

## ***V 1.4 Effective November 25, 2024***

CEIS places great importance on your privacy and the protection of your personal data. We take all reasonable precautions to ensure its protection.

The purpose of this Policy is to inform you about the processing of personal data that is carried out in connection with 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 French law of January 6, 1978 as amended.

We have prepared two documents aimed at 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 during registration for the FIC (this policy).
- a specific document on the cookies we use ([the cookie management policy](#)).

The terms "we" or "our" used in this Privacy Policy refer to the company CEIS.

In the following sections of this document, we use the terms "personal data", "personal information", and "information" interchangeably to refer to information that personally identifies you (surname, first name, professional address, etc.) or data that is linked to you (answers to questions on our forms), as well as connection or navigation data on our site (if applicable, IP address, date and time of connection).

You will find answers to your questions, categorized 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 their processing**
- 4. Retention periods**  
Table summarizing the data collected, purposes, legal bases, and retention periods by processing activity, knowing that all these processing operations may be subject to anonymous statistics:
- 5. Specific case of booth consultations and participation in conferences and events organized with our partners**

6. **Specific case of CORIIN**
7. **Specific case of the Trust & Safety Forum**
8. **Confidentiality and security measures**
9. **Data recipients**
10. **International data transfer**
11. **Rights of access, rectification and erasure**
12. **Contact us to exercise your rights**
13. **Modification of our Privacy Policy**
14. **Use of cookies**

## 1. Who are we?

CEIS is a simplified joint-stock company with a capital of €150,510, registered with the Paris Trade and Companies Register under number 414881821 and whose registered office is located at 17 Avenue Hoche, 75008 PARIS.

We are the data controller as defined by Regulation (EU) 2016/679, the General Data Protection Regulation (hereinafter referred to as the "GDPR"), for the processing of personal data carried out in connection with the organization of the INCYBER Forum (FIC), as described below, and joint controller for the data collected during booth visits, conferences, presentations, and events organized with our partners (see paragraph 5 below), as well as for CORIIN events (see paragraph 6 below) and the Trust & Safety Forum (see paragraph 7 below).

As such, we are committed to complying with the applicable legal framework and, in particular, to taking all reasonable measures to ensure the accuracy and relevance of personal data in light of the purposes for which CEIS (hereinafter also referred to as the "Organizer") processes them.

## 2. Scope

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

- Booths, conferences (FIC Talk, technical demonstrations, etc.), and events organized with our partners – see §5;
- Specific events associated with the FIC ("associated events"), including Cybersecurity For Industry, ID Forum, OSINT day, CORIIN, see §6, Web3 Security Summit, InCyber Invest day, and the Trust & Safety Forum, see §7. Your participation in these events is through your registration for the FIC;
- Subsequent events to the FIC organized by CEIS or co-organized with our partners (hereinafter referred to as 'subsequent events'), such as INCYBER news breakfasts and webinars.

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

We have created a comprehensive table detailing, for each data category, the legal basis justifying its collection and processing, the purpose of such use, and the planned retention period. This table can be found at the end of paragraph 4 of this policy and is directly accessible via this link.

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

- **Professionals in cybersecurity, economic intelligence, digital investigation, and digital trust;**
- **Students, retirees, and job seekers in these fields.**

The personal data we collect on these occasions is collected for the following purposes:

- Your registration data (surname, first name, contact details, email address, position, title, company name and sector, and possibly professional address, company's role in the cybersecurity ecosystem, areas of interest, purpose of visit, days of attendance, country) allows you to register for this FIC or associated events, including CORIIN. Your registration request for the FIC, once accepted, allows the creation of your access badge and your personal space on the SWAPCARD tool. This personal space allows you to prepare for your visit (agenda management, etc.) and to "network" with other participants. Your email address is your account identifier. It can also be used to create an account for you on the b2match matchmaking platform to allow you to interact with other VIP participants. The legal basis for this processing is the contract governing your participation in our events and constituting the contractual terms of your visit.
- Data from official documents allowing verification of your identity (ID card, etc.) and access control are collected to implement site security measures. 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 (arrival date, departure date, payment date, reservation date, etc.) to enable the management of your hotel reservations (if applicable), the management of meal reservations in our partner restaurants (if 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 on the basis of compliance with our legal obligations.
- We may also be required, as part of our partnerships with participating companies and FIC sponsors, to process your account data to carry out communication actions, for the benefit of the latter, 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 data and registration data are used for the purpose of managing invitations to future professional events concerning cybersecurity, economic intelligence, digital investigation or digital trust (subsequent events as described in paragraph 2 of this policy) that we ourselves, or some of our partners, will organize on similar themes and more broadly to

