Privacy Statements:

EEAS – European Union External Action Service

How they store collected information?

Collected data are stored on the servers of the EEAS, the operations of which abide by the security decisions of the High Representative of the Union for Foreign Affairs and Security Policy and provisions established by the EEAS Directorate General for Budget and Administration for these kinds of servers and services.

Out of the drives available on the server, the specific compartment of Group Share Drive (:Y) designated to the division GLOBAL 1 will be used. Personal Data will be processed by assigned staff members. Files will have authorised access.

For processing purposes, temporary physical copies of the data may be created. When not in use, these copies will be stored in a secured manner (locked cabinet, etc..)

The event mobile application – EVENTUM BOT

How they use collected information?

Eventum bot may collect and use Users personal information for the following purposes:

- To run and operate their Site
- They may need your information display content on the Site correctly.
- To improve customer service
- Information you provide helps them respond to your customer service requests and support needs more efficiently.
- To personalize user experience
- They may use information in the aggregate to understand how their Users as a group use the services and resources provided on their Site.
- To improve their Site
- They may use feedback you provide to improve their products and services.
- To run a promotion, contest, survey or other Site feature
- To send Users information they agreed to receive about topics they think will be of interest to them.
- To send periodic emails
- They may use the email address to send User information and updates pertaining to their order. It may also be used to respond to their inquiries, questions, and/or other requests.

How they protect your information?

They adopt appropriate data collection, storage and processing practices and security measures to protect against unauthorised access, alteration, disclosure or destruction of your personal information, username, password, transaction information and data stored on their Site.

Sharing your personal information

They do not sell, trade, or rent Users personal identification information to others. They may share generic aggregated demographic information not linked to any personal identification information regarding visitors and users with their business partners, trusted affiliates and advertisers for the purposes outlined above. They may use third party service providers to help us operate their business and the Site or administer activities on their behalf, such as sending out newsletters or surveys. They may share your information with these third parties for those limited purposes provided that you have given them your permission.

GDPR compliance

The Collected personal data is stored only within European Union and partners involved comply with personal data protection requirements and GDPR.
Personal data without a repeated consent is stored for 24 months and after that is anonymised.

THON Hotel EU

How they use collected information?

In order to manage hotel bookings and offer accommodation to their guests, it is necessary for us to process data including name, address, date of birth, details of the stay (name of hotel, room number, price, payment method, number of nights, number of guests etc.), passport number (only for guests with registered address abroad), employer (for overnight stays covered by a corporate agreement).

How they protect your information?

They take information security seriously and have established appropriate security measures to safeguard the integrity, availability and confidentiality of your personal data. Access to your personal information is limited to employees who have a professional need for such access. They will provide training to employees and third parties where relevant, to promote awareness of the Olav Thon Group's privacy policy and procedures.

Sharing your personal information

They will only share your personal information with other companies in the Olav Thon Group to the extent necessary to maintain day-to-day operations. As Thon Holding is responsible for the administrative work within the Olav Thon Group, this means that personal information processed by Thon Hotels, including Thon DISCOVERY, and Thon Eiendom, including the customer clubs, as well as Time Park, will be shared with Thon Holding. Beyond that, personal information about hotel operations and Thon DISCOVERY will be shared with the companies within Thon Hotels. The legal basis for this is a legitimate interest, as they want to streamline operations and provide the best possible service.

Unpaid bills will be passed to collection companies. They will also share your personal information with public authorities to the extent necessary to meet their legal obligations.

Beyond this, they will not share your personal information with other businesses unless you consent to this.

How long do they store your personal data?

Personal data will not be stored any longer than necessary to fulfil the purpose of the processing or any statutory requirements placed on them; for example, the Norwegian Accounting Act requires them to keep detailed purchasing history for five years.

They will also delete personal information about you if you ask them to, unless they have a legal requirement or statutory obligation to keep your personal data for longer.

Where is your personal information stored?

Personal information processed by the Olav Thon Group is all stored on servers in Norway and Europe. They do not store personal information in countries outside the EU/EEA. Personal information processed in connection with Thon DISCOVERY is stored on the vendor's servers in Frankfurt.

Aventri

Aventri is a fully hosted, multitenant, SaaS based platform for meeting and event management and participant registration. It allows users to access and utilize the system 24/7 via the Internet using just a web browser. All data is viewable in real-time.

How Aventri use collected information?

