PRIVACY NOTICE

Thank you so much for choosing to find out more about Transparency International by visiting our website. As transparency is at the core of our organisation and how we operate, we've tried to explain to you in the clearest way possible what information we collect, how we use it and what rights you have in relation to it within this Privacy Notice. We've included a Glossary at the end of this Privacy Notice to explain any capitalised letters or terms that we've used in this Privacy Notice in order to make it as user-friendly as possible.

If for any reason any part of this Privacy Notice is not clear enough for you, please do get in touch with our Data Protection Compliance Team at dataprotection@transparency.org as we welcome any feedback to improve it. This is because we care deeply about data protection and we know that when you share your information with us, it is because you trust us, and we are committed to maintaining that trust.

1. ABOUT US

We hold the powerful and corrupt to account through a variety of activities including raising awareness of corruption and its impact, promoting transparency and accountability in politics and business, developing coalitions to address corruption, developing, and disseminating tools to curb corruption as well as supporting institutions to combat corruption.

We are leading global action against corruption with our international Secretariat in Berlin and through national chapters in more than 100 countries. This Privacy Notice primarily applies to the international Secretariat and covers all website users, newsletter subscribers, candidates for vacancies, participants seeking to join our network of experts as well as suppliers that engage with us.

2. DATA PROTECTION LEGAL REQUIREMENTS

We Process your Personal Data only to the extent permissible under statutory provisions, in particular, under the German Federal Data Protection Act (Bundesdatenschutzgesetz) and the European Union's General Data Protection Regulation ("EU GDPR"); our Data Protection Compliance Team keeps up to date with current Data Protection Laws.

Data Protection Laws have created the concepts of a "Data Controller" and a "Data Processor". Transparency International acts in the capacity of a Data Controller. A Data Controller determines the purposes and means of Personal Data Processing (Article 4(7) of the EU GDPR) which means that we decide what, when and how we Process any Personal Data that we receive.

The Data Controller details for our Transparency International Secretariat are as follows:

- Legal entity: Transparency International e. V.
- Address: Alt-Moabit 96, 10559 Berlin, Germany
- Telephone: +49 30 343820 0

Our lead Data Protection Supervisory Authority for our international secretariat is the Berlin Commissioner for Data Protection and Freedom of Information.

3. DIFFERENT TYPES OF PERSONAL DATA

We collect, use, store and transfer different kinds of Personal Data depending on our relationship with you. In general, we collect the following types:

- Identity Data (e.g. first name, maiden name, last name, title, date of birth).
- Contact Data (e.g. phone number, email address, address).
- Profile Data (e.g. your interests, education, professional experience).
- Communications & Marketing Data (e.g. your preferences in respect of cookies and marketing).
- Financial & Transaction Data (e.g. bank account details, invoices, payment details and history).
- Technical & Usage Data (e.g. internet protocol addresses, browser type and version, time zone settings and location and information about how you use our websites).

We also collect, use and share "Aggregated Data" such as statistical or demographic data for other purposes including research and analysis. Aggregated Data could be derived from your Personal Data but is not considered Personal Data under Data Protection Laws as this data will not directly or indirectly reveal your identity. For example, we may aggregate your Technical & Usage Data to calculate the percentage of users accessing a specific page on the website. However, if we combine or connect Aggregated Data with your Personal Data so that it can directly or indirectly identify you, we treat the combined data as Personal Data which will be used in accordance with this Privacy Notice.

We occasionally collect some Special Category Personal Data about you (such as information about your health where you are a prospective member of staff). We only collect this type of Personal Data when we have a legal ground in which to do so (i.e., you have given us your Consent and chosen to provide us with this data), Art. 9(2) of the EU GDPR. We do not collect any Criminal Convictions Data, Art. 10 of the EU GDPR, except in the employment context and where we are permitted by law to do so when completing background checks on prospective staff.

4. "I AM A WEBSITE USER" OR "I AM A NEWSLETTER SUBSCRIBER"

What do we collect? We collect Technical & Usage Data (for tracking purposes). We also collect Identity Data, Contact Data and Communications & Marketing Data (if you decide to get in touch with us).

How do we collect this? As you interact with our websites (Transparency.org and knowledgehub.transparency.org and iaccseries.org and j4t.org), we automatically collect this data about you by using cookies and similar technologies (check out our Cookie Notice. For Knowledge Hub you can find the Cookie Notice here. For the IACC you can find the Cookie Notice here and for Journalists for Transparency, here). We also collect this data through our direct interactions with you such as when you subscribe to our newsletters, contact us or participate in our surveys and events.

