MOTT MACDONALD

# Data Protection Terms for Moata

## 1 Introduction

1.1 We recognise the importance of keeping safe and secure any Personal Information which we Process on behalf of our customers in providing our services. In particular, we hold certain accreditations to the following recognised security frameworks: the National Cyber Security Centre's CyberEssentials+ accreditation and ISO27001. We also proactively pursue a security improvement roadmap for Moata.

1.2 These are our Data Protection Terms for Moata and should be read in conjunction with our General Terms. They set out the data protection-related terms and conditions that apply, and form part of, a Contract between you and us for Moata Services.

1.3 Words and expressions defined in our General Terms have the same meaning in these Data Protection Terms. In addition, words and expressions defined in these Data Protection Terms have the following meanings:

**Controller** means a person which, alone or jointly with others, determines the purposes and means of the Processing of Personal Information;

**Data Protection Laws** means all laws and regulations relating to the Processing of Personal Information as the same may be in force from time to time, including any such laws and regulations set out in our Local Contract Terms;

**Data Subject** means the individual to which the Personal Information relates;

**Information Notice** has the meaning given in Section 4.2;

**Personal Information** means any information relating to an identified or identifiable living individual;

**Personal Information Breach** means the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Information;

**Processing** means any operation or set of operations which is performed on Personal Information or on sets of Personal Information, whether or not by automated means, and **Process**, **Processes** and **Processed** shall be construed accordingly;

**Processor** means a person which Processes Personal Information on behalf of a Controller; and

**Sub-processors** has the meaning given in Section 3.6.

## 2 These Data Protection Terms

2.1 These Data Protection Terms shall automatically apply to, and form part of, a Contract and shall survive the termination or expiry of the Contract.

## 3 Where we are your Processor

3.1 The performance by us of our obligations under a Contract will require us to Process Personal Information on your behalf. In such circumstances:

(a) you alone will determine the purposes for which and the manner in which Personal Information will be Processed by us on your behalf under the Contract;

(b) you will be the Controller in respect of all such Personal Information; and

(c) we will be your Processor in respect of all such Personal Information.

3.2 In respect of a Contract, and except as otherwise agreed between you and us in writing (in the Order Form or otherwise), the particulars of any Processing to be carried out by us on your behalf under the Contract will, in respect of each of the Moata Services, be as set out in Appendix A to these Data Protection Terms.

3.3 Where, under or in connection with a Contract, we Process Personal Information on your behalf:

(a) we will comply with our obligations as a Processor under the Data Protection Laws to which we are subject;

(b) you will comply with your obligations as a Controller under the Data Protection Laws to which you are subject and ensure that your transfer of the Personal Information to us, and our Processing of the Personal Information in accordance with the Contract, complies with the Data Protection Laws to which you are subject;

(c) we will Process the Personal Information only: (**i**) on your written instructions (which include the terms and conditions of the Contract, and which may constitute specific instructions, or instructions of a general nature, as set out in the Contract or any other document agreed between you and us in writing pursuant to or in connection with the Contract) and to the extent reasonably necessary for the performance by us of our obligations under the Contract. We will inform you if, in our opinion, Processing the Personal Information in accordance with a written instruction received from you or in the performance of our obligations under the Contract infringes the Data Protection Laws to which either you (in your capacity as a Controller) or we (in our capacity as a Processor) are subject; or (**ii**) as otherwise required by applicable law, in which case we will inform you of that legal requirement before Processing the Personal Information (unless that law prohibits us from informing you);

(d) we will ensure that all persons authorised by us to Process the Personal Information: (**i**) Process the Personal Information in accordance with the provisions of this Section 3; and (**ii**) are under an appropriate contractual or other legal obligation to keep the Personal Information confidential;

(e) we will, taking into account the nature, scope, context and purposes of the Processing and the risks to Data Subjects, implement appropriate technical and organisational measures that look to: (**i**) ensure the security of the Personal Information; and (**ii**) prevent Personal Information Breaches. Details of the security and other arrangements that the Mott MacDonald Group has in place in respect of Moata is available in Appendix B of the latest version of these Data Protection Terms, which is available on our website for Moata;

