



Data Subject Access Request Policy

3 February 2023

Mastek Legal Function

Division: Mastek Legal



## DATA SUBJECT ACCESS REQUEST POLICY

### 1. **Purpose**

- 1.1 This document sets out Mastek Group Companies\* policy for responding to data subject access requests ("DSAR") as per General Data Protection Regulations ("GDPR"), California Consumer Privacy Act 2018 ("CCPA") and all international data privacy laws and regulations for data subjects to access their personal data information held by Mastek's Group Companies.
- 1.2 We welcome the rights of access to your personal data information and we are committed to operating openly and to meeting all reasonable personal data information requests. This procedure shall be used by all Mastek's Group Companies ("Mastek") employees, consultants and independent contractors, interns or temporary workers in all countries in which Mastek operates and/or conducts business. For the purpose of the CCPA, this sets out our obligations as a "business" and a "service provider", as those terms are defined under the CCPA.

In order to obtain your personal information, please follow the steps outlined in our procedure detailed below.

### 2. **Definitions**

\*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 System Qatar WLL, Evolutionary Systems (Singapore) Pte Limited, Evolutionary Systems Pty Limited, Evolutionary Systems Corp., Evolutionary System Co. Limited, Evolutionary Consultancy Services (Malaysia) SDN BHD, Evolutionary Systems Canada Limited, Newbury Cloud Inc., Evolutionary Systems B.V., Mastek (UK) Limited, Mastek Arabia FZ LLC, Mastek Inc., Trans America Information Systems Inc., Mastek Digital Inc., Evolutionary Systems Saudi LLC, Evosys Kuwait WLL, Evolutionary Systems Bahrain WLL, Evolutionary Systems Consultancy LLC, Evolutionary Systems Egypt LLC.

Data Controller – The entity that determines the purpose and means of processing personal data and is synonymous with "PII Controller."

Data Processor – The entity that processes personal data on behalf of the data controller and is synonymous with "PII Processor."

Data Protection Laws – All applicable data protection and data privacy laws and regulations, including but not limited to the General Data Protection Regulation (GDPR), Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) and the California Consumer Privacy Act (CCPA).

Data Subject – The identified or identifiable person or household to whom personal data relates.

Personal Data – The meaning ascribed to "personally identifiable information"

and “personal information,” or “personal data.” Also personal information is any data, in both physical and electronic form, related to an identified or identifiable person. It includes anything that can be used to identify a person directly or indirectly, by means of for example his or her physical attributes, economic, cultural or social identity.

Processing - Any operation or set of operations that is performed on personal data, whether or not by automatic means, such as collection, recording, organization structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Processing also includes transferring or disclosing personal data to third parties.

Special Category Data - Information about an individual's race or ethnic origin, sexual orientation, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data (eye color, hair color, height), medical history, or criminal convictions and offenses or related security measures.

### 3. **What is a Data Subject Access Request (“DSAR”)?**

3.1 A DSAR gives individuals the right to know what information is held about them. It provides a framework to ensure that personal information is handled properly.

3.2 Mastek ensures that anyone of our staff who processes personal data information must comply with eight principles to make sure that personal information is:

- Fairly and lawfully processed
- Processed for specific and lawful purposes
- Adequate, relevant and not excessive
- Accurate and up to date
- Not kept for longer than is necessary
- Processed in line with the individuals' rights
- Secure
- Not transferred to other countries without adequate protection

3.4 Secondly, it provides individuals with important rights, including the right to find out what personal information is held on computer and paper records.

#### **Data Subject Access Rights**

In many jurisdictions, including but not limited to California in the United States, Canada, the UK and the European Economic Area (EEA), Mastek, as a data controller, is required to take appropriate measures to provide data subjects with access to personal data it processes with respect to them. Access should be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language.



The data subject may also have the right to receive the following from Mastek in regards to processing of personal data information:

1. The purpose of the processing;
2. The categories of personal data concerned;
3. The recipients or categories of recipient to whom the personal data has been or will be disclosed;
4. The period of time in which the personal data will be stored or, if not possible, the criteria used to determine that period;
5. Information as to the source of personal data about the data subject held by Mastek (if not provided by the data subject);
6. Information about the existence of automated decision-making, including profiling
7. Information about safeguards Mastek has put in place where personal data is transferred to a third country (e.g., under the GDPR, a country that is not a signatory to the GDPR and has not received an adequacy decision from the European Commission);

The data subject may also have the right to receive the following from Mastek if located in California:

1. Confirmation as to whether Mastek processes personal data about the data subject;
2. The purpose of the processing;
3. The categories of personal data concerned;
4. The recipients or categories of recipient to whom the personal data has been or will be disclosed;
5. Information as to the source of personal data about the data subject held by Mastek (if not provided by the data subject);
6. The right to opt out of the "sale" by Mastek of personal data about the data subject, as "sale" is defined under the CCPA. Please email your request to our Data Protection Officer at [data.protection@mastek.com](mailto:data.protection@mastek.com)

Although not as prescriptive as the GDPR and CCPA, PIPEDA has been interpreted to contain the same data subject access rights. Thus, the aforementioned rights apply to those in Canada as well. For data subjects located in other jurisdictions, Mastek will provide the same information upon request and will review applicable data privacy legislation to determine whether different or additional rights apply to data subjects.

