SYNBEE

D7.3 DATA MANAGEMENT PLAN

Funded by the European Union under the Grant Agreement No 101100509. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Innovation Council and SMEs Executive Agency (EISMEA). Neither the European Union nor the granting authorities can be held responsible for them.

Grant Agreement: 101100509

DOC. REFERENCE	D7.3 Data Management Plan
Version	1.0
WORK PACKAGE No	7 – Coordination and management
LED BENEFICIARY	eureKARE SA
AUTHOR	Alexandra Chukas
REWIEVERS	All Partners
DATE	27/07/2023
TYPE	R – DOCUMENT, REPORT
DISSEMINATION LEVEL	CONFIDENTIAL

VERSION	DATE	RESPONSIBLE	DESCRIPTION
Version 1.0	27/07/2023	eureKARE	First version for review
Version 2.0	28/07/2023	eureKARE	Final version

Funded by the European Union under the Grant Agreement No 101100509.
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Innovation Council and SMEs Executive Agency (EISMEA).
Neitherthe European Union nor the granting authorities can be held responsible for them.

EXECUTIVE SUMMARY

This Data Management Plan is intended to support SYNBEE partners in the management of data efficient and compliant with the regulation in force. Different project tasks intend data collection and processing:

1. The project aims to perform a SWOT (Strength, Weakness, Opportunities, Threats) analysis in the field of synthetic biology innovation ecosystems in Europe. SWOT analysis will be performed based on the responses received from stakeholders across Europe in the field of synthetic biology via a questionnaire and interviews. The collected data will be analysed to form best practices between the 4 types of innovation ecosystems (Lead, Strong, Moderate and Emerging) existing in the EU countries.
2. The project will also propose two training/coaching programs: #1 "From Idea to Startup: Igniting Entrepreneurial Success"; #2 "Unlock Your Potential: Empowering Academia for Private Sector Success". To implement both programs, the consortium will need to identify the candidates / teams searching for support (training, mentoring, supervision), as well as industry, investors, consulting representatives, ready to train, mentor, supervise. It will also be necessary to understand the profiles of both sides to allow for the most appropriate matches.

All the data will be collected either from open sources or with an informed consent form the concerned participants. They will have a possibility to ask to delete any data related to them at any time.

The data collection will take place throughout the project duration.

Funded by the European Union under the Grant Agreement No 101100509. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Innovation Council and SMEs Executive Agency (EISMEA). Neitherthe European Union nor the granting authorities can be held responsible for them.

ABBREVIATIONS AND ACRONYMS

CAGR	Compound annual growth rate
DPO	Data Protection Officer
EU	European Union
GDPR	General Data Protection Regulation
KOL	Key opinion leader
SME	Small and medium size enterprise
SynBio	Synthetic biology
SWOT	Strengths, weaknesses, opportunities, threats
TLO	Technology licensing office
TU Delft	Technical University Delft
VC	Venture capital

Funded by the European Union under the Grant Agreement No 101100509.
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Innovation Council and SMEs Executive Agency (EISMEA).
Neitherthe European Union nor the granting authorities can be held responsible for them.

Table of contents

Funded by the European Union under the Grant Agreement No 101100509.
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Innovation Council and SMEs Executive Agency (EISMEA).
Neitherthe European Union nor the granting authorities can be held responsible for them.

INTRODUCTION

The SYNBEE project aims to boost entrepreneurial education in synthetic biology and bring together key players within the space, including academic centers of excellence and their accelerators, incubators, and technology transfer offices, as well as industry partners and investors. The SYNBEE consortium with its networks covers 25 EU countries, including 7 emerging and 6 moderate ecosystems. All the proposal beneficiaries (7) are from the European Union, they are complementary, have a strong track record and are recognized innovators, keen on entrepreneurship, but most importantly, they are the core of the European synthetic biology space. The SYNBEE consortium is supported by 8 excellent associated partners.

Purpose of this document is to describe internal SYNBEE policies and procedures related to the data management (collection, storage, sharing, archiving) in the frame of the SYNBEE project.

Funded by the European Union under the Grant Agreement No 101100509.
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Innovation Council and SMEs Executive Agency (EISMEA).
Neitherthe European Union nor the granting authorities can be held responsible for them.

1. ADMINISTRATIVE FRAMEWORK

Funding institution: *European Union*
Grant Agreement number: *101100509*
Acronym : *SYNBEE*
Title: *expanding Synthetic Biology Entrepreneurial Ecosystems*
Project coordinator: *Alexandra Chukas (alexandra.chukas@eurekare.eu)*
Organisation of the coordinator: *eureKARE SA, 128 rue de la Boétie, Paris, 75008, France*
Project dates and duration :

Start date: 15/01//2023
End date : 14/01/2025
Duration: 24 months

Project summary

Synthetic biology is a disruptive technology that enables completely new processes and products for industry, medical applications and food production, it makes the processes and products cheaper and more sustainable. SynBio will renew and challenge many major industries. The estimated overall market to be affected by SynBio exceeds $13 trillion. The global SynBio market is expected to grow from $5.3 billion in 2019 to $18.9 billion by 2024 with a CAGR of 28.8%. Leading European research organizations have a proven scientific record of excellence in the field. However, European science remains largely under-exploited commercially. One impact factor is difficulty to quickly consolidate transdisciplinary teams. Indeed, there is a need for clearer vision on the necessary current and future skills, required by the industry. SynBio is a relatively young discipline, made up of multiple sub-divisions, thus searching for a right profile (KOL, researcher, intern) is time-consuming for industrial companies, and can be even longer for startups. While the boom of accelerators and incubators and entrepreneurial training have driven start-up creation, the lack of specific thematic approaches can hinder the creation and/or maturation of SynBio start-ups. The SYNBEE project will address these challenges by:

(i) SWOT analysis, matrix of best practices, mapping of academic profiles and industry in SynBio.

(ii) General and SynBio-specific entrepreneurial training in close interaction with the industry.

Funded by the European Union under the Grant Agreement No 101100509. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Innovation Council and SMEs Executive Agency (EISMEA). Neitherthe European Union nor the granting authorities can be held responsible for them.

(iii) Networking, matchmaking between candidates and hosting and mentoring industrial partners, hackathons, pitch contests.

(iv) Creation of a path from talented student to startup creation and investor workshops.

(v) Policy making and mentoring between ecosystems.

(vi) Specific focus will be brought to women in SynBio.

SYNBEE will be implemented by key SynBio academia, industry, accelerators, investors from 25 EU countries, including 7 emerging and 6 moderate ecosystems.

Project partners:

Beneficiaries:

1. eureKARE SA (France)
2. HAME UNIVERSITY OF APPLIED SCIENCE LTD (Finland)
3. TECHNISCHE UNIVERSITEIT DELFT (Netherlands)
4. INRAE TRANSFERT SAS (Toulouse White Biotechnology / IBISBA) (France)
5. Biocatalyst Foundation (Latvia)
6. F6S NETWORK IRELAND LIMITED (Ireland)
7. Riga Technical University (Latvia)

Associated partners:

8. Max Planck Institute of Biochemistry (Germany)
9. Imperial College London / London Biofoundry (UK)
10. Potter Clarkson (UK)
11. Start Codon Limited (UK)
12. iGEM (USA)
13. COMMISSARIAT A L ENERGIE ATOMIQUE ET AUX ENERGIES ALTERNATIVES (France)
14. German Association for Synthetic Biology e. V. (Germany)
15. EUSynBioS (France) – in progress

Funded by the European Union under the Grant Agreement No 101100509. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Innovation Council and SMEs Executive Agency (EISMEA). Neitherthe European Union nor the granting authorities can be held responsible for them.

2. DATA MANAGEMENT PLAN

Identification and affiliation of the author of the DMP: *Same as coordinator*
Date of creation of DMP: *27/07/2023*
Current version: *V1*

2.1 DATA COLLECTION

The purpose of the data collection is to achieve the objectives of the project, among others to produce a SWOT analysis and allow more efficient matchmaking between the stakeholders of the synthetic biology community, to then generate better results and broad impact.

Origin of the data:

- open/semi-open access information available online (Google, PubMed, Crunchbase, PitchBook),
- Qualtrix – based survey replies (anonymised questionnaire, informed consent form),
- Self-manifestation by concerned teams and candidates, through an online form or interviews (informed consent form).

Format of the data collection:

- an online Qualtrix survey tool;
- a database in an Excel-based structure, facilitating seamless updates and maintenance to reflect the evolving landscape of candidates and projects throughout the project duration.

Data collection period: 01/02/2023-31/01/2025

Dataset collection methods

- Use of existing databases in open access (Crunchbase, Pitchbook);
- Inclusion of the networks of the project partners (SynCellEU, BIOCONNECT, etc.);
- Advertising the project at relevant events, invitation to join the community;
- Spontaneous invitation of teams and individual researchers to join the database and participate to the project activities.

Funded by the European Union under the Grant Agreement No 101100509. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Innovation Council and SMEs Executive Agency (EISMEA). Neitherthe European Union nor the granting authorities can be held responsible for them.

Data storage: the database will be hosted within the secured SYNBEE SharePoint platform, accessible only to authorized users within the consortium. This secure environment ensures that candidates' data remains protected and confidential.