(f) we will, taking into account the nature of the Processing, implement appropriate technical and organisational measures to assist you to comply with your obligations under the Data Protection Laws to which you are subject to respond to requests from Data Subjects to exercise their legal rights in relation to their Personal Information;

(g) we will, taking into account the nature of the processing activities and the information available to us, assist you to comply with your obligations in respect of such Personal Information under the Data Protection Laws to which you are subject in relation to: (**i**) keeping Personal Information secure; (**ii**) dealing with Personal Information Breaches; (**iii**) carrying out data protection impact assessments; (**iv**) dealing with requests from Data Subjects to exercise their legal rights in relation to their Personal Information; and (**v**) investigations and enquiries by data protection regulatory authorities;

(h) we will notify you without undue delay after becoming aware of a Personal Information Breach in respect of the Personal Information;

(i) we will, at your option, and to the extent technically possible, permanently and securely delete or return to you all the

Personal Information promptly on termination of the Contract, and delete any existing copies of the Personal Information (except to the extent that we are required to retain copies of the Personal Information by any law to which we are subject), in each case on the basis set out in the further terms and conditions of the Contract; and

(j) we will conduct audits of the systems/solutions we use to Process Personal Information as your Processor under the Contract on a periodic basis. Upon request, we will make available a summary of the key findings of our latest audit, to you once we have received and reviewed the report, except that we may redact (and we are not required to disclose) any commercially sensitive or confidential information, or any information that might jeopardise the security or integrity of our systems, solutions or services. Any material issues identified by the audit will be addressed by us. In addition to the audits we undertake, we will make available to you all information necessary to demonstrate compliance with our obligations under this Section 3 that you, acting reasonably, request from us from time to time. To the extent that our audit reports or summaries, and the information we make available to you in response to any questions you ask, do not provide sufficient evidence of our compliance with this Section 3, then you, or a qualified and independent auditor of your choosing that is also acceptable to us, may audit our compliance with this Section 3. The date, timeframe and scope of any such audit will be mutually agreed by you and us. In addition, any such audit shall be undertaken at your cost and you agree to reimburse us for any time and expenses we incur preparing for, and participating in, your audit. The audit must be undertaken remotely on not less than 45 days' prior written notice. You shall also ensure that the audit is undertaken in compliance with our security and confidentiality requirements, as notified by us to you, which you acknowledge are necessary to protect the confidential and Personal Information of the Mott MacDonald Group and our other customers as well as the security and integrity of our systems, solutions and services. You will provide a copy of the results of your audit to us within 20 Business Days of its completion and we may share the same within the Mott MacDonald Group and with our respective service providers and professional advisers (including technology and data security providers, lawyers and consultants).

3.4 We may charge you for the time and expenses incurred by us in providing any assistance required by you pursuant to Sections 3.3(f), 3.3(g), 3.3(i) and/or 3.3(j). Such charges will be calculated at our standard rates, which we will confirm to you at the time of any such request. Our expenses will be recharged at cost. We will invoice you for such amounts, together with any applicable VAT, and you must pay any such invoice within 30 days of its date of issue.

3.5 We shall not, in respect of a Contract, be liable to you for any failure to provide the Moata Services to the extent that such failure is due, either directly or indirectly, to complying with an instruction from you pursuant to Section 3.3(c) or the Data Protection Laws to which either we or you are subject.

3.6 We may engage third party Processors to Process Personal Information on your behalf (**Sub-processors**) in the course of performing our obligations under a Contract and providing the Moata Services. These Sub-processors may be other members of the Mott MacDonald Group, or third party organisations – such as hosting and other services providers. Notwithstanding any other provision of the Contract, we will remain fully liable and responsible to you subject to and in accordance with the Contract for all acts and omissions of the Sub-processors in relation to their Processing of the Personal Information.

3.7 A list of the Sub-processors currently used by us in respect of each Moata Service, and which are approved by you, are set out in Appendix A to these Data Protection Terms. Where we engage an additional or replacement Sub-processor to Process Personal Information on your behalf, we will notify you (by email or any other means) of the change before the Processing starts.