#### 4. **How do you make a data subject access request?**

- 4.1 A data subject access request is a written request for personal information (known as personal data) held about you by Mastek. You have the right to see what personal information we hold about you, you are entitled to be given a description of the information, what we use it for, who we might pass it onto, and any information we might have about the source of the information.



All data subjects are encouraged to complete our Data Subject Request Form (“DSR”) when submitting a DSR form which can be found in Appendix B located at the end of this policy. By completing the DSR form will allow Mastek to respond faster and more efficiently to your DSAR request. If a DSAR is received by other means such as by email, then please forward your DSAR request to our Data Protection Officer at [data.protection@mastek.com](mailto:data.protection@mastek.com).

5. **What is personal information?**

5.1 Personal information is any data, in both physical and electronic form, related to an identified or identifiable person. It includes anything that can be used to identify a person directly or indirectly, by means of for example his or her physical attributes, economic, cultural or social identity.

5.2 Further information on what amounts to personal data can be found at **Appendix A**, located at the end of this policy.

5.3 **What do we do when we receive a data subject access request?**

**Identification Check**

5.4 We will first check that we have enough information to be sure of your identity. Often we will have no reason to doubt a person’s identity, for example, if we have regularly corresponded with them. However, if we have good cause to doubt your identity we can ask you to provide any evidence we reasonably need to confirm your identity. For example, we may ask you for a piece of information held in your records that we would expect you to know: a witnessed copy of your signature or proof of your address.

5.5 If the person requesting the information is a relative/representative of the individual concerned, then the relative/representative is entitled to personal data about themselves but must supply the individual’s consent for the release of their personal data.

5.6 Should you make a data subject access request but you are not the data subject, you must stipulate the basis under which you consider makes you entitled to the information.

**Collation of information**

5.7 We will check that we have enough information to find the records you requested. If we feel we need more information, then we will promptly ask you for this. We will gather any manual or electronically held information, including emails that may contain your personal data information.

5.8 If we have identified information that relates to third parties, we will write to them asking whether there is any reason why this information should not be disclosed. We do not have to supply the information to you unless the other party has provided their consent or it is reasonable to do so without their consent. If the third party objects to the information being disclosed we may seek legal advice on what action we should take.

5.9 Before sharing any information that relates to third parties, we will where possible anonymise information that identifies third parties not already known to the individual (e.g. Mastek employees), and edit information that might affect another party’s privacy.



5.10 Once any queries around the information requested have been resolved, copies of the information will be provided to you with a URL link and a password to safely and securely view and access your personal data information.

5.11 We will explain any complex terms or abbreviations contained within the information when it is shared with you. We will also provide a copy of any information electronically that you have seen before containing your personal data information.

6. **Will we charge a fee?**

6.1 We will not charge a fee, however if we do charge an administrative fee, then we will inform you promptly of this, for example if your DSAR request is manifestly excessive or unfounded.

7. **What is the timeframe for Mastek to respond to subject access requests?**

7.1 We shall respond in one calendar month starting from when we have received all the information necessary to identify you, to identify the information requested, and any administrative fee if applicable, to provide you with the information or to provide an explanation about why we are unable to provide the information. In many cases, it will be possible to respond in advance of the one month target and we will aim to do so where possible.

If, however we require more time to respond to your DSAR request after one month due to the complexity or volume of the data for example, then we shall notify you.

8. **Are there any grounds we can rely on for not complying with a subject access request?**

**Previous request**

8.1 If you have made a previous subject access request we must respond if a reasonable interval has elapsed since the previous request. A reasonable interval will be determined upon the nature of the information, the time that has elapsed, and the number of changes that have occurred to the information since the last request.

9. **Exemptions**

9.1 There are a number of exemptions to our duty to disclose personal data and we may seek legal advice if we consider that they might apply. Some exemptions that would be apply are for example: Information covered by legal professional privilege, information about another person's person data information, business as usual data, financial business information unrelated to the data subject. A data subject is only entitled to receive information about their own personal data information.

10. **What if you identify an error or you would like to update your records held at Mastek?**

10.1 If we agree that the information is inaccurate, we will correct it and where practicable, destroy the inaccurate information. We will consider informing any relevant third party of the correction.



