

## **Privacy Policy**

*V 1.2 Applicable as of January 3, 2024*

*CEIS attaches great importance to your privacy and the protection of your personal data and takes all reasonable precautions to ensure their protection.*

*The purpose of this Policy is to inform you about the processing of personal data that is implemented on the occasion of the organization of the INCYBER Forum (FIC), in accordance with the General Data Protection Regulation or "GDPR" of the European Union of April 27, 2016 (n°2016/679) and the amended law of January 6, 1978.*

*We have drawn up two documents with the aim of informing you about how we collect, use and protect your personal data in the context of our various services:*

- a policy dedicated to personal data collected via our website and as part of FIC registration (this policy).*
- a specific document concerning the cookies we use (the [cookie management policy](#)).*

*The terms "we", "us" and "our" used in this Privacy Policy refer to CEIS.*

*In the remainder of this document, we use the terms "personal data", "personal data" and "personal information" interchangeably to refer to information that identifies you personally (surnames, first names, business addresses, etc.) or, data that is linked to you (answers to questions on our forms), as well as connection or browsing data on our site (where applicable, IP address, date and time of connection).*

*You will find answers to your questions classified by theme in the following sections:*

- 1. Who are we?*
- 2. Scope of application*
- 3. Purposes, types of personal data collected and legal basis for processing*
- 4. Retention periods*
- 5. Confidentiality and security measures*
- 6. Recipients of data*
- 7. International data transfer*
- 8. Rights of access, rectification and deletion*
- 9. Contact us to exercise your rights*

10. *Specific case of CORIIN*
11. *Trust & Safety Forum*
12. *Modification of our Privacy Policy*
13. *Use of cookies*

## **1. Who is CEIS?**

*CEIS is a société par actions simplifiée (simplified joint stock company) with a capital of €150,510, registered with the Paris Trade and Companies Registry under number 414881821 and whose registered office is located at 17 Avenue Hoche, 75008 PARIS.*

*We are the data controller within the meaning of Regulation (EU) 2016/679 of the General Data Protection Regulation (hereinafter "GDPR"), for the procedures and processing of personal data that are implemented on the occasion of the organization of the INCYBER Forum (FIC), as described below, and jointly responsible regarding the CORIIN events (see in specific case paragraph 10 below) and Trust & Safety Forum (see in specific case paragraph 11 below).*

*As such, we undertake to comply with the legal provisions in force and in particular to take all reasonable steps to ensure the accuracy and relevance of personal data with regard to the purposes for which CEIS (hereinafter also "the Organizer") processes them.*

## **2. Scope of application**

*This Policy covers all data processing related to the organization of the FIC event, as well as to :*

- Specific events associated with the FIC ("associated events"), including the Cybersecurity For Industry, ID & KYC Forum, OSINT, CORIIN, Web3 Security Summit and Trust & Safety Forum. You can register for these events when you register for FIC;*
- Post-FIC events organized by CEIS or co-organized with our partners (hereinafter referred to as "post-FIC events"), such as INCYBER news breakfasts, webinars, etc.*

## **3. Purposes, types of personal data collected and legal basis for processing**

*We have produced a summary table listing, for each type of data, the legal basis on which it is collected and processed, the associated purpose, and the applicable retention period. This table can be found at the end of paragraph 4 of this policy.*

*Participation in the FIC, associated events and subsequent events is strictly reserved for :*

- Professionals in the fields of cybersecurity, business intelligence, digital investigation and digital trust;

- Students, retirees and job seekers in these fields.

The personal data we collect on these occasions is used for the following purposes;

- Your registration data (surname, first name, contact details, email address, job title, company name and sector and business address if applicable, company's role in the cybersecurity ecosystem, fields and interests, purpose of visit, days of visit, country). This information will enable you to register for this FIC and related events, in particular CORIIN. Your FIC registration request, once accepted, enables the creation of your access badge and your personal space on the SWAPCARD tool. This personal space enables you to prepare your visit (agenda management, etc.) and to network with other participants. Your e-mail address is your account identifier. The legal basis for this processing is the contract governing your participation in our events and constituting the contractual conditions for your visit.

- Data from official documents used to verify your identity (identity card, etc.) and control access are collected in order to implement security measures on the premises. The legal basis for this processing is our legitimate interest in ensuring the security of the site, or in certain specific cases, the existence of a regulatory obligation.