Expected size/volume of the data: <50 GB

Data utility: innovation management. Data might be useful to technology transfer offices, economic development agencies, industry, academia, investors community working in the field of synthetic biology (bioengineering, biomanufacturing). All the data will be for the consortium internal use only (matchmaking of candidates and relevant industry partners, mentors, etc.). A particular information could be available to other interested stakeholders, if/when a specific consent has been provided by the concerned team/candidate.

2.2 DATA COLLECTION IN WP1_SWOT ANALYSIS

For the SYNBEE project, the following documents have been prepared/obtained and are kept on file for the **WP1_SWOT analysis:**

(i) Final version of study protocol as submitted to TU Delft Human Research Ethics Committee (HREC) (Annex 1).

(ii) Approval letter from the HREC (Annex 2).

(iii) Consent forms for the online survey in Qualtrix and the interviews (Annex 3).

Data description and collection or re-use of existing data. General description of the type of data SYNBEE will be working with, including any re-used data:

Type of data	**File format**	**How will data be collected (for reused data: source and terms of use)?**	**Purpose of processing**	**Storage location**	**Who will have access to the data**
Responses generated for	.csv files	Online survey	To understand and explore gaps	Project Storage Drive.	The project team

Funded by the European Union under the Grant Agreement No 101100509. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Innovation Council and SMEs Executive Agency (EISMEA). Neitherthe European Union nor the granting authorities can be held responsible for them.

a survey with a questionnaire regarding the synthetic biology field.			between the 4 different innovation ecosystems across Europe. To form best practices by performing a SWOT analysis of the 4 ecosystems.	Qualtrics tool licensed version by TU Delft will be used to collect survey responses	(Project leader - Dr. Sindhu Naik and programme manager - Dr. Stefania Usai)
Transcripts of interviews from few of the survey respondents who provide consent to be contacted for a follow up interview.	.doc files	face-to-face or virtual interviews	To understand and explore gaps between the 4 different innovation ecosystems across Europe. To form best practices by performing a SWOT analysis of the 4 ecosystems.	Project Storage Drive. We will use Microsoft Teams to conduct virtual interviews.	The project team (Project leader - Dr. Sindhu Naik and programme manager - Dr. Stefania Usai)
Audio recordings of the interviews conducted will be stored until transcripts can be made from them. The audio recordings will then be deleted.	.M4A files	face-to-face or virtual interviews	To understand and explore gaps between the 4 different innovation ecosystems across Europe. To form best practices by performing a SWOT analysis of the 4 ecosystems.	Project Storage Drive. We will use a handheld recorder to audio record the interviews.	The project team (Project leader - Dr. Sindhu Naik and programme manager - Dr. Stefania Usai)

What documentation will accompany data:

- README file or other documentation explaining how data is organized
- Methodology of data collection

Funded by the European Union under the Grant Agreement No 101100509. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Innovation Council and SMEs Executive Agency (EISMEA). Neitherthe European Union nor the granting authorities can be held responsible for them.

Storage and backup during research process: During the project lifetime, data will be stored and backed-up at the Project Storage at TU Delft.

Legal and ethical requirements, codes of conduct: The research involves human subjects or 3rd party datasets collected from human participants. We will work with personal data. We will use the contact details (work email) to contact participants for a follow-up interview after they have given us consent during the survey to be contacted. They will then provide us with an email address to be contacted at a later date. This information will be temporarily stored for organizational purposes.
We will not work with any other types of confidential or classified data or code.

Management of the ownership of the data and intellectual property rights to the data: The SWOT analysis done based on the data generated from the survey will be published in a deliverable report which will be publicly accessible. This data does not hold any intellectual property value as it is only an assessment of the current ecosystem in the field of synthetic biology in Europe.

Which personal data will be processed: We will collect the information about the stakeholder age and gender to assure balanced and representative focus group, as well as the information about the stakeholder group the respondent belongs to. The following categories of stakeholders will be contacted:

- Policy Makers: Public government institutions
- Industry: Research and Development , Scouting intel personnel for Leads
- Start-up CEO's: C-level executives at start-ups
- Post-docs: Both in scientific and vocational studies
- PhD Students: Both in scientific and vocational studies
- Master's Students: Both in scientific and vocational studies
- Bachelor's Students: Both in scientific and vocational studies
- Researchers/ PIs: Academic institutions, research institutes
- Investors: VC's , funding agencies, business angels.
- Accelerators: Institutions helping start-ups in the early stages of their existence
- Incubators: Institutions which provide space and resources for the startups, from early stage to growth stage.

Funded by the European Union under the Grant Agreement No 101100509.
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Innovation Council and SMEs Executive Agency (EISMEA).
Neitherthe European Union nor the granting authorities can be held responsible for them.

- Universities (Innovation centres): Academic institutions, Tech transfer teams, technology licensing offices (TLOs), Innovation centres

We will have audio recordings collected during interviews which will be deleted once they have been transcribed.

In the frame of the SYNBEE project, we will not collect and/or process sensitive personal data such as sexual lifestyle, ethnicity, political opinion, religious or philosophical condition.

Personal data will not be shared with individuals/organisations outside of the EEA (European Economic Area).

The legal ground for personal data processing is an informed consent. It will be proposed in the form of an opening statement at the beginning of the survey. All the participants will be provided with an opening statement and made clear if they press "continue" button on the survey, they will be providing us the informed consent to process the collected data. The signed consent forms will be stored at the Project Storage at TU Delft.

What will happen with personal research data after the end of the research project: Anonymized or aggregated data will be shared with other project participants. A SWOT Analysis results obtained from the survey analytics will be developed into a report which will be shared with European Commission as a project deliverable and also with the project collaborators. The survey respondents will be anonymized.

Will your study participants be asked for their consent for data sharing: Yes.

Participants who do not agree will not go ahead with the survey and hence we will have no data collected from those participants who do not agree to share the data.

Data sharing and long-term preservation: The data produced from the survey will be converted into a report and shared with the project partners and European commission as a deliverable of the project. The data will be shared before the deliverable deadline set in the grant proposal. The SWOT analysis will be completed and report submitted by the end of October 2023. The data/code will be released under the license CC BY.

Data management responsibilities and resources: TU Delft is the lead beneficiary for the SWOT analysis deliverable of the project. The lead coordinating partner is eureKARE

Funded by the European Union under the Grant Agreement No 101100509.
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Innovation Council and SMEs Executive Agency (EISMEA).
Neitherthe European Union nor the granting authorities can be held responsible for them.

(https://eurekare.eu/), who will be responsible in managing rest of the deliverables of the project.

Dr. Sindhu Naik is corresponding researcher for the data resulting from this activity. In her absence, Dr. Stefania Usai, Programme manager (T: +31 (0)15 2786643; E: s.usai@tudelft.nl), will be responsible for the data resulting from this project in the part relevant to the SWOT activities.

What resources (for example financial and time) will be dedicated to data management and ensuring that data will be FAIR (Findable, Accessible, Interoperable, Re-usable): There is a personnel cost involved and included in the project budget, which is project leader appointed to manage the data management part of the project. The survey itself will be conducted using one of the TU Delft approved tools and for which TUD already has the license required. The data received from the survey will be stored in the project drive and we do not expect to exceed the space and therefore there are no additional costs of long term preservation.

2.3 Data Management for WP2-4 matchmaking activities

For the WP2-4 matchmaking activities, we will need to construct a database of profiles, teams and projects. General description of the type of data SYNBEE will be working with, including any re-used data:

Type of data	**File format**	**How will data be Collected?**	**Purpose of processing**	**Storage location**	**Who will have access to the data**
Responses generated within an online form, filled-in by the candidates, willing to participate to the program	Excel files	Online form	To identify stakeholders, teams, projects in synthetic biology across Europe. To form teams willing to start up a company or to join existing team.	Project SharePoint	The project beneficiaries

Funded by the European Union under the Grant Agreement No 101100509. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Innovation Council and SMEs Executive Agency (EISMEA). Neitherthe European Union nor the granting authorities can be held responsible for them.

What documentation will accompany data:

- README file or other documentation explaining how data is organized;
- Methodology of data collection.

Storage and backup during research process: During the project lifetime, data will be stored on the SYNBEE project SharePoint and backed-up at the Project Storage on the protected eureKARE server.

Legal and ethical requirements, codes of conduct: The research involves human subjects or 3rd party datasets collected from human participants. We will work with personal data. We will use the contact details (work email) to contact participants for a follow-up interview after they have given us consent during the survey to be contacted. They will then provide us with an email address to be contacted at a later date. This information will be temporarily stored for organizational purposes.
We will not work with any other types of confidential or classified data or code.

Management of the ownership of the data and intellectual property rights to the data: The consolidated database might be useful to technology transfer offices, economic development agencies, industry, academia, investors community working in the field of synthetic biology (bioengineering, biomanufacturing). All the data will be for the consortium internal use only (matchmaking of candidates and relevant industry partners, mentors, etc.). A particular information could be available to other interested stakeholders, if/when a specific consent has been provided by the concerned team/candidate.

Which personal data will be processed: We will collect the information about the stakeholder gender to assure balanced impact for the community, as well as the information about the stakeholder training, professional experience, achievements and interests to match stakeholders with the most relevant other stakeholders. The following categories of stakeholders will be invited to participate:

- Research community: senior researchers, post-docs, PhD students, Master's students;
- Big industry, SMEs, startups;
- Investors: VC's , funding agencies, business angels;
- Accelerators, incubators, startup studios, technology transfer offices;
- Consulting companies.

