Privacy Notice

In order to provide for safe handling of personal data, technical and organisational measures are taken at all levels of processing, subject to regular reassessment. We collect individual data only to the extent necessary for the purpose of offering content and/or to serve contact requests.

We comply with the applicable regulations of the Bundesdatenschutzgesetz (BDSG) and the Telemediengesetz (TMG) of the Federal Republic of Germany, as well as (and in particular) the EU General Data Protection Regulation (GDPR).

In addition to this basic privacy notice, we selectively and as needed may make available amendments concerning more specific processing. Details depend on the purpose of the processing. This privacy notice therefore covers basic information mainly for visitors of this web site and/or people contacting us by a supported means of communication.

Requests for information, corrections, and objections can be sent at any time in writing to

> Tim Nicholas Rühlig
> Utrikespolitiska institutet
> Box 27035
> SE-102 51 Stockholm
> Sweden

or electronically to

> contact [at] timruhlig.eu .

Please consider our instructions for secure e-mail use.

Further details on the right to information, correction, and restriction/erasure can be found in the relevant subsections of section "Collecting and processing of personal data".

1. Web presence concerned

Our web presence includes the following Internet domains and their subdomains, which are all covered by this privacy policy:

- timruhlig.eu
- timruehlig.eu

2. Controller according to GDPR

Controller as of GDPR and its current national implementation and amendments (BDSG):

> Tim Nicholas Rühlig
> Utrikespolitiska institutet
> Box 27035

SE-102 51 Stockholm
Sweden

E-mail: contact [at] timruhlig.eu
Phone: +46-8-511 768 27

Please consider our instructions for secure e-mail use.

3. Responsible supervisory authority

You can contact the Hessian Data Protection Officer as follows:

Der Hessische Beauftragte für Datenschutz und Informationsfreiheit
Postfach 31 63
65021 Wiesbaden
Germany

Phone: +49 611 1408 0
Fax: +49 611 1408 611
E-mail: poststelle@datenschutz.hessen.de
Web: https://datenschutz.hessen.de/

Please consider our instructions for secure e-mail use. In particular, please note that you may send PGP-encrypted messages to the above e-mail address. The corresponding PGP key is available on the above web pages.

4. Filing a complaint

If you are of the opinion that the processing of your personal data violates the GDPR, you have the right to file a complaint with the above-mentioned supervisory authority or another competent supervisory authority of the Federal Republic of Germany, your place of work or the place of presumed violation, notwithstanding any other administrative or judicial remedy.

The supervisory authority to which the complaint has been lodged shall inform the complainant of the status and results of the complaint, including the possibility of a judicial remedy under Art. 78 GDPR.

5. Collecting and processing of personal data

5.1. Volume of data

We process personal data of our users only as far as necessary to provide our web presence and contents as well as potential other merits. Processing of personal data is only carried out with consent of the affected user, with an exception for cases precluding prior consent for substantial reasons if such processing of data is permitted by legal regulations.

5.2. General legal basis

Insofar as we obtain the consent of the data subject for the processing of personal data, Art. 6 para. 1 lit. a GDPR serves as the legal basis.

In the processing of personal data required for the performance of a contract to which the data subject is a party, Art. 6 para. 1 lit. b GDPR serves as the legal basis. This also applies to processing operations that are necessary to carry out pre-contractual measures.

Insofar as the processing of personal data is required to fulfil a legal obligation to which we are subject, Art. 6 para. 1 lit. c GDPR serves as the legal basis.

In the event that vital interests of the data subject or another natural person require the processing of personal data, Art. 6 para. 1 lit. d GDPR serves as the legal basis.

If processing is necessary to safeguard a legitimate interest of us or a third party and if the interests, fundamental rights, and freedoms of the data subject do not outweigh the first-mentioned interest, Art. 6 para. 1 letter f GDPR serves as the legal basis for processing. This aspect is taken into account as required in the respective context of the following subsections.

5.3. Visiting our web pages

No explicit transmission of personal data (registration, etc) is necessary for the use of our public web pages. Nevertheless, implicit usage data is generated during each visit, which can also be personal data.

1. For technical reasons, we temporarily store the following information for each retrieval of a web page, a web page component, or a download from our web presence: the IP address of the visitor, the time stamp of the retrieval, the address of the referencing web page, the address of the retrieved resource, the method of retrieval (GET/POST/....), the status/error code of the request, the size of the data transmitted, and information provided by the visitor's system on version and type of web browser and possibly operating system. This information is required to deliver the Web content and, if necessary, to support session management.
2. In addition, this information is fully stored in our log files and archived for at most seven days for security and technical optimization purposes. Such data will not be

used for other purposes, in particular not transmitted to third parties. Furthermore, it is stored separately from other personal data of the user.

