



DCAF - Geneva Centre for Security Sector Governance
International Security Sector Advisory Teams (ISSAT)
Platform Privacy and Cookies Policy

Last Updated: February 2024

1. Preamble

DCAF's International Security Sector Advisory Teams ("**ISSAT**") provides practical support to the international community in its effort to improve security and justice, primarily in conflict-affected and fragile states. ISSAT aims to develop and promote good security and justice reform practices and principles, notably by helping its members to build their capacity to support national and regional security and justice reform processes.

In order to accomplish these goals and missions, ISSAT notably operates a web-based platform, available at www.issat.dcaf.ch (the/our "**Platform**") and managed by ISSAT. The Platform is divided into two sections, namely:

- 1.1. A public section with information about ISSAT, and;
- 1.2. A Community of Practice (hereafter, "**Community of Practice**") for registered members, which provides for knowledge and learning exchanges on ISSAT activities. The Community of Practice is a private community deemed of use for ISSAT International Partner's Group Members working in the area of security, justice and development efforts to Official Development Assistance (ODA) recipient countries.

For the sake of clarity, the Platform, as defined herein, includes the main www.issat.dcaf.ch site and all extensions related to the private Community of Practice.

The present privacy and cookies policy ("**Privacy Policy**") explains how information relating to an identified or identifiable individual ("**Personal Data**") is collected, used and protected through the Platform. Please read this Privacy Policy carefully before using the Platform.

By browsing and using our Platform, you acknowledge that your Personal Data will be collected and processed in accordance with this Privacy Policy. If you do not wish your Personal Data to be processed according to the present Privacy Policy, we kindly ask you not to use our Platform.

2. Data Controller

The controller of Personal Data processed on this Platform is DCAF - Geneva Centre for Security Sector Governance ("**DCAF**", or "**we**", "**us**" or "**our**"), located at Chemin Eugène-Rigot 2E, CH-1211 Geneva, Switzerland. As mentioned above, the Platform is more specifically managed by ISSAT and can be contacted at issatcop@dcf.ch.

3. What is Personal Data?

Personal Data means any information relating to an identified or identifiable natural person, i.e. an individual, regardless of the form in which it is expressed. Personal Data is information that identifies you as an individual, directly or indirectly, in particular by reference to identifiers such as a name, surname, location data, an online identifier, e-mail address, etc.

4. Collection of Personal Data, and Our Use of Such Personal Data

4.1 Sources of Collection

The Personal Data we collect through our Platform can be divided into two categories:

- a) Cookies
- b) Personal Data you provide us with

4.2 Cookies

4.2.1 Cookies are files containing a small amount of data that are sent from a website/application to your browser and stored on your device (computer or mobile device). Other tracking technologies, such as beacons, tags, and scripts (“**Similar Technologies**”), may also be used to collect and track information and to improve and analyze the use of our Platform.

4.2.2 Using cookies, we may collect Personal Data when you use our Platform, for example we may identify certain usage data when you browse or click on content.

4.2.3 We collect the following information and Personal Data through the use of cookies, Similar Technologies:

- a) Device Data
 - (i) IP address of the requesting internet-enabled device;
 - (ii) Location of the requesting internet-enabled device based on the IP address;
 - (iii) Website or application from which the access was made (referrer URL);
 - (iv) Device names and browser subscription data (if PWA module is used).
- b) Web Analytics
 - (i) Visitor behaviour;
 - (ii) Account information, such as registration date, last login dates and last access dates;
 - (iii) Your Social media accounts;
 - (iv) The resources you access and use on the Platform, such as posts, events, discussions, content follows, file uploads, profile tags, etc.

4.2.4 In order to control or limit the collection of this information, you can:

- (i) If available, set up your browser to refuse all cookies and Similar Technologies or to indicate when a cookie or a Similar Technology is used;
- (ii) Delete cookies and Similar Technologies and clear your browsing data directly from your browser's settings.

Please note that if you refuse or block certain cookies, you may not have access to certain features and/or functionalities of the Platform.

