CyberPeace Institute
Campus Biotech Innovation Park
15 avenue de Sécheron
1202 Genève, Suisse

Simplified Privacy Information Notice and Consent Declaration

The CyberPeace Institute is an independent and neutral non-governmental organization whose mission is to ensure the rights of people to security, dignity and equity in cyberspace. We work in close collaboration with relevant partners to reduce the harms from cyberattacks on people's lives worldwide. To achieve our mission, we collect personal data for the purposes of helping you and others understand and limit the impact of cyberattacks. We are committed to giving you full control of your personal data, and you can email us at privacy@cyberpeaceinstitute.org with any question, comment or request regarding your data, including any request to exercise your data protection rights.

We are based in Avenue de Sécheron 15, 1202, Geneva, Switzerland and we act as Data Controller for your personal data, which we process on the basis of Swiss Federal Act on Data Protection ("FADP") of 19 June 1992 (Status as of 1 March 2019, and subsequent updates). In addition, due to our global reach, we comply with the General Data Protection Regulation (Reg. (EU) 2016/679 or "GDPR"), where applicable.

Definitions

- **Data –** In the context of this Notice *Data* essentially refers to digital assets. Digital assets are any machines that are deployed on the Internet by your organization and are identified by specific IP addresses, CIDR blocks or domains. IP addresses are considered as Personal Data. In limited cases, and if you ask us to do so, we may process identity data (Name, Last Name). Furthermore, even though we do not request any sensitive data from you, it is possible that such data may appear in the comparisons and matches carried out in the course of our activities.
- **Data Processing –** Processing covers a wide range of operations performed on personal data, including by manual or automated means. It includes the collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of personal data.
- **Threats** – Any circumstance or event with the potential to adversely impact a digital asset through unauthorized access, destruction, disclosure, modification of data, and/or denial of service.
- **Vulnerability** – The existence of a weakness, design, or implementation error that can lead to an unexpected, undesirable event compromising the security of the computer system, network, application, or protocol involved.

If you provide your consent using the Consent Declaration below, we will process your data for the following purposes:

1) Detecting cyber threats and vulnerabilities related to your organization's IT environment

We use your data to determine whether your IT environment is associated with any known threats or vulnerabilities. We process your *Data*, notably by regularly cross-checking and analysing it against our own internal databases, or the databases of one or more of the Institute's vetted partners. Monitoring of new activity and the generation of alerts will permit the CyberPeace Institute's dedicated team of analysts to be warned in the case of newly identified threat or vulnerability and contact your organization in relevant cases.

CyberPeace Institute
Campus Biotech Innovation Park
15 avenue de Sécheron
1202 Genève, Suisse

2) **Analyzing cyber threats and vulnerabilities related to your organization's IT environment to identify trends or emerging issues across the not for profit sector**

We use your *Data* to aggregate information relating to the identified threats and vulnerabilities of your IT environment with those of other not for profit organizations in order to identify specific trends and emerging issues associated with the not for profit sector. For this purpose, we will use your *Data* to identify the threats and vulnerabilities but any analysis and findings generated from the aggregation of the information will not include *data* identifiers such as specific IP address, CIDR block or domain.

For the two processing purposes, information relating to your *data* and identified threats and trends, will be stored in the CyberPeace Institute's secure systems for the duration of our partnership or for a 5-year period, following which we will ask you whether you'd like us to continue storing your data or not.

More details about the processing activities and your privacy rights are found in the attached Annex, which you must read before signing the Consent Declaration.

CyberPeace Institute
Campus Biotech Innovation Park
15 avenue de Sécheron
1202 Genève, Suisse

Annex - Details of Data Processing carried out by the CyberPeace Institute

The CyberPeace Institute is committed to making privacy easy to understand for everyone. We believe that providing transparent information is a fundamental component of peace in cyberspace. By providing information about data processing in plain and accessible language, we hope to encourage people to take the time to read this notice and to understand how they can exercise their rights.

The Simplified Privacy Information Notice provides the main details about the processing purposes and is intended to give you a quick overview of how we process your data. This Annex contains more information and explains our processing activities in more detail.

1. Legal basis for data processing

Due to the potentially sensitive nature of the personal data we collect, we ask for express, informed, and free consent, which can be given using the attached Consent Declaration for all agreed purposes.

The consent to any data processing activity can be withdrawn at any time, by sending an email to privacy@cyberpeaceinstitute.org. The withdrawal of consent will not affect the validity of the data processing carried up until the moment of withdrawal. After we receive the email by which the consent is withdrawn for a data processing activity, we will cease the processing of the concerned personal data for that activity and delete it.

