

## **GDPR Privacy Policy**

The protection of your personal data is of great importance to Association for Nuclear Technology in Medicine (“ANTM”). This Privacy Policy therefore intends to inform you about how the ANTM, who may act as data controllers or processors, collect and processes your personal data that you submit or disclose to us, in the case where the General Data Protection Regulation ("GDPR") applies to such collection or processing.

ANTM collects, uses, and stores a variety of data, including Personal Data as Secretariat of ITCCIR. ANTM is committed to ensure the privacy of Personal Data throughout its global activities, and make sure its employees and business partners also take the necessary measures to protect Personal Data.

This Privacy Policy sets out the basis on which any personal data we collect from you, or that you provide to us, will be processed by us. Our Privacy Policy applies to you in the case where the GDPR applies to such collection or processing and is available on our website and through other channels. In all your dealings with us you must ensure that others you may represent are aware of the content of our Privacy Policy and consent to you on their behalf.

We encourage you to read this Privacy Policy carefully. If you do not wish your personal data to be used by us as set out in this Privacy Policy, please do not provide us with your personal data. Please note that in such a case, we may not be able to provide you with our services, and your customer experience may be impacted.

### **1. Your Personal Data**

This refers to a combination of personal data such as your name, address, telephone number, email address, travel preference and special needs/disabilities/dietary requirements that you supply us or is supplied to us, including your social preference, activities and any information about other persons you represent such as those on your registration. Your personal data is collected when you contact us, make a registration, use our website(s)/apps, link to or from our website(s)/apps, connect with us via social media and any other engagement we or our business partner have with you.

### **2. Processing of Your Personal Data**

#### **Data processes**

We may collect and process your personal data for the purposes set out below and disclose your personal data to our service providers who act as 'controller' or 'processor' on our behalf. These purposes include:"

- a.** Fulfilling the contract with you and legal obligations (Articles 6(1)(b) and (c) of the GDPR: In order for you to travel abroad, it may be mandatory as required by government authorities at the point of departure and/or destination to disclose and process your personal data for immigration, border control and/or any other purposes. Also we need to provide airlines/accommodation providers/travel agent with your name, passport number, contact details, and other related information in accordance with their terms and conditions. If you do not provide us with this personal data, we might not be able to offer our services to you.
- b.** Fulfilling your and our legitimate interests (Article 6(1)(f) of the GDPR): Where it is in both your and our benefit that we further process your personal data as part of our business administration, maintaining service

quality, customer care, business management, risk assessment/management, security, and operation purposes.

- c. Consent: For marketing purposes and other similar data processes that may require your authorization for their processing (Article 6(1)(a) of the GDPR). We will usually inform you before collecting your data if we intend to use your data for such purposes or if we intend to disclose your personal data to any third party for such purposes. You can exercise your right to prevent such processing by checking certain boxes on the forms we used to collect your data.
- d. Explicit consent (Article 9(2)(a) of the GDPR): Information such as health or religion may be considered 'sensitive personal data' under the GDPR. This personal data might include information necessary to arrange bookings and travel plans, including your allergies, disabilities, and other relevant health information. We collect it to provide you with our services, cater to your needs or act in your interest, and we are only prepared to accept sensitive personal data on the condition that we have your positive consent.

We will process your data for as long as possible in order to fulfil our service to you and comply with the applicable fiscal, tax, securities and commercial law regulations on retention of business and financial documentation.

### **Children**

Our services are intended for adult customers. However, we may knowingly collect and process personal data on children under sixteen (16). On these occasions, we will take account of this event when processing the personal data of children and implementing the legal basis for such processing. For example, where the processing of personal data of children is based on their consent such as the processing of his/her sensitive personal data, we will seek the consent of parents, tutors, or other adults holding parental responsibility over children, if required under the GDPR.

### **Links to other sites**

We may propose hypertext links from our websites to third-party websites or Internet sources. We do not control and cannot be held liable for third parties' privacy practices and content. Please read carefully their privacy policies to find out how they collect and process your personal data.

### **Data transfers**

#### **Service providers**

For the purpose of providing you with our services, including your booking of flight, hotel, security, incident/accident management etc., we may disclose and process your personal data outside of the EEA countries. In order for you to travel abroad, it may be mandatory as required by government authorities at the point of departure and/or destination to disclose and process your data for immigration, border control and/or any other purposes. Also we need to provide airlines/accommodation providers with your name, passport number, contact detail, etc. in accordance with their terms and conditions.

### **Legal compliance and security**

It may be necessary for us — by law, legal process, litigation, and/or requests from public and governmental authorities within or outside your country of residence — to disclose your personal data. We may also disclose

your personal data if we determine that, due to purposes of national security, law enforcement, or other issues of public importance, the disclosure is necessary or appropriate.

We may also disclose your personal data if we determine in good faith that disclosure is reasonably necessary to protect our rights and pursue available remedies, enforce our terms and conditions, investigate fraud, or protect our operations or users.

