Last Updated: 11/06/2024

Japan APPI Privacy Notice

Japan APPI Privacy Notice supplements our GENERAL PRIVACY POLICY that covers all FPF operations involving the collection, use, disclosure, and other processing of personal information including personal information of those who are in Japan: organizing events, managing relationships with our stakeholders and the public, and the use of our Portal and websites by additionally covering the requirements that are set by the Act on the Protection of Personal Information (Act No. 57 of 2003) ("**APPI**") and all other applicable laws and regulations in relation to our handling of personal information of those who are in Japan that FPF collects from applicants for events such as our Japan Privacy Symposium and/or for our memberships.

WHAT PERSONAL INFORMATION WE COLLECT AND USE

Processing personal information is incidental to our operations. The categories of personal information we process on a regular basis are **names (first, last, and nickname), professional affiliation, contact details** (including job title, mailing address, and professional email address), **brief biographies, and communications you send us**.

We also collect personal information from users that access our websites, including users that join our Portal. In addition to the categories described above, **we collect information about what content users of our Portal have interacted with and submitted**, and users of the Portal may also choose to voluntarily provide us with any the following information in association with a user account:

1. Social media accounts linked to user account
2. Profile photograph
3. Opt-ins/opt-outs for marketing & working group selections
4. Working group membership selections
5. A free-text user account bio
6. User-user interactions — posts visible to the community, private "direct messages", "connection/friends" selections
7. Technical information (browser, IP address, information retrieved through cookies)
8. Registration for FPF/associated events

We occasionally process **travel schedules for our guests** and **payment information for reimbursements**, as well as **images of the participants to our events**.

As a rule, we obtain personal information directly from you. In limited situations, we also use information we observe about you. This happens when you visit our website, if you accept cookies (see our WEBSITE/COOKIE PRIVACY POLICY for more details), when we receive information on whether you opened or not the emails with our Newsletters (unless you block this tracking). If you use our Portal, we process information about the content that you have posted and/or interacted with through the use of the Portal. Additionally, FPF collects some personal information about new users of the Portal from FPF stakeholders, where new users are added to the Portal as part of their relationship with FPF.

If you are someone we would appreciate engaging with as part of our core activity, such as a privacy professional, member of the media, or public official, we obtain your contact details and affiliation from third parties or from publicly available sources.

WHY AND HOW WE USE YOUR PERSONAL INFORMATION

We use this personal information to send you communications related to our work, invitations for events or to facilitate your participation to our working groups, for conferences and other events, and to enable your use of the Portal as is described in The Future of Privacy Forum Portal Terms and Conditions.

Our email delivery vendor will use a web beacon which tracks whether recipients have opened the emails we send in order to provide us open rate information about our email communications. Please choose plain text email in order to decline this tracking. We collect information from users of the Portal regarding the submission and sharing of content in order to provide the Portal service.

WHO HAS ACCESS TO YOUR DATA

Sometimes we share your information with our partners. This happens when we co-organize events, panels, or engage in initiatives jointly with other entities. The information we share is limited to name,

affiliation and contact information, and exceptionally it may include biographic information.
We also share your information to third parties that are our vendors and process personal information on our behalf and for no other purposes. We use:

- an email delivery service,
- an email and virtual common workplace service provider,
- a provider of cloud services,
- an online conference system provider,
- a Customer Relationship Management service provider,
- an online registration service provider (for participation to events we organize),
- a hosting service for our Portal
- a website analytics provider

All of these service providers are based in the US and are bound by written agreement to use personal information obtained from FPF for FPF purposes only and in accordance with our instructions.
We will share your information with authorities only if the law requires us to.

PROVISION OF PERSONAL DATA TO THIRD PARTIES AND EXTRATERRITORIAL TRANSFERS

FPF shall comply with the APPI and all other relevant laws and regulations regarding the provision of personal data to third parties and extraterritorial transfers, including, where necessary, obtaining the consent of the relevant individual. In relation to some of the personal information handled by FPF, the consent of the individual concerned under the APPI shall not be obtained, as the provision and extraterritorial transfer of said personal information to third parties is conducted in a manner that can ensure the continued implementation of measures equivalent to those required to be taken by personal information handling business operators under the APPI below.

- Provision to third parties and extraterritorial transfer among FPF entities in accordance with our General Privacy Policy, which is commonly applied throughout FPF entities.
- Provision to third parties and extraterritorial transfer such as third parties that are our vendors as described above in accordance with written agreements.