4.2.5 The following cookies are used on the Platform:

NAME	PROVIDER	TYPE	DURATION	DESCRIPTION	COUNTRY
SSESS*	Open Social	Necessary		Used to identify authenticated users.	
has_js	Open Social	Necessary		The data is used to indicate whether the visitor's browser has JavaScript enabled.	
apbct_antibot	Cleantalk	Functional		This cookie is used to distinguish between humans and bots. This is beneficial for the Platform, in order to make valid reports on the use of the Platform.	Germany
apbct_cookies_test	Cleantalk	Functional		Used in order to detect spam and improve the Platform's security. Does not store visitor specific data.	Germany
apbct_prev_referer	Cleantalk	Functional		Used by the Platform to identify and eliminate spam on the Platform's comment-function.	Germany
apbct_timestamp	Cleantalk	Functional		Used in order to detect spam and improve the Platform's security. Does not store visitor specific data.	Germany
ct_check_js	Cleantalk	Functional		Used in order to detect spam and improve the Platform's security.	Germany
ct_fkp_timestamp	Cleantalk	Functional		Used in order to detect spam and improve the Platform's security. Does not store visitor specific data.	Germany
ct_has_scrolled	Cleantalk	Functional		This cookie is used to distinguish between humans and bots.	Germany
ct_pointer_data	Cleantalk	Functional		Used in order to detect spam and improve the Platform's security. Does not store visitor specific data.	Germany
ct_ps_timestamp	Cleantalk	Functional		Used in order to detect spam and improve the Platform's security. Does not store visitor specific data.	Germany

ct_sfw_pass_key	Cleantalk	Functional		Used by the Platform to identify and eliminate spam on the Platform's comment-function.	Germany
ct_timezone	Cleantalk	Functional		Used in order to detect spam and improve the Platform's security.	Germany
Analytics	Matomo	Functional		Analyze traffic and help us to improve your user experience.	Germany

4.2.6 Should you choose to embed content from third-parties when using our Platform, such as (but not limited to) content from Facebook, Twitter and YouTube, please note that such third-parties may set Cookies, notably in order allow you and other users of our Platform to connect to certain social networks and to provide certain services and additional features (including the ability to instantly see videos or share social posts). These third-parties may also use cookies to collect information with respect to your browsing habits in order to can present you with digital content that may be of interest. Please note that DCAF is not the data controller of the processing of personal data *via* the use of such third-party cookies, and that such processing is not subject to the present Privacy Policy. For information regarding the way that your personal data is processed by the aforementioned third-parties, please visit the privacy statements of such third parties: [Facebook](#), [Twitter](#) and [Youtube](#).

For what purpose do we collect this information?

4.2.7 We use cookies that we collect in order to:

- (i) Operate the Platform (session-related information)
- (ii) Authorize access to the Platform,
- (iii) Make certain features of the Platform available to you and to offer you additional functionalities;
- (iv) Monitor the Platform's usage (notably the overall popularity of the Platform and typical users paths through the Platform) and improve the Platform's services
- (v) Store information about your preferences, allowing us to customize the Platform according to your individual interests;
- (vi) Speed up your searches;
- (vii) Produce aggregate insights that do not identify you;
- (viii) Identify you and log your use, recognize you when you return to our Platform, track the activity on our Platform and hold certain information,
- (ix) Identify our Community members and allow online interaction.

Grounds for processing

- 4.2.8 Where we use cookies to operate our Platform and for security purposes, we process your Personal Data through cookies on the basis of our legitimate interest.
- 4.2.9 In addition, cookies and other functionalities mentioned above which would go beyond the purposes of our legitimate interests (for example: Analytics Cookies), are implemented upon your acceptance by means of our cookie banner that appears on our Platform.

4.3 Personal data Provided by You

- 4.3.1 We collect the Personal Data you have provided us on a voluntary basis, when, through our Platform, you:
- (i) Create an account to access the Community of Practice and a user profile;
 - (ii) Sign up for our newsletter;
 - (iii) Enter into, participate in or create a member group, a discussion, a topic, an album or an event;
 - (iv) When you contact us using the Platform's contact form.
- 4.3.2 Such Personal Data may include: your e-mail address, first and last name, date of birth, address and/or location, profile and/or banner image, the organization for which you work, the function you hold in this organization and expertise you may have, a self-introduction or profile's summary, your language, time-zone and phone number, your user name and password and your opinions and other communications shared on the Platform.
- 4.3.3 Kindly note that Community of Practice is restricted to registered users only and enables interaction amongst community members. In order to enable such interaction, certain elements of your Personal Data are visible to other Platform users, namely your profile, including your first and last name, and other Personal Data you choose to share, including the content you upload and the Personal Data as selected in your privacy settings.

