support of all Mastek employees is anticipated and expected.

c) Fair, lawful, transparent processing

Lawfulness

There are a number of circumstances in which Mastek may lawfully process an individual's personal information and an individual's explicit consent is not always required. Whether 'consent' operates at the legal basis for processing or not, Mastek will consider the circumstances carefully and record in writing the basis upon which it processes such personal information before the personal information is processed.

Generally, with the exception of unsolicited direct marketing activities undertaken by Mastek by electronic means, or where Mastek is processing special categories of personal information, Mastek employees should seek to avoid using consent as the lawful basis for the relevant processing activity or, if consent is procured, seek to use such consent as a secondary lawful basis for the processing activity in question.

Line managers, and project and function leads shall consider and make a written record of the 'legal basis' for processing personal information entrusted to them on one or more of the following headings:

I. **Consent**

Where consent is required or used by Mastek as the basis for lawful processing we will always use clear, plain language. We provide a Privacy Notice showing why we want the data and how we will use it. We will use a positive opt-in where we use personal information for direct marketing, except as may otherwise be permitted by the PECR.

We will make it clear that individuals have the right to withdraw their consent (see later, Data Subject Rights)

Consent will never be a pre-condition to obtaining a service from Mastek and we will regularly review consents and keep a written record of all consents.

II. **Legitimate Interest**

Where Mastek relies on a legitimate interest to process personal information we will keep a record and perform a legitimate interests assessment (LIA) to demonstrate compliance, and keep this LIA under review. We will check processing is necessary and we will balance the Data Subject's interests against the legitimate interests of Mastek. Mastek will only use the personal information as the Data Subject may reasonably expect.

We will take additional care in the processing of personal information relating to children when using legitimate interests as the basis for processing.

III. **Performance or negotiation of contracts**

When processing personal information on behalf of customers and with others with whom we do business, or with employees, contractors and/or workers, our lawful basis will be the contract we have with that person, or the contract we are negotiating.

IV. **Legal Obligation**

Mastek may need to process personal information for a common law or statutory reason. When we do this, we will ensure such processing is necessary and ensure we have a sound legal basis in connection with any such processing taking legal advice as may be required.

Fairness and transparency

Mastek collects and processes personal information as part of its customer contract obligations, for the management of staff and employee benefits, to attract new business, and for other reasons. A detailed explanation of the categories of personal information and the reasons that Mastek processes such personal information is set out in the Mastek Privacy Notice at: https://www.mastek.com/privacy-notice

Through the Mastek Privacy Notice (which may also be referred to as the Fair Processing Notice (FPN)), Mastek aims to be clear, open and honest with data subjects about the purposes for, and the manner in which, it collects, handles and uses their personal information. Employees are encouraged to review the FPN on a regular basis to understand how and why Mastek processes their personal information. Any concerns or queries about the content of the FPN should be directed to Head of Legal, UK.

Mastek will only process personal information that has been obtained fairly and lawfully, in line with data subjects' expectations and in a manner that will not have any adverse effects on them.

d) **Purpose limitation and compatibility**

Mastek must only process personal information for specific and legitimate purposes and not further process personal information in a manner that is incompatible with such purpose.

This means that Mastek shall:

- clearly set out in its Fair Processing Notice (FPN) why it is collecting personal information;
- ensure that its records (i.e. its inventory) details the purpose with respect to each processing activity, and that any contracts under which personal data is processed do the same; and
- ensure that any further processing activity undertaken beyond the original purpose is linked and similar to the original purpose and that is does not have an unjustified impact on the individual.

e) **Data minimisation**

Mastek shall ensure that any personal data processed by, for or on behalf of it is:

- adequate to fulfil the purpose for which it was collected;
- relevant to the purpose for which it was collected;
- limited as necessary for the purpose for which it was collected.

f) **Accuracy of personal information**

Mastek shall ensure that all personal information processed by it from time to time is up to date and accurate, such that it is not incorrect or misleading.

Employees, workers and contractors shall ensure that any changes to their personal information that is held by Mastek in connection with their employment or engagement are brought to the attention of Mastek without delay.

g) **Storage limitation**

Mastek shall only keep personal data for as long as is necessary taking into account the purpose for which it was obtained.

Once personal information has fulfilled its useful purpose, Mastek will securely erase or anonymise it, as appropriate.