Funded by the European Union under the Grant Agreement No 101100509. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Innovation Council and SMEs Executive Agency (EISMEA). Neitherthe European Union nor the granting authorities can be held responsible for them.

Database structure.

The meticulously designed database lies at the heart of the SYNBEE project, playing a pivotal role in shaping the program's ecosystem and fostering seamless collaboration between stakeholders. The main database will be organized into two distinct streams, each capturing essential information specific to the respective program participants:

Stream #1: From Idea to Startup: Igniting Entrepreneurial Success

Team Compositions:

Detailed records of teams aspiring to create start-ups will be compiled, including information about team members, their backgrounds (academic track record: publications, international network, supervision, grants; business-oriented mindset: patents, previous startup creation/tech transfer experience, participation to the boards of private companies, specific previous training), individual roles within the team, any missing expertise and profiles which will be necessary at a later stage. This will foster transparency and facilitate effective team dynamics as well as overall business planning.

Key Topics of Interest:

The database will document the primary areas of interest that teams intend to explore and develop within the realm of synthetic biology (based on the team background and previous projects, as well as current topic). This will enable efficient matchmaking, tailored support and mentorship from experts in their specific domain.

Readiness for Start-Up Creation:

We will assess the readiness level of each team to initiate start-up ventures (TRL level, preliminary data, available network, already raised funds, if any, previous links with the industry and/or investors, any existing recognition: prizes/awards from competitions, hackathons, startup operational creation process knowledge, team completion, etc.), vision, and commitment to entrepreneurship.

Progress Towards Proof of Concept (PoC):

Critical milestones achieved in implementing Proof of Concept (PoC) will be meticulously tracked, offering insights into the teams' technical advancements, feasibility of their proposed ideas, confirming or adjusting the methodology to make it robust and assure efficient and optimal validation process. The proposed projects could be adjusted based on market needs and industry/investor vision.

Funded by the European Union under the Grant Agreement No 101100509. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Innovation Council and SMEs Executive Agency (EISMEA). Neitherthe European Union nor the granting authorities can be held responsible for them.

Fundraising and Business Plan Development:

Information regarding fundraising efforts and the process of crafting comprehensive business plans will be recorded. This will allow us to better guide teams in fundraising and outlining viable business strategies.

Stream #2: Unlock Your Potential: Empowering Students for Private Sector Success

Backgrounds and Motivations:

Detailed profiles of individual participants will be captured, encompassing their academic, professional, and personal backgrounds, as well as their motivations for joining the SYNBEE program.

Transversal Skills and Networking Aspirations:

The database will include a comprehensive record of participants' transversal skills, showcasing their diverse skill sets that go beyond traditional academic qualifications. We will also document their aspirations for networking and collaborating within the synthetic biology industry.

Specific Fields of Interest:

Participants' areas of interest within synthetic biology will be documented, spanning domains such as energy, health, environment, consumer goods, and more. We will also note the person's target field of activity (industry, consulting, financial institutions, self-employment, etc.). This will enable targeted mentorship and training tailored to their chosen field and interests. This will also help us to better match profiles with the industry, consulting companies, investment institutions, searching for relevant profiles.

In the frame of the SYNBEE project, we will not collect and/or process sensitive personal data such as sexual lifestyle, ethnicity, political opinion, religious or philosophical condition.

Personal data will not be shared with individuals/organizations outside of the EEA (European Economic Area).

Funded by the European Union under the Grant Agreement No 101100509. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Innovation Council and SMEs Executive Agency (EISMEA). Neitherthe European Union nor the granting authorities can be held responsible for them.

The legal ground for personal data processing is an informed consent. It will be proposed in the form of an opening statement at the beginning of the form All the participants will be provided with an opening statement and made clear if they press “continue” button on the survey, they will be providing us the informed consent to process the collected data. The signed consent forms will be stored on the project SharePoint.

What will happen with personal data after the end of the project: project progress will be covered in a report which will be shared with the European Commission as a project deliverable. All the personal data will be anonymized. Information about the created, developed companies/projects will be made public with the consent from the concerned teams, to showcase the project progress and impact.

Will your participants be asked for their consent for data sharing: Yes.

Participants who do not agree will not go ahead with the form and hence we will have no data collected from those participants who do not agree to share the data.

Data sharing and long-term preservation: The data produced from the form will be converted into a report and shared with the project partners and European Commission as a deliverable of the project. The data will be shared before the project end set in the grant proposal (January 14, 2025).

What resources (for example financial and time) will be dedicated to data management and ensuring that data will be FAIR (Findable, Accessible, Interoperable, Re-usable): There is a personnel cost involved and included in the project budget, which is project leader appointed to manage the data management part of the project. The form will be available on the tool, for which eureKARE has the required license. The data received from the form will be stored on the project SharePoint and we do not expect to exceed the space and therefore there are no additional costs of long term preservation.

2.4 GDPR Considerations

SYNBEE is committed to the utmost data privacy and protection, ensuring that candidates' information is handled with the highest level of care and in strict compliance with GDPR regulations. Key aspects of our GDPR considerations include:

Funded by the European Union under the Grant Agreement No 101100509. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Innovation Council and SMEs Executive Agency (EISMEA). Neitherthe European Union nor the granting authorities can be held responsible for them.

EXPLICIT CONSENT:

Before incorporating candidates' information into the database, explicit consent will be obtained from each individual, ensuring they are fully aware of the purpose and usage of their data within the SYNBEE program.

SECURE STORAGE:

The database will be hosted within the secured SYNBEE SharePoint platform, accessible only to authorized users within the consortium. This secure environment ensures that candidates' data remains protected and confidential.

RELEVANT USE ONLY:

Candidates' information will be used exclusively for program-related purposes, such as team matching, mentorship, and collaboration opportunities, thereby ensuring that the data is utilized in a manner that aligns with the SYNBEE program's objectives.

By adhering to stringent GDPR considerations, SYNBEE ensures that data privacy is upheld in our program, installing trust and confidence among candidates as they embark on their journey in synthetic biology entrepreneurship.

2.5 DATA MANAGEMENT DURING THE PROJECT

Alexandra Chukas (T: +33 (0)6 16 69 20 57; E: alexandra.chukas@eurekare.eu), project coordinator, is responsible for data management during the project. All the project beneficiaries are responsible for data collection and processing. eureKARE is responsible for data storage, archiving and sharing.

Data will be stored on the project SharePoint, with user access control and sharing permissions. A procedure for directories and files naming, and rules for metadata documentation, will be shared within projects members.

Each file is named as follows: FileName_date.

Funded by the European Union under the Grant Agreement No 101100509. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Innovation Council and SMEs Executive Agency (EISMEA). Neitherthe European Union nor the granting authorities can be held responsible for them.

Quality control procedure for the data: regular meetings between the data generators and the project coordinator. In case of questions or concerns, we will contact the quality control department and the DPO.

2.6 DATA SHARING, DISSEMINATION AND RE-USE

Data sharing during the project takes place between the project partners who have signed the Grant Agreement and the Consortium Agreement.

Data sharing, dissemination and re-use after the project (FAIR): the project dataset and corresponding metadata might be shared upon request and with the consent from the concerned candidate/team.

2.7 ARCHIVING AND PRESERVATION

Storage and backup during the project:

- The Qualtrix data (SWOT-related survey) will be stored in the Project Storage at TU Delft.
- The matchmaking-related data will be stored on the SYNBEE SharePoint and backed-up on the protected eureKARE data storage system following the IT department policy and procedure.

Long-term preservation after the project:

- The Qualtrix data will be archived in the Project Storage at TU Delft.
- The matchmaking-related data will be stored on the protected eureKARE data storage system.

3 DATA PROTECTION OFFICER (DPO)

The company Privacy Partners, UAB, Lithuanian business registry ID 304846919, address Smolensko str. 6-407, LT-03201, Vilnius, Lithuania, has been appointed as the SYNBEE Data Protection Officer, and will be supporting all Data Protection Officer operations: data subject access requests, customer claims and requests, supervision of GDPR implementation, risks assessment, incidents resolution, communication with Personal Data Protection authorities.

Information about the DPO qualifications can be found in Annex 4.

Funded by the European Union under the Grant Agreement No 101100509. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Innovation Council and SMEs Executive Agency (EISMEA). Neitherthe European Union nor the granting authorities can be held responsible for them.

ANNEX 1_FINAL VERSION OF STUDY PROTOCOL AS SUBMITTED TO TU DELFT HUMAN RESEARCH ETHICS COMMITTEE (HREC)

Delft University of Technology
HUMAN RESEARCH ETHICS
CHECKLIST FOR HUMAN RESEARCH
(Version January 2022)

IMPORTANT NOTES ON PREPARING THIS CHECKLIST

1. An HREC application should be submitted for every research study that involves human participants (as Research Subjects) carried out by TU Delft researchers
2. Your HREC application should be submitted and approved **before** potential participants are approached to take part in your study
3. All submissions from Master's Students for their research thesis need approval from the relevant Responsible Researcher
4. The Responsible Researcher must indicate their approval of the completeness and quality of the submission by signing and dating this form OR by providing approval to the corresponding researcher via email (included as a PDF with the full HREC submission)
5. There are various aspects of human research compliance which fall outside of the remit of the HREC, but which must be in place to obtain HREC approval. These often require input from internal or external experts such as Faculty Data Stewards, Faculty HSE advisors, the TU Delft Privacy Team or external Medical research partners.
6. You can find detailed guidance on completing your HREC application here
7. Please note that incomplete submissions (whether in terms of documentation or the information provided therein) will be returned for completion **prior to any assessment**
8. If you have any feedback on any aspect of the HREC approval tools and/or process you can leave your comments here

Funded by the European Union under the Grant Agreement No 101100509. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Innovation Council and SMEs Executive Agency (EISMEA). Neitherthe European Union nor the granting authorities can be held responsible for them.