For what purpose do we collect this information?

- 4.3.4 We collect the Personal Data you provide to us on a voluntary basis in order to provide the services you have requested, namely to:
- (i) Create your account and validate your registration into the Community of Practice;
 - (ii) Publish your profile for other Community of Practice members to view;
 - (iii) Allow you to use certain functionalities provided for in the Community of Practice, such as the creation or the participation in member groups, discussions, albums, topics or events;
 - (iv) Send you a newsletter;
 - (v) Inform you, through push notifications, of updates in the Community of Practice.

Grounds for processing

4.3.5 We process the Personal Data you have provided us on the basis of the execution of the contract, i.e. the terms of use of the Platform.

5. Disclosure of Your Personal Data to Third Parties

5.1. The Personal Data collected are primarily intended for communicating with you and improving our services. However, we may give certain independent contractors and affiliates access to the Personal Data in order to assist us with the operation of our Platform, as well as data management and marketing activities. This is the case for our contractor Open Social, based in the Netherlands and who manages the Platform, and their system maintenance subcontractors (Platform.sh) and cloud server provider (OVHcloud) which hosts the Platform, both located in France. Our newsletter provider (Brevo) is located in France.

5.2. We have taken all necessary steps to ensure that your Personal Data is processed securely and in accordance with this Privacy Policy and applicable laws. Through the implementation of the appropriate contracts, our contractor Open Social is committed to protect your Personal Data using procedures similar to ours.

6. Disclosure of Your Personal Data to Authorities

6.1. We may disclose, in accordance with applicable law, some of your Personal Data (including your communications) to the authorities if we consider it necessary for security purposes, to investigate possible fraud and/or attempts to harm other users of our Platform. Hence, we may use your Personal Data to investigate, respond to and resolve complaints or disputes relating to our Platform.

6.2. It is possible that we will need to disclose your Personal Data when required by law or if we have good faith belief that disclosure is necessary to:

- (i) Investigate, prevent, or take actions regarding suspected or actual illegal activities or to assist government enforcement agencies;
- (ii) Enforce our agreements with you;
- (iii) Investigate and defend ourselves against any third-party claims or allegations;
- (iv) Protect the security or integrity of our Platform; or
- (v) Exercise or protect the rights and safety of our users, employees, or others.

6.3. We attempt to notify users about third-party requests for their Personal Data when appropriate in our judgment and technically feasible, unless prohibited by law or by an authority decision or when the request is an emergency. We may dispute such requests when we believe, in our

discretion, that the requests are too broad, vague or lack proper authority, but we do not promise to challenge every request.

- 6.4. The purpose of sharing your Personal Data with the aforementioned authorities, is to comply with a legal obligation to which we are subject.

7. No Disclosure of Your Personal Data for Commercial Purposes

- 7.1. We do not sell your Personal Data to third parties. We do not share or otherwise make available your Personal Data to third parties, except as provided in this Privacy Policy.

8. Cross-border Communication of Personal Data

- 8.1. For some of the third-party service providers, we may transfer your data to one of their databases outside Switzerland or the European Economic Area, potentially including countries which may not have an adequate level of protection for your Personal Data compared with that provided in Switzerland or the European Economic Area. In such event and unless provided otherwise in this Privacy Policy, we enter into agreements with such third-parties ensuring an adequate level of protection for your Personal Data. By providing us with your Personal Data or by accepting analytic cookies, you agree that we may transfer, store and process your Personal Data outside of Switzerland and the European Economic Area – in particular in the USA – and acknowledge that governments in certain countries such as the USA have broad powers to access data for security, crime prevention and detection and law enforcement purposes.

