



MMGEIS

MASTER MENTORS GEO-ENABLING INDIAN SCHOLARS

Privacy Statement

Regardless of whether you are a user or a visitor to Master Mentors Geo-Enabling Indian Scholars ('MMGEIS') website (hereinafter referred as 'MMGEIS', 'we', 'us' or 'our'), or someone we deal with in our day to day business, we respect the privacy of individual/visitor and are committed to take reasonable precautions to protect information consisting of Personal information and 'Sensitive Personal Data or Information' (SPDI) ("Information") of visitors of this MMGEIS website and comply with all legal, regulatory and/or contractual obligations related to privacy. This statement highlights our privacy practices regarding Personal Information that we collect and store about you through this website, www.mmgeis.in (the 'Site') and also for those Personal Information that you provide us while participating in our program, events and campaigns.

Additional information on our personal data practices may be provided in contractual agreements, supplemental privacy statements, or notices provided to you prior to or at the time of collection of your personal data. For the purpose of this Policy, any reference to "Program" is a reference to all the educational and/ or learning program and associated events and/ or campaigns offered by MMGEIS, whether available online or offline, and any reference to 'Site(s)' is a reference to any of the MMGEIS' websites (including any mobile version of such websites).

Our use of your personal data is governed by this Policy as it may be updated from time-to-time. Your use of our Site(s) or Program, and any dispute over privacy, is subject to this Policy and our Terms of Use (which are incorporated by reference into this Policy) and any written contract for Program between you and us or any person who provides you with access to our Program. Depending upon your interactions with MMGEIS, other terms may also be applicable to you and our use of your personal data. By using our Site(s) or Program you are contracting with MMGEIS C/o Centre for Knowledge Sovereignty, A 99, Sector 47, Noida, Uttar Pradesh – 201301.

How to contact us

Our postal address for any questions is:

Information Officer– Data Protection and Privacy
MMGEIS C/o Centre for Knowledge Sovereignty,
A 99, Sector 47, Noida, Uttar Pradesh – 201301
Our email address for any questions is: info@mmgeis.in

Personal data we collect about you and how we collect it

Account Information: Contact and related information that allows us to communicate with you. We obtain this information when you visit our Site(s) and/or register to any of our Program or to receive information about our Program. We collect or receive information from you when you sign up for our Program, create an online account with us, make an enrolment, request details or a call back, submit a technical, user or billing support request, participate in a contest or survey, provide us with feedback or otherwise contact us. The type of information that we collect depends on your interaction with us, but may include, your name, address, telephone number (business or personal), email address (business or personal), postal/billing and communication address (business or residential), and any other information that you choose to provide or is necessary for us to deliver the services to you.

Information related to your commercial and non-commercial relationship with us, such as the services we provide to you, the telephone numbers you call and text, your payment history, your credit history, your credit card numbers, social security number (where permitted by law), security codes and your service history.

Technical & Usage Information related to the services we provide to you, including information about how you use our networks, services, products or websites. Some examples include:

- **Equipment Data:** Information that relates to and identifies the equipment on our and your networks that you may use or with which you interface for the services you are receiving. Information might include equipment type, device identifiers, device status, serial numbers, settings, configuration, and software type.
- **Network Performance & Usage:** Information about the operation of the equipment, services and applications you use on our networks. Examples of this might include: wireless device location and type; call records including where a call was made from and to as well as its date, time, duration and cost (call records for queries, tickets etc. submitted by you, for quality and monitoring purposes only); the number of text messages sent and received; voice minutes used; bandwidth used and similar information (though We also collect information like transmission rates and delays, data associated with remote monitoring services and security characteristics, and information about your use of our interconnected voice over internet protocol (VoIP) services (including services purchased offline).
- **Web Browsing & Mobile Application Information:** such as IP addresses, URLs, data transmission rates, and delays. We may also receive information about the pages you visit, the time you spend on them, the links or advertisements you see, click on and follow, the referring URL or the webpage that led you to our Sites, the search terms you enter, how often you open an application, how long you spend using any downloaded app and other similar information. Please see the section "Our Use of Cookies and other Tracking Mechanisms" below for more information on this. We may also have access to personal data contained in applications and other features of your mobile device if you expressly permit us to do so while you are using any of our applications on that device.
- **Location, direction and journey information:** this will be collected based on any connected device you may use our services on. It includes your ZIP/postal code and street address, as well as the whereabouts of your wireless device. Location Information is generated when your device communicates with cell towers, Wi-Fi routers or access points and/or with other technologies. Any connected device that you own, or which is otherwise linked to you will generate such information that will then be associated with you.
- **Video footage/images:** when you visit our premises, we may also collect information about you on CCTV as part of our security and crime prevention measures.