3.8 You agree that we and our Sub-processors may transfer or Process Personal Information on your behalf outside of the country where we are established. We will ensure that any such transfer or Processing is conducted in accordance with the requirements of the Data Protection Laws to which you are subject in respect of international transfers. In particular, before sharing any Personal Information across international borders, we will ensure that appropriate safeguards are in place. Those safeguards will normally include, without prejudice to our foregoing obligations, data encryption, role-based access permissions, and legal agreements that facilitate the lawful cross-border transfer of Personal Information.

3.9 We may terminate a Contract (or part of it, such as your subscription to a particular Moata Product or the provision of a particular set of Moata Consultancy Services) with immediate effect by giving you notice of such termination in the event that you: (**i**) object to our use of any Sub-processor; or (**ii**) give us any instruction in relation to the Personal Information that we Process on your behalf that is incompatible with the Contract or the Moata Services that we provide to you under the Contract.

## 4 Where we are a Controller

4.1 In respect of a Contract, we are the Controller of the Personal Information we Process in relation to the management of the Contract and the administration of our business relationship with you. This means that we are responsible for ensuring that we comply with all Data Protection Laws to which we are subject when Processing such Personal Information.

4.2 We are committed to data protection compliance and this Section 4 and our privacy notices (together, our **Information Notice**) provide detailed information about how we Process Personal Information as a Controller.

4.3 In particular, this Section 4 provides a high-level summary of some of the key ways that we Process Personal Information as a Controller in respect of Moata. To find out about this in more detail, please refer to our privacy notice for Moata, which is available at: https://www.mottmac.com/article/73313/digital-solutions-privacy-notice-moata. Our privacy notice for Moata is also supplemented by our online tracking technologies privacy notice, which is available at: https://www.mottmac.com/online-tracking-technologies-privacy-notice).

4.4 The Personal Information that we Process in connection with the management of a Contract and the administration of our business relationship with you includes information such as:

(a) personal identification information – for example: name, title;

(b) contact information – for example: email, phone number (if volunteered);

(c) account login information – for example: login ID, other information used to access and/or secure our digital solutions;

(d) any other information you or any of your Users volunteer – for example: feedback, opinions, information provided in survey and questionnaire responses; and

(e) information relating to your Authorised Users' use of Moata and the Moata Products – please see Section 4.5 below for more information.

4.5 The main purposes for which we Process Personal Information as a Controller include to: (**i**) manage our business relationship with you, including to manage and administer your account and subscription for Moata Services under a Contract; (**ii**) conduct project management activities and provide support; (**iii**) respond to queries and other communications; (**iv**) promote Moata and our services, where relevant and appropriate ; and (**v**) comply with our legal and regulatory requirements and respond to legal

claims. We may also Process the Personal Information of Authorised Users and the individuals through whom we conduct our business relationship with you for marketing purposes. Where we do this, we will do so in compliance with all relevant marketing and data protection laws. To find out more about the Personal Information we Process as a Controller and why, please refer to our privacy notice for Moata, which is available at: https://www.mottmac.com/article/73313/digital-solutions-privacy-notice-moata.

4.6 Moata and the Moata Products also allow us to track and monitor: (**i**) the geographic region/area from which Authorised Users access and use Moata and the Moata Products and, where applicable, the type of internet browser that is being used to access such services; and (**ii**) how and when, and how often, Authorised Users access and use the Moata Products – including, by way of example, the type of pages, features and functions that Authorised Users click on and use (as applicable), and how often Authorised Users access and use those pages, features and functions. We use this information to: (**i**) understand how and where Moata and the Moata Products are being used and to provide, develop and enhance our products, services and solutions (for example, we monitor usage to identify potential problems with Moata and the Moata Products (such as slow response) or usage that breaches our Terms); and (**ii**) inform discussions with our customers about their product, service and solution needs and the contractual arrangements we have in place with them. We do this through: (**i**) the collection of information such as the user and login credentials of Authorised Users, IP addresses and the data created through the use of Moata and the Moata Products; and (**ii**) the use of cookies and other data collection and monitoring tools/technologies. Please see our online tracking technologies privacy notice for further information about cookies and other similar technologies that we use, which is available here: https://www.mottmac.com/online-tracking-technologies-privacy-notice.