I. Applicant Information

PROJECT TITLE:	SYNBEE: EXPANDING SYNTHETIC BIOLOGY ENTREPRENEURIAL ECOSYSTEMS
Research period: *Over what period of time will this specific part of the research take place*	**May 2023-Feb 2025**
Faculty:	**Bionanoscience**
Department:	**Applied Sciences**
Type of the research project: *(Bachelor's, Master's, DreamTeam, PhD, PostDoc, Senior Researcher, Organisational etc.)*	**European Co-ordination & Support Action Project**
Funder of research: *(EU, NWO, TUD, other – in which case please elaborate)*	**European Commission**
Name of Corresponding Researcher: *(If different from the Responsible Researcher)*	**Dr. Sindhu Naik**
E-mail Corresponding Researcher: *(If different from the Responsible Researcher)*	**s.n.naik@tudelft.nl**
Position of Corresponding Researcher: *(Masters, DreamTeam, PhD, PostDoc, Assistant/ Associate/ Full Professor)*	**Project Leader**
Name of Responsible Researcher: ***Note:*** *all student work must have a named Responsible Researcher to approve, sign and submit this application*	**Dr. Stefania Usai**
E-mail of Responsible Researcher: *Please ensure that an institutional email address (**no Gmail, Yahoo, etc.**) is used for all project documentation/ communications including Informed Consent materials*	**s.usai@tudelft.nl**
Position of Responsible Researcher : *(PhD, PostDoc, Associate/ Assistant/ Full Professor)*	**Programme Manager**

II. Research Overview

NOTE: *You can find more guidance on completing this checklist here*

a) Please summarise your research very briefly (100-200 words)

What are you looking into, who is involved, how many participants there will be, how they will be recruited and what are they expected to do?

Add your text here – (please avoid jargon and abbrevations)
The project aims to perform a SWOT (Strength, Weakness, Opportunities, Threat) analysis in the field of synthetic biology innovation ecosystems. SWOT analysis will be performed based on the responses received from stakeholders across Europe in the field of synthetic biology via a questionnaire and also through interviews. The data collected will be analysed to form best practices between the 4 types of innovation ecosystems (Lead, Strong, Moderate and Emerging) existing in the EU countries.

b) **If your application is an additional project** related to an existing approved HREC submission, please provide a brief explanation including the existing relevant HREC submission number/s.

Add your text here – (please avoid jargon and abbrevations)

Funded by the European Union under the Grant Agreement No 101100509. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Innovation Council and SMEs Executive Agency (EISMEA). Neitherthe European Union nor the granting authorities can be held responsible for them.

NA

c) **If your application is a simple extension of, or amendment to,** an existing approved HREC submission, you can simply submit an HREC Amendment Form as a submission through LabServant.

III. Risk Assessment and Mitigation Plan

NOTE: You can find more guidance on completing this checklist here

Please complete the following table in full for all points to which your answer is "yes". Bear in mind that the vast majority of projects involving human participants as Research Subjects also involve the collection of Personally Identifiable Information (PII) and/or Personally Identifiable Research Data (PIRD) which may pose potential risks to participants as detailed in Section G: Data Processing and Privacy below.

To ensure alignment between your risk assessment, data management and what you agree with your Research Subjects you can use the last two columns in the table below to refer to specific points in your Data Management Plan (DMP) and Informed Consent Form (ICF) – **but this is not compulsory**.

It's worth noting that you're much more likely to need to resubmit your application if you neglect to identify potential risks, than if you identify a potential risk and demonstrate how you will mitigate it. If necessary, the HREC will always work with you and colleagues in the Privacy Team and Data Management Services to see how, if at all possible, your research can be conducted.

			If YES please complete the Risk Assessment and Mitigation Plan columns below.		*Please provide the relevant reference #*	
ISSUE	**Yes**	**No**	**RISK ASSESSMENT – what risks could arise?** *Please ensure that you list ALL of the actual risks that could potentially arise – do not simply state whether you consider any such risks are important!*	**MITIGATION PLAN – what mitigating steps will you take?** *Please ensure that you summarise what actual mitigation measures you will take for each potential risk identified – do not simply state that you will e.g. comply with regulations.*	**DMP**	**ICF**
A: Partners and collaboration						
1. Will the research be carried out in collaboration with additional organisational partners such as: • One or more collaborating research and/or commercial organisations • Either a research, or a work experience internship provider[1] *[1] If yes, please include the graduation agreement in this application*	**Yes**		The project is carried out with other collaborating partners from across Europe, namely., **Participating Organisation Legal Name** / **Country** eureKABIOME – FR HAMEEN AMMATTIKORKEAKOULU OY – FI TECHNISCHE UNIVERSITEIT DELFT – NL	All partners belong to the European Economic Area and abide by the European data policy laws.		

Funded by the European Union under the Grant Agreement No 101100509. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Innovation Council and SMEs Executive Agency (EISMEA). Neitherthe European Union nor the granting authorities can be held responsible for them.

			If YES please complete the Risk Assessment and Mitigation Plan columns below.		*Please provide the relevant reference #*	
ISSUE	**Yes**	**No**	**RISK ASSESSMENT – what risks could arise?** *Please ensure that you list ALL of the actual risks that could potentially arise – do not simply state whether you consider any such risks are important!*	**MITIGATION PLAN – what mitigating steps will you take?** *Please ensure that you summarise what actual mitigation measures you will take for each potential risk identified – do not simply state that you will e.g. comply with regulations.*	**DMP**	**ICF**
			INRAE TRANSFERT SAS FR Biocatalyst Foundation LV F6S Network Ireland Limited IE RIGAS TEHNISKA UNIVERSITATE LV MAX-PLANCK-GESELLSCHAFT ZUR FORDERUNG DER WISSENSCHAFTEN EV DE IMPERIAL COLLEGE OF SCIENCE TECHNOLOGY AND MEDICINE UK Potter Clarkson LLP UK Start Codon Limited UK iGEM Foundation Inc US COMMISSARIAT A L ENERGIE ATOMIQUE ET AUX ENERGIES ALTERNATIVES FR German Association for Synthetic Biology e. V. DE			
2. Is this research dependent on a Data Transfer or Processing Agreement with a collaborating partner or third party supplier? *If yes please provide a copy of the signed DTA/DPA*		**No**				

			If YES please complete the Risk Assessment and Mitigation Plan columns below.		*Please provide the relevant reference #*	
ISSUE	**Yes**	**No**	**RISK ASSESSMENT – what risks could arise?** *Please ensure that you list ALL of the actual risks that could potentially arise – do not simply state whether you consider any such risks are important!*	**MITIGATION PLAN – what mitigating steps will you take?** *Please ensure that you summarise what actual mitigation measures you will take for each potential risk identified – do not simply state that you will e.g. comply with regulations.*	**DMP**	**ICF**
3. Has this research been approved by another (external) research ethics committee (e.g.: HREC and/or MREC/METC)? *If yes, please provide a copy of the approval (if possible) and summarise any key points in your Risk Management section below*		**No**				
B: Location						
4. Will the research take place in a country or countries, other than the Netherlands, within the EU?	**Yes**		Please refer to question 1 for the list of countries taking part in the research.	All participating countries belong to the European economic area and will follow European laws.		
5. Will the research take place in a country or countries outside the EU?		**No**				
6. Will the research take place in a place/region or of higher risk – including known dangerous locations (in any country) or locations with non-democratic regimes?		**No**				
C: Participants						
7. Will the study involve participants who **may** be vulnerable and possibly (legally) unable to give informed consent? (e.g., children below the legal age for giving consent, people with learning difficulties, people living in care or nursing homes,).		**No**				
8. Will the study involve participants who **may** be vulnerable under specific circumstances and in specific contexts, such as victims and witnesses of violence, including domestic violence; sex workers; members of minority groups, refugees, irregular migrants or dissidents?		**No**				
9. Are the participants, outside the context of the research, in a dependent or subordinate position to the investigator (such as own children, own students or employees of either TU Delft and/or a collaborating partner organisation)? *It is essential that you safeguard against possible adverse consequences of this situation (such as allowing a student's failure to participate to your satisfaction to affect your evaluation of their coursework).*	**Yes**		The survey will be sent out to stakeholders who can be students/employees at TU Delft and other organisations who are partners in the project consortium.	The key personnel who are part of the project will not be answering the survey questions in order to not bias the results. The participants however will be anonymous unless they give us explicit consent to retain their identification details to contact them later for an interview. All other participants will be anonymous and their identity cannot be tracked based on their answers. Hence, there will be no social consequences to the participants being in the same organization as the researchers in a sub-ordinate position. No personnel in the project is directly or indirectly able to influence the grading of the student.		