3. After at most seven days in the log archive, the IP address is automatically anonymized by suitable means. To this end we remove or irreversibly replace the least significant 16 bits (IPv4) or 80 bits (IPv6) of the IP address. The remaining data is then only used in long-term technical/statistical evaluation and can no longer be traced back to individuals.
4. For immediate statistical purposes, the above information may also be processed upon each visit of our web pages and stored in a format preserving statistical properties only, with no correlation to individual identifiers.

Temporary storage of data and log files is covered by Art. 6 para. 1 lit. f GDPR. Both aspects are absolutely necessary for the operation of the web presence; in this regard the user has no possibility of objection.

5.4. Use of cookies, tracking

To provide essential basic functions beyond simple viewing functionality (individual settings, session management, and recognition of the login status) we may use so-called cookies. These are small data records that are stored on the visitor's browser by the respective web service and either contain the corresponding information directly or allow it to be associated on the server side. This can already occur the first time you visit a web page.

This mechanism allows a longer-term identification of the user, which may be necessary for authentication purposes and for full functionality of certain pages.

To eliminate the risk of unsolicited tracking, our use of cookies is very limited: If set at all, they are automatically deleted (as far as possible) after the end of the associated browser session. Our cookies may associate information about login status, language settings, sorting criteria for lists, and/or similar essential functions.

Cookies set by us can be deleted directly by the user at any time in order to prevent further storage/use of the respective information. This can cause session management to be interrupted, web-based services to be logged off, and/or individual settings to be reset. Furthermore, permanent deactivation of cookies can lead to permanent problems or restrictions in this context.

We do not use cookies to analyse the usage behaviour on our or other websites.

Furthermore, our web pages do not apply cookies or external resources for tracking or advertising. The creation of content is subject to corresponding internal guidelines; problematic embedding/transmission are technically prevented (as far as possible) or at least regularly checked for.

The processing of personal data using cookies that are technically necessary is covered by Art. 6 para. 1 lit. f GDPR. Our legitimate interest arises from the above description.

5.5. Use of e-mail

When contacting us by e-mail, please note that during transmission, sensitive data is only protected if e-mail encryption is used. You will find more information in the section "Data protection by encryption".

Messages sent to us should only include data that is required for the respective transaction, as we usually need to keep an original message for the time of processing the request, the duration of the resulting interaction, and any subsequent minimum storage periods. Selective deletion of transmitted data is therefore not always possible. Alternatively, blocking may be an option (see "Restriction and erasure").

The obligation to retain original e-mail messages also implies the recording of all information contained in message headers (including delivery logging, IP addresses contained therein, time stamps, and other message attributes).

Messages or message components are only forwarded to third parties if this is necessary or unavoidable for processing of the request. The fact and the extent of the data transmitted will be indicated in good time as required.

Notwithstanding the above handling, we will report obviously misdirected messages to the sender (if possible) and delete them immediately (without further retention).

Furthermore, if you are the recipient of a misdirected message from our side, we ask you to inform us and to delete the message immediately.

5.6. Storage of required data

Duration and extent of the preservation of personal data depend on the respective requirements of carrying out desired or necessary processes. Corresponding obligations on reporting and storage arise from (among other things) legal requirements and significantly define the overall parameters.

In principle, we only store objectively required data, and such preservation ends with the end of the requirement, i.e. erasure is performed immediately without further request, if no legal regulation opposes it.

For reasons of traceability, some processes (beyond viewing of our web pages) require a minimum storage period of three to six months. The storage periods can be further extended by legal obligation.

However, this as well as other uses can be objected to. Further information can be found in the subsection "Objection".

5.7. Automated copies

Irrespective of the above, automated copies are made within the scope of data redundancy and data backup. However, these do not extend the circle of authorized users and only serve availability and security.

5.8. Disclosure of data to third parties

Data will only be passed on to third parties if

- required by the specific relationship with the person concerned or by the nature of the service (other than just viewing our web pages),
- requested by supervisory authorities, inspection bodies, or law enforcement authorities in the context of threat prevention, security auditing, or law enforcement, or
- required by other legal obligations.