We may collect the above personal data in the course of providing services to you or to someone who has provided you with access to our services. We may obtain this information in a number of ways, for example:

- directly from you: for example, when you or someone on your behalf enrolls to the Program or provide your details in order to register/ subscribe to our Program, submit a web enquiry or set up an account with us;
- automatically: when personal data is generated through your use of our services or our Sites; and
- from third party sources: we sometimes collect personal data about you from trusted third parties, in connection with services that we provide to you or propose to provide to you, where appropriate and to the extent we have a justified basis to do so. These include fraud-prevention agencies, business directories, credit check reference/vetting agencies and connected network providers. Anyone who provides you with access to your services may also provide us with your personal data in that context.

We may combine the personal data that we receive from such other sources with personal data you give to us and with information we automatically collect about you, for example where we need to run a credit check, and then compile a profile of you based on the credit check data and the personal data you have provided.

How do we use the personal data we collect?

We set out below some of the ways in which we process personal data:

- to fulfil obligations under contract. This includes providing our services to you; to communicate with you about your use of our services; to obtain and process payment from you and to fulfil your enrolments and any obligations on us relating to those Program;
- for the purpose for which you specifically provided the information to us, including, to respond to your inquiries, to provide any information that you request, to address technical support tickets, and to provide service support;
- to make our Program and communications more relevant to you, including generating participant profiles, delivering customized content to you, to offer location customization, personalized help and instructions, and to otherwise tailor your experiences while using our Sites or our services;
- to better understand how users and other third parties access and use our Sites and Program, both on an aggregated and individualized basis;
- to administer, monitor, improve and customize our Sites and Program, for our internal operations, including troubleshooting, network management and network optimisation, research and analytical purposes, so that we can provide our users with a better experience;
- to investigate, prevent or take action regarding illegal activities, fraud, threats to our property or personnel and violations of our Terms of Use and/or applicable law and also to meet our legal and regulatory obligations;
- to notify you about our new Program releases and service development, alerts, events, updates prices, terms, special offers and associated campaigns and promotions (including via newsletters). Therefore, we and selected third parties may use your personal data to send you marketing communications about services based on your preferences and interest. You have a choice and can object to our use of your personal data for marketing purposes. When we are required by law to do so, we will obtain your consent before using your personal data for marketing purposes. If you do opt out, we will stop sending you marketing communications, but we will continue sending you non-marketing communications that relate to the services you are using (for example billing information, software update communications, password resets etc);

- if you attend an event, we may process information about you gathered in relation to the event and may share information about your attendance with your company. We may also permit designated event partner or conference sponsors to send you communications related to the event if you have shared your contact information at the event. Please note that sponsors from other companies may directly request information about you at their conference booths or presentations, and their use of your personal data that you provide to them will be subject to their privacy policies;
- to assist us in advertising our Program in various mediums including, sending promotional emails, advertising our Program on third party sites and social media platforms, direct mail, and by telemarketing;
- where we ask you for specific consent to a use of your personal data, we will use it in the ways we explain at the time of obtaining that consent; and
- in any way required by law, regulation or the public interest such as in response to requests or orders by government or law enforcement authorities conducting an investigation or to respond to an emergency. This use may require us to disclose your personal data including contact details and/or information about your usage of our services to relevant authorities or to block, intercept or otherwise interfere with your use of our services and any personal data generated by that usage. Achieving a balance between, on the one hand ensuring protections for the privacy and other fundamental human rights that may be exercised through use of our services and, on the other, the exercise of lawful investigatory powers for the public good on the other can be complicated. We do not accede to such requests without careful consideration of all the circumstances. Even where we are legally obliged to disclose personal data, we will give careful consideration to the extent to which doing so will infringe on the fundamental rights, including the right to privacy, of any person whose personal data is to be disclosed or intercepted and we take whatever steps are practicable to mitigate and minimise any such infringement.

What lawful reasons do we have for processing personal data?

We may rely on the following lawful reasons when we collect and use personal data to operate our business and provide our services:

- **Contract** – We may process personal data in order to perform our contractual obligations.
- **Consent** - We may rely on your freely given consent at the time you provided your personal data to us.
- **Legitimate interests** – We may rely on legitimate interests based on our evaluation that the processing is fair, reasonable and balanced.

These include:

- **Delivering services to our users** – To deliver the services our users have engaged us to provide.
- **Direct marketing** – To deliver timely market insights and specialty knowledge we believe is welcomed by our users, subscribers and individuals who have interacted with us.
- **Legal obligations and public interests** – We may process personal data in order to meet regulatory and public interest obligations or mandates.