Funded by the European Union under the Grant Agreement No 101100509. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Innovation Council and SMEs Executive Agency (EISMEA). Neitherthe European Union nor the granting authorities can be held responsible for them.

			If YES please complete the Risk Assessment and Mitigation Plan columns below.		*Please provide the relevant reference #*	
ISSUE	**Yes**	**No**	**RISK ASSESSMENT – what risks could arise?** *Please ensure that you list ALL of the actual risks that could potentially arise – do not simply state whether you consider any such risks are important!*	**MITIGATION PLAN – what mitigating steps will you take?** *Please ensure that you summarise what actual mitigation measures you will take for each potential risk identified – do not simply state that you will e.g. comply with regulations.*	**DMP**	**ICF**
10. Is there a high possibility of re-identification for your participants? (e.g., do they have a very specialist job of which there are only a small number in a given country, are they members of a small community, or employees from a partner company collaborating in the research? Or are they one of only a handful of (expert) participants in the study?		**No**				
D: Recruiting Participants						
11. Will your participants be recruited through your own, professional, channels such as conference attendance lists, or through specific network/s such as self-help groups	**Yes**		Participants from different sectors of stakeholders in different countries will be reached out by pre-existing contacts curated by previous projects such as European Synthetic Cell Initiative by TU Delft. Also, contact lists curated by partners in the current project consortium will be utilized to get increased participation in the survey.	• Consent forms with an opening statement instructing the participants that participation is voluntary and anonymous will be sent out along with the survey. Parameters such as the sector of the stakeholders will be captured to help with the analysis of the survey outcome and to derive the matrix of best practices. • At the end of the survey a not mandatory question will be asked to assess if the participant is wiiling to be contacted for an interview at a later stage of the survey analysis. In case a deeper understanding of the viewpoints expressed by the individual is necessary and valuable for the research. For ex: An aspect of lack in resources in emerging innovation ecosystem which requires a serious attention from the policy makers to be addressed to help expand the innovation ecosystem in the field of Synthetic Biology.		ICF
12. Will the participants be recruited or accessed in the longer term by a (legal or customary) gatekeeper? (e.g., an adult professional working with children; a community leader or family member who has this customary role – within or outside the EU; the data producer of a long-term cohort study)		**No**				
13. Will you be recruiting your participants through a crowd-sourcing service and/or involve a third party data-gathering service, such as a survey platform?		**No**				
14. Will you be offering any financial, or other, remuneration to participants, and might this induce or bias participation?		**No**				

			If YES please complete the Risk Assessment and Mitigation Plan columns below.		*Please provide the relevant reference #*	
ISSUE	**Yes**	**No**	**RISK ASSESSMENT – what risks could arise?** *Please ensure that you list ALL of the actual risks that could potentially arise – do not simply state whether you consider any such risks are important!*	**MITIGATION PLAN – what mitigating steps will you take?** *Please ensure that you summarise what actual mitigation measures you will take for each potential risk identified – do not simply state that you will e.g. comply with regulations.*	**DMP**	**ICF**
E: Subject Matter *Research related to medical questions/health may require special attention. See also the website of the CCMO before contacting the HREC.*						
15. Will your research involve any of the following: • Medical research and/or clinical trials • Invasive sampling and/or medical imaging • Medical and *In Vitro Diagnostic Medical* Devices Research		**No**				
16. Will drugs, placebos, or other substances (e.g., drinks, foods, food or drink constituents, dietary supplements) be administered to the study participants? *If yes see here to determine whether medical ethical approval is required*		**No**				
17. Will blood or tissue samples be obtained from participants? *If yes see here to determine whether medical ethical approval is required*		**No**				
18. Does the study risk causing psychological stress or anxiety beyond that normally encountered by the participants in their life outside research?		**No**				
19. Will the study involve discussion of personal sensitive data which could put participants at increased legal, financial, reputational, security or other risk? (e.g., financial data, location data, data relating to children or other vulnerable groups) *Definitions of sensitive personal data, and special cases are provided on the TUD Privacy Team website.*		**No**				
20. Will the study involve disclosing commercially or professionally sensitive, or confidential information? (e.g., relating to decision-making processes or business strategies which might, for example, be of interest to competitors)	**Yes**		There is a small probability that might involve a participant to disclose sensitive information during an interview.	The information will be deleted and not made public to safeguard the participant's interests.		
21. Has your study been identified by the TU Delft Privacy Team as requiring a Data Processing Impact Assessment (DPIA)? *If yes please attach the advice/ approval from the Privacy Team to this application*		**No**				
22. Does your research investigate causes or areas of conflict? *If yes please confirm that your fieldwork has been discussed with the appropriate safety/security advisors and approved by your Department/Faculty.*		**No**				
23. Does your research involve observing illegal activities or data processed or provided by authorities responsible for preventing, investigating, detecting or prosecuting criminal offences *If so please confirm that your work has been discussed with the appropriate legal advisors and approved by your Department/Faculty.*		**No**				

Funded by the European Union under the Grant Agreement No 101100509. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Innovation Council and SMEs Executive Agency (EISMEA). Neitherthe European Union nor the granting authorities can be held responsible for them.

			If YES please complete the Risk Assessment and Mitigation Plan columns below.		*Please provide the relevant reference #*	
ISSUE	**Yes**	**No**	**RISK ASSESSMENT – what risks could arise?** *Please ensure that you list ALL of the actual risks that could potentially arise – do not simply state whether you consider any such risks are important!*	**MITIGATION PLAN – what mitigating steps will you take?** *Please ensure that you summarise what actual mitigation measures you will take for each potential risk identified – do not simply state that you will e.g. comply with regulations.*	**DMP**	**ICF**
F: Research Methods						
24. Will it be necessary for participants to take part in the study without their knowledge and consent at the time? (e.g., covert observation of people in non-public places).		**No**				
25. Will the study involve actively deceiving the participants? (For example, will participants be deliberately falsely informed, will information be withheld from them or will they be misled in such a way that they are likely to object or show unease when debriefed about the study).		**No**				
26. Is pain or more than mild discomfort likely to result from the study? And/or could your research activity cause an accident involving (non-) participants?		**No**				
27. Will the experiment involve the use of devices that are not 'CE' certified? *Only, if 'yes': continue with the following questions:*		**No**				
• Was the device built in-house?						
• Was it inspected by a safety expert at TU Delft? *If yes, please provide a signed device report*						
• If it was not built in-house and not CE-certified, was it inspected by some other, qualified authority in safety and approved? *If yes, please provide records of the inspection*						
28. Will your research involve face-to-face encounters with your participants and if so how will you assess and address Covid considerations?	**Yes**		We will be reaching out to few stakeholders who have given us consent for interviews to get a deeper understanding of the opinions in the field of synthetic biology to innovate. There could be instances where a face-to-face interaction is necessary to be able to get a sense of their infrastructure and research abilities.	Most of the interviews will be conducted virtually and if necessary, face-to-face interviews will be held following the guidelines issued by RIVM (Netherlands). Measures such as, stay home if sick, distancing in busy places along with wearing a face mask, hygiene and ventilation measures if in a meeting room will be followed.		
29. Will your research involve **either:** a) "big data", combined datasets, new data-gathering or new data-merging techniques which might lead to re-identification of your participants **and/or** b) artificial intelligence or algorithm training where, for example biased datasets could lead to biased outcomes?		**No**				
G: Data Processing and Privacy						
30. Will the research involve collecting, processing and/or storing any directly identifiable PII (Personally Identifiable Information) including name or email	**Yes**		We will collect contact information from those individuals who consent to be contacted for an interview at a later stage at the end of the	The participant will be given the option to withdraw such a consent at a later point and this will be communicated in the question.		

			If YES please complete the Risk Assessment and Mitigation Plan columns below.		*Please provide the relevant reference #*	
ISSUE	**Yes**	**No**	**RISK ASSESSMENT – what risks could arise?** *Please ensure that you list ALL of the actual risks that could potentially arise – do not simply state whether you consider any such risks are important!*	**MITIGATION PLAN – what mitigating steps will you take?** *Please ensure that you summarise what actual mitigation measures you will take for each potential risk identified – do not simply state that you will e.g. comply with regulations.*	**DMP**	**ICF**
address that will be used for administrative purposes only? (eg: obtaining Informed Consent or disbursing remuneration)			questionnaire. This question will be not-mandatory to answer. This information will be stored for administrative purposes and also to contact them for the interview.	This contact details will not be shared with other consortium members. The details will be stored at TU Delft project data drive as it is secure. The interviews might be recorded, in which case, a transcript of the interview will be made and the recording will be deleted as this is less risk of losing confidential data.		
31. Will the research involve collecting, processing and/or storing any directly or indirectly identifiable PIRD (Personally Identifiable Research Data) including videos, pictures, IP address, gender, age etc and **what other Personal Research Data** (including personal or professional views) will you be collecting?	**Yes**		Personal and professional views regarding the strength, weakness, opportunities and threats in the capabilities for innovation in the Synthetic Biology field will be collected during the interviews with participants who have given us prior consent.	Interviews can be traced back to the survey questionnaire of the participant. However, this is done with a prior consent from the participant and the involvement is clearly defined in the consent form.		
32. Will this research involve collecting data from the internet, social media and/or publicly available datasets which have been originally contributed by human participants		**No**				
33. Will your research findings be published in one or more forms in the public domain, as e.g., Masters thesis, journal publication, conference presentation or wider public dissemination?	**Yes**		A communication and dissemination plan is part of the project.	However, the research will not hold any re-identifiable details of the participants but a broader sector of the stakeholder group they belong to.		
34. Will your research data be archived for re-use and/or teaching in an open, private or semi-open archive?	**Yes**		Please refer to question 33.			