5.9. Right to information and rectification

In principle, every person has a right of access to their personal data stored by us, including the possibility of negative information, i.e. the confirmation that no personal data of the respective person is available or can be attributed to them. If such data is available, a request for information by the data subject may cover the following information:

1. Purposes for which your personal data is processed;
2. categories of such data;
3. recipients or categories of recipients (third parties) to whom this information has/will be disclosed;
4. intended retention period of this data (if palpable) or criteria for a foreseeable determination of the storage period;
5. applicable right to rectification, erasure, and restriction of such data, to limitation of processing, and to objection to such processing;
6. existing right of complaint to a supervisory authority;
7. available information on the origin of the data if it was not collected in direct contact with the person concerned;
8. the existence of automated decision-making in accordance with Art. 22 paras. 1 and 4 GDPR and, if applicable, meaningful information on the logic involved and the significance and intended effects of such processing for the data subject;
9. completed or intended transfer of data to a third country or an international organisation, as well as appropriate safeguards in accordance with Art. 46 GDPR relating to the transfer.

Please note that an attribution to a person must be possible. Corresponding identifying features have to be provided to us and, if necessary, authenticated by further information. This is needed in order to protect the data from unauthorized external access.

In addition, we can only consider data that has unique identifying features. We cannot provide information on data that is only linked to IP addresses or other features that we cannot attribute to a person.

Naturally, you may submit requests to rectify verifiable errors or augment insufficient information in the corresponding databases for continued adequate use. We will take them into account immediately (after checking for authenticity, if necessary).

See also subsection "Restriction of data-related rights".

5.10. Right to data portability

The data subject has the right to receive the personal data concerning them (which they have provided) in a structured, common, and machine-readable format. Furthermore, they have the right to transmission of this data to another controller without obstruction, or to have it transferred directly between two controllers, provided

1. processing is based on consent pursuant to Art. 6 para. 1 lit. a GDPR or Art. 9 para. 2 lit. a GDPR, or on a contract pursuant to Art. 6 para. 1 lit. b GDPR and
2. processing is carried out by means of automated procedures and the desired transmission is technically feasible.

This must not adversely affect rights and freedoms of other persons.

The right to data portability does not apply to the processing of personal data necessary for the performance of a task in the public interest that has been vested in us.

5.11. Automated decision-making

The data subject has the right not to be subject to a decision based exclusively on automated processing which has legal effects against them or significantly affects them in a similar manner. This right *does not apply* if the decision

- is necessary for entering into, or performance of, a contract between the person and us, and we take "appropriate measures" as set out below,
- is permitted by law of the Union or the Federal Republic of Germany, and that law lays down "appropriate measures" as set out below, or
- is made with express consent of the person, and we take "appropriate measures" as set out below.

The right *does apply* if the decision is based on special categories of personal data pursuant to Art. 9 para. 1 GDPR, unless Art. 9 para. 2 lit. a or g GDPR applies.

The so-called *appropriate measures* required by the referring cases above are those which are suitable to safeguard the rights, freedoms, and legitimate interests of the person, including at least the right to obtain human intervention on our part, to express one's point of view, and to contest the decision.

We do not apply automated decision making (in particular, do not apply profiling) pursuant to Art. 22 GDPR. Nevertheless, we use automated treatment of spam or malware in e-mail messages and in the context of input or contributions on our web pages, to the extent necessary for operational security or at the express request of the respective recipient.

According to the current interpretation, this type of automation does not fulfil the criteria of Art. 22 para. 1 GDPR.

5.12. Withdrawal of consent

The data subject may withdraw their consent to the processing of their data at any time pursuant to Art. 6 para. 1 lit. a or Art. 9 para. 2 lit. a GDPR, which, if possible, puts an end to the processing and leads to immediate erasure or, alternatively, restriction of the data concerned. Further details are described in the subsection "Restriction and erasure".

See also subsection "Restriction of data-related rights".

5.13. Objection

Pursuant to Art. 21 para. 1 or 2 GDPR, the data subject may at any time object to the processing of data carried out pursuant to Art. 6 para. 1 lit. e or f GDPR, which, if possible, puts an end to the processing and leads to immediate erasure or, alternatively, restriction of the data concerned. Further details are described in the subsection "Restriction and erasure".

Notwithstanding Directive 2002/58/EC, data subjects may exercise their right of objection in relation to the use of information society services by means of automated procedures using technical specifications (defensive measures).

See also subsection "Restriction of data-related rights".

5.14. Restriction and erasure

Unneeded personal data will be regularly and immediately deleted by us. This also covers the deletion of all redundantly stored copies and backups of data (possibly with a technical delay), as well as informing all third parties that have been recipients of permissible/necessary transmission of data (if possible, and with a potential delay caused by further storage obligations).