9. Protection of Your Personal Data and Notification of Personal Data breach

- 9.1. We are committed to using commercially reasonable means to prevent exposure or disclosure of your Personal Data. In particular, we implement and maintain measures (including administrative, physical, and technical measures) to manage unauthorised disclosures or exposures of your Personal Data.
- 9.2. In the event of a data breach, or in the event that we suspect a data breach, we will (i) use our best efforts to promptly notify you, where technically feasible, and (ii) cooperate with you to investigate and resolve the data breach, including, without limitation, by providing reasonable assistance to you in notifying injured third-parties. We will give you prompt access to such records related to a data breach as you may reasonably request; provided this does not give you access to records belonging to, or compromising the security of, other users.

9.3. In the event of a data breach, or in the event that we suspect a data breach, we will in addition notify the competent authorities in accordance with applicable law.

10. Management of Your Personal Data (Your Rights)

10.1. **Right to access and update** your Personal data: Wherever we process your Personal Data, we take reasonable steps to ensure that your Personal Data is kept accurate and up-to date for the purposes for which it was collected.

10.2. **Right to delete** your Personal Data: You may request the deletion of your Personal Data at any time, subject to any retention obligations imposed on us.

10.3. **Right of rectification:** You have the right to obtain the rectification of your Personal Data if it is inaccurate or incomplete.

10.4. **Right to object to processing:** To the extent permitted by law, you have the right to object our processing of your Personal Data.

10.5. **Right to limit processing:** To the extent permitted by law, you have the right to obtain a limitation of the processing of your Personal Data.

10.6. **Right to data portability of Personal Data:** You have the right to be provided with a copy of the Personal Data we have on you in a structured, machine-readable and commonly used format.

10.7. **Right to withdraw consent:** To the extent permitted by law, you have the right to withdraw your consent at any time when the processing of your Personal Data is based on it. However, it should be noted that such withdrawal:

- (i) does not affect the lawfulness of any processing carried out prior to such withdrawal and based on your consent; and
- (ii) may result in you no longer being able to use certain features of the Platform.

10.8. **Right to complain to a supervisory authority:** You have the right to complain to any competent supervisory authority about the collection and use of your Personal Data.

We may ask you to prove your identity before responding to a request based on the above rights or otherwise related to your Personal Data. In order to exercise your rights described above, you may make your request in writing by sending an email to us at the following address: issatcop@dcaf.ch, or by post to the following address: DCAF - Geneva Centre for security Sector Governance Chemin Eugène-Rigot 2E, CH-1211 Geneva, Switzerland.

11. Retention of Your Personal Data

11.1. We retain the Personal Data you provide to the extent necessary to provide you access to and use of our Platform and its functionalities (like for instance our newsletters), as well as to the

extent necessary to comply with our legal obligations (for example, if we are required to retain your Personal Data to comply with applicable laws), to resolve disputes, or enforce our legal agreements we have entered into and our internal policies.

- 11.2. The storage period of cookies depends on their purpose and is the same for everyone. We may retain de-personalized (i.e anonymous) information after the deletion of your Personal Data for an indefinite period of time. Site Managers do have the option to remove all the data associated with a user account upon deletion.

12. Amendment of This Privacy Policy

- 12.1. We may change this Privacy Policy at any time by posting a new version on this page or on a successor page, without prior notification. If we make changes to this Policy, we will notify you through a notice on the Platform home page. By continuing to access or use our Platform after such notification becomes effective, you acknowledge the processing of your Personal Data in accordance with the revised Privacy Policy. If you do not wish your Personal Data to be processed in accordance with the revised Privacy Policy, please do not use our Platform.
- 12.2. The new version of the Privacy Policy will become effective on the date it is posted, which will be listed at the top of the page as the new effective date.

13. Questions

- 13.1. Should you have questions or complaints regarding the present Privacy Policy, please contact us by e-mail at jssatcop@dcaf.ch.
- 13.2. You can also reach us by post at: DCAF - Geneva Centre for security Sector Governance, Chemin Eugène-Rigot 2E, CH-1211 Geneva, Switzerland.

* * * * *

In addition to the above Privacy Policy, more information about DCAF's data protection principles is available in the [DCAF's Charter Governing Data Privacy](#).