Funded by the European Union under the Grant Agreement No 101100509. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Innovation Council and SMEs Executive Agency (EISMEA). Neitherthe European Union nor the granting authorities can be held responsible for them.

H: More on Informed Consent and Data Management

NOTE: You can find guidance and templates for preparing your Informed Consent materials) here

Your research involves human participants as Research Subjects if you are recruiting them or actively involving or influencing, manipulating or directing them in any way in your research activities. This means you must seek informed consent and agree/ implement appropriate safeguards regardless of whether you are collecting any PIRD.

Where you are also collecting PIRD, and using Informed Consent as the legal basis for your research, you need to also make sure that your IC materials are clear on any related risks and the mitigating measures you will take – including through responsible data management.

Got a comment on this checklist or the HREC process? You can leave your comments here

IV. Signature/s

Please note that by signing this checklist list as the sole, or Responsible, researcher you are providing approval of the completeness and quality of the submission, as well as confirming alignment between GDPR, Data Management and Informed Consent requirements.

Name of Corresponding Researcher (if different from the Responsible Researcher) (print)

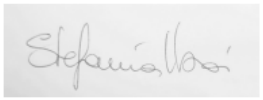
Dr. Sindhu Naik

Signature of Corresponding Researcher: 

Date: 13 March 2023

Name of Responsible Researcher (print)

Dr. Stefania Usai

Signature (or upload consent by mail) Responsible Researcher: 

Date: 13 March 2023

V. Completing your HREC application

Please use the following list to check that you have provided all relevant documentation

Required:

- **Always:** This completed HREC checklist
- **Always:** A data management plan (reviewed, where necessary, by a data-steward)
- **Usually:** A complete Informed Consent form (including Participant Information) and/or Opening Statement (for online consent)

Funded by the European Union under the Grant Agreement No 101100509. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Innovation Council and SMEs Executive Agency (EISMEA). Neitherthe European Union nor the granting authorities can be held responsible for them.

Please also attach any of the following, if relevant to your research:

Document or approval	Contact/s
Full Research Ethics Application	After the assessment of your initial application **HREC will let you know if and when you need to submit additional information**
Signed, valid Device Report	Your Faculty HSE advisor
Ethics approval from an external Medical Committee	TU Delft Policy Advisor, Medical (Devices) Research
Ethics approval from an external Research Ethics Committee	Please append, if possible, with your submission
Approved Data Transfer or Data Processing Agreement	Your Faculty Data Steward and/or TU Delft Privacy Team
Approved Graduation Agreement	Your Master's thesis supervisor
Data Processing Impact Assessment (DPIA)	TU Delft Privacy Team
Other specific requirement	Please reference/explain in your checklist and append with your submission

Funded by the European Union under the Grant Agreement No 101100509. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Innovation Council and SMEs Executive Agency (EISMEA). Neitherthe European Union nor the granting authorities can be held responsible for them.

SYNBEE: EXPANDING SYNTHETIC BIOLOGY ENTREPRENEURIAL ECOSYSTEMS

0. Administrative questions

1. Name of data management support staff consulted during the preparation of this plan.

My faculty data steward, Esther Plomp, has reviewed this DMP on 17th March 2023.

2. Date of consultation with support staff.

2023-03-07

I. Data description and collection or re-use of existing data

3. Provide a general description of the type of data you will be working with, including any re-used data:

Type of data	File format(s)	How will data be collected (for re-used data: source and terms of use)?	Purpose of processing	Storage location	Who will have access to the data
Responses generated for a survey with a questionnaire regarding the synthetic biology field.	.csv files	Online survey	To understand and explore gaps between the 4 different innovation ecosystems across Europe. To form best practices by performing a SWOT analysis of the 4 ecosystems.	Project Storage Drive. Qualtrics tool licensed version by TU Delft will be used to collect survey responses.	The project team (Project leader - Dr. Sindhu Naik and programme manager - Dr. Stefania Usai)
Transcripts of interviews from few of the survey respondents who provide consent to be contacted for a follow up interview.	.doc files.	face-to-face or virtual interviews	To understand and explore gaps between the 4 different innovation ecosystems across Europe. To form best practices by performing a SWOT analysis of the 4 ecosystems.	Project Storage Drive. We will use Microsoft Teams to conduct virtual interviews.	The project team (Project leader - Dr. Sindhu Naik and programme manager - Dr. Stefania Usai)
Audio recordings of the interviews conducted will be stored until transcripts can be made from them. The audio recordings will then be deleted.	.M4A files	face-to-face or virtual interviews	To understand and explore gaps between the 4 different innovation ecosystems across Europe. To form best practices by performing a SWOT analysis of the 4 ecosystems.	Project Storage Drive. We will use a handheld recorder to audio record the interviews.	The project team (Project leader - Dr. Sindhu Naik and programme manager - Dr. Stefania Usai)

4. How much data storage will you require during the project lifetime?

- < 250 GB

II. Documentation and data quality

5. What documentation will accompany data?

- README file or other documentation explaining how data is organised
- Methodology of data collection

III. Storage and backup during research process

6. Where will the data (and code, if applicable) be stored and backed-up during the project lifetime?

- Project Storage at TU Delft

IV. Legal and ethical requirements, codes of conduct

7. Does your research involve human subjects or 3rd party datasets collected from human participants?

- Yes

8A. Will you work with personal data? (information about an identified or identifiable natural person)

Created using DMPonline. Last modified 20 March 2023

Funded by the European Union under the Grant Agreement No 101100509.
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Innovation Council and SMEs Executive Agency (EISMEA).
Neitherthe European Union nor the granting authorities can be held responsible for them.

If you are not sure which option to select, ask your Faculty Data Steward for advice. You can also check with the privacy website or contact the privacy team: privacy-tud@tudelft.nl

- Yes

We will use the contact details (work email) to contact them for a follow-up interview after they have given us consent during the survey to be contacted. They will then provide us with an email address to be contacted at a later date. This information will be temporarily stored for organisational purposes.

8B. Will you work with any other types of confidential or classified data or code as listed below? (tick all that apply)

If you are not sure which option to select, ask your Faculty Data Steward for advice.

- No, I will not work with any confidential or classified data/code

9. How will ownership of the data and intellectual property rights to the data be managed?

For projects involving commercially-sensitive research or research involving third parties, seek advice of your Faculty Contract Manager when answering this question. If this is not the case, you can use the example below.

The SWOT analysis done based on the data generated from the survey will be published in a deliverable report which will be publicly accessable. This data does not hold any intellectual property value as it is only an assessment of the current ecosystem in the field of synthetic biology in Europe.

10. Which personal data will you process? Tick all that apply

- Other types of personal data - please explain below
- Email addresses and/or other addresses for digital communication

We will collect the information of which category of stakeholder group does the individual belong to - For eg: if the respondent is from R&D of an industry, a master's or a bachelor's student, an employee of a start-up company etc.
We will also have audio recordings collected during interviews which will be deleted once they have been transcribed.

11. Please list the categories of data subjects

Stakeholders	Definitions
Policy Makers	Public government institutions
Accelerators	Institutions helping start-ups with a minimum viable product (MVP)
Industry	Research and Development , Scouting intel personnel for Leads
Start-up CEO's	C-level executives at start-ups
Post-docs	Both in scientific and vocational studies
PhD Students	Both in scientific and vocational studies
Master's Students	Both in scientific and vocational studies
Bachelor's Students	Both in scientific and vocational studies
Researchers PI's	Academic institutions, research institutes
Investors	VC's , funding agencies, angel investors.
Incubators	Institutions which provide space and resources for the full spectrum of startups, from early stage to growth stage.
Universities (Innovation centres)	Academic institutions, Tech transfer teams, technology licensing offices (TLOs), Innovation centres

12. Will you be sharing personal data with individuals/organisations outside of the EEA (European Economic Area)?

- No

15. What is the legal ground for personal data processing?

- Informed consent

Informed consent in the form of an opening statement will be provided at the beginning of the survey.

16. Please describe the informed consent procedure you will follow:

All participants will be provided with an opening statement and made clear if they press continue on the survey, they will be providing us the informed consent to process the collected data.

17. Where will you store the signed consent forms?

- Same storage solutions as explained in question 6

Funded by the European Union under the Grant Agreement No 101100509.
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Innovation Council and SMEs Executive Agency (EISMEA).
Neitherthe European Union nor the granting authorities can be held responsible for them.

18. Does the processing of the personal data result in a high risk to the data subjects?

If the processing of the personal data results in a high risk to the data subjects, it is required to perform a Data Protection Impact Assessment (DPIA). In order to determine if there is a high risk for the data subjects, please check if any of the options below that are applicable to the processing of the personal data during your research (check all that apply).
If two or more of the options listed below apply, you will have to complete the DPIA. Please get in touch with the privacy team: privacy-tud@tudelft.nl to receive support with DPIA.
If only one of the options listed below applies, your project might need a DPIA. Please get in touch with the privacy team: privacy-tud@tudelft.nl to get advice as to whether DPIA is necessary.
If you have any additional comments, please add them in the box below.