4.7 Where you or any of your Users provide any Personal Information to us under or in connection with a Contract, you shall: (**i**) make sure the information is accurate and, where necessary, up to date; and (**ii**) inform each relevant individual that you (or someone on your behalf, such as the relevant Subcontractor) is giving their Personal Information to us and that their information will be Processed by us in the manner and for the purpose described in the Information Notice, unless applicable data protection laws allow us to Process that individual's Personal Information in line with the Information Notice without such information being given to the individual.

4.8 You acknowledge and agree that: (**i**) we will assume that we may Process all Personal Information that you or your Users provide to us in accordance with the Information Notice; and (**ii**) accordingly, you shall (and shall ensure that your Users shall) only provide to us Personal Information that we can Process in accordance with the Information Notice. In addition, and in order to help us to use only the Personal Information that we need for the purposes for which we Process such information, you shall (and you shall ensure that your Users shall) only provide to us the Personal Information that we specifically ask you and/or your Users to share with us.

4.9 If you or any of your Authorised Users have any questions in relation to our use of Personal Information, you or your Authorised Users may contact us at privacy@mottmac.com.

MOTT MACDONALD

## Appendix A: Particulars of Processing and Sub-processors

**Particulars of Processing**

The particulars of Processing to be carried out by us on your behalf under or in connection with a Contract are set out in the table below:

| Particular | Explanation |
|---|---|
| **Subject matter and duration of the Processing** | We have contracted with you to provide certain of our Moata products and/or consultancy services to you and your Users. As part of these arrangements, we will Process Personal Information controlled by you as your Processor.<br>The Personal Information that we Process in connection with the provision of the Moata Services and the performance of our other obligations under a Contract will be determined by you – for example, based on the Customer Data uploaded by you (or by a person on your behalf, such one of your Users) into Moata and the Moata Products.<br>In respect of a Contract, we will Process such Personal Information: (**i**) for the duration of the Contract; and (**ii**) for the period after the termination or expiry of the Contract during which we have any surviving obligations that require us to Process such Personal Information or you continue to store such information on our systems. |
| **Nature and purpose of the Processing** | In respect of a Contract, we will Process Personal Information only to the extent necessary for the purpose of the provision of the Moata Services and in performing all other obligations under and in accordance with the provisions of the Contract. |
| **Categories and types of Personal Information being Processed** | The types of Personal Information being Processed by us under a Contract will be determined by you and may (depending on the product(s) and/or services for which you subscribe) include:<br>• Non-special categories of Personal Information – including:<br>  ○ Property or asset information: land or property ownership information, photographs and/or footage of property as part of surveys or other client project related activities, details of other property owners. For example, if as part of the project you are looking to acquire land, you may require us to Process information on who owns that land;<br>  ○ Project-related information: including information on persons that have rights or interests in such projects (including objectors and complainants). For example, if you are undertaking a consultation process, you may need us to Process information relating to the parties that need to, or have been, consulted;<br>  ○ Information relating to the persons involved in each project, including: availability, professional qualifications, registrations and experience and work tasks. For example, as part of the Moata Land Management product survey module, you may need us to Process information on which surveyors are available to carry out works and the credentials of such persons;<br>  ○ Individual information, openly-available or where provided and input by you, as part of an inventory or asset management system or process, for example; and<br>  ○ Any other non-special category information you volunteer and input. For example, personal details including first names, last names, email addresses and phone numbers.<br>• Special category or other sensitive types of Personal Information and/or criminal convictions or offence Personal Information, subject to our prior agreement in writing to our Processing of such information in accordance with the General Terms. For example, Personal Information: (**i**) revealing racial or ethnic origin; (**ii**) revealing political opinions; (**iii**) revealing religious or philosophical beliefs; (**iv**) revealing trade union membership; (**v**) revealing genetic data; (**vi**) revealing biometric data; (vii) concerning health matters; (**viii**) concerning a person's sex life; (**ix**) concerning a person's sexual orientation; (**x**) concerning a person's criminal offences or convictions; or (**xi**) concerning persons under the age of 18. Where you or any of your Authorised Users upload information of this nature, you must inform us immediately. |
| **Categories of Data Subjects** | In respect of a Contract, the category of Data Subjects to which the Personal Information relates will be determined by you.<br>It will include staff such as employees, directors, volunteers, agents, temporary and casual workers and other personnel engaged by you or your Subcontractors.<br>It will include any person whose Personal Information is included in the documents and other materials in respect of which you use our services and solutions.<br>Example categories of Data Subject may include: staff including volunteers, agents, temporary and casual workers; suppliers; complainants, objectors, correspondents and enquiries; land owners; persons that have rights over land; persons who work for or are associated with government, public authorities, NGOs, charities, protest and pressure groups, campaigners and any other persons involved in or in any way concerned with infrastructure projects of any nature. |

