**CYBER SECURITY AND INFORMATION SECURITY QUESTIONNAIRE**

**ANNEX**

**APPLICATIONS FOR THE PROVISION OF CONFIDENTIAL STATISTICAL DATA FOR CONDUCTING RESEARCH**

This questionnaire, together with other publicly available information, the Statistical Office's knowledge from previous cases of disclosure of confidential statistical data (hereinafter referred to as 'CSD') for scientific purposes to the applicant, and information provided by the applicant in the form of annexes to this questionnaire, **serves to verify whether the research entity requesting CSD from the Statistical Office has the capacity to protect the data disclosed.**

**The information in this questionnaire is confidential**, the content and the data collected are subject to internal classification according to the directive of the Statistical Office of the Slovak Republic SME-8/2022 Cyber and Information Security Policy. After a period of ten years from the end of the obligations under the contract for the provision of CSD, or immediately after the request for CSD has been rejected, **the paper form of this questionnaire will be shredded and its completed electronic form deleted.**

It is **mandatory to fill** **in all the information** provided in this questionnaire.

Please note that the **correct completion of this questionnaire requires expertise**, so it should be completed by the person who is responsible for information security and cybersecurity in your research entity.

1. **Basic information about the research entity:**

|  |  |
| --- | --- |
| Name (Business name) | Type |

|  |  |
| --- | --- |
| Web address | Type |

|  |  |
| --- | --- |
| Business ID1) | Type |

|  |  |
| --- | --- |
| Address | Type |

|  |  |
| --- | --- |
| Name and address of the establishment (organisational unit) to which the CSD are provided | Type |

1. **Please describe the security measures implemented on the premises, equipment, CSD processing processes and users of the applicant's CSD:**

|  |  |
| --- | --- |
| Please describe physical security measures: | Type |

|  |  |
| --- | --- |
| Please describe the measures to ensure the separation of CSD processing and results from the internal network and from the external environment: | Type |

|  |  |
| --- | --- |
| Please describe the measures to ensure the confidentiality and integrity of the CSD and the results of their analysis. Describe how to monitor access to and work with CSD: | Type |

1. **Does your research entity have a valid quality management process and/or cybersecurity certification (e.g. ISO 9001, ISO 27001, ISO 20000)?**



If yes, please provide information about the certificate in the following field: certificate number, expiry date and attach the certificate to the annexes:

|  |
| --- |
| Type |

1. **Are you registered in the Register of Operators of Essential Services pursuant to Act No.69/2018 on Cyber Security and on Amendments to Certain Acts, as amended, or pursuant to Directive (EU) 2022/2555 of the European Parliament and of the Council of 14th December 2022 on measures to ensure a high common level of security for networks and information systems in the Union, amending Regulation (EU) no. 910/2014 and Directive (EU) 2018/1972 and repeals Directive (EU) 2016/1148 (NIS 2 Directive)?**



If yes, please enter your registration number in the field below and include a link to verify this information:

|  |
| --- |
| Type |

1. **Has a security audit been performed in your research entity, for example in the Information Security Management System according to the international standard ISO/IEC 27001:2013?**



If yes, indicate in the following field the name of the organisation, the protocol number, the date of the security audit and the overall result of the assessment:

|  |
| --- |
| Type |

1. **If you answered no to questions 3, 4 and 5, please provide the requested information on the security measures (technical, organisational and personnel) taken by your research entity to ensure the confidentiality, integrity and availability of the information:**

Own internal security documentation (e.g. organisational directive, security project):

|  |  |
| --- | --- |
| **Name** | **Web address on which the document is published** |
| Type | Type |
| Type | Type |

If the documentation is not made available on the Internet, the researcher is obliged to submit these documents to the statistical office and mention them in point 8 of the questionnaire or describe the security measures taken by the researcher in the following field:

|  |  |
| --- | --- |
| Please briefly describe the technical measures: | Type |

|  |  |
| --- | --- |
| Please briefly describe the technical measures: | Type |

|  |  |
| --- | --- |
| Please briefly describe the technical measures: | Type |

1. **Please indicate whether your research entity has recorded a security incident (e.g. data leakage or data loss) or faced administrative action by a local cybersecurity or data protection entity (violation of current cybersecurity or data protection legislation) in the past two years since the submission of this application for a CSD to conduct research?**

If yes, state the reason, the date and the amount of the sanction:

|  |
| --- |
| Type |

1. **List the annexes you attach to the questionnaire:**

|  |
| --- |
| Type |

1. **Processing clause**

They shall submit the data and be responsible for its content:

|  |  |
| --- | --- |
| **Name and surname, title** | **Function/ Job title and name of establishment** |
| Type | Type |
| Type | Type |

**Explanatory notes:**

**Shortcuts**

Business ID the identification number of the organisation

CSD confidential statistical data

ISMS Information Security Management System

ISO International Organization for Standardization

IEC International Electronic Comitee

SME designation for a directive of the Statistical Office of the Slovak Republic

**Concepts**

Link – is a link between parts (nodes) of hypertext documents or hypermedia documents.

Confidentiality – a security requirement, the fulfilment of which means that the information contained in the document is not accessible to unauthorised persons.

Integrity – a data security requirement, the fulfilment of which means that the data cannot be altered without the owner or addressee being able to detect it.

Availability – the requirement to make system resources available to the authorised person whenever requested.