- We collect your identity data and data relating to the management of reservations and payments (date of arrival, date of departure, date of payment, date of reservation, etc.) to enable the management of your hotel reservations (where applicable), the management of meal reservations in our partner restaurants (where applicable), as well as the management of the status of payments for these services. The legal basis for this processing of personal data is the performance of the contract. We also process this data for accounting purposes, in order to comply with our legal obligations.

- In the context of our partnerships with participating companies and sponsors of the FIC, we may also need to process your account data in order to carry out communication actions on their behalf, and in particular to invite you to an event organized by them during the FIC. The legal basis for this data processing is our legitimate interest.

- Your account and registration data are used to manage invitations to future professional events concerning cybersecurity, economic intelligence, digital investigation or digital confidence (subsequent events as described in paragraph 2 of this policy) that we or some of our partners will organize on similar themes and, more generally, to carry out any prospecting operations in connection with these themes (newsletters, publications) addressed to your professional contact details. The legal basis for processing your data for these purposes is our legitimate interest.

- If you are a student or retired, your account and registration data may be used to manage invitations to future events that we or some of our partners will organize in connection with the FIC, notably concerning cybersecurity, economic intelligence, digital investigation or digital trust,

on the basis of your consent. CEIS will thus be able to invite you by e-mail to future events that we organize, similar to the FIC, and you will have the possibility of unsubscribing from this mailing list.

- Your contact details and areas of interest, for the purposes of managing our newsletters, on the basis of your legitimate interest if you are a professional and on the basis of your consent if you are a student or retired person.

- We process the data we collect when you register and take part in the FIC in order to produce statistics. These statistics are carried out on the basis of our legitimate interest, which is reflected in the need to manage our activity in order to improve our services.

- The recording of event logs to trace your activity (IP, date and time of connection, disconnection, etc.) for IT security purposes. This data processing is carried out on the legal basis of our legitimate interest in maintaining the cybersecurity of our information systems.

Please note: the information marked with an asterisk (\*) on the various data collection forms we use is essential for processing your request.

Concerning the collection of personal data linked to your Internet browsing (cookies), we invite you to read our dedicated [cookie management policy](#).

#### **4. Retention periods**

For each type of data, we have drawn up a summary table listing the legal basis on which it is collected and processed, the associated purpose, and the applicable retention period. This table can be found at the end of this paragraph.

Your personal information will not be kept beyond the time strictly necessary. In particular

- Your account data is kept for as long as it remains active. Your account will be deleted after three years of inactivity.

- Your event registration data is kept for the duration of the event, then stored in an "intermediate" database (equivalent to an archive) for a total period of three years from your last registration. At the end of this period, your data is anonymized. It may be rendered anonymous if, in the meantime, you request the deletion of your online account.

- Identity data required to control access to the event will be deleted immediately after the event.

- Data relating to the management of reservations and payments (date of arrival, date of departure, date of payment, date of reservation, etc.) will be kept for the duration of the contract in the active database and in intermediate archiving for five years for the purposes of processing transaction disputes and claims, and for ten years for the management of our accounting obligations.

- Visitors' contractual data is kept for three years.

- Accounting data is archived for ten years.

- Data required for canvassing operations are processed for a period of three years, unless you object before the end of this period. Your objection may take the form of unsubscribing from a newsletter or invitation via the unsubscribe link associated with the message.

- Event logs may be kept for a maximum of twelve months, based on our legitimate interest in ensuring the security of our information system.

**Summary table of data collected, purposes, legal basis and retention periods by processing activity, bearing in mind that all such processing may be subject to anonymous statistical analysis:**