- None of the above applies

22. What will happen with personal research data after the end of the research project?

- Anonymised or aggregated data will be shared with others

A SWOT Analysis results obtained from the survey analytics will be developed into a report which will be shared with European Commission as a project deliverable and also with the project collaborators. The survey respondents will be anonymised.

25. Will your study participants be asked for their consent for data sharing?

- Yes, in consent form - please explain below what you will do with data from participants who did not consent to data sharing

Participants who do not agree will not go ahead with the survey and hence we will have no data collected from those participants who do not agree to data sharing.

V. Data sharing and long-term preservation

27. Apart from personal data mentioned in question 22, will any other data be publicly shared?

- All other non-personal data (and code) produced in the project

29. How will you share research data (and code), including the one mentioned in question 22?

- My data will be shared in a different way - please explain below

The data produced from the survey will be converted into a report and shared with the project partners and European commission as a deliverable of the project.

30. How much of your data will be shared in a research data repository?

- < 100 GB

31. When will the data (or code) be shared?

- Other - please explain

The data will be shared before the deliverable deadline set in the grant proposal. The SWOT analysis needs to be completed and report submitted by the end of October 2023.

32. Under what licence will be the data/code released?

- CC BY

VI. Data management responsibilities and resources

33. Is TU Delft the lead institution for this project?

- No - please provide details of the lead institution below and TU Delft's role in the project

TU Delft is the lead beneficiary for the SWOT analysis deliverable of the project. However, the lead co-ordinating partner is EureKare (https://eurekare.eu/), who will be responsible in managing rest of the deliverables of the project and TU Delft is only providing a supporting role in those other activities.

Funded by the European Union under the Grant Agreement No 101100509.
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Innovation Council and SMEs Executive Agency (EISMEA).
Neitherthe European Union nor the granting authorities can be held responsible for them.

34. If you leave TU Delft (or are unavailable), who is going to be responsible for the data resulting from this project?

Dr. Stefania Usai
Programme manager
Innovation & Impact Centre, Unit Research Funding EU
& **Dept. of Bionanoscience, Faculty Of Applied Sciences**

Delft University of Technology
Van der Maasweg 9, 2629 HZ Delft
T: +31 (0)15 2786643
E: s.usai@tudelft.nl

35. What resources (for example financial and time) will be dedicated to data management and ensuring that data will be FAIR (Findable, Accessible, Interoperable, Re-usable)?

There is a personnel cost involved and included in the project budget, which is project leader appointed to manage the data management part of the project.
The survey itself will be conducted using one of the TU Delft approved tools and for which TUD already has the license required. The data recieved from the survey will be stored in the project drive and we do not expect to exceed the space and therefore there are no additional costs of long term preservation.

Funded by the European Union under the Grant Agreement No 101100509.
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Innovation Council and SMEs Executive Agency (EISMEA).
Neitherthe European Union nor the granting authorities can be held responsible for them.

ANNEX 2_APPROVAL LETTER FROM THE HREC

Date 24-Mar-2023
Contact person Dr. Cath Cotton, Policy Advisor Academic Integrity
E-mail c.m.cotton@tudelft.nl

TU Delft Delft University of Technology

Human Research Ethics Committee TU Delft
(http://hrec.tudelft.nl)

Visiting address
Jaffalaan 5 (building 31)
2628 BX Delft

Postal address
P.O. Box 5015 2600 GA Delft
The Netherlands

Ethics Approval Application: SYNBEE: EXPANDING SYNTHETIC BIOLOGY ENTREPRENEURIAL ECOSYSTEMS
Applicant: Naik, Sindhu

Dear Sindhu Naik,

It is a pleasure to inform you that your application mentioned above has been approved.

Thanks very much for your submission to the HREC which has been conditionally approved. Please note that this approval is subject to your ensuring that the following condition/s is/are fulfilled:

1) Where there are collaborating (including funding) partners, appropriate formal agreements including clarity on responsibilities, including data ownership, responsibilities and access, should be in place and that relevant aspects of such agreements (such as access to raw or other data) are clear in the Informed Consent.
2) Make sure that no ip addresses are collected.

In addition to any specific conditions or notes, the HREC provides the following standard advice to all applicants:

- In light of recent tax changes, we advise that you confirm any proposed remuneration of research subjects with your faculty contract manager before going ahead.
- Please make sure when you carry out your research that you confirm contemporary covid protocols with your faculty HSE advisor, and that ongoing covid risks and precautions are flagged in the informed consent with particular attention to this where there are physically vulnerable (eg: elderly or with underlying conditions) participants involved.
- Our default advice is not to publish transcripts or transcript summaries, but to retain these privately for specific purposes/checking; and if they are to be made public then only if fully anonymised and the transcript/summary itself approved by participants for specific purpose.

Good luck with your research!

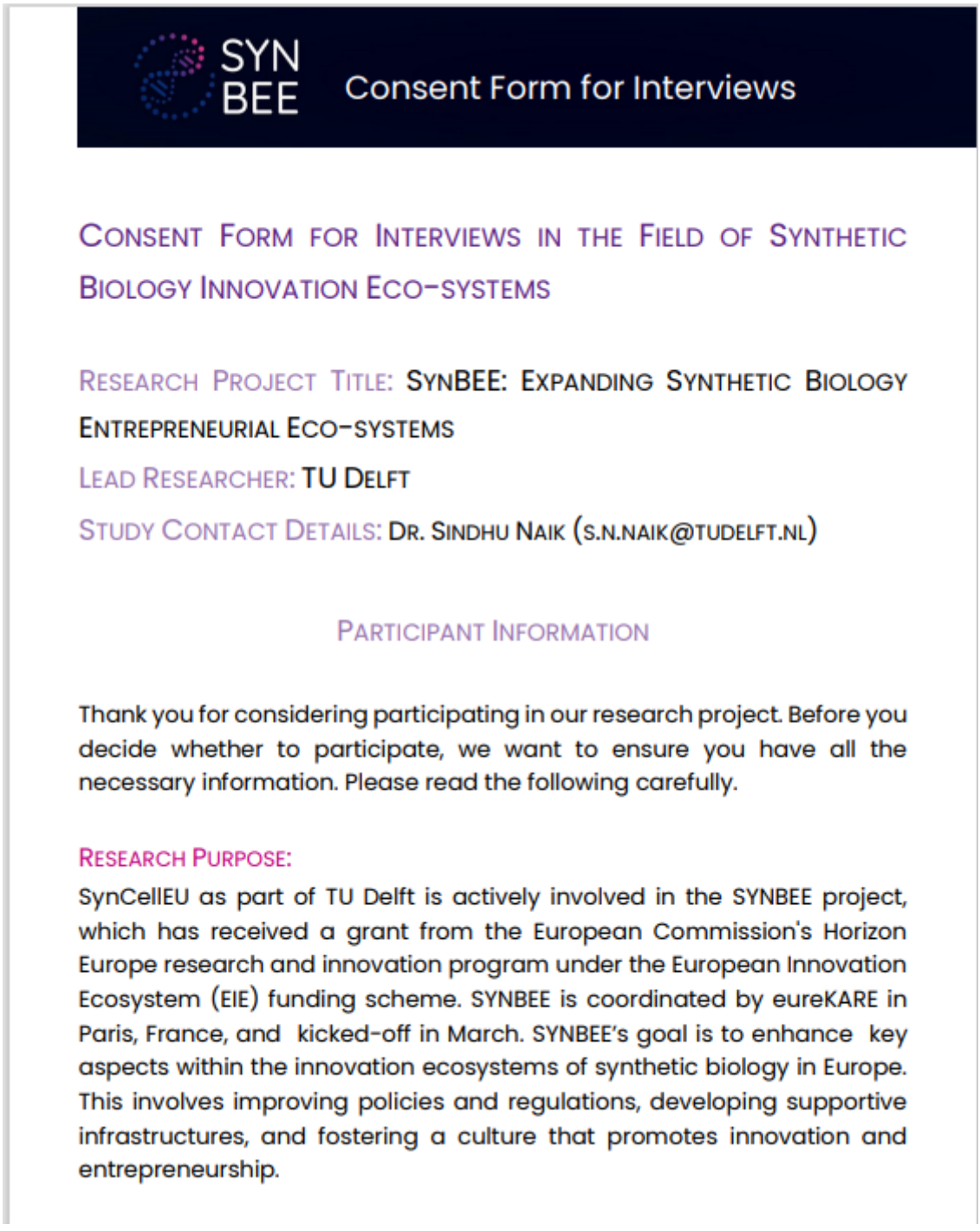
Sincerely,

Funded by the European Union under the Grant Agreement No 101100509. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Innovation Council and SMEs Executive Agency (EISMEA). Neitherthe European Union nor the granting authorities can be held responsible for them.

Dr. Ir. U. Pesch
Chair HREC
Faculty of Technology, Policy and Management

Funded by the European Union under the Grant Agreement No 101100509.
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Innovation Council and SMEs Executive Agency (EISMEA).
Neitherthe European Union nor the granting authorities can be held responsible for them.

