# GOVERNMENT DISCLOSURE REQUESTS POLICY

## 1. Background

1.1. As a global technology company Tech Mahindra may receive requests from law enforcement and other government agencies, courts and litigation parties across the world for access to customer data, or Tech Mahindra's own employee data, in connection with legal investigations and proceedings ("**Disclosure Requests**"). Disclosure Requests – and their potential impact on privacy and data security - are increasingly an area of scrutiny for Tech Mahindra's customers and regulators.

1.2. This document sets out globally applicable standards which govern Tech Mahindra's approach to responding to Disclosure Requests. These standards are intended to ensure Tech Mahindra (i) complies with data protection and privacy laws which apply across its operating locations; and (ii) maintains customer, regulator and public trust in its privacy practices.

## 2. Executive Summary - Tech Mahindra's Approach to Disclosure Requests

2.1. This document reasonably create balance between lawful assistance to government and privacy and security concerns that Tech Mahindra shares with its customers.

2.2. Whilst Tech Mahindra is committed to assisting government agencies where lawful to do so, any Disclosure Requests must meet the conditions stipulated in this document, as well as all other applicable Tech Mahindra policies and requirements. In summary, Disclosure Requests must:

2.2.1. comply with certain minimum procedural requirements;

2.2.2. respect key privacy considerations; and

2.2.3. comply with additional requirements (if any) under local laws.

## 3. Structure of this Policy

3.1. This document sets out the globally applicable policy ("**Policy**") for privacy compliance in the context of receiving, analyzing and responding to Disclosure Requests.

3.2. This Policy should be followed for all Disclosure Requests, unless and solely to the extent that it is incompatible with local laws. Any deviation from this Policy must be discussed and agreed with TechM DPO.

3.3. The annex to this document contains a template for documenting Disclosure Requests.

3.4. In considering the applicability of local privacy law considerations, Tech Mahindra will take into account the fact that different requirements may apply to personal data that has been imported from another jurisdiction, and that privacy standards may be required to 'travel with' the imported data, in the form of contractual obligations placed on Tech Mahindra as a data importer in a foreign jurisdiction such as India.

3.5. In this document, "**personal data**" refers to data that relates to an identified or identifiable individual.

## 4. Requirements for All Requests

4.1. All Disclosure Requests must be made by means of a signed document, issued in accordance with all local legal requirements. That document must identify:

4.1.1. the government agency making the request;

4.1.2. the authorized representative of the agency submitting the request including, where applicable, their title and rank;

4.1.3. the legal basis or power for the request;

4.1.4. the specific data sought;

4.1.5. the purpose for the request, which should allow Tech Mahindra to determine whether the disclosure of the requested data is necessary and proportionate in the circumstances (see section 5.2).

4.2. Where an applicable Tech Mahindra template exists (see the Annex to this document), Tech Mahindra will use all reasonable endeavors to ensure that the template is used by the government agency or concern SPOC of Tech Mahindra, or (where this is not possible) that any other document otherwise used contains the information required by the template.

## 5. Privacy Considerations

5.1. **Notice.** To ensure compliance with transparency requirements under privacy, data protection and consumer protection laws, Tech Mahindra will ensure that, wherever possible, disclosures are anticipated in privacy notices maintained by Tech Mahindra (including on its website, and in the form of any privacy notices given to employees). Privacy notices will outline the nature and types of disclosures made, including the relevant government agencies to whom disclosures are made. It is recognized that in some cases full transparency may not be feasible, due to the exceptional nature or sensitivity of a request. However, Tech Mahindra will make every effort to provide a full explanation in its privacy notices.

5.2. **Necessity.** Tech Mahindra will ensure that personal data is only disclosed where the agency has demonstrated a precise basis in law for the request, and a clear and legitimate purpose for the request has been provided, and where Tech Mahindra has a good faith belief that the disclosure of personal data is reasonably necessary and proportionate in connection with the stated purpose.

5.3. **Minimization.** In all cases, Tech Mahindra will disclose the minimum amount of personal data necessary to satisfy the purpose for the request. In particular, Tech Mahindra will seek to limit the blanket or bulk disclosure of documentation or data that contains personal data, disclosing only selected extracts or specific data fields where this would suffice. Tech Mahindra will resist Disclosure Requests whose scope is massive, disproportionate, or indiscriminate in a manner that would go beyond what is necessary in a democratic society or for compliance with applicable laws.