Mastek shall regularly review the data it holds and the retention periods of the same, ensuring that it can justify the personal information it holds at all times.

Mastek has implemented a Data Backup and Retention Policy (PLIS02) that sets out standard retention period for particular types of data, including personal information. Employees are required to familiarise themselves with the relevant retention periods for any personal information held under their responsibility.

Mastek will carefully consider and promptly action any valid and justified requests for erasure that it receives from data subjects.

h) **Integrity and confidentiality (security)**

Mastek is required by law to ensure that it has in place appropriate technical and organisational measures to protect the personal information that it holds.

In deciding what is appropriate, Mastek will endeavour to reflect the state of the art and will implement measures which are cost appropriate taking into account the risks posed by the processing activity to the rights of data subjects.

Mastek shall look to implement obfuscating methods such as encryption at rest and in transit, and pseudonymisation, wherever possible.

Mastek's Information Security team maintains policies and governance documents ("IT Security Framework") which are designed to ensure the confidentiality, integrity and ongoing availability of Mastek's data handling systems. The IT Framework is referred to in the References section at the end of this policy.

Mastek employees are required to maintain the confidentiality of the personal data they process for or on behalf of Mastek, including complying with the confidentiality provisions contained in their employment contracts and any additional confidentiality obligations imposed by third party contracts. Personal Information will only be shared with those individuals or entities that have a strict need to have access to the personal information for the specific purpose for which it was procured.

Mastek understands that individuals expect Mastek only to disclose their personal information in limited circumstances and that otherwise, their personal information shall be kept secure and not be disclosed. Mastek's Privacy Notice describes the ways in which Mastek may use an individual's personal information and the circumstances in which disclosures may occur. Line managers, and project and functional leads shall ensure compliance with the Privacy Notice.

i) **International (restricted) data transfers**

Mastek is required to ensure that all transfers of personal information made by it to a recipient based outside of the EU is protected by an appropriate safeguard (or an adequacy decision from the EU Commission or a valid exception), such it can provide assurance that the level of protection afforded to the personal information whilst it is outside of the EU is commensurate with the standards of protection mandated by the GDPR, DPA '18 and other EU and UK legislation.

Mastek's employees, contractors and workers are required to consider before effecting any transfer of personal information outside of the EU whether they can achieve their aims without transferring the data. If they cannot, such staff are required to consult with Mastek Legal prior to effecting any transfer such that appropriate safeguards can be established.

Typically, when dealing with customers or suppliers, such adequate safeguards will require the EU Standard Contractual Clauses to be inserted into the relevant contract under which personal data is being transferred.

Employees should be vigilant for any transfers of personal information between Mastek (UK) Limited and Mastek Limited or any of its other subsidiary companies based in India or the United States of America. Such transfers will also need appropriate safeguards or exceptions and Mastek Legal will advise as to what those are on a case by case basis.

j) **Data Protection Impact Assessments (DPIA)**

As mandated by law, Mastek will perform Data Protection Impact Assessments (DPIAs) with respect to any processing activities that are likely to result in a high risk to individuals to assess potential data protection risks associated with such actions, identify any relevant mitigations, and act in accordance with the other processes and guidance forming the Mastek Data Protection Framework.

Mastek will also, in line with good industry practice, perform DPIAs for any other significant projects which require processing of personal information. To be clear, the obligation to perform DPIAs is not limited to new customer projects and internal work; line managers, and/or functional and project leads must ensure that current, ongoing business practice meets the requirements of this Policy.

Mastek's Line Manager's and/or project and function leads must ensure that the data protection principles and information security risks have been considered at the initial/design stage by completing a DPIA. The Line Manager, and/or project and function leads shall ensure the DPIA remains under review, but specifically during and post phase regularly thereafter. The Information Security Manager must support completion of the DPIA to ensure that the appropriate technical controls and/or associated risks have been identified. DPIA applies at the initial/design stage of all new/existing systems, services, products and business practices that involve the processing of personal data information and this will include, but not limited to;

- Processing personal data on a large scale;
- Processing biometric data;
- Using new technologies;
- Processing personal data information for marketing purposes

k) **Privacy by Design and Privacy by Default Division**

Line managers, and project and function leads shall ensure they practice and implement Privacy by Design within their respective functional and project areas, throughout the design phase and commencement of any system, service, process or customer project that handles personal information and at all times thereafter.