### **Safeguards to protect your personal data**

Where we share your data with a data processor, we will put the appropriate legal framework in place in order to cover such transfer and processing (Articles 26, 28 and 29). Furthermore, where we transfer your data from EEA to any entity outside the EEA, we will put appropriate legal frameworks in place, notably Binding Corporate Rules (Article 47 GDPR), controller-to-controller (2004/915/EC) and controller-to-processor (2010/87/EU) Standard Contract Clauses approved by the European Commission, in order to cover such transfers (Articles 44 ff. GDPR), or we will share your data based on rules of the GDPR.

By submitting your personal data, you agree to this transfer, storing or processing. We will take all steps reasonably necessary to ensure that your data is treated securely and in accordance with this Privacy Policy, in particular, by adopting Binding Corporate Rules and Standard Contract Clauses where possible.

### **3. Our Records of Data Processes**

We handle records of all processing of personal data in accordance with the obligations established by the GDPR (Article 30), both where we might act as a controller or as a processor. In these records, we reflect all the information necessary in order to comply with the GDPR and cooperate with the supervisory authorities as required (Article 31).

### **4. Security Measures**

We process your personal data in a manner that ensures their appropriate security, including protection against unauthorised or unlawful processing, accidental loss, destruction or damage. We use appropriate technical or organisational measures to achieve this level of protection (Article 25(1) and 32 GDPR).

We will retain your personal information for as long as it is necessary to fulfill the purposes outlined in this Privacy Policy, unless a longer retention period is required or permitted by law.

### **5. Notification of Data Breaches to the Competent Supervisory Authorities**

In case of breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed, we identify it and assess it promptly. Depending on the outcome of our assessment, we will make the requisite notifications to the supervisory authorities and communications to the affected data subjects, which might include you (Articles 33 and 34 GDPR).

### **6. Processing Likely to Result in High Risk to your Rights and Freedoms**

If we identify data processing activities that may result in high risk to your rights and freedoms (Article 35 of the GDPR), we will assess it internally and either stop it or ensure that the processing is compliant with the GDPR or that appropriate technical and organisational safeguards are in place in order to proceed with it.

In case of doubt, we will contact the competent Data Protection Supervisory Authority in order to obtain their advice and recommendations (Article 36 GDPR).

## **7. Your Rights**

You have the following rights:

- Access to personal data: You have the right to be provided full information about your personal data that we hold.
- Data correction: You have the right to require that we correct any incorrect information we hold about you.
- Data deletion: You may also have the right to ask that we delete your personal data. Please note that certain conditions may apply to the exercise of this right.
- Restriction on processing of personal data: You may have the right to ask that we restrict the use of your personal data. Please note that certain may conditions apply to the exercise of this right.
- Object to processing of personal data: You may have the right to object to the use of your personal data by us. Please note that certain conditions may apply to the exercise of this right.
- Portability of personal data: You may have the right to receive your personal data in a structured and commonly used format. Please note that certain conditions may apply to the exercise of this right.
- You also have the right to obtain from us a copy of the Binding Corporate Rules or of any Standard Contract Clauses that we use if we transfer your personal data outside the EEA and take such arrangement.

To exercise your rights, or if you require further information about how your personal data is used by us, you can write to us at: [itccir@antm.or.jp](mailto:itccir@antm.or.jp) or [support@antm.or.jp](mailto:support@antm.or.jp).

Following is the procedure when you want to execute these rights;

- 1) Upon receiving your request, we will contact you to confirm the request is being handled, and we will indicate the reasonable timeframe for us to respond.
- 2) Our Data Protection officer (DPO) will make an initial assessment of the request to decide whether it is a valid request and whether confirmation of identity is required.
- 3) If no further action from you is required, we will proceed with the processing of your request.
- 4) At the end of our assessment and internal procedure, we will provide a confirmation as to our compliance or processing of your request.
- 5) For any unfounded or excessive (e.g., further repeated) requests, we may charge a reasonable fee based on administrative costs.

## **8. When you want to complain about your personal data**

You can bring complaints in writing by contacting the ITCCIR Secretariat at [itccir@antm.or.jp](mailto:itccir@antm.or.jp), or DPO at [support@antm.or.jp](mailto:support@antm.or.jp).

After receiving the complaint we will send an acknowledgement of receipt within one week to you. The confirmation may include further questions necessary for the clarification of the issues. We will provide an answer to you as soon as reasonably practicable, but no later than one month upon receiving the complaint. If, due to complexity of the complaint, a substantive response within one month cannot be provided, you will be notified with a reasonable estimate of the timeframe, but not exceeding two months from the notice.

You may also raise the complaint to the relevant Data Protection Authority or lodge a claim with a court of competent jurisdiction.

## **9. Changes to our Privacy Policy**

We may revise or update this Privacy Policy from time to time. Any changes we may make to our Privacy Policy in the future will be posted on this webpage. If we make changes which we believe are significant, we will

inform you through the website to the extent possible and seek your consent where applicable.

## **10. Contact**

Questions, comments and requests regarding this Privacy Policy are welcomed and should be addressed to [itccir@antm.or.jp](mailto:itccir@antm.or.jp) or [support@antm.or.jp](mailto:support@antm.or.jp).