To respond to your inquiries and fulfill your requests, and to provide you with customer support when you ask for it.
To send you updates, newsletters and other content that you have requested or subscribed to, as well as informational materials regarding their Services.
To provide you with technical and administrative information relating to their Sites and Services, such as security notices, Service-related status reports, and changes to our policies or terms of use. Please note that these communications are considered part of their Services and you may not opt out of them.
If you have consented and it is in compliance with applicable laws, to send you marketing communications regarding products and services that we believe may be of interest to you. If you later decide that you no longer want to receive this type of marketing or promotional information, you may opt-out at any time by clicking the "Unsubscribe" button at the bottom of the marketing communication, or contacting us at the email or mailing address provided in the "Contact Information" section of this Privacy Policy.
To personalize your experience on the Sites by offering content tailored to your preferences.
For their internal business purposes that include administering your access and use of any Aventri Services, data analysis, securely identifying you when you log onto a Service, fraud monitoring and prevention, enhancing or modifying their Sites and Services, determining the effectiveness of their promotional campaigns, billing you for Services, and operating their business.
As necessary for us to comply with applicable law.
Also, please note that if information is aggregated or anonymized so that it is no longer reasonably associated or trackable to an identifiable natural person, it is no longer considered "Personal

Information" under this Privacy Policy and Aventri may use it for any legitimate and lawful business purpose.

How they protect your information?

All data collection takes place under a secure protocol: HTTPS (128-bit SSL). Data in transit is encrypted using AES with 128bit Rijndael keys. PCI data remains encrypted in the same way at rest. Data backups are performed daily and retained for up to 35 days. Backups are stored in S3 in each AWS server region. PCI data within backups is encrypted. All data is stored in a MySQL database. Uploaded files are the only exception to this as they are stored as files on Amazon's S3 service.

Sharing your personal information

- Personal Information. Except as provided in this Privacy Policy, Aventri will not disclose, transfer, sell, trade, rent, or otherwise provide your Personal Information to any third party, without your consent.
- Aggregated Data. Aventri may share aggregated, non-personally identifying information, log data and usage statistics with third parties for purposes including demographic, industry and marketing analysis.
- Subsidiaries and Affiliates. Aventri discloses Personal Information to its subsidiaries and affiliates for the purposes described in this Privacy Notice. Aventri, Inc. is the entity responsible for the management of Personal Information shared among Aventri subsidiaries and affiliates.
- Service Providers. Aventri may use third party contractors to provide certain services and perform functions on their behalf. Examples include providing cloud-hosting capabilities, offering chat-bot functionality, processing credit card payments, providing marketing assistance, and performing statistical analysis relating to usage of their Sites and Services. Aventri may provide your Personal Information only to the extent necessary for such third party service provider to perform the duties for which it has been retained by Aventri. Any such third parties will be bound to strict confidentiality and use obligations with respect to your Personal Information, which are no less protective than those set out in this Privacy Policy.
- Clients. If you are accessing any Site or Service as an administrator or authorized user of a Client, or as an Event Attendee for an event organized by a Client, Aventri is permitted to provide the Client with your information, including but not limited to your Personal Information, access information and usage data.
- Legal and Contractual Compliance. Aventri may disclose your information to government or law enforcement officials, regulatory agencies or other third parties (such as attorneys or regulatory service providers), as necessary to (i) comply with applicable laws or regulations, (ii) cooperate with governmental or law enforcement investigations, (iii) respond to legal claims or processes, (iv) protect the safety and legal rights of the public or any individual, (v) detect, prevent or remedy any suspected fraud, market manipulation or illegal, tortious or wrongful activity; or (vi) enforce applicable Client Agreements or other Aventri contracts to which you have agreed. However, this does not include selling, renting or sharing or otherwise disclosing Personal Information for commercial purposes in a way that is contrary to the commitments made in this Privacy Policy.

- Business Transfers. If Aventri is acquired by, acquires or is merged with another company, Aventri may transfer Personal and Non-Personal Information about you to such company. However, in the event of such a transfer, your information will remain subject to the protections of this Privacy Policy. Aventri will notify you if your information is subject to a business transfer and becomes subject to the other company's privacy policy.
- Third Party Websites and External Links. Their Sites may contain links to websites (including social media sites) owned and operated by third parties. When you click on such links, you may leave their Website and be directed to the third parties' websites. These websites may themselves collect Personal Information about you. If you submit information to any of those sites, your information is governed by their privacy policies, which may differ from those of Aventri. Aventri is not, and will not be, responsible for the privacy practices or security of any such websites, and we urge you to read their privacy policies carefully.
- their Blogs and Social Media Pages. As we discuss above, you may disclose Personal Information during your participation in their Blogs or on Social Media Sites, including on message boards, in chats, and on any social media site on which you are able to post information and content. This Personal Information may appear in public ways, including through search engines or other publicly available platforms, and can be "crawled" or may be searchable by third parties. Please do not post any information that you do not want to be disclosed to the public.
- Upon Your Consent. Other than as set out above, you will receive notice when information about you might go to third parties, and you will have an opportunity to consent to Aventri sharing this information.

