RISK TALK – Data protection notice

Declaration of Consent

Declaration of consent for the participants of the interactive community "RISK TALK" on the storage and use of personal data by the InsuResilience Secretariat (c/o Deutsche Gesellschaft für Internationale Zusammenarbeit GmbH) in Bonn, Germany.

As the protection and security of personal data is high priority for the InsuResilience Secretariat (c/o Deutsche Gesellschaft für Internationale Zusammenarbeit GmbH), this declaration explains what data relating to the participants of the interactive community "RISK TALK" is collected and the purpose for which it is used. We strictly adhere to the rules of the German Federal Data Protection Act (BDSG).

0. About RISK TALK

RISK TALK is intended to facilitate and encourage communication and collaboration between the climate change risk transfer community and to spread knowledge throughout this community available for all and everywhere. Participation is on a voluntary basis and by default questions are asked will remain anonymous. The company that developed that tool is the Swiss company called Starmind. Starmind Brain Technology uses artificial intelligence to map the expertise network and creates a dynamic corporate memory to leverage critical know-how.

1. Data transmission / data logging

When you would like to use RISK TALK, you have to register and sign in with your email address and a password. The Web server automatically records log files that cannot be assigned to a specific person. This data includes, for example, the browser type and version, operating system used, referrer URL (the previously visited page), IP address of the requesting computer, access date and time of the server request and the client's file request (file name and URL). This data is used for troubleshooting and error handling purposes, it is temporarily stored on servers that are not connected with your personal information and is not subject of evaluations or statistics. It will not be passed on to third parties for commercial or non-commercial purposes. All participants must carefully read the privacy regulations of Starmind.

2. Use of personal data

Personal data will only be collected or processed if you provide this information voluntarily, e. g. as part of a registration. Your data will not be passed on to third parties, unless required by law. The data will be used exclusively for the declared purposes. Any other use will always be dependent on your consent being obtained again. The participants confirm, using the interactive community "RISK TALK" and sharing personal data is voluntary.

Contact details, such as names and emails, which are transmitted in connection with this interactive community "RISK TALK" are stored on Starmind servers in Switzerland and used solely for query purposes. The Starmind data center infrastructure meets the needs of customers with very high security requirements. The data center is provided by a trusted partner and is guided by ISO/IEC 27002 and is ISO/IEC 27001-certified.

Any data and information disclosed by the participants of the interactive community "RISK TALK" will be stored until 31.03.2019 as this is the project end of the InsuResilience Secretariat. However, there might be a possibility of prolongation.

What personal information does Starmind collect over time?

During the setup of your account we collect personal information that we refer to as "direct information". This information includes:

- First name
- last name
- email
- your company (optional)
- location (optional)

While you are active on RISK TALK, Starmind collects additional information that is refered to as "indirect information". This information includes:

- Questions
- solutions
- search queries
- comments you create on RISK TALK

In addition, Starmind stores the relations between you and certain topics over time.

How does Starmind use my personal information?

The Starmind algorithms use the "indirect information" to establish a complete profile about your personal expertise in certain topics. This information is needed to be able to determine if you are an expert or if you could be interested in a certain question. From time to time, Starmind may use indirect informations to send personalized notification messages about the latest happenings within your Starmind Network.

Who has access to my personal information?

When you use RISK TALK the personal information and content you created is visible to other users. An important exception is your complete name if you created a question. This information is never visible to any user. A limited set of user managers from the InsuResilience Secretariat can search for certain expertise. They can also create a list with the TOP experts for a certain topic. It is not and will never be possible to create a negative evaluation.

In addition, a project leader of Starmind has access to your profile and your generated content. This access is required to support the user managers from the InsuResilience Secretariat during the pilot phase in setting up a network. Starmind Data-Analysts or Algorithm-Engineers have access to anonymous information like "User 1 logged in on 1/1/2014 at 12:00". This information is provided in an aggregated manner and used to help improve the core algorithm to get better results in finding the best possible experts for a question.

3. Informing, modifying and deleting your data

The person signing this declaration is entitled to enquire about his/her personal data, and to demand that the data will be erased. The consent given to use personal data can also be revoked at any time. In accordance with applicable law, you can ask us in writing at any time whether and which personal data we have stored about you.

Can questions and answers be erased?

If any question is not according to the RISK TALK Code of Conduct Rules, the questions will be deleted by the User Manager. The user manager is an employee of the InsuResilience Secretariat (c/o GIZ). In addition, answers that are not suitable according to the RISK TALK Code of Conduct (e.g. including advertisement) can be erased.

4. Security of your data

Starmind uses appropriate technical and organisational measures to secure your data against unintentional or intentional falsification, destruction, loss or access by unauthorised persons. Access to your personal data is restricted to InsuResilience Secretariat (c/o Deutsche Gesellschaft für Internationale Zusammenarbeit GmbH) and Starmind staff only who need to process the data for the above-mentioned purpose, and who will handle the information you provide in a proper and confidential manner. The data will not be passed on to any other third parties.

When sending very sensitive data or information, it is recommended to use the postal service, as complete data security by e-mail cannot be guaranteed.

Is any content from the community published to the outside world?

A limited selection of data originating from Starmind is automatically published on the Clearing House Portal (include final URL) accessible to nonregistered users on an automatic basis. These are:

The newest questions asked in the community will be shown (not showing the name of the originator of the question)

The names of the experts most active in the community concerning various topics are shown based on tags generated by Starmind. Only the name of the expert is shown. Whether an expert is shown here is determined solely by the AI of Starmind on basis of the experts´ activity in the community, not by the InsuResilience Secretariat c/o Deutsche Gesellschaft für Internationale Zusammenarbeit GmbH.

Can anyone publish any of my contributions outside the community?

The rights to the content posted in forms of answers or comments in this community remain with the expert posting the content. Our community rules explicitly forbid the publication of any content, discussion or comments outside the RISK TALK community without the explicit consent of the originator of the content in question. A violation of this rule will result in the immediate exclusion from the community.

5. Note on the Starmind algorithm

The algorithm of Starmind is learning through every interaction on the Network. They are differentiated by "indirect interaction" (looking at a question / following a question etc.) and

"direct interaction" (answering, commenting, rating a question). Direct interaction is weighed higher by the Algorithm, therefore, people that read questions on certain topics often will not be linked as strongly with the topic as people who answer a lot of questions about it.

You can help the algorithm to find out about the best content by evaluating answers by a star system. High ranking answers will be shown first and people who give a lot of high ranking answers are being seen as an expert in the field. Members of the community can also comment the answers, in order to give further information, ask a question about the answer or indicate why they evaluated the answer high or low. This all counts as direct interaction for the Algorithm.

6. Cookies

On some of the pages, so-called "session cookies" are used to make it easier for you to use RISK TALK. These are small text files that are stored on your hard drive for the duration of your visit to RISK TALK and are deleted when you exit the browser, depending on the settings of your browser program. These cookies do not retrieve any information about you stored on your hard drive and do not affect your PC or files. Most browsers are set up to accept cookies automatically. However, you can deactivate the storage of cookies or set your browser to notify you when cookies are sent. It is however recommended to activate Cookies, in order to return to the interactive community "RISK TALK", once questioning or answering has been interrupted.

If you have any questions about this privacy policy, or if you would like to revoke your consent. If you would like to delete your account, please send an email or fax to: InsuResilience@giz.de or secretariat@insuresilience.org., **F +49 (0)6196 79-1115**