carry out any prospecting operations in connection with these themes (newsletters, publications) addressed to your professional contact details. The legal basis for the processing of your data for these purposes is our legitimate interest.

- If you are a student or retiree, your account data and registration data may be used for the purpose of managing invitations to future events that we ourselves or some of our partners will organize in connection with the FIC, concerning in particular cybersecurity, economic intelligence, digital investigation or digital trust, on the basis of your consent. CEIS may thus invite you by email to future events that we organize, similar to the FIC, and you will have the opportunity to unsubscribe from this mailing list.
- Your contact details and your areas of interest, for the purpose of managing our newsletters, on the basis of our legitimate interest if you are a professional and on the basis of your consent if you are a student or retiree.
- We process the data that we have collected during your registration and participation in the FIC in order to produce statistics. These statistics are produced on the basis of our legitimate interest, which is translated by the need to manage our activity in order to improve our services in particular.
- The recording of event logs constituting the traceability of your activity (IP, date and time of connection, disconnection, etc.) for the purpose of IT security. 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 indicated by an asterisk (\*) in the various collection forms that we use is essential for the processing of your request.

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

#### 4. Data Retention Periods

We have created a summary table listing, for each type of data, the legal basis for its collection and processing, the purpose associated with it, and the applicable retention period. This table can be found at the end of this paragraph and is directly accessible via this [link](#).

Your personal information will not be retained for longer than is strictly necessary. In particular:

- Your account data is retained as long as your account remains active. The account is deleted after three years of inactivity.
- Your registration data for our events is retained 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 anonymized if, in the meantime, you request the deletion of your online account.
- Identity data necessary for access control to the event will be deleted immediately after the event.
- Data relating to the management of reservations and payments (arrival date, departure date, payment date, reservation date, etc.) will be retained for the duration of the contract in an active



database and in intermediate archiving for five years for the purpose of processing transaction disputes and claims, and for ten years for the management of our accounting obligations.

- Contractual data of visitors is retained for three years.
- Accounting data is archived for ten years.
- Data necessary for prospecting operations is processed for a period of three years, unless you object before the end of this period. You may object in particular by unsubscribing from a newsletter or invitation via the unsubscribe link associated with the message.
- Event logs may be retained for a maximum period of twelve months, based on our legitimate interest in ensuring the security of our information system.

Summary table of collected data, purposes, legal bases, and retention periods by processing activity, knowing that all these processing activities may be subject to anonymous statistics:

Data Collected	Purpose	Legal Basis	Retention Period
Registration data: name, first name, contact details, email address, position, title, company name and sector (and possibly professional address), company's role in the cybersecurity ecosystem, areas of interest, purpose of visit, days of visit, country	Registration management	Contractual measures	During the event in active database, then 3 years in intermediate archive
Identity data	Access control	Legitimate interest	Deleted immediately after the event
Identity data and data related to the management of reservations (events, hotel nights, etc.) and payments (arrival date, departure date, payment date, reservation date, etc.)	Management of reservations and payment status	Contractual measures	During the contract in active database and 5 years in intermediate archive

Identity data and data related to the management of reservations and payments (arrival date, departure date, payment date, reservation date, etc.)	Accounting management	Legal obligation	10 years
Account data: name, first name, contact details, language, email address	Invitation to events organized by FIC partners	Legitimate interest	During the event
Professionals: Account data and registration data	Commercial prospecting and management of our newsletters	Legitimate interest	3 years
Students, retirees: Account data and registration data	Commercial prospecting and management of our newsletters	Consent	3 years
Event logs (IP, date and time of connection, disconnection, etc.)	Maintaining the cybersecurity of our information system	Legitimate interest	Up to 12 months

## 5. Specific Case of Stand Consultations and Participation in Conferences and Activities Organized with Our Partners

In the case of stand consultations and participation in conferences and activities organized with our partners, CEIS is jointly responsible for processing bilaterally with each of the partners in question. Your personal data will be processed by CEIS on behalf of CEIS and the partner in question as part of the organization of the event, attendance at stands, and monitoring of attendance at conferences, presentations, and activities during the INCYBER Forum.