Upon request, we also arrange for the premature delisting or deletion of existing, originally necessary data, based on

- withdrawal of consent pursuant to Art. 6 para. 1 lit. a or Art. 9 para. 2 lit. a GDPR in the absence of any other legal basis for processing,
- an objection to the processing pursuant to Art. 21 para. 1 GDPR in the absence of overriding justified grounds,
- an objection to processing pursuant to Art. 21 para. 2 GDPR, or
- the notification of unlawful processing.

Even without explicit withdrawal or objection, previously required data will be deleted at the earliest possible time; more details are given in the subsection "Storage of required data".

Please note that data approved for publication can only be deleted to the extent of copies within our scope of influence. Copies already made within the scope of independent third

parties naturally remain unaffected by this. In accordance with Art. 17 para. 1 GDPR, we will attempt to arrange for the erasure of further copies or at least of references thereto, but are subject to practical restrictions.

It should be noted that in individual cases, due to

- legal storage obligations,
- pending enforcement of rights and claims,
- technical requirements,
- legitimate interests of the data subject,
- legitimate interests of another natural or legal person, or
- other public interest of the Union or of a Member State,

erasure may be postponed. We will inform you of this in the given case and will arrange for the corresponding data to be restricted, i.e. its use to be limited to the remaining necessary/permissible purpose, as a substitute, or as a transitional measure.

Restriction also applies if

- the data subject has lodged an objection to the processing pursuant to Art. 21 para. 1 GDPR and it has not yet been determined whether our justified reasons predominate,
- the accuracy of the data is in doubt, for as long as further clarification continues, or
- after unlawful processing, if the data subject explicitly objects to the required erasure of their data.

If the remaining grounds for the restriction no longer prevail, automatic erasure is performed as soon as possible.

See also subsection "Restriction of data-related rights".

5.15. Restriction of data-related rights

The right to information, rectification, restriction, and erasure may be limited insofar as its fulfilment can be expected to substantially hamper or prevent research or statistical purposes pursuant to Art. 89 para. 1 GDPR. This restriction can result from the necessity of general research, statistical evaluations, archiving purposes, and/or overall historical preservation.

In addition, there are restrictions insofar as the processing of existing data is necessary

- to exercise freedom of expression and information;
- to fulfil a legal obligation which requires processing under the law of the Union or the Federal Republic of Germany, or to perform a task in the public interest that has been vested in us;

- for reasons of public interest in the area of public health in accordance with Art. 9 para. 2 lit. h and i and Art. 9 para. 3 GDPR;
- for archiving purposes in the public interest, for scientific or historical research purposes, or for statistical purposes pursuant to Art. 89 para. 1 GDPR, insofar as the above-mentioned law is likely to make it impossible or seriously impair the attainment of the objectives of such processing; and
- to assert, exercise, or defend legal claims.

6. Security

In order to protect stored data against unauthorized access, manipulation, and loss, we regularly check the security of our systems as part of suitable technical and organisational measures.

Within this context, both internal and external security checks are carried out. Automated internal security checks may also cover passwords for individual restricted access, where applicable. Both newly selected and existing passwords are subjected to adequate triviality tests and checked for other known weaknesses. An affected user will be notified of any weaknesses found. If they pose an imminent danger, access restrictions may temporarily be imposed until all weaknesses have been remedied.

Personal passwords of our users, where applicable, will never be stored in clear text or transmitted to third parties in any form during the course of such security measures or regular operation, with the exception of transmission of initial/temporary passwords over restricted communication channels, as well as short-term processing on our systems for registration or authentication.

7. Data protection by encryption

For the best possible protection of the data of our visitors, partners, and members, our web pages and all other services dealing with personal data apply TLS encryption.

In the case of web services, this is indicated by addresses with the prefix **https://**.

In addition, our systems declare obligatory encryption for visitors of our web pages (HSTS), which leads to an encrypted connection being established by current browsers even after a web address of an unencrypted resource (i.e. without prefix or with prefix **http://**) has been entered.

With a modern browser, this protects all transmitted data (especially login data and other sensitive information) against reading by unauthorized third parties.

In addition, we support a number of methods for secure direct communication. Please contact us for details.

8. Links to external resources

Our web presence may contain links to other web pages and to external downloads which are beyond our sphere of influence. By selecting such links you will leave the scope of this privacy notice.

Accordingly, we cannot assume any responsibility for the use of those external resources and traces of data left there. Nevertheless, if we are made aware of problematic offers, we will immediately remove the corresponding links.