**Approved Sub-processors**

The following persons are, in respect of a Contract, approved as Sub-processors of Personal Information:

| Sub-processor(s) | Purpose(s) | Location(s) | Additional Information |
|---|---|---|---|
| **Other members of the Mott MacDonald Group** | Where, for the purposes of providing the Moata Services to you via leveraging a global team, we may need to share Personal Information with other members of the Mott MacDonald Group. | Global – our registered companies can be found here: Registered Companies - Mott MacDonald. More information available upon request in relation to specific Contract. | Primarily, we deliver services out of the UK, US, Australia and New Zealand. By default, the team servicing your deployment will be the one in the most appropriate time-zone or the same location as the project. |
| **Microsoft Corporation and its affiliates** | Microsoft Azure for the purposes of hosting and data storage. | United Kingdom by default. | Information in relation to how Microsoft processes personal information and associated security controls can be found here: Microsoft Service Trust Portal |
| **Bentley Systems, Incorporated and its affiliates** | Processing customer login information in relation to Moata Intelligent Content via Bentley Connection Client or website. Applicable only where you subscribe for Moata Intelligent Content. | United Kingdom and United States. | Information in relation to how Bentley Systems processes personal information can be found here: Data Processing Addendum \| Bentley Systems and GDPR Compliance Statement \| Bentley Systems. Associated security controls and accreditations can be found here: Trust Center \| Bentley \| Infrastructure Engineering Software |
| **Zendesk, Incorporated and its affiliates** | Processing of customer service (support) tickets, where you or your Users may raise and ask us to resolve certain technical issues. | European Economic Area (EEA). | Hosted by Amazon Web Services (AWS). |
| **Environmental Systems Research Institute, Incorporated and its affiliates, including Esri Global, Incorporated** | Processing your and your Users' login information where we provide certain integrations with the Esri variant of our Moata Geospatial product, in particular, with ArcGIS Online. | United States by default. | Information in relation to how Esri processes personal information can be found here: General Data Protection Regulation (GDPR) \| Esri. Associated security controls and accreditations can be found here: Esri Managed Cloud Services—ArcGIS Trust Center \| Documentation |
| **Google** | We collect anonymised usage data (via cookies and similar technologies) through Google Analytics in order to detect issues and improve the performance of our services. | United States and Europe | N/A |
| **Amazon Web Services** | Certain time-series, predictive modelling and spatial analytical capabilities ("analytical engine") used within some Moata Products. | Australia | Hosted by Amazon Web Services (AWS). GDPR - Amazon Web Services (AWS) |

**Appendix B: Technical and Organisational Security Controls:**

We are committed to ensuring the secure processing of personal information in accordance with Data Protection Laws. We recognise the importance of protecting the privacy and confidentiality of individuals' personal data and have implemented a comprehensive set of organisational and technical controls to safeguard this information.

**Organisational Controls:**

Data Protection Officer (DPO): We have appointed a dedicated Data Protection Officer responsible for overseeing our data protection activities, ensuring compliance with Data Protection Laws, and acting as a point of contact for data subjects and supervisory authorities. They are reachable at privacy@mottmac.com. We are registered with the Information Commissioner's Office, registration number: Z5496409. A copy of the registration certificate can be provided upon request.

Data Protection Policies: We have developed and implemented comprehensive data protection policies and procedures that outline the principles, responsibilities, and obligations for handling personal information. These policies are regularly reviewed and updated to reflect any changes in applicable data protection laws and regulations. Our policies are available on our website: Our policies - Mott MacDonald. A commitment to "Respecting privacy and data protection" is also included in the Protecting our assets and reputation section of Our Code.

Management Systems: We have a robust information security management system (ISMS) and hold an accreditation to ISO27001, as well as NCSC Cyber Essentials +, and run regular internal and external audits in relation to our controls and their implementation.