2. Detecting cyber threats and vulnerabilities related to your organization's IT environment

To determine whether your IT environment may be associated with any cyber threats or vulnerabilities, we will use your data as defined in the definitions section.

Once the data is stored we will use it to automatically and regularly check for any matches against data points with the CyberPeace Institute's internal databases or the databases of one or more of the Institute's vetted partners. We expand the checks to include partner databases so as to increase our likelihood of detecting threats and vulnerabilities by increasing the number of data sources against which we query.

> If a match is identified, an automatic alert will be generated and securely transferred to a CyberPeace Institute analyst to assess its validity, accuracy and relevance. In the case where a match is considered valid, accurate and relevant to your Organization's cybersecurity, you will be informed through a secure communication channel. The *Data* will continue to be stored in the CyberPeace Institute's systems to provide a continuous monitoring of your IT environment to detect any new threats or vulnerabilities.
>
> If no match is identified, the data will continue to be stored in the CyberPeace Institute's systems to provide a continuous monitoring of your IT environment to detect any new threats or vulnerabilities.

We store the data for the duration of our partnership or for a 5-year period, following which we will ask you whether you'd like us to continue storing your data or not.

CyberPeace Institute
Campus Biotech Innovation Park
15 avenue de Sécheron
1202 Genève, Suisse

3. **Analyzing cyber threats and vulnerabilities related to your organization's IT environment to identify trends or emerging issues across the not for profit sector**

If you provide your consent, we will carry out continuous investigative and analysis activities to determine whether the threats and vulnerabilities associated with your IT environment are similar or different to the threats and vulnerabilities associated with other organizations within your sector.

The activities that we may carry out for this purpose include:

- Identifying other organizations whose IT systems are associated with similar or different threats and vulnerabilities to your own. This will allow us to understand if:
    - organizations within your sector are facing similar threats and vulnerabilities to yours,
    - organizations within your sector are facing similar threats and vulnerabilities to other sectors,
    - organizations within your sector are being specifically targeted by specific cyberattacks or are subject to indiscriminate attacks
- Identifying trends and emerging issues relating to cyber threats and vulnerabilities including for example how these are changing over time, their geographical representation, the types of organizations impacted
- Identifying the modus operandi most used against the not for profit sector
- Potentially identifying the malicious actors that may be targeting the not for profit sector
- Identifying and prioritizing the types of capacity building and training the CyberPeace Institute should deliver to reduce the harm from cyber threats against not for profit organizations
- Producing CyberPeace Institute Analysis Reports to inform your organization and others of our findings

Any findings or reports will be limited to aggregate data that has been irreversibly anonymised.

4. **Security measures and confidentiality**

We understand that we are trusted with personal (and in some case sensitive) data and we know we have a responsibility to process this *Data* in a confidential manner and for the minimum time necessary in order to achieve the purposes described above.

To ensure the security of the processing activities and the protection of data, we are taking the following measures:

- we provide you with a secure transfer link for you to share your data with us
- we have assigned a team of developers and data scientists to process your data
- we have assigned a team of analysts and data scientists to analyze your data
- we process data under the Swiss Federal Act on Data Protection (FADP)
- we delete all unnecessary data during the “triage” phase of data processing

CyberPeace Institute
Campus Biotech Innovation Park
15 avenue de Sécheron
1202 Genève, Suisse

5. Your privacy rights

Each Data subject can exercise various rights in relation to his/her personal data. These rights are not absolute, and limitations may apply depending on the specific case. Each data subject rights request (DSR) is carefully evaluated by our legal counsel, who will reply to each DSR within 30 days from the date of receipt of all the information needed to process the request.

Below is a list of rights that the Data Subject is entitled to exercise in connection with his/her personal data:

- Right of access to the personal data we store about the Data Subject
- Right to rectification of incorrect data
- Right to erasure (right to be forgotten)
- Right to restriction of processing
- Right to data portability
- Right to object to data processing
- Right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning you or similarly significantly affects you.

To exercise any of these rights, kindly contact us at the email address above. To be sure that the request is coming from the Data Subject (and not from somebody pretending to be the Data Subject), we may ask the Data Subject to provide us with additional information to confirm identity. If the Data Subject provides any such information to us, then we will only use it to respond to his/her request.

You may also send us postal mail with your requests to: CyberPeace Institute, Avenue de Sécheron 15, Genève 1202, Switzerland. Please specify on the envelope “Data Protection Request”. Please note that we are not responsible for delays or failures of the postal service, so we do encourage you to send your requests by email or by registered mail, if possible.

Should you be unsatisfied with the response received, or should you wish to lodge a complaint, you may do so by contacting a data protection supervisory authority. A list of contact details of EU supervisory authorities is available here.