

Information security requirements when procuring services (P+R 143)

Forward:

GIZ works with a large number of service providers to help it deliver its services worldwide. That often involves providing these contractors with information for which GIZ is responsible, either in digital or analogue form. In such cases, responsibility for the information remains with GIZ. GIZ is also responsible for information that it asks service providers to produce or process on its behalf.

This questionnaire will help you decide what level of protection is required for information that is produced, used or processed by contractors from which you plan to procure services. The level of protection given to the information should reflect the scale of any negative impacts on GIZ and third parties if it were to be unintentionally published, modified, deleted, lost or temporarily misused.

If the information is sensitive, you are advised and may be required to seek advice from the Information Security Management Team. In such cases, this will be flagged up automatically during the questionnaire. In some cases, where the assessment does not identify any particular information security risks, the tool will indicate that GIZ's General Terms and Conditions of Contract (AVB) offer sufficient protection. In all other cases, this questionnaire will provide an information security annex to the contract that reflects the required level of protection.

See P+R Rule 143 for details of the obligations arising from the completed questionnaire and the 'Information security' annex to the contract, which – if applicable – will be automatically generated based on the answers you provide.

Project title

Country Office

giz

Service Procurement
for International
Development (SIZ) Unit

1. Key service procurement data

Requirement requester

SRMO

Responsible staff member

SRMO

2. Description of service to be procured

Enter a brief description of the service to be procured. Feel free to use existing text, e.g. from the project description.

Brief description of the service to be procured

Emergency response on security and safety incidents e.g. intrusion or any construct that affects the safety of staff and to be provided by Gardaworld

3. Is GIZ information at risk?

When providing the service, will the contractor be able to access or process information that originates from or has been produced for GIZ? (Please note: If the answer here is 'no', you do not need to complete any other parts of the form.)

Please note: When a service is procured, it is very rare that no GIZ information will be processed. If you are in any doubt as to whether GIZ information will be processed, please seek advice from the Sectoral Department Data Protection: data-protection@giz.de/Information Security Management Team (ISMT: IT Service Portal)/the Information Security Officers (ISOs), especially ismt@giz.de digital deliverables for our partners.

If you nevertheless conclude that the service provider will not process any information that originates from or is produced for GIZ, apart from the data necessary to administer the contract (e.g. exchange of contract documents, contract details of the contracting parties), you can enter 'No' in the answer box. If you answer 'No' at this point, that completes the information security assessment. If you answer 'Yes', please complete the rest of the questionnaire in full in order to determine the level of information security required.

Yes

4. Selection of procurement category/categories

What is the procurement category of the service to be procured (up to two different categories can be selected)?

Please select the appropriate procurement category. You can choose from: 'Software development', 'Outsourcing IT', 'Building infrastructure' and 'Other' (for services that do not fit into one of the first two categories). If you select the 'Other' category, you only need to complete the rest of the questionnaire if the commissioning party, third-party funding provider or service recipient (partner) has contractually stipulated particular information security requirements and/or the service provider is required to process produce information classified as 'secret' for national security reasons by the commissioning party, third-party funding provider or service recipient (partner). If you are unsure about the category or the use of the questionnaire, please seek advice from ISMT/the ISOs in the field structure or from the Data Helpdesk in the Sectoral Department.

Procurement category 1

Other

For 'Procurement category 2' below, make a selection only if the service involves more than one category. Otherwise leave the answer as 'N/A' (not applicable).

Procurement category 2

N/A

You will find notes on the procurement category 'Other' under 'Useful knowledge' in P+R Rule 143.

Is a provision needed to specify countries from which services must not be provided for information security reasons?

No

For security reasons, it may be advisable or even necessary to stipulate that data involved in providing the services must not be processed in certain countries.

If this is the case, please select 'Yes' for this question and specify the countries in the listed contract areas provided at the end of the questionnaire. GIZ rules P+R 281 and 148 already stipulate that GIZ data must not be processed in certain locations (e.g. public places), and are applicable regardless of whether you enter 'Yes' or 'No' here. If the place of service delivery is defined in the Terms of Reference, you can answer 'No'.

Examples of procurement scenarios where you need to restrict the place of service delivery:

- Politically sensitive studies should be conducted outside the country in question, if necessary.
- Services for country A should not be delivered from country B if a conflict exists or is developing between these countries.

5. Information on contract formulation

Will the provisions in the General Terms and Conditions on information security form part of the contract?

Yes

The General Terms and Conditions (AVB) are usually integrated into contracts for the procurement of services and works.