The partner in question is the one:

- who sponsors the conference in which you participate (via the scanning of your badge at the entrance);

- or who organizes the activity in which you participate (via the scanning of your badge), such as the provision of free drinks, etc.;
- or at whose stand you have visited and agreed to have your badge scanned.
- The data concerned is your account data and your registration data.

CEIS and the partner in question undertake to respect the commitments and obligations aimed at ensuring the security and confidentiality of this data and to ensure compliance with these terms by their employees, personnel or agents, permanent or not, as well as by their subcontractors, in particular by transmitting similar commitments and obligations to them. In this regard, CEIS and the partner in question undertake that persons authorized to process personal data are trained in matters of personal data security and undertake confidentiality or are subject to an appropriate legal obligation of confidentiality.

CEIS will be the point of contact for the exercise of your rights, and, as such, will assume and coordinate the responses to participants concerning the joint processing carried out. CEIS is also responsible for informing you about the processing concerned, and responsible for notifying you of any data breaches that may occur.

At the end of the INCYBER Forum, the personal data collected on this occasion, and in particular the email addresses of registered persons, may be processed by CEIS on the one hand and by the partner in question on the other, each acting as an independent data controller, as part of their commercial prospecting and management of their newsletters. Each partner in question will inform you on this occasion of the modalities for processing this information and exercising your rights, each partner being the entity to contact to exercise them. If, following receipt of a message from one of the partners, you do not wish to receive any communication from them, you simply need to inform them directly, on this occasion or subsequently.

## 6. Specific Case of CORIIN

In the specific context of your participation in CORIIN through 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 as part of the organization of the event and the management of registrations.

CEIS and CECYF undertake to respect the commitments and obligations aimed at ensuring the security and confidentiality of your data and to ensure compliance with these terms by their employees, personnel or agents, permanent or not, as well as by their subcontractors, in particular by transmitting similar commitments and obligations to them. In this regard, CEIS and CECYF undertake that persons authorized to process personal data are trained in matters of personal data security and undertake confidentiality or are subject to an appropriate legal obligation of confidentiality.

CEIS will be the point of contact for the exercise of your rights, and, as such, will assume and coordinate the responses concerning the joint processing carried out. CEIS is also responsible for informing you about the processing concerned, and responsible for notifying you of any data breaches that may occur.

At the end of the INCYBER Forum, the personal data collected on this occasion, and in particular the email addresses of registered persons, may be processed by CEIS on the one hand and by CECYF on the other, each acting as an independent data controller, as part of their commercial prospecting and management of their newsletters. CECYF will inform you on this occasion of the modalities for processing this information and exercising your rights, CECYF being the entity to contact to exercise them.

If, following receipt of a message from CECYF, you do not wish to receive any communication from them, you simply need to inform them directly, on this occasion or subsequently.

## 7. 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 hand. Your personal data will be processed by CEIS on behalf of CEIS, SOCOGI, and HMC Group LLC as part of the organization of the event and the management of 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 compliance with these terms by their employees, personnel or agents, permanent or not, as well as by their subcontractors, in particular by transmitting similar commitments and obligations to them. In this regard, CEIS, SOCOGI, and HMC Group LLC undertake that persons authorized to process personal data are trained in matters of personal data security and undertake confidentiality or are subject to an appropriate legal obligation of confidentiality.

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

At the end of the INCYBER Forum, the personal data collected on this occasion, and in particular the email addresses of registered persons, may be processed by CEIS, SOCOGI, and HMC Group LLC, each acting as an independent data controller, as part of their commercial prospecting and management of their newsletters. Each of them will inform you on this occasion of the modalities for processing this information and exercising your rights, each of them being the entity to contact to exercise them.