When do we share or disclose your personal data we collect?

Subject to obtaining your consent as may be required in some jurisdictions, we may share or disclose your personal data as necessary for the purposes described above and as further detailed below:

- **Affiliates:** We may disclose the personal data we collect from you to our subsidiaries/affiliates. Where permitted by law and with your consent where required, our affiliates may use your information for the purposes indicated in this Policy, including to market their products and services to you. In processing your personal data, our affiliates follow practices at least as protective as those described in this Policy.
- **Business, Sales and Marketing Partners:** We may offer some of our services together with or through third parties who may be system integrators, resellers, solution partners, network partners and affinity organizations. If we do so, we will need to share your personal data with these third parties to assist in providing and marketing that Service to you, as well as to enable the third parties to market their own products and services to you (with your permission, if required). We may also share your personal data with companies that are system integrators, resellers, solution partners, network partners and affinity organizations, and whom we believe might offer products and services of interest to you (again with your permission, if required).
- **Third-Party Service Providers:** We employ other companies and individuals to perform functions that are necessary for the provision of the services or for any of the purposes described above. Examples include: where permitted, jointly offering a product or service, sending communications, processing payments, assessing credit and compliance risks to give you access to our services, fraud and financial crime prevention detection and prosecution, analysing data, providing marketing and sales assistance (including advertising and event management), user relationship management, providing training, these third parties include; system integrators, resellers, solution partners, network partners, affinity organizations, third party vendors, service providers, contractors or agents, and other carriers or providers that we may disclose personal data to where necessary to provide our services or fulfil your requests or orders, as well as entities that provide website hosting, service/order fulfilment, customer service, and credit card processing, effecting payments, among others. These third-party service providers have access to personal data needed to perform the functions we have entrusted to them but may not use it for other purposes where they process your personal data on our behalf. Whenever we share personal data with third parties, we take steps to ensure that third party contracts contain appropriate protections for your personal data.
- **Business Transfers:** If we are acquired by or merge with another company, or if substantially all of our assets are transferred to another company (which may occur as part of bankruptcy proceedings), we may transfer your personal data to the other company. We may also need to disclose your personal data before any such acquisition or merger, for example to our advisers and any prospective purchaser's adviser.
- **Legal Protection and in Response to Legal Process:** We may disclose the personal data we you hold about in order to comply with applicable law, in response to or to pursue judicial proceedings, court orders and in other legal processes. We may also disclose, transfer or share it when we believe in good faith that disclosure is necessary: to protect or enforce our rights; protect your safety or the safety of others; investigate or prevent fraud; to respond to government requests – including from government and national or international law enforcement authorities outside of your country of residence – or for national security, public safety and/or law enforcement purposes. Personal data shall only be disclosed when we in good faith believe that we are obliged to do so in accordance with the law or that there are compelling reasons of public interest for us to do so. This will only be after a careful evaluation of all legal requirements and other relevant considerations, including any infringement on the fundamental rights to privacy or freedom of expression that might be impacted by the disclosure.

- **Sharing Aggregated and De-Identified Information:** We may use your personal data to create aggregated and anonymised information which we may share with third parties. Nobody can identify you from that anonymised information. In other circumstances we may pseudonymise your personal data before sharing it with a third party so that we can re-associate you with the information once it has been processed and returned to us. Whilst the third party will not be able to identify you from the pseudonymised information, we will still be able to. We treat pseudonymised data as though it were personal data and ensure the same level of protection for it when sharing with third parties.

Where do we transfer your personal data?

Information we hold about you may be transferred to countries:

- where we do business;
- which are linked to your engagement with us;
- from which you regularly receive or transmit information; or
- where our third parties conduct their activities.
- These countries may have less stringent privacy laws than we do, so any information they hold can become subject to their laws and disclosure requirements, including disclosure to governmental bodies, regulatory agencies and private persons. In addition, a number of countries have agreements under which information is exchanged with other countries for law enforcement, tax and other purposes.

We may also transfer your personal data when:

- the transfer is to a country deemed to provide adequate protection of your personal data by the European Commission/ enforcement agencies; or
- where you have consented to the transfer.
- For EU residents, when we, or our permitted third parties, transfer your personal data outside the EEA, we will impose contractual obligations on the recipients of that data to protect your personal data to the standard required in the EEA. We or they may also require the recipient to subscribe to international frameworks intended to enable secure data sharing. If we transfer your personal data outside the EEA in other circumstances (for example, because we have to by law), we will make sure it remains adequately protected.

We may share non-personal, anonymised and aggregated information with third parties for several purposes, including data analytics, research, submissions, thought leadership and promotional activity.