Mastek shall take appropriate lengths to integrate data protection into its processing activities and business practices, from the design stage right through the lifecycle. Such lengths may entail (amongst other things) the development of new IT systems or new policies, processes and practices.

Employees, staff and contractors processing personal information for or on behalf of Mastek are required to consider data protection issues pro-actively in the performance of their responsibilities.

Employees, staff and contractors processing personal information for or on behalf of Mastek shall, at all times, ensure that they only process such personal information as is strictly necessary to achieve the purpose for which it was procured.

l) **Special categories of personal information and criminal records data**

Where we process special categories of personal information, and/or criminal offences and convictions data provided by the customer or otherwise, we will always seek an additional assurance (generally by way of contract) that explicit consent has been given by the data subject, or that processing is necessary to protect the data subject's vital interests or such activity is legitimate or otherwise permitted by the GDPR. Legal should be consulted prior to any processing of special category personal information and/or criminal records data.

4. **DATA SUBJECT RIGHTS AND FREEDOMS**

In addition to their general rights under the GDPR, individuals have certain specific rights as set out below. Mastek is committed to fulfilling its obligations and will ensure that these specific data subject's rights are achieved.

Individuals have the following rights with respect to their personal information processed by Mastek where Mastek acts as a data controller*:

1. to be informed of how their personal information is used;
2. to access their personal information and supplementary information;
3. to seek rectification of any inaccurate personal information;
4. to erasure of their personal information from Mastek's systems ("right to be forgotten");
5. to restrict Mastek's processing of their personal information;
6. to require Mastek to port their personal information to another data controller;

7. to object to Mastek's processing of their personal data;
8. in relation to automated decision making and profiling.

* Certain rights are only available in particular circumstances.

If an individual wishes to make a request in connection with any of their data subject rights, the individual may send an email to Global Head of Legal Affairs, Vimal Dangri at data.protection@mastek.com and the DPO at Dianna.Anthony@mastek.com

Individuals making any such request should note that a request may be delayed or refused if they provide incomplete data, or where Mastek requires further information from the requesting individual to allow it to respond to or fulfil the request.

Where Mastek receives a data subject access request ("DSAR"), the DPO will oversee the response to the individual. The DPO will be responsible for (amongst other things) liaising with the individual, considering the validity of the request and/or whether sufficient information has been provided to enable Mastek to take action in relation to the request, and for mobilising and overseeing a team within Mastek, comprised of

Stakeholders from Human Resources, Information Security and/or any other relevant functions, as necessary.

Where the DPO requires assistance from Mastek employees in relation to a Data Subject Access Request (DSAR), or any other data subject right, Mastek employees shall provide all necessary cooperation and support to ensure that Mastek meets its obligation to respond fully to DSAR request.

In the event that a Mastek employee, contractor or worker directly receives, or is aware of Mastek receiving a DSAR or any other data subject right, they should raise this fact immediately to the Global Head of Legal Affairs, Vimal Dangri at data.protection@mastek.com, the legal team data.protection@mastek.com and the DPO at Dianna.Anthony@mastek.com .

The DPO is responsible for overseeing responses in relation to all other data subject rights too, except to the extent that the DPO has delegated responsibility for managing responses to particular rights requests to Human Resources.

5. **SECURITY, INCIDENT MANAGEMENT AND REPORTING**

Mastek understands that poor information security leaves systems and services at risk and may cause real harm and distress to individuals.

Security Mastek will continually monitor, test, assess and where necessary, make and implement changes to its data security systems including its risk analysis processes, security of processing, organisational policies, and physical and technical measures.

Where appropriate we will use, our proprietary KAMELEON or other pseudonymisation tool and encryption to mask personal information.

We are ISO 27001 certified. We comply with the UK Government Cyber Essentials obligations and other industry standard data security requirements.

b) **Incident management**

Mastek is under strict obligation to promptly report data protection breaches to the regulator, its customers, and/or the individuals affected, as appropriate.

To ensure that Mastek meets its obligations in a timely manner, Mastek employees, contractors and workers are required to be vigilant for personal information incidents and to report the same to Mahesh Juttiyavar, Chief Information Security Officer, Vimal Dangri, Global Head of Legal Affairs and Dianna Anthony, Data Protection Officer at data.protection@mastek.com and Dianna Anthony, DPO at Dianna.Anthony@mastek.com

A personal information incident comprises any situation where the integrity, confidentiality, availability or protection afforded to personal information has been, will be, or could potentially be compromised in any way.