If, following receipt of a message from one of the partners, you do not wish to receive any communication from them, you simply need to inform them directly, on this occasion or subsequently.

## 8. Confidentiality and Security Measures

We take all necessary and reasonable measures (physical, logistical, organizational) to protect your data when it is transmitted on our site or applications, in particular against loss, misuse, unauthorized access, disclosure, alteration or destruction, through security measures such as vulnerability detection,



deployment of the 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 accordance with our confidentiality and security requirements in the constitution of files, exchanges with our partners and subcontractors, and the transfer of this data (see below).

## 9. Data Recipients

The personal information you may provide may be accessed by our company's staff and our subcontractors strictly within the framework of the purposes we have presented to you. In this regard, we inform you that we have entered into strict security and confidentiality clauses with our subcontractors, in accordance with Article 28 of the GDPR, specifying in particular the security objectives to be achieved.

We may be required to communicate your registration data to the following entities:

- The managers of the venues hosting the events and the security services if necessary. As indicated above, these managers may also carry out an identity check;
- Our subcontractor Swapcard allowing us to offer you the mobile networking platform used to manage the management of personal spaces, networking between participants or the appointment scheduling module.
- Our subcontractor b2match, which allows us to offer you facilitated networking according to your profile, and to exchange with other VIP participants, if you choose to connect to the account we offer you;
- Our partner 42k, which offers a referral service for companies in the cybersecurity field, to whom we transmit the email address of the company contact, if you indicate that you are interested in this offer during your registration;
- The partners in charge of the Les Jeudis and Cybermatch platforms, if you are looking for a job and have expressed your wish to communicate your data during the registration process,
- Our subcontractor LENI, in charge of hosting account and registration data;
- Our partner bnetwork to which we communicate the data relating to your reservation when you make a hotel overnight stay reservation directly on our website as part of the purchase of a pack or during the registration process;
- The hotels and restaurants to which we communicate the data relating to your reservations, in order to allow you to access these services, and which act as independent data controllers.

As part of our partnerships with participating companies and sponsors of the FIC, we may collect certain data with our partners during the event and make this data available to them at the end of the event. This data is collected in particular via the badge and the Swapcard 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 these partners after the FIC for commercial purposes. They then act as independent data controllers. If, following receipt of a message from one of your partners, you do not wish to receive any communication from them, you simply need to inform them directly, on this occasion or subsequently.
- Exhibitors at the FIC to whom you have communicated your contact details, in particular by scanning your badge, on the occasion of your visit to their stands, attendance at a conference they sponsor or during a free consumption offer. Following the FIC, you may be contacted by the exhibitor in question, who then acts as an independent data controller. If you do not wish to receive any communication from them, you simply need to inform them directly, on this occasion or subsequently.

Finally, we may be required to communicate personal information at the request of any public authority as part of a mandatory 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.

## 10. International Data Transfers

We may transfer your personal data to service providers outside the European Economic Area (EEA). In this case, please be assured that they are subject to specific rules and measures to ensure an 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 a level of protection recognized as adequate by the European Commission, etc.).

For more information, you can contact our Data Protection Officer at the following address: [dpo@forum-incyber.com](mailto:dpo@forum-incyber.com)

## 11. Rights of Access, Rectification and Erasure

We remind you that you have the right:

- To be informed about how your data is processed;
- To access your data;
- To object to the processing of your data, and in particular to the use of your data for commercial prospecting purposes;
- To temporarily restrict certain uses of your data, for the time of a rectification or verification of your data in particular;
- To rectify incorrect information, as well as to request us to delete certain information;

- To withdraw your consent to the processing of your data, if this 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.

## 12. 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 justify your identity and the relevance of your request.

If, despite our response, you were not satisfied, you have the possibility to contact directly the Commission Nationale Informatique et Liberté (CNIL) at the following address <https://www.cnil.fr/fr/vous-souhaitez-contacter-la-cnil>.

## 13. Modification of our Privacy Policy

If we were to modify our Privacy Policy, we would inform you by any appropriate means.

## 14. Use of Cookies

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