5.4. **Accuracy**. Tech Mahindra will ensure that personal data disclosed to a government agency is (to the best of Tech Mahindra's knowledge) accurate and up-to-date, and that it correctly corresponds to the individual who is the subject of the Disclosure Request, recognizing there may be a risk of harm to an individual from inadvertent disclosure of personal data relating to an individual who is not the subject of the request.

5.5. **Security.** Tech Mahindra will ensure that a secure mechanism is in place for the transfer of personal data to a government agency, for example: a secure file transfer protocol (SFTP), encrypted email, transfer of encrypted storage media or use of a secure government-controlled channel. Documents containing personal data should be password protected and the list of recipients should be limited to the identified, authorized government agency representative(s) who submitted the relevant request. This approach will limit distribution of the data to known parties and on a need-to-know basis. Where Tech Mahindra is acting as a data processor (see section 6.3) specific technical controls (which would also apply to any response to a Disclosure Request) might be required by Tech Mahindra's customer.

5.6. **Lawful Basis.** Where applicable under local data protection laws (including in the EEA and UK), Tech Mahindra will establish and document a lawful basis for any disclosures of personal data. The lawful

basis will be specific to each disclosure but may relate to compliance with a legal obligation that applies to Tech Mahindra, or Tech Mahindra's legitimate interest in assisting with the prevention and detection of crime by facilitating a lawful government request. If acting on behalf of a customer as a data processor, it will be Tech Mahindra's customer that determines whether a lawful basis applies.

## 6. Customer Notification

6.1. Wherever feasible to do so, Tech Mahindra will give prior notice to a customer of any Disclosure Request for personal data that it processes on that customer's behalf. Where the urgency of a request means that prior notice is impractical, Tech Mahindra will provide subsequent notice at the earliest reasonable opportunity. It is also recognized that in some cases Tech Mahindra may be legally prohibited from providing advance notice.

6.2. Tech Mahindra will not directly notify an individual that their data has been the subject of a request, unless expressly required by applicable law or contractual obligation.

*Notification requirements for EEA and UK customers*

6.3. **Tech Mahindra as Data Processor.** Where Tech Mahindra – acting as a data processor on behalf of an EEA or UK customer - receives a request for disclosure of personal data from a law enforcement authority or state security body of a non-EEA country, it will first assess on a case-by-case basis (taking into account the factors in this document, as well as local legal requirements) whether the Disclosure Request is legally valid and binding on Tech Mahindra. If the request is valid, Tech Mahindra will inform its customer (unless legally prohibited from doing so) and will allow the customer to determine the appropriate response to the request, in line with the customer's role as the data controller.

6.4. **Tech Mahindra as Data Controller.** Where Tech Mahindra – acting as a data controller in the EEA or UK (for example in relation to its EEA or UK employee data) – receives a request for disclosure of personal data from a law enforcement authority or state security body of a non-EEA country, it will follow the requirements of this Policy in determining its own response to the request.

## 7. Reviewing Requests

7.1. All Disclosure Requests received by Tech Mahindra shall be reviewed to ensure consistency with the principles set out in this document to ensure:

7.1.1. the Disclosure Request is consistent with the basic procedural requirements set out in section 4; and

7.1.2. any disclosure of information would be compatible with the privacy considerations set out in section 5.

## 8. Challenging Requests

8.1. Unless compelled to do so by law, Tech Mahindra will only disclose information in response to a Disclosure Request where the validity of the request has been confirmed by reference to the factors set out in this Policy. Any Disclosure Request that is not legally valid and binding on Tech Mahindra will be resisted in accordance with applicable law.

8.2. Tech Mahindra may at any time resist or challenge a Disclosure Request where (without limitation): (i) disclosure would be contrary to interests which Tech Mahindra wishes to protect or preserve; (ii) there are other improprieties or irregularities with the request; (iii) personal data have been requested which are of a particularly sensitive or unusual nature, in the context of the request; or (iv) Tech Mahindra

has made a contractual commitment to a customer or other interested third party to resist or challenge requests in a particular context.