Employees should ensure they refer to such matters as "incidents" rather than "breaches" until CISO, Global Head of Legal Affairs, and DPO have determined the matter to constitute a "breach".

Mastek has further written guidance within Mastek's Data Breach Policy which can be obtained on Mastek's internal share point link to assist employees with identifying and escalating personal information incidents appropriately and it is also located on www.mastek.com/privacy-notice.

c) General IT security Incidents

IT Security Incidents may or may not involve the breach or disclosure of personal information. Mastek has a specific Policy for dealing with the reporting and management of such incidents in addition to the mechanism for reporting a personal information breach described above: Incident Management Policy, which forms part of the Mastek Data Protection Framework.

6. **NON APPLICATION**

Whilst the Data Protection Legislation applies in the vast majority of circumstances, it is important to be aware that they do not apply in every circumstance where Mastek processes or controls an individual's personal information. Mastek Legal will advise where this is the case

7. **CHILDREN**

Children have the same rights as adults. Additionally, a child's personal information merits particular protection under the GDPR. Children need particular protection when we are collecting and processing their personal data because they may be less aware of the risks involved. Mastek Legal should be engaged in advance at all times where children's personal information is, or may be, processed by, for or on behalf of Mastek.

8. **TRAINING, ASSESSMENT AND INTERNAL COMPLIANCE**

Mastek's compliance with the Data Protection Legislation, this Policy and the Mastek Data Protection Framework depends on every member of staff globally (including its employees, consultants and contractors) being aware of the company's legal requirements and critically, each and every such person demonstrating that they and their functional area or Project practices this Policy.

Accordingly, it is a mandatory requirement of each such person to complete the Mastek corporate online Training and Assessment programme available on MastekNet at least once every 12 months and where requested to do so, to provide compliance reports in the relevant form to the Head of Legal, UK within the requested timeframe. If the Head of Legal, UK recommends any corrective actions, staff will comply with such recommendations where requested to do so, without delay and as a priority. On completion of any such corrective action, the relevant member of staff will report the same in writing, to the Head of Legal, UK.

The company will perform internal data protection compliance audits and other external and Customer audits as required.

9. **DATA PROTECTION OFFICER**

Mastek has appointed a Data Protection Officer ("DPO") Dianna Anthony and her email address is Dianna.Anthony@Mastek.com and data.protection@mastek.com

Mastek fully supports the DPO in all Data Protection compliance matters and will ensure the provision of such resources as may reasonably be required.

10. **POLICY REVISIONS**

Mastek will regularly review this Privacy Policy and reserves the right to change this Privacy Policy at any time. Mastek recommends every member of staff, Customers, Suppliers and others affected by it to refer to this Privacy Policy, to check it regularly for material changes

11. **REFERENCES**

As part of the Mastek Data Protection Framework, Mastek will maintain governance measures designed to minimise the risk of breaches and protect personal information. Our corporate Policies, processes, Guidance and other documentation cited below form part of that governance framework.

The Mastek Data Protection Framework includes the following document references:

- Privacy Notice
- The Security Incident Management Policy
- Information Security Policy Statement
- Information Security User Training Policy
- Information Exchange Policy
- Record Maintenance and Record Control Policy
- Data Backup and Retention Policy
- Network Security Policy
- Personal Security Policy
- Physical and Environmental Policy
- Security Policy Manual
- Social Media Policy
- System Logging and Auditing Policy
- Third Party Access Control Policy
- Wireless Policy
- Acceptable Use Policy
- Information Security at Mastek

11a) **How do staff at Mastek Process Personal Data?**

Everyone who works for, or on behalf of, the Company has some responsibility for ensuring data is collected, stored and handled appropriately, in line with this policy and the Company's Data Security policies.

Everyone who works for MASTEK Limited and each of its subsidiary companies (see list of companies at the end of this policy) are responsible for reviewing this policy and any risks in relation to the processing of data. You should direct any questions in relation to this policy to the Data Protection Officer, Dianna Anthony at data.protection@mastek.com.