What's our legal ground(s) for Processing? One or more of the following apply:

- Consent (i.e. in that you are choosing to provide us with your details so that we can contact you) in accordance with Article 6(1)(a) of the EU GDPR. For our newsletters, we follow the double-opt in procedure and give you the option to unsubscribe at any point in time.

- Legitimate Interests (i.e. its necessary for our Legitimate Interests in running and developing our organisation and in particular, our websites) in accordance with Article 6(1)(f) of the EU GDPR.
- Legal obligation (i.e. its necessary for us to comply with a legal obligation such as in the instance where you no longer wish to be contacted for marketing purposes) in accordance with Article 6(1)(c) of the EU GDPR.

Thank you so much for visiting our website, following us and showing an interest in our work. If you have any thoughts or questions, please do feel free to contact us on ti@transparency.org. If you share our vision of a world in which government, politics, business, civil society and the daily lives of people are free of corruption, please also follow us on the following platforms LinkedIn, Twitter, Facebook, Instagram, YouTube and TikTok.

5. "I AM SEEKING TO REGISTER FOR THE IACC CONFERENCE, SIGN UP FOR THE YOUNG JOURNALISTS INITIATIVE OR THE SOCIAL ENTREPRENEUR INITIATIVE"

What do we collect?

- Identity Data (e.g. first name, maiden name, last name, title, date of birth).
- Contact Data (e.g. phone number, email address, address).
- Profile Data (e.g. your interests, education, professional experience).
- Communications & Marketing Data (e.g. your preferences in respect of cookies and marketing).
- Financial & Transaction Data (e.g. bank account details, invoices, payment details and history).
- Technical & Usage Data (e.g. internet protocol addresses, browser type and version, time zone settings and location and information about how you use our websites).
- Video and audio recordings and photography:

Video and audio recordings and photography will be conducted during the event for documentation and evaluation and for publication of the recordings on www.iaccseries.org and www.transparency.org, and on the IACC's and Transparency International's social media platforms, including Twitter, Facebook, Instagram, LinkedIn, YouTube and TikTok. Pictures will also be shared with journalists covering the conference for publication in non-IACC/Transparency International outlets. Making recordings of the online and in person event and publishing them on these platforms is an essential purpose of the IACC event. When you participate in the IACC event, you consent to any such filming, photography and live streaming.

- Joining the in-person event:

Audio and video recordings as well as pictures will be taken during the event. Some parts of the event may be live streamed. If you are not a speaker and you are not actively participating in the event, we understand that there are situations where you want to avoid being one of the central subjects in pictures or videos. We ask you to make your wishes known to our staff upon entering. We may ask you to wear a special lanyard or other form of sign that allows the photographer(s) to recognise you. You will be informed by signs at the entrance area of the event about filming, photography and live streaming.

- Joining online:

In addition to the chat in which all participants can write messages using their login name, the recordings may also contain audio or video recordings of you, provided that you have actively participated in the event as a speaker or participant and by voluntarily enabling the respective functions (microphone, camera) on your own device. Your login name will be the default, but you have the option of participating anonymously by entering a pseudonym when joining an event and by leaving your camera and microphone deactivated. If you do not want to be recorded, please do not turn on your camera or video.

How do we collect this? As you interact with our websites (transparency.org and iaccseries.org), we automatically collect data about you by using cookies and similar technologies. We also collect data through our direct interactions with you, such as when you register for the IACC event, apply to an open call for the young journalists initiative or organise a workshop for the event, contact us or participate in our surveys and events.

What are our legal ground(s) for Processing? One or more of the following apply:

- Consent (i.e. that you agree to recordings during the event, or to receive information and updates regarding future IACC Series events) in accordance with Article 6(1)(a) of the EU GDPR. For our newsletters, we give you the option to unsubscribe at any point in time.
- Legitimate Interests (i.e. it's necessary for our Legitimate Interests in planning, organising and conducting the IACC event and to provide you with information regarding the IACC event up to one year after the event took place, or when you are recorded as part of a group of people) in accordance with Article 6(1)(f) of the EU GDPR.
- Legal obligation (i.e. it's necessary for us to comply with a legal obligation such as in the instance where you no longer wish to be contacted for marketing purposes) in accordance with Article 6(1)(c) of the EU GDPR.
- Contract (i.e. in that we need this information to enter into or perform a contract with you) in accordance with Article 6(1)(b) of the EU GDPR.