The foreign countries to which the extraterritorial transfer of personal data may be provided are Belgium, Singapore, Israel and the United States. For information on the personal information protection systems of these countries, please refer to the following:

- The personal information protection system in Belgium:
  - Belgium is an EEA member country and is prescribed by the Personal Information Protection Commission of Japan as a country establishing a personal information protection system recognized to have equivalent standards to that in Japan in regard to the protection of an individual's rights and interests.
  - https://www.ppc.go.jp/files/pdf/200201_h31iinkaikokuji01.pdf
- The personal information protection system in Singapore:
  - Survey of the personal information protection system in Singapore (Personal Information Protection Commission, Japan)
- The personal information protection system in Israel:
  - Survey of the personal information protection system in Israel (Personal Information Protection Commission, Japan)
- The personal information protection system in the United States:
  - Survey of the personal information protection system in the United States (Personal Information Protection Commission, Japan)

JOINT USE OF PERSONAL DATA

S&K Brussels LPC and Japan DPO Association may jointly use personal data acquired by FPF in accordance with the description below.

a) Scope of joint use

S&K Brussels LPC and Japan DPO Association

b) Person(s) responsible for the management of said personal data

Future of Privacy Forum

c) Purpose of use and categories of personal information to be jointly used by the persons using the data

	Purposes of Joint Use of Personal Information	Categories of Personal Data to be Jointly Used
1.	to send you communications related to our work, invitations for events or to facilitate your participation to our working groups, for	Names (first, last, and nickname), professional affiliation, contact details (including job title, mailing address, and professional email

	conferences and other events, and to enable your use of the Portal	address), brief biographies, and communications you send us.

SECURITY MANAGEMENT OF PERSONAL DATA

FPF takes the following appropriate measures to prevent disclosure, loss, impairment, and or any other mishandling of personal data:

a) Formulation of a basic policy

This Japan APPI Privacy Notice has been established as a basic policy to ensure the appropriate handling of personal information and to provide a point of contact for questions and complaints.

b) Establishment of rules for the handling of personal data

Basic handling procedures have been established for the collection, use, and storage of personal data.

c) Organizational security management measures

(i) The responsible person confirms that personal information is handled in accordance with the established handling procedures.

(ii) A reporting and communication system from employees to the responsible person has been established.

d) Human security management measures

(i) Regular training is provided to employees, etc., on points to keep in mind regarding the handling of personal data.

(ii) Matters relating to the confidentiality of personal information are included in employment contracts and outsourcing agreements.

e) Physical security management measures

(i) Measures are taken to ensure that personal data cannot be easily accessed by anyone other than employees, etc., who are authorized to handle personal data and the relevant individual.

(ii) Measures are taken to prevent theft or loss of equipment, electronic media, and documents that handle personal information.

(iii) Measures are taken to ensure that personal information is not easily revealed when equipment, electronic media, etc., that handle personal information are transported, including transfers between offices of FPF.

f) Technical security management measures

(i) Equipment capable of handling personal data and employees, etc., who handle such equipment are clearly identified to prevent unwanted access to personal data.

(ii) Mechanisms are in place to protect information systems that handle personal information from unauthorized external access or unauthorized software.

g) Understanding the external environment

FPF handles and stores personal information on servers located in the United States, which are provided by a cloud service provider located in the United States.

- Survey of the personal information protection system in the United States (Personal Information Protection Commission, Japan)

S&K Brussels LPC stores personal information on servers located in Japan, which are provided by a cloud service provider located in Japan.

Japan DPO Association stores personal information on servers located in Japan, which are provided by a cloud service provider located in Japan.

REQUESTS FOR NOTIFICATION OF PURPOSES OF USE, DISCLOSURE, CORRECTION, DISCONTINUATION OF USE, OR OTHER HANDLING OF PERSONAL INFORMATION

Upon receiving a request to disclose the retained personal data or its purpose(s) of use; to disclose, correct, supplement or delete the personal information; to temporarily suspend or permanently discontinue the use of the personal data; to discontinue the provision of personal data to a third party; etc., FPF shall, after confirming the identity and relevance of the person making the request, respond promptly and in good faith, in accordance with the provisions of the APPI. Please note that we may not be able to respond to a request if it does not satisfy the requirements prescribed by the APPI, or if there is cause to decline the request in accordance with applicable laws and regulations.

CONTACT FOR INQUIRIES

If you have concerns, questions or requests about how we process personal data, write to us at info@fpf.org.