- You should only access Personal Data if you need it for the work you do for, or on behalf of the Company and only if you are authorised to do so. You should only use the data for the specified lawful purpose for which it was obtained.
- You should not share Personal Data informally.
- You should keep Personal Data secure and not share it with unauthorised people

- You should regularly review and, where required or requested, update Personal Data you deal with. This includes telling us if your own contact details change.
- You should not make unnecessary copies of Personal Data and should keep and dispose of any copies securely.
- You should use strong passwords and not share your passwords with any other person.
- You should lock your computer screens when not at your desk.
- Personal Data should be encrypted before being transferred electronically to authorised external contacts.
- Consider anonymising data or using separate keys/codes so that the Data Subject cannot be identified.
- Do not save Personal Data to your own personal computers or other devices.
- Personal Data should never be transferred outside the European Economic Area except in compliance with the law and authorisation.
- You should lock drawers and filing cabinets. Do not leave paper with Personal Data lying about.
- You should not take Personal Data away from Company's premises without authorisation from your line manager
- Personal Data should be shredded and disposed of securely when you have finished with it.
- You should ask for help from management if you are unsure about data protection or if you notice any areas of data protection or security we can improve upon.

Any deliberate or negligent breach of this policy by you may result in disciplinary action being taken against you.

It is a criminal offence to conceal or destroy Personal Data which is part of a subject access request (see below). This conduct would also amount to gross misconduct under our disciplinary procedure, which could result in your dismissal.

It should be noted that whilst this list provides examples, this is by no means an exhaustive list and you may be notified of other specific rules from time to time.

What purposes can Personal Data be processed for by Mastek staff?

Personal Data must be collected only for specified, explicit and legitimate purposes. It must not be further processed in any manner incompatible with those purposes.

Personal Data cannot be used for new, different or incompatible purposes from that disclosed when it was first obtained, unless you have informed the Data Subject of the new purposes and they have consented where necessary.

Is there a limit to how much Personal Data can be collected and processed?

Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

You may only Process Personal Data when performing your job duties requires it. You cannot Process Personal Data for any reason unrelated to your job duties.

You may only collect and Process Personal Data that you require for your job duties: do not collect excessive data. Ensure any Personal Data collected is adequate and relevant for the intended purposes.

You must ensure that when Personal Data is no longer needed for specified purposes, it is deleted or anonymised in accordance with the Company's data retention guidelines.

Here at Mastek, we take privacy seriously. We take every possible precaution to protect personal data information and actively work to avoid any data protection breaches which could compromise our data security, or the personal rights of individuals, our clients, customers, stakeholders and anyone else associated with our company.

To mitigate the risk that any such data compromise could pose, we have developed this policy which is an integral part of our compliance responsibilities and it is designed to develop clear lines of responsibility for everyone at Mastek when managing and processing personal data information.

To date, Mastek have not had any data breaches raised against it by any data protection supervisory authority.

12. **GLOSSARY OF TERMS**

Mastek Group Companies ("Mastek"): Includes the following list of Mastek business entities: Mastek Enterprise Solutions Private Limited (formerly known as Trans American Information Systems Private Limited), Evolutionary Systems Corp & Newbury Cloud Inc., Mastek Digital Inc. Evolutionary Systems Canada Limited, Mastek Arabia FZ LLC, Evolutionary Systems Consultancy LLC, Evolutionary Systems Egypt LLC, Evolutionary Systems Saudi LLC, Evolutionary Systems Bahrain WLL, Evosys Kuwait WLL, Evolutionary Systems Qatar WLL, Evolutionary Systems Singapore Pte Ltd., Evosys Consultancy Services (Malaysia) Sdn Bhd., Mastek Systems Pty Ltd., Evolutionary Systems B.V. – Netherlands, Evolutionary Systems B.V. – Romania Branch

Biometric data: personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.

Controller: controller determines the purposes and means of processing personal data.

Data Protection Legislation: the GDPR, the UK Data Protection Act 2018, PECR, and all applicable law about the processing of personal data and privacy;

Data Subject: an identifiable natural 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 the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

GDPR: the EU General Data Protection Regulation EU 2016/679 Genetic data: personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.;

ICO: the Office of the UK Information Commissioner.

Joint Controller: a legal person that together with one or more other legal persons acts in the capacity of a Controller.

Personal information and personal data: any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural 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 the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Pseudonymisation: the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

PECR: The Privacy and Electronic Communications (EC Directive) Regulations 2003 as derived from EU Directive 2002/58/EC, its associated and amending regulations, and such legislation as may substitute or replace such legislation.

Processor: responsible for processing personal data on behalf of a controller.

Special categories of personal data: personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.