6. "I AM SEEKING TO JOIN THE NETWORK OF EXPERTS" OR "I AM A CANDIDATE APPLYING FOR A VACANCY"

What do we collect? We collect Technical & Usage Data (for tracking purposes). We also collect Identity Data, Contact Data, Profile Data and Communications & Marketing Data (such as information submitted as part of your application to join us).

How do we collect this? As you interact with our websites, we automatically collect this data about you by using cookies and similar technologies (check out our Cookie Notice here). We also collect this data through our direct interactions with you and third parties (such as recruitment agencies or your references).

In our application process we are using Softgarden as service provider. Please read Softgarden's Privacy Notice for more information.

What's our legal ground(s) for Processing? One or more of the following apply:

- Consent (i.e. in that you are choosing to provide us with your details as part of your application) in accordance with Article 6(1)(a) of the EU GDPR.
- Contract (i.e. in that we need this information to check your application and potentially enter into a contract with you) in accordance with Article 6(1)(b) of the EU GDPR and § 26 BDSG.

7. "I AM A POTENTIAL DONOR" OR "I AM AN EXISTING DONOR"

Thank you very much for considering us or already supporting our mission. We are grateful for the range of donors that support us including government agencies, multilateral institutions, foundations, the private sector and individuals. Please read our Donor Privacy Notice for more information. We also invite you to contact our fundraising team directly on donations@transparency.org should you have any questions or wish to discuss the Donor Privacy Notice further.

8. "I AM A POTENTIAL SUPPLIER" OR "I AM AN EXISTING SUPPLIER"

What do we collect? We collect Technical & Usage Data for tracking purposes. We also collect Identity Data, Contact Data, Profile Data and Financial & Transaction Data for when we are engaging you for your services.

How do we collect this? As you interact with our websites, we automatically collect this data about you by using cookies and similar technologies (check out our Cookie Notice here). We also collect this data through our direct interactions with you (i.e. we will hold Personal Data on your staff that have engaged with us).

What's our legal ground(s) for Processing? One or more of the following apply:

- Contract (i.e. in that we need this information to enter into or perform a contract with you) in accordance with Article 6(1)(b) of the EU GDPR.
- Legitimate Interests (i.e. its necessary for our Legitimate Interests in keeping records for planning and strategic purposes) in accordance with Article 6(1)(f) of the EU GDPR.
- Legal obligation (i.e. its necessary for us to comply with a legal obligation such as in respect to our financial, tax and legal and compliance affairs) in accordance with Article 6(1)(c) of the EU GDPR.

9. SHARING YOUR PERSONAL DATA

We transmit your Personal Data only to the extent permissible under statutory provisions or if you have given your Consent in individual cases.

We share your Personal Data with our staff in order for them to fulfil their roles and work towards our mission. All of our contractual documentation with workers, employees and independent contractors includes confidentiality and data protection obligations.

We share your Personal Data with third-party organisations that we use for various purposes.

- Some of these third-party organisation act in the capacity of a Data Controller whereas others act in the capacity of a Data Processor.

- In both circumstances, we enter into the appropriate contractual documentation with our third-party organisations when sharing your Personal Data.
- For example, with any Data Processors we ensure that the contractual terms required under Article 28 of the EU GDPR are incorporated.

We will only share your Personal Data when necessary and have outlined categories of recipients of third-party organisations with whom we share it with:

- Technology companies (e.g. Google, Microsoft, Salesforce, Pardot, Infogram) that provide us with desktop and cloud-based products, solutions and services which we need in order to achieve our mission.
- Payment providers (e.g. Stripe) that we use to Process any donations received from you.
- Professional advisers such as law firms, banks and accountancy firms, as we need to engage with them for the purposes of our business.
- Data Protection Supervisory Authorities, regulators and other governmental authorities, as we need to engage with them for the purposes of them governing our operations.

We choose our service providers carefully and require all third-party organisations to respect the security of your Personal Data and to treat it in accordance with Data Protection Laws. We enter into contractual documentation with all of our third-party organisations (with the exception of Data Protection Supervisory Authorities, regulators and governmental authorities) which include the appropriate data protection clauses.

10. TRANSFERRING DATA ACROSS BORDERS

We share your Personal Data within our international secretariat and amongst our chapters and with certain third-party organisations, as described above.