8.3. Where required to do so by contract or applicable law, or where otherwise determined by Tech Mahindra to be appropriate, Tech Mahindra may assist a customer or individual to exercise rights of redress with respect to a government agency.

## 9. Training and Guidance

9.1. Tech Mahindra will provide training to staff members who deal with Disclosure Requests, in order to ensure that they are familiar with the requirements of this document, and with local law privacy considerations in their jurisdiction as these relate to Disclosure Requests.

9.2. Tech Mahindra's Data Protection Officer for the EU and UK has been consulted on the preparation of this Policy and can be contacted in relation to Disclosure Requests involving data originating from those jurisdictions.

**Annex - Template form**

Law enforcement agencies wishing to make a Disclosure Request should be asked to complete Part 1 of the form set out below (or provide sufficient information to the Tech Mahindra response team to be able to complete the details on this form). This information is required to allow Tech Mahindra to properly validate the request. Part 2 of the form should be completed by Tech Mahindra in relation to whether the internal procedures have been followed.

Where the law enforcement agency refuses to use this form, the information provided in Part 1 should be checked against the information requested on this form.

| **Government / Law Enforcement Information Request**<br><br>**This request will be reviewed in accordance with Tech Mahindra's Global Privacy Policy for Government and Law Enforcement Data Access Requests.** | |
|---|---|
| **Part 1: to be completed by Government or Law Enforcement Agency** | |
| **Government or Law Enforcement Agency** | **Country**: |
| | **Agency Name**: |
| **Requesting Officer** | **Name & Title/Rank**: |
| | **Contact details, including official Government or Law Enforcement Email Address**: |
| **Case Context** | **Case Date & Location**: |
| | **Case Type & Overview:** |
| **Information Context** | **Purpose of the request.** Please (i) explain the purpose for the request; and (ii) explain why the requested information is necessary for this purpose:<br>[*Examples of potential purposes include:*<br>- *The prevention or detection of crime;*<br>- *The apprehension or prosecution of offenders;*<br>- *The assessment or collection of a tax duty or an imposition of a similar nature.* ] |

| | |
|---|---|
| | **Information Requested from Tech Mahindra.** (Note: Information requested should be as specific as possible relative to the case context) |
| | **Legal Basis for Request.** (Requesting officer should indicate a specific provision in their domestic law, for example the relevant article or section of an Act which authorizes the collection of information from a third-party entity such as Tech Mahindra for the purposes of prevention, detection or investigation of offences): |
| **Method of disclosure** | **a) Form**<br>• Via secure file transfer protocol to the following location:<br>• Via (registered) post<br>• Via encrypted e-mail<br>**b) Please identify any authorized recipients other than the officer completing this form, and provide their law enforcement contact details:** |
| **Right of redress** | **Please identify the mechanism available for an interested party (Tech Mahindra; its customer; an underlying data subject) to issue a complaint or challenge regarding the Request or the subsequent use of the data by the Law Enforcement Agency.** |
| **Signature of requesting officer:** | **……**<br>**Date: ……** |

| Part 2 : to be completed by Tech Mahindra | |
|---|---|
| **Lawful basis (relevant where Tech Mahindra is acting as a data controller, including where a legal obligation applies to Tech Mahindra as a data processor)** | Indicate which lawful basis Tech Mahindra will be able to rely on to support this disclosure:<br><br>☐ Tech Mahindra's legitimate interest in assisting with the prevention and detection of crime by facilitating a lawful government request<br>☐ Compliance with a legal obligation that applies to Tech Mahindra (for example, a court order requiring disclosure). Please give details of the obligation: …<br>☐ Other. Please specify… |
| **Privacy Considerations** | Confirm that each of the following privacy considerations (as explained in further detail in the Global Privacy Policy for Government and Law Enforcement Data Access Requests) has been taken into account when considering this request:<br><br>☐ Notice;<br>☐ Necessity;<br>☐ Minimization;<br>☐ Accuracy;<br>☐ Security. |
| **DISCLOSURE: YES/NO** | Yes, all formal conditions are met and request is well motivated<br><br>No, because:<br><br>• requested information is not available to Tech Mahindra<br>• request is disproportionate<br>• request should be made to [other third party]<br>• other reason ….<br><br>No, because the following additional information is needed: |