| <i>Collected data</i>   | <i>Purpose</i>  | <i>Legal basis</i>          | <i>Shelf life</i>   |
|---|---|-----------------------------|---|
| <i>Registration details: surname, first name, contact details, email address, company (and business address if provided), job title, areas of interest, country, etc.</i> | <i>Registration management</i>                            | <i>Contractual measures</i> | <i>For the duration of the event in active database<br/>3 years intermediate archiving<br/>Anonymised after 3 years</i> |
| <i>Identity data</i>  | <i>Access control</i>                                     | <i>Legitimate interest</i>  | <i>Deleted immediately after the event</i>  |
| <i>Identity data and data relating to the management of reservations and payments (date of arrival, date of departure, date of payment, date of reservation, etc.).</i>   | <i>Management of reservations and payment status</i>      | <i>Contractual measures</i> | <i>For the duration of the contract in active database and 5 years in intermediate archiving</i>                        |
| <i>Identity data and data relating to the management of reservations and payments (date of arrival, date of departure, date of payment, date of reservation, etc.).</i>   | <i>Accounting management</i>                              | <i>Legal obligation</i>     | <i>10 years</i>   |
| <i>Your account details: surname, first name, contact details, language, email address</i>  | <i>Invitations to events organised by FIC partners</i>    | <i>Legitimate interest</i>  | <i>3 years</i>  |
| <i>Students, pensioners: your account and registration details</i>  | <i>Commercial communication and newsletter management</i> | <i>Consent</i>              | <i>3 years</i>  |



|  |   |                            |                  |
|--|---|----------------------------|------------------|
| <i>Event logs (IP, date and time of connection, disconnection, etc.)</i> | <i>Maintaining the cyber security of our information system</i> | <i>Legitimate interest</i> | <i>12 months</i> |
|--|---|----------------------------|------------------|

### **5. Confidentiality and security measures**

*We take all necessary and reasonable measures (physical, logistical, organizational) to protect your data at the time of transmission to our site or applications, in particular against loss, misuse, unauthorized access, disclosure, alteration or destruction, via security measures such as vulnerability detection, deployment of HTTPS protocol, implementation of pseudonymization and anonymization processes, etc.*

*Depending on the type of data collected and its purposes, processing is carried out only by authorized personnel, in compliance with our confidentiality and security requirements for the creation of files, exchanges with our partners and subcontractors, and the transfer of such data (see below).*

### **6. Recipients of data**

*The personal information you are likely to provide may be consulted by our company's staff and our subcontractors within the strict framework of the purposes we have presented to you. In this respect, we would like to point out that we have signed strict security and confidentiality clauses with our subcontractors, in compliance with Article 28 of the RGPD, specifying in particular the security objectives that must be achieved.*

*We may need to communicate your registration data to the following entities:*

- Managers of venues hosting events and security services should this prove necessary. As indicated above, these managers may also verify your identity;*
- Our subcontractor Swapcard, enabling us to offer you the mobile networking platform used to manage personal spaces, networking between participants and the appointment booking module.*
- Our subcontractor LENI, in charge of hosting account and registration data;*
- The partner in charge of the CYBERJOBS platform, if you are looking for a job and have expressed your wish to communicate your data during the registration process:*
- The hotels and restaurants to which we communicate your reservation data, in order to enable you to access these services, and who act in this capacity as independent data processors.*

*As part of our partnerships with participating companies and sponsors of the FIC, we may collect certain data on behalf of our partners during the event and communicate it to these partners, notably via the Swapcard badge and application. More specifically*

*- Partners who sponsor or contribute to the organization of ancillary events, as described in article 2 of this policy, in which you participate and to whom you communicate your data on the occasion of your participation in the ancillary event. You may be contacted by the said partners following the FIC for commercial purposes. These partners act as data processors. If, following receipt of a message from one of your partners, you do not wish to receive any communication from them, simply inform them directly, on this occasion or at a later date.*

*- FIC exhibitors to whom you have given your contact details, notably by scanning your badge, when you visit their stands or when you are offered a free drink. Following the FIC, you may be contacted by the exhibitor in question, who acts as data controller. If you do not wish to receive any communication from the exhibitor, simply inform them directly, on this occasion or at a later date.*

*Finally, we may be required to communicate personal information at the request of any public authority in the context of a compulsory legal procedure, or in the event of a proven risk that could affect our information system and have an impact on our activities or the conduct thereof, or the fundamental rights of third parties concerned.*

## **7. International data transfer**

*We may transfer your personal data to service providers outside the European Economic Area (EEA). In this case, please be assured that they are bound by specific rules and measures to ensure the appropriate level of security for the protection of your personal data. This means that we will base our transfers on the applicable regulations (standard contractual clauses approved by the European Commission in our contracts with third parties outside the EEA, transfer to countries with protection recognized as adequate by the European Commission, etc.).*