How long do they store your personal data?

PThey will retain your Personal Information for as long as necessary to fulfill the purposes for which it was collected and processed, or until you request deletion as described in this Privacy Policy.
Aventri will retain Personal Information they collect from their Clients or Event Attendees, and process on behalf of a Client, for as long as necessary to provide their Services to the Client and will maintain any such information controlled by a Client in accordance with the Client's instructions, including any applicable Client Agreement terms, and as required by applicable law.

They will also retain and use Personal Information for a period of time required to comply with their legal, tax, audit or regulatory obligations, to resolve disputes, and to enforce their agreements.
Aventri may retain Non-Personal Information for as long as necessary for the purposes and uses described in this Privacy Policy, including as necessary for Aventri to pursue legitimate and lawful business interests.

Travel Agency – T&T

How T&T use collected information ?

In the course of the Company's operations, data is collected in order to enable the provision of its services. This data is necessary for the fulfilment of the Company's contractual obligations to clients.
Any personal data collected by the Company is ordinary (namely, data relating to the name, email address, ID or passport numbers of clients or persons representing such clients, TIN, profession, address, phone

numbers, credit or debit card numbers, and any tax documents necessary to invoice the services provided etc.), The collection and processing of such data is intended to enable the provision of better and faster service by the Company.

Sharing your personal information

As part of our operations, any data collected by the Company may be transferred to third parties or third countries. Such transfer applies exclusively to data required for the provision of services requested by the client and the discharge of other contractual obligations for the implementation of any project. All cooperation agreements between the Company and third parties explicitly stipulate that the contracting third parties must comply with the Regulation. Furthermore, such data may be transmitted to any judicial and/or tax authorities and/or lawyers.

How they protect your information ?

The Company shall keep such personal data in printed and/or electronic form.

- The Company shall keep all client, vendor and employee details, as well as any electronic correspondence with the data subjects in electronic form in files stored on an external server installed at its registered office. Each PC has a unique password which is changed from time to time and which is known and managed by Controller and/or any authorised employee working under his/her direct supervision. Any processing by unauthorised users is prohibited. However, in cases where it is absolutely necessary and with the personal responsibility of the Controller or his/her authorised employees, data may be stored on USBs kept under lock and key, as well as on electronic reading devices (PCs and notebooks, tablets and smartphones) owned and used by the Company.

The Company shall update and monitor its security technology on an ongoing basis. The Company shall restrict access to your personal data to employees who need to know such information. In addition, the Company shall provide training to its employees on the importance of confidentiality and non-disclosure as well as on the security of personal data. Among other means, the Company applies technical and administrative measures and procedures to protect such data from any loss, alteration, unauthorised processing or modification, including but not limited to encryption, detection and management of security breaches, *use of information systems and software installed on PCs in such a way that minimises the use of personal data and/or user identification data*, adoption of individual procedures for the retention and safe deletion/destruction of personal data.

Copies of all data kept in electronic form are also kept in back-up files stored on an external hard disk kept in the Director's office that can be locked, and the only person who has the key is the Legal Representative of the Company. All electronic devices where personal data is stored must not be exposed in places accessible to the public or where their display screen can be viewed by any person other than the authorised users of such devices.

- The Company keeps paper-based files of clients, vendors and employees (and, specifically, documents including the details of clients, vendors, employees and others) that are stored in cabinets or archive boxes secured with locks in the Company's administration offices which are

accessible only by the Legal Representative/Controller of the Company, and the Company has also installed an alarm and fire warning system.

How long do they store your personal data?

Personal data is retained for the duration of such relation (contractual obligations) with the data subjects.

The personal data of clients are retained for a period of at least fifteen (15) years to enable the Company to fulfil its obligation to submit accurate information to the tax or other administrative authorities.

Where is your personal information stored?

The Company shall keep all client, vendor and employee details, as well as any electronic correspondence with the data subjects in electronic form in files stored on an external server installed at its registered office.

Downtown Europe

Sharing your personal information

The only people who have access to this data are the Downtown Europe staff members.

Where is your personal information stored?

Files are stored on the server in the office of Downtown Europe, running the Windows Foundation Server 2012 operating system.

The data is also stored (as a backup) on 2 backup devices: 1 in the office and 1 at a remote location. Again, only Downtown Europe staff have access to this data.

Emails are stored on Microsoft servers in the cloud, using their Office 365 platform.

Personal data will not be stored any longer than necessary to fulfil the purpose of the processing or any statutory requirements placed on them. They will retain Personal Information for a period of time required (seven years) to comply with their legal, tax, audit or regulatory obligations.