ANNEX 3_CONSENT FORMS FOR THE SWOT ACTIVITY



SYN BEE Consent Form for Interviews

CONSENT FORM FOR INTERVIEWS IN THE FIELD OF SYNTHETIC BIOLOGY INNOVATION ECO-SYSTEMS

RESEARCH PROJECT TITLE: SYNBEE: EXPANDING SYNTHETIC BIOLOGY ENTREPRENEURIAL ECO-SYSTEMS

LEAD RESEARCHER: TU DELFT

STUDY CONTACT DETAILS: DR. SINDHU NAIK (S.N.NAIK@TUDELFT.NL)

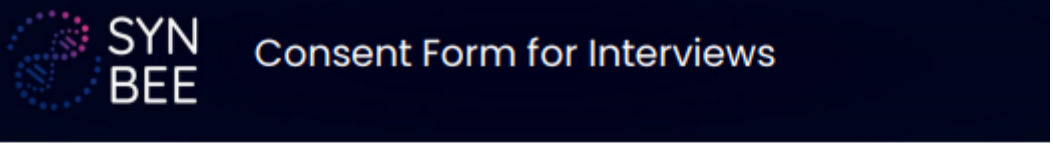
PARTICIPANT INFORMATION

Thank you for considering participating in our research project. Before you decide whether to participate, we want to ensure you have all the necessary information. Please read the following carefully.

RESEARCH PURPOSE:

SynCellEU as part of TU Delft is actively involved in the SYNBEE project, which has received a grant from the European Commission's Horizon Europe research and innovation program under the European Innovation Ecosystem (EIE) funding scheme. SYNBEE is coordinated by eureKARE in Paris, France, and kicked-off in March. SYNBEE's goal is to enhance key aspects within the innovation ecosystems of synthetic biology in Europe. This involves improving policies and regulations, developing supportive infrastructures, and fostering a culture that promotes innovation and entrepreneurship.

Funded by the European Union under the Grant Agreement No 101100509. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Innovation Council and SMEs Executive Agency (EISMEA). Neitherthe European Union nor the granting authorities can be held responsible for them.



The purpose of this study is to gather your valuable perspective that will assist us in identifying strengths, weaknesses, opportunities, and threats (SWOT analysis) within the European synthetic biology community. The interview questions will cover various aspects, including research and development, funding and investment, regulatory frameworks, education and training, industry-academia collaborations, and more. We aim to gather insights from key stakeholders like yourself to create a SWOT analysis of the field.

Research Participation:

Your participation in this study is entirely voluntary. If you choose to participate, you will be asked to engage in an interview with the research team. The interview will be recorded for transcription purposes to create accurate records of the conversation. Your participation is essential for the success of this study. You have the right to withdraw at any time without providing a reason by contacting Dr. Sindhu Naik.

Explicit Consent Points:

Please carefully read the following points and indicate your consent by ticking the appropriate boxes:

PLEASE TICK THE APPROPRIATE BOXES	Yes	No
A: GENERAL AGREEMENT – RESEARCH GOALS, PARTICPANT TASKS AND VOLUNTARY PARTICIPATION		
1. I have read and understood the study information dated [*DD/MM/YYYY*], or it has been read to me. I have been able to ask questions about the study and my questions have been answered to my satisfaction.	☐	☐

Funded by the European Union under the Grant Agreement No 101100509. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Innovation Council and SMEs Executive Agency (EISMEA). Neitherthe European Union nor the granting authorities can be held responsible for them.

Consent Form for Interviews

PLEASE TICK THE APPROPRIATE BOXES	Yes	No
2. I consent voluntarily to be a participant in this study and understand that I can refuse to answer questions and I can withdraw from the study at any time, without having to give a reason.	☐	☐
3. I understand that taking part in the study involves being recorded either on the teams meeting platform or audio only for the purpose of transcription of the interview.	☐	☐
B: POTENTIAL RISKS OF PARTICIPATING (INCLUDING DATA PROTECTION)		
4. I understand that taking part in the study involves the risk of being identified with possible quotations (anonymised) used to create a SWOT analysis.	☐	☐
5. I understand that taking part in the study also involves collecting specific personally identifiable information (PII) [Name and workplace identifiers]. This information will be anonymised [quotes in the report] and will only be accessible to the study team, but has the potential risk of my identity being revealed.	☐	☐
6. The interview data will be stored securely using a TU Delft network drive, and will be deleted once the project is completed. I understand that these measures will be taken to minimize the threat of a data breach and protect my identity in the event of such a breach.	☐	☐
C: Research Publication, Dissemination, and Application		
7. I understand that after the research study, the de-identified information I provide will be used for SWOT analysis report submitted to the European commission	☐	☐

Funded by the European Union under the Grant Agreement No 101100509.
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Innovation Council and SMEs Executive Agency (EISMEA).
Neitherthe European Union nor the granting authorities can be held responsible for them.

Consent Form for Interviews

SIGNATURES

By signing below, I acknowledge that I have read and understood the information provided in the Participant Information and Explicit Consent Points. I voluntarily agree to participate in the research project and consent to the collection, processing, and management of my data as described.

LIENE BRIEDE

NAME OF PARTICIPANT [PRINTED] **SIGNATURE** **DATE**

I, as the researcher, have accurately read out the information sheet to the potential participant and ensured that they understand the details of their consent.

SINDHU NAIK

RESEARCHER NAME [PRINTED] **SIGNATURE** **DATE**

Study contact details for further information: Dr. Sindhu Naik (Email: s.n.naik@tudelft.nl)

Funded by the European Union under the Grant Agreement No 101100509. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Innovation Council and SMEs Executive Agency (EISMEA). Neitherthe European Union nor the granting authorities can be held responsible for them.

Opening statement for the SYNBEE online survey.

The final sentence functions in a way that signifies participants' consent when they proceed by clicking the "Continue" button to access the survey (Print screen here under).

The opening statement:

You are cordially invited to participate in a research study entitled "SynBEE: Expanding Synthetic Biology Entrepreneurial Ecosystems" by University of Delft (TUD), in collaboration with partners such as eureKARE, Häme University of Applied Sciences (HAMK), Toulouse White Biotechnology (TWB), Biocatalyst, F6S, and Riga Technical University (RTU).

This study, funded by the European Commission under grant agreement 101100509, asks several questions that enable us to decipher gaps and challenges faced for innovation in the field of synthetic biology in Europe. The survey takes approximately 15 minutes to complete, and the data will be used to conduct a SWOT analysis per ecosystem to identify gaps in skills, necessary infrastructure, and facilitate knowledge exchange and mentoring between universities across different ecosystems. The purpose is to adapt training programs to meet industry needs, enhancing candidates' employability and mobility across various business cultures, sectors, and geographies.

We take data privacy seriously, and to the best of our ability, we will keep your answers confidential. We will not collect any personal identifying data unless it is provided by the participant with prior consent for an interview. If you consent, your contact information will be stored securely at the University of Delft project drive for organizational purposes. The information will be deleted after the completion of the interview.

Your participation is entirely voluntary, and you may withdraw at any time. If you have any questions or remarks, please feel free to contact Dr. Sindhu Naik (s.n.naik@tudelft.nl). If you agree to participate, please press "continue" to proceed with the survey.

Funded by the European Union under the Grant Agreement No 101100509. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Innovation Council and SMEs Executive Agency (EISMEA). Neitherthe European Union nor the granting authorities can be held responsible for them.

ANNEX 4_DPO QUALIFICATIONS DOCUMENTS

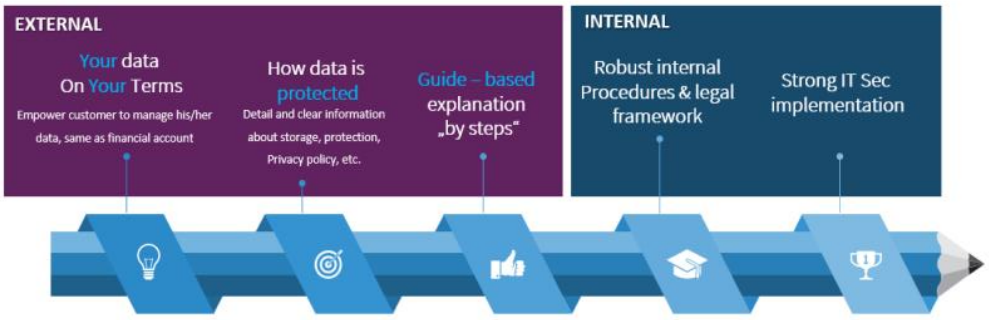
Funded by the European Union under the Grant Agreement No 101100509.
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Innovation Council and SMEs Executive Agency (EISMEA).
Neitherthe European Union nor the granting authorities can be held responsible for them.

1. GDPR AND IT SECURITY FOR FINTECH INDUSTRY

Most of the business operations of financial businesses are based to personal data collection, strict and secure user authentication, also access sensitive information - financials, credit history, transactions. In some cases operations „on behalf of customer", like payment initiation services can be utilized. This naturally imposes very strict privacy requirements. At the same time KYC and AML regulatory requirements make fintech responsible for keeping track about their customers and their operations for very long retention periods, which typically is contradictory to good privacy practices. Only solution here – Information Security Management System (ISMS) which is balanced and well aligned with enterprise Privacy Program and allocated necessary resources: DAP (Data Protection Officer) and CISO (Chief Information Security Officer) with clear mandate from top management to carry out all necessary activities to protect privacy and security of all core financial business operations. Below we do shortly introduce our concept for integrated GRC services.

1.1 Key blocks of Privacy & GDPR compliance