*For further information, please contact our Data Protection Officer at [dpo@forum-incyber.com](mailto:dpo@forum-incyber.com).*

## **8. Rights of access, rectification and deletion**

*We remind you that you have the right :*

- To be informed about the way in which your data is processed;*
- To access your data;*
- To object to your data being processed, and in particular to your data being used for commercial prospecting purposes;*
- To temporarily restrict certain uses of your data, in particular while your data is being rectified or verified;*
- Rectify incorrect information, or ask us to delete certain information;*
- To withdraw your consent to the processing of your data, if such processing is based on this legal basis (see table below);*
- To define directives concerning the fate of your personal data after your death, in application of article 32 of the law of January 6, 1978.*

## **9. Contact us to exercise your rights**

*The protection of personal data is a fundamental right, and you may at any time contact our Data Protection Officer by email ([dpo@forum-incyber.com](mailto:dpo@forum-incyber.com)) or, failing that, by post addressed to our DPO and sent to the following address: 17 Avenue Hoche, 75008 PARIS. However, we reserve the right to ask you to prove your identity and the relevance of your request.*

*If, despite our reply, you are still not satisfied, you can contact the Commission Nationale Informatique et Liberté (CNIL) directly at <https://www.cnil.fr/fr/vous-souhaitez-contacter-la-cnil>.*

## **10. Specific case of CORIIN**

*In the specific context of your participation in CORIIN via the purchase of the dedicated Pack, CEIS is jointly responsible for processing with the French Cybercrime Expert Center (CECYF). Your personal data will be processed by CEIS on behalf of CEIS and CECYF for the purposes of organizing the event and managing registrations.*

*CEIS and CECYF undertake to respect the commitments and obligations aimed at ensuring the security and confidentiality of personal data and to ensure that the terms thereof are respected by their employees, staff or agents, whether permanent or not, as well as by their possible subcontractors, in particular by transmitting similar commitments and obligations to them. In this respect, CEIS and CECYF undertake to ensure that persons authorized to process personal data are trained in personal data security issues and are committed to confidentiality or are subject to an appropriate legal obligation of confidentiality.*

*CEIS will be the point of contact for exercising the rights of CORIIN participants, and as such will assume and coordinate responses to participants concerning the processing carried out jointly. CEIS is also in charge of informing them about the processing concerned, and is responsible for notifying any data breaches that may occur.*

*The personal data collected on this occasion, and in particular the e-mail addresses of registered persons, may be processed by CEIS on the one hand and by CECYF on the other, each as an independent data controller, within the framework of their commercial prospecting and the management of their newsletters.*

## **11. Specific case of the Trust & Safety Forum**

*In the specific context of your participation in the Trust & Safety Forum, CEIS is jointly responsible for processing with SOCOGI on the one hand and HMC Group LLC on the other. Your personal data will be processed by CEIS on behalf of CEIS, SOCOGI and HMC Group LLC for the purposes of organizing the event and managing registrations.*

*CEIS, SOCOGI and HMC Group LLC undertake to respect the commitments and obligations aimed at ensuring the security and confidentiality of personal data and to ensure that the terms thereof are respected by their employees, personnel or agents, whether permanent or not, as well as by their possible subcontractors, notably by transmitting similar commitments and obligations to them. In this respect, CEIS, SOCOGI and HMC Group LLC undertake to ensure that persons authorized to process personal data are trained in personal data security issues and are*



*committed to confidentiality or are subject to an appropriate legal obligation of confidentiality.*

*CEIS will be the point of contact for the exercise of Trust & Safety Forum participants' rights, and as such will assume and coordinate responses to participants concerning the processing carried out jointly. CEIS is also responsible for informing them about the processing concerned, and for notifying them of any data breaches that may occur.*

*The personal data collected on this occasion, and in particular the e-mail addresses of registered persons, may be processed by CEIS, SOCOGI and HMC Group LLC, each as independent data processors, in the context of their commercial prospecting and the management of their newsletters.*

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

*Should we change our Privacy Policy, we will inform you by any appropriate means.*

### **12. Use of cookies**

*We remind you that you will find details of your rights regarding your personal data and its management within the framework of the functionalities of our site and its mode of operation in our dedicated [Cookie Management Policy](#).*