FICEC – Finnish Center of Expertise for Cybersecurity – Privacy Policy

1 Name of the register	FICEC – Finnish Center of Expertise for Cybersecurity Privacy Policy
2 Data Controller	Jyväskylä University of Applied Sciences Ltd (a.k.a. Jamk) P.O. Box 207, 40101 Jyväskylä Business ID 1006550–2 University of Jyväskylä P.O. Box 35, 40014 University of Jyväskylä Business ID: 0245894–7
3 Contact person in matters concerning the register, contact information during office hours	Jamk: Project Manager Antti Teppo Piippukatu 2, 40100 Jyväskylä antti.teppo@jamk.fi | +358505668533 University of Jyväskylä, Faculty of Information Technology: Coordinator Antti Kariluoto Mattilanniemi 2, C225.4, 40100 Jyväskylä antti.j.e.kariluoto@jyu.fi | +358442852431
4 Processing of personal data and its purpose	The legal basis for the processing of personal data is the consent of the data subject. The purpose of the FICEC register and the personal data it contains is to support the Centre of Expertise in its objectives. The aim of the Centre of Excellence is to promote the growth of Finland's national cyber security capability through research and education. The purpose of the register is to collect information related to the organisation and activities of the Centre of Expertise, for example, for the implementation of cooperation, communication with different target groups, and the implementation of projects, studies, studies and evaluations and events carried out at the Centre of Expertise. The aim of the surveys, interviews, evaluations, workshops and events carried out at the Centre of Expertise is to promote the cyber security expertise of companies and organisations by

	assembling project consortia, applying for funding and implementing R&D projects. Summaries and evaluation reports are made of the results, which are used in events and various publications. The results can also be used for scientific research. The results will not be shared with third parties. The primary target group of the above-mentioned measures are companies and organizations that want to increase their cybersecurity awareness and capabilities. The register processes the personal data of the representatives of the above-mentioned target groups. The data is collected electronically using the Webropol survey program provided by Jamk, the digital platforms and tools used in the Centre of Expertise, e-mail and telephone, interviews and participant lists. The above-mentioned data to be collected, e.g. in surveys and interviews, will be treated confidentially in accordance with the guidelines on research ethics in accordance with the responsible conduct of research. Accordingly, no individual person can be identified from the results of the study. All personal data collected during the project will be processed confidentially as required by the National Data Protection Act (1050/2018) and the EU General Data Protection Regulation (2016/679).
5 Data content of the register	The data stored in the register include: • Company name, industry and contact information • Lists of participants in the Centres of Expertise's events (e.g. workshops, seminars): person's name, contact information, company • Identity data related to the Centre of Excellence's activities, such as the digital platforms and tools used; • Other information related to the Centre of Expertise's activities, cooperation and communication
6 Grounds for processing	Data subject's consent. According to the EU's General Data Protection Regulation, the legal basis for the processing of personal data is the person's consent. The activities of the FICEC Centre of Excellence, data collection and their management.

7 Regular sources of information	The data stored in the register is obtained from persons in the Competence Centre's projects, surveys and interviews, through the user data of the digital platforms and tools used in the Competence Centre, in events related to the measures of the Competence Centre, carried out remotely or face-to-face, and in other events or contexts where the data subject discloses their data. The people involved in the administration of the FIDEC Centre of Expertise work at JAMK University of Applied Sciences and the University of Jyväskylä.
8 Regular disclosure of data and transfer of data outside the EU or the European Economic Area	The information is not regularly disclosed to other parties. Data may be disclosed to the extent that this has been agreed with the data subject. The data will not be transferred outside the EU EEA. The above-mentioned controller processes the data. The information required by the funders of projects carried out at the Centre of Expertise may be disclosed to the project funders in connection with reporting, such as participant information and event participant lists.
9 Principles of register protection	Care is taken in the processing of the register and the data processed with the help of information systems is appropriately protected. When register data is stored on Internet servers, the physical and digital security of their hardware is appropriately ensured. The controller ensures that the stored data, server access rights and other information critical to the security of personal data are handled confidentially and only by the employees whose job description includes it. Manually collected data is stored in electronic format and stored on a server (paper material is destroyed). The controller's servers are in a locked and access-controlled data center. Access to the servers is only allowed to administrators. Individual respondents cannot be identified from the published results and reports related to the measures taken by the Centre of Expertise (e.g. surveys, interviews, lists of participants in events). The data is stored in accordance with Jamk's information security guidelines. Outdated and unnecessary data will be disposed of in a reliable and relevant manner.

10 Retention period of personal data or criteria for determining the retention period	The controller retains personal data in its own systems/archives at least for the period required by the reporting of the Development of the Cyber Security Centre of Excellence -project, 1.1.2025-31.8.2027. Personal data is stored for as long as it is necessary to carry out the purposes for which personal data is processed, as defined in this privacy policy. Due to the obligations of the Accounting Act or other prescriptive laws, it may be necessary to store data for longer than the above-mentioned period. The data subject has the right to request the deletion of their personal data, e.g. when the data is no longer needed for the purpose for which it was collected, or if the data subject withdraws their consent (Data Protection Act 1050/2018). The controller processes the deletion request and informs the data subject of the measures. If the deletion request is unfounded or excessive, the controller may charge a reasonable fee or refuse to comply with the deletion request.
11 Profiling and automated decision-making	Personal data is not used for automated decision-making or profiling.
12 Rights of the data subject	More information about the data protection officer and the rights of the data subject and how to implement them is available on Jamk's data protection page.