Whenever your Personal Data travels outside of the European Economic Area ("**EEA**"), we ensure that it's protected by putting in one of the following safeguards:

- We only transfer your Personal Data to countries that have been deemed to provide an adequate level of protection for Personal Data by the European Commission (through what is known as an "adequacy decision"). Examples of countries which have received an adequacy decision include Argentina, Japan and the United Kingdom.
- We only transfer your Personal Data where we have entered into specific contractual terms with an organisation outside of the EEA which states that they will ensure that your Personal Data has the same level of protection as if it were in the EEA. These specific contractual terms are found in the European Union's Standard Contractual Clauses.
- We only transfer your data if you have explicitly consented to the proposed data transfer and we have provided you with all necessary information about the risks associated with the transfer.

If you want to find out the specific mechanism used when transferring your Personal Data out of the EEA, please contact our Data Protection Compliance Team.

11. DATA RETENTION

We will only keep your Personal Data for as long as reasonably necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, regulatory, tax, accounting or reporting requirements, or to fulfil our (post-)contractual obligations. We may retain your Personal Data for a longer period in the event of a complaint or if we reasonably believe there is a prospect of litigation in respect to our relationship with you, or if you have given us your Consent to do so.

To determine the appropriate retention period for Personal Data, we consider the amount, nature and sensitivity of the Personal Data, the potential risk of harm from unauthorised use or disclosure of your Personal Data, the purposes for which we Process your Personal Data and whether we can achieve those purposes through other means, and the applicable legal, regulatory, tax, accounting or other requirements.

In this section we have outlined our standard retention periods for some of the Personal Data mentioned in this Privacy Notice:

- Any Personal Data in connection with a successful application for a vacancy will be stored as part of your personal file. In case it did not come to a job offer we will delete your Personal Data 6 months after the end of the application process, or 2 years after the end of the application process in case you gave us your Consent to do so.
- Your Personal Data in our logfiles will generally be deleted after 2 months.
- As a newsletter recipient, your Personal Data will be deleted 3 years after you have revoked your Consent to receive our newsletters.
- Any Personal Data in connection with the IACC conference will generally be deleted after 1 year, except for when registrants have asked to stay informed about the IACC, and except for the recordings and content of the workshops and plenary sessions. We may retain your Personal Data for a longer period in the event that you have given us your Consent to do so.
- Due to statutory storage duties Personal Data that is relevant for our financial statements may be stored for up to 10 years according to Art. 147 of the Fiscal Code of Germany.

As a note, in some circumstances we will anonymise your Personal Data (so that it can no longer be associated with you) for research or statistical purposes, in which case we may use this information without further notice to you.

12. YOUR DATA SUBJECT RIGHTS

Under certain circumstances, you have specific rights in respect of the Personal Data that we Process about you. The fulfilment of the legal requirements to exercise these rights must be assessed on a case-by-case basis. Your rights include:

- the right of access to the Personal Data we hold about you, in accordance with Article 15 of the EU GDPR.
- the right to rectify (i.e. correct) your Personal Data where it is inaccurate or incomplete, in accordance with Article 16 of the EU GDPR.
- the right to delete your Personal Data, in accordance with Article 17 of the EU GDPR, but only in specific circumstances, for example where the Personal Data is no longer necessary in

relation to the purpose for which it was originally collected or Processed. It may not therefore always be possible for us to delete all of the information we hold about you if you request this, for example, if we have an ongoing contractual relationship with you.

- the right to restrict Processing in specific circumstances, in accordance with Article 18 of the EU GDPR, for example while we are reviewing the accuracy or completeness of data or deciding on whether any request for erasure is valid.
- the right to data portability which means the right to receive, move, copy or transfer your Personal Data to another Data Controller, in accordance with Article 20 of the EU GDPR. You have the right to this when we are Processing your Personal Data based on Consent or on a contract and the Processing is carried out by automated means.
- the right to object to Processing in cases where Processing is based upon our Legitimate Interests or where Processing is for direct marketing purposes, in accordance with Article 21 of the EU GDPR.
- the right to withdraw consent to our Processing of your Personal Data, in accordance with Article 7(3) of the EU GDPR, at any time with effect for the future.
- the right to lodge a complaint with the appropriate Data Protection Supervisory Authority, in accordance with Article 13(2)(d) of the EU GDPR.

If you wish to exercise any of the rights set out above, please contact our Data Protection Compliance Team. You will not have to pay a fee to access your Personal Data or to exercise any of the other rights. However, we may charge a reasonable fee if your request is clearly unfounded, repetitive or excessive. Alternatively, we could refuse to comply with your request in these circumstances.

We may need to request specific information from you to help us confirm your identity. This is a security measure in your own interest to ensure that Personal Data is not disclosed to any person who has no right to receive it. We may also contact you to ask for further information in relation to your request to speed up our response.