Employee Training and Awareness: We provide regular training and awareness programs to our employees, emphasising the importance of data protection, their responsibilities in handling personal information, and the procedures they should follow to ensure its security. All Mott MacDonald employees and temporary workers must complete mandatory privacy and data protection training on an annual basis, within 30 days of commencing employment at Mott MacDonald.

Data Processing Agreements: We have established data processing agreements (DPAs) with our clients and other relevant third-party service providers to clearly define the responsibilities and obligations of each party in relation to the processing of personal data. These agreements include provisions to ensure that personal data is processed securely and in compliance with applicable data protection laws. We also have appropriate intra-group transfer agreements based on the relevant set of "Standard Contractual Clauses" approved by the European Commission.

Data Privacy Impact Assessments: We maintain appropriate data privacy impact assessment(s) (DPIAs) for high-risk processing activities to enable the implementation of appropriate controls and risk mitigation measures.

Service Provision and Vendor Management: We leverage service providers and vendors with a demonstrated track-record in the industry. Our services are provisioned through assured platforms – in particular Microsoft Azure (more information can be found here: Microsoft Service Trust Portal). We exercise due diligence procedures in any procurement exercises and ensure appropriate safeguards are in place where we utilise any sub processors.

Business Continuity: We maintain processes and technical measures ensuring redundancy in our systems and business operations, assuring we can maintain business continuity in the event of a disruption.

**Technical Controls:**

Data Encryption: We utilise encryption techniques to protect personal data during transmission and storage. This includes the use of industry-standard encryption protocols for data in transit, such as Transport Layer Security, and encryption at rest for data stored in databases or other storage systems. We adopt an API-first approach, which ensures data transfers between our services utilise secure HTTPS (SSL/TLS) encryption at all times.

Access Controls: We enforce strict access controls to limit access to personal data only to authorised individuals who have a legitimate need to access it, including supporting single sign-on (SSO) and multifactor authentication (MFA). Access is granted based on roles and responsibilities, role-based-access-controls (RBAC), and we regularly review and update access privileges to ensure they are appropriate and aligned with the principle of least privilege. Administrative access controls are automatically deprovisioned periodically. We utilise Microsoft Azure B2C as our identity provider, though which all exposed service end-points are authenticated using the secure OAuth2.0 standard.

Data Management: As a minimum, we logically separate all customer data and maintain appropriate measures to prevent data of one customer being exposed or accessed by another customer. We implement monitoring & logging mechanisms to trace data accessibility, where appropriate, to support identification of any suspicious activity with respect to access to personal information. Where personal data is used for any testing and development, we implement appropriate safeguards such as data masking and anonymisation. We regularly perform data backups and implement a robust disaster recovery plan to ensure availability and integrity of personal information in the event of system failures.

System and Network Security: We have implemented robust security measures to protect our systems and networks against unauthorised access, malicious activities, and other security threats. These measures include firewalls, intrusion detection and prevention systems, regular vulnerability assessments, and security patching. We perform regular penetration testing across our products, along with static code and vulnerability assessments.

Incident Response and Breach Notification: We have established an incident response plan to effectively manage and respond to any security incidents or breaches involving personal data. This includes procedures for promptly investigating incidents, mitigating their impact, and notifying relevant parties, including data protection authorities and affected individuals, as required by the Data Protection Laws. In parallel with our Moata incident support, we run a dedicated ServiceNow service and Security Operations Centre where security incidents can be reported to a team monitoring this 24 hours a day, 7 days a week.

Data Minimisation and Retention: We implement data minimisation principles to ensure that personal data is only collected and processed for specific and legitimate purposes. We retain personal data only for as long as necessary to fulfil the purposes for which it was collected or as required by applicable laws and regulations.

Device security: Our organisation does not support the use of removable media. All devices are controlled and maintained by a centrally managed service, ensuring relevant security updates are enforced within appropriate timescales. Internal storage media are fitted with device encryption (e.g. BitLocker) to prevent misuse in the event a device is lost or stolen.

These organisational and technical controls are regularly reviewed, tested, and updated to adapt to evolving security risks and changes in the regulatory landscape. By implementing these measures, we aim to ensure the secure processing of personal information and demonstrate our commitment to protecting the privacy and rights of individuals as outlined in the Data Protection Laws.