How MMGEIS protects your personal data?

We use a range of measures to ensure we keep your personal data secure, accurate and up to date. These include but not limited to:

- education and training to relevant staff to ensure they are aware of our privacy obligations when handling personal data;
- administrative and technical controls to restrict access to personal data to a 'need to know' basis;
- technological security measures, including fire walls, encryption and anti-virus software;
- we may apply pseudonymisation, de-identification and anonymisation techniques in efforts to further protect personal data; and
- physical security measures, such as security passes to access our premises.

- The transmission of data over the internet (including by e-mail) is never completely secure. So although we use appropriate measures to try to protect personal data, we cannot guarantee the security of data transmitted to us or by us.

What are your data protection rights?

Your data protection rights are highlighted here.

- **Access** – You can ask us to verify whether we are processing personal data about you, and if so, to provide more specific information.
- **Correction** – You can ask us to correct our records if you believe they contain incorrect or incomplete information about you.
- **Erasure** – You can ask us to erase (delete) your personal data after you withdraw your consent to processing or when we no longer need it for the purpose it was originally collected.
- **Processing restrictions** – You can ask us to temporarily restrict our processing of your personal data if you contest the accuracy of your personal data, prefer to restrict its use rather than having us erase it, or need us to preserve it for you to establish, exercise, or defend a legal claim. A temporary restriction may apply while verifying whether we have overriding legitimate grounds to process it. You can ask us to inform you before we lift that temporary processing restriction.
- **Data portability** – In some circumstances, where you have provided personal data to us, you can ask us to transmit that personal data (in a structured, commonly used, and machine-readable format) directly to another company if it is technically feasible.
- **Automated Individual Decision-making** – You can ask us to review any decisions made about you which we made solely based on automated processing, including profiling, that produced legal effects concerning you or similarly significantly affected you.
- **Right to Object to Direct Marketing including Profiling** – You can object to our use of your personal data for direct marketing purposes, including profiling. We may need to keep some minimal information to comply with your request to cease marketing to you.
- **Right to Withdraw Consent** – You can withdraw your consent that you have previously given to one or more specified purposes to process your personal data. This will not affect the lawfulness of any processing carried out before you withdraw your consent. It may mean we are not able to provide certain services to you and we will advise you if this is the case.

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information or to exercise any of your other rights. This helps us to ensure that personal data is not disclosed to any person who has no right to receive it. No fee is required to make a request unless your request is clearly unfounded or excessive. Depending on the circumstances, we may be unable to comply with your request based on other lawful grounds.

Do we use Cookies?

Our Site(s) may use cookies. Where cookies are used, a statement will be sent to your browser explaining the use of cookies. To learn more, please refer to our cookie policy.

How long will MMGEIS retain your personal data?

We seek to ensure that we only keep your personal data for the longest of:

- the period necessary for the relevant activity or services;
- any retention period that is required by law; or
- the period in which litigation or investigations might arise in respect of the services.

Do we link to other websites?

Our websites may contain links to other sites that are not governed by this Privacy Policy. Please review the destination websites' privacy policies before submitting personal data on those sites. Whilst we try to link only to sites that share our high standards and respect for privacy, we are not responsible for the content, security, or privacy practices employed by other sites.

Choice

You have a choice about how MMGEIS should use your personal information to communicate with you, to send you marketing information, to provide you with customized and relevant advertising, and whether you want to stay signed into your account.

Communication Preferences

You can control the methods by which MMGEIS may contact you about your account. You can also control your member-to-member communications, preferences settings and can choose which newsletters and promotions you want to receive.

Marketing

If you do not wish to receive marketing communications from MMGEIS, you can unsubscribe from the link in the email you received, change your communication preferences within MMGEIS, or indicate your communication preferences within the direct communication from us. Keep in mind, MMGEIS does not sell or rent your personal information to third parties for their marketing purposes without your explicit consent.

Changes to this privacy statement:

From time to time we may update this statement. When we do, we will publish the changes on this Site. If you do not agree with these changes, you should discontinue your use of our Site. If material changes are made to this Statement, we will notify users by e-mail or by placing a prominent notice on this Site.

This Privacy Policy was last updated 04 January 2024.

How to contact us, request access to your personal data or contact MMGEIS with questions or feedback?

For Data Protection related questions or feedback:

If you have a question, comment, or complaint or wish to access a copy of your personal data or to correct it if you believe it is inaccurate, you can reach MMGEIS at info@mmgeis.in

For India Data Protection Act related questions or feedback:

If you have a question or a complaint about this Privacy Notice, MMGEIS privacy policy or its information handling practices, you can reach MMGEIS at info@mmgeis.in