If you would like to exercise your right to have your personal data rectified (i.e., changed, updated, or corrected) or erased (i.e., deleted) or to restrict or object to processing of your personal data, please submit your request by email to our Data Protection Officer at [data.protection@mastek.com](mailto:data.protection@mastek.com)

11. **What if a data subject requests that Mastek stop processing their personal data?**

11.1 You can send an email to our Data Protection Officer at [data.protection@mastek.com](mailto:data.protection@mastek.com) to request Mastek to stop processing your personal data altogether by making a deletion of data request. We will respond and complete your deletion in 30 days from the date of your request. If there is any personal data information that we are required to retain your personal information about you for example, tax information or other legal or regulatory obligation, then we shall notify you.

12. **Our complaints procedure**

12.1 If you are not satisfied with our actions relating to your DSAR request or deletion request, you can seek recourse through our internal complaints procedure, the Data Protection Supervisory Authority or the courts.

12.2 The Data Protection Officer (DPO) will deal with any written complaint about the way a request has been handled and about what information has been disclosed. The DPO's contact details are Mastek, Pennant House, 2 Napier Court, Reading, RG1 8BW, Email address: [data.protection@mastek.com](mailto:data.protection@mastek.com), telephone number: 0118 903 5700.

12.3 If you remain dissatisfied, then you have the right to refer the matter to the relevant Data Protection Authority listed below:

United Kingdom - Information Commissioner's Office Wycliffe House Water Lane Wilmslow Cheshire SK9 5AF Telephone: 01625 545 745 Fax: 01625 524 510 Email: [enquiries@ico.gsi.gov.uk](mailto:enquiries@ico.gsi.gov.uk)

California, USA – California Privacy Protection Agency (CCPA), Mailing Address: 2101 Arena Blvd Sacramento, CA 95834 Email: [info@coppa.co.gov](mailto:info@coppa.co.gov)

Texas, USA – Office of the Texas Attorney General, Telephone Number: (800)621-0508, Mailing Address: PO Box 12548, Austin, Texas 78711-2548

Toronto, Canada – Information and Privacy Commissioner of Ontario (IPC), Telephone Number: (+416) 326 3333, Toll Free Telephone Number: 1-800-387-0073, Mailing Address: Information and Privacy Commissioner of Ontario. 2 Bloor Street East, Suite 1400, Toronto, Ontario, M4W 1A8,

Bahrain – Personal Data Protection Authority email: [dp-team@moj.gov.bh](mailto:dp-team@moj.gov.bh), Telephone Number (+973) 175 133 14, (+973) 175 133 21, (+973) 175 133 41



13. **Appendix A**

- 13.1 Personal data is information that relates to a living individual who can be identified from the information and which affects the privacy of that individual, either in a personal or professional capacity. Any expression of opinion about the individual or any indication of the intentions of any person in respect of the individual will be personal data.
- 13.2 Provided the information in question can be linked to an identifiable individual, the following are examples of personal data:
- an individual's salary or other financial information
  - information about an individual's family life or personal circumstances, employment or personal circumstances, any opinion about an individual's state of mind
  - sensitive personal information – an individual's racial or ethnic origin, political opinions, religious beliefs, physical or mental health, sexual orientation, criminal record and membership of a trade union.
- 13.3 The following are examples of information, which will not normally be personal data:
- Mere reference to a person's name, where the name is not associated with any other personal information
  - The content of that document or email does not amount to personal data about the individual unless there is other information about the individual in it.
- 13.4 If a document has been sent by a third party, that contains information about an individual which relates to their personal or professional life, then it is personal data.





**Appendix B**

**Data Subject Request Form**

First Name	
Last Name	
Email	
Company	
Country	

**What is your relationship to Mastek (select all that apply)?**

Customer	
Partner	
Vendor/Supplier	
Former Employee or Contractor	
Other (please describe)	

**Authorized agent acting on behalf of the above (please provide your full name and contact information)**

--

**Details of Request (select all that apply):**

1.	Confirmation as to whether Mastek, as a data controller, processes my personal data	
2.	Categories of sources from which Mastek has collected my personal data	
3.	Purposes for processing my personal data (including the purposes for Mastek's collection, disclosure)	
4.	Categories of my personal data processed (including categories that have been collected,	

5.	disclosed for business purposes) Recipients to whom my personal data has been or will be disclosed	
6.	Retention period or policy criteria for retention of my personal data	
7.	Safeguards relating to transfer of my personal data outside of the EU, if applicable	
8.	Copy of my personal data controlled and processed by Mastek	
9.	Any other DSAR request not listed above. Please specify your DSAR request here.	

**Please do not enter sensitive personal information or protected health information into this form.**

We will confirm receipt of a request submitted via this DSR form. If you do not receive confirmation within 7 days, then please email your DSAR request to our Data Protection Officer at [data.protection@mastek.com](mailto:data.protection@mastek.com).