However, they are not part of contracts for (1) construction work, (2) works and services for German properties, or (3) materials and equipment where the contract includes a service element. In these cases, please answer 'No'.

6. Required level of protection for GIZ information in relation to contracts for services

The purpose of this assessment is to determine the level of information security required in order to protect information that will be processed or produced by contractors when providing the service. The required level of protection is assessed/determined on the basis of three protection goals:

- confidentiality, which means that only authorized persons have access to the information;
- integrity, which means that the information available is complete and unmodified (correct);
- availability, which means that information is always accessible when needed.

Please briefly describe the information that will be processed in the service to be procured.

In the event of an incident, the information collected will personal identification information (PII) e.g. names, passports, bank account details, employment information among others.

Based on this description of the information, ask yourself what could happen to the information in the worst but realistically possible scenario in terms of the three protection goals and what implications this would have. The level of protection required is based on the worst conceivable outcome. To identify the appropriate level, work through the six damage categories in the following table and ask yourself what could be the greatest realistic damage in this category. The highest classification in a damage category is then taken as the required protection level for the specific protection goal.

To determine the required protection level for confidentiality, imagine that the data could be viewed by third parties. This can happen for a variety of reasons, such as unintentional publication, sending emails to the wrong recipients, or the service provider being hacked. What could happen in the worst, but realistically possible scenario?

In the event of a loss of confidentiality, the worst conceivable outcome under each heading would be:	Financial damage Needs to damage listed at least EUR 100,000	Impaired performance of tasks Needs to include requirement of performance of tasks (exception of initiative sub-processes)	Adverse internal or external impact Does not lead to an incident in which the information becomes known only to a select group of people (e.g. IT-CSC)	Violation of laws, regulations, contracts Needs to enter violations of laws, contractual agreements or regulations. Priority administrative offences	Impaired control of own's personal data Needs to enter violations of Data Protection Regulation (the rights to control one's personal data)	Physical and mental impairment Does not lead to physical or psychological damage or harassment. Physical or psychological harm is a harassment in no respect	Resulting required level of protection from confidentiality risks	Medium (2)
Phase select an option from the drop-down menu in each of the 6 columns								
Brief explanation	*Enter explanation here*							
In the event of a loss of integrity, the worst conceivable outcome under each heading would be:	Financial damage Needs to damage listed at least EUR 100,000	Impaired performance of tasks Needs to include requirement of performance of tasks (exception of initiative sub-processes)	Adverse internal or external impact Does not lead to an incident in which the information becomes known only to a select group of people (e.g. IT-CSC)	Violation of laws, regulations, contracts Needs to enter violations of laws, contractual agreements or regulations. Priority administrative offences	Impaired control of own's personal data Needs to enter violations of Data Protection Regulation (the rights to control one's personal data)	Physical and mental impairment Does not lead to physical or psychological damage or harassment. Physical or psychological harm is a harassment in no respect	Resulting required level of protection from integrity risks	Medium (2)
Phase select an option from the drop-down menu in each of the 6 columns								
Brief explanation	*Enter explanation here*							
In the event of a loss of availability, the worst conceivable outcome under each heading would be:	Financial damage Needs to damage listed at least EUR 100,000	Impaired performance of tasks Needs to include requirement of performance of tasks (exception of initiative sub-processes)	Adverse internal or external impact Does not lead to an incident in which the information becomes known only to a select group of people (e.g. IT-CSC)	Violation of laws, regulations, contracts Needs to enter violations of laws, contractual agreements or regulations. Priority administrative offences	Impaired control of own's personal data Needs to enter violations of Data Protection Regulation (the rights to control one's personal data)	Physical and mental impairment Does not lead to physical or psychological damage or harassment. Physical or psychological harm is a harassment in no respect	Resulting required level of protection from availability risks	Medium (2)
Phase select an option from the drop-down menu in each of the 6 columns								
Brief explanation	*Enter explanation here*							
Overall protection requirement	Medium (2)							

7. Further action

Involve ISMT/ISOs

Not necessary

ISMT via GIZ Service Portal

Issued on

Comments by ISMT

Include in IT emergency management

Not necessary

ISMT via GIZ Service Portal

Issued on

Comments by IT business continuity management

Comments by requirement requester

Assessment completed

No

The questionnaire has not been completed, please check your answers.

The information security requirements are automatically generated in the form of a contract annex. The requirement requester should download the annex via the following link and submit it to the procuring unit together with the questionnaire.

The questionnaire has not been completed, please check your answers.

GIZ INTERNAL

1/1