We try to respond to all legitimate requests within one month. It could take us longer than one month if your request is particularly complex or you have made a number of requests. In this case, we will notify you and keep you updated.

13. DATA SECURITY

We have put in place appropriate technical and organisational security measures to prevent your Personal Data from being accidentally lost, falsified, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your Personal Data to the workers, employees, independent contractors and other third-party organisations who have a reason to know. We have put in place guidelines, procedures and plans to deal with any suspected or actual personal data breaches. Please be aware that despite the application of due care and attention to the respective current technical standards loss of or damage to your Personal Data cannot be ruled out (especially the use of cloud-based services, email communication, mobile communication and video conferences harbour certain risks).

14. THIRD-PARTY LINKS AND SOCIAL MEDIA PLUGINS

Our websites may include links to third-party websites, plug-ins and applications. Clicking on those links or enabling those connections may allow third parties to collect or share data about you.

For example, when you access our websites, there are certain components employed by Facebook, Instagram, Twitter, LinkedIn, YouTube and Vimeo that are integrated within our websites and these components prompt your browser to download a unique identifier which give these other organisations more insight on your browsing activities, such as the specific pages on our websites that you have visited.

We do not control these third-party websites, plug-ins and applications and are not responsible for their privacy statements and the data that they collect. If you have an account with Facebook, Instagram, Twitter, LinkedIn, YouTube and Vimeo and you do not want these third parties to have access to your browsing activities, we recommend that you log out of your accounts before accessing our websites. When you leave our websites, we encourage you to read the privacy documentation of every website you visit.

15. CONTACT US

To get in touch with our Data Protection Compliance Team, please contact us on dataprotection@transparency.org.

Or you can contact us by post:

Transparency International e.V.

Data Protection Officer

Alt-Moabit 96

10559 Berlin

Germany

If you have any concerns and/or are not happy with our approach, you have the right to make a complaint to the Data Protection Supervisory Authority which is the Berlin Commissioner for Data Protection and Freedom of Information.

You can contact this Data Protection Supervisory Authority by using the following details:

- Address: Friedrichstr. 219, 10969 Berlin
- Email: mailbox@datenschutz-berlin.de
- Phone: 030 13889-0

Data Protection Laws are constantly evolving, and we endeavour to maintain best practice. However, we recognise that we may not always get it right. If you are not satisfied by the way we handle your Personal Data or wish to discuss our processes, we would like to hear from you and recommend that you contact us in the first instance.

16. GLOSSARY

Consent: refers to when an individual gives agreement which is freely given, specific, informed and is an unambiguous indication of their wishes. It is done by a statement or by a clear positive action in respect of the Processing of any Personal Data relating to them.

Criminal Convictions Data: refers to Personal Data relating to criminal convictions and offences and includes Personal Data relating to criminal allegations and proceedings.

Data Controller: refers to an organisation that determines when, why and how to Process Personal Data. It is responsible for establishing practices and policies in line with Data Protection Laws. There are certain circumstances where we act as a Data Controller.

Data Protection Laws: refers to the European Union's General Data Protection Regulation 2016/679 ("**EU GDPR**") and local data protection law including the German Federal Data Protection Act (also known as the Bundesdatenschutzgesetz).

Data Processor: refers to an organisation that Processes Personal Data on behalf of a Data Controller. It is also responsible for establishing practices and policies in line with Data Protection Laws and its contractual obligations with Data Controllers.

Data Protection Supervisory Authority: refers to independent public authorities / regulators that supervise, through investigative and corrective powers, the application of Data Protection Law. They provide expert advice on data protection issues and handle complaints lodged against violations of the EU GDPR and the relevant national laws.

European Economic Area ("EEA"): refers to the 27 countries in the European Union, Iceland, Liechtenstein and Norway.

Legitimate Interest: refers to when an organisation's interests are legitimate (as they need to do something to operate and be successful) and these interests do not override an individual's interests or fundamental rights and freedoms. We make sure to consider and balance any potential impact on individuals (both positive and negative) and their rights before we Process any Personal Data for our Legitimate Interests.

Personal Data: refers to any information identifying an individual or information relating to an individual that an organisation can identify (directly or indirectly) from that data alone or in combination with other identifiers that it Processes. Personal Data includes Special Category Personal Data, Criminal Convictions Data and pseudonymised Personal Data. Personal Data excludes anonymous data or data that has had the identity of an individual permanently removed.

Processing or Process: refers to any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties.

Special Category Personal Data: refers to information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data.

This Privacy Notice was last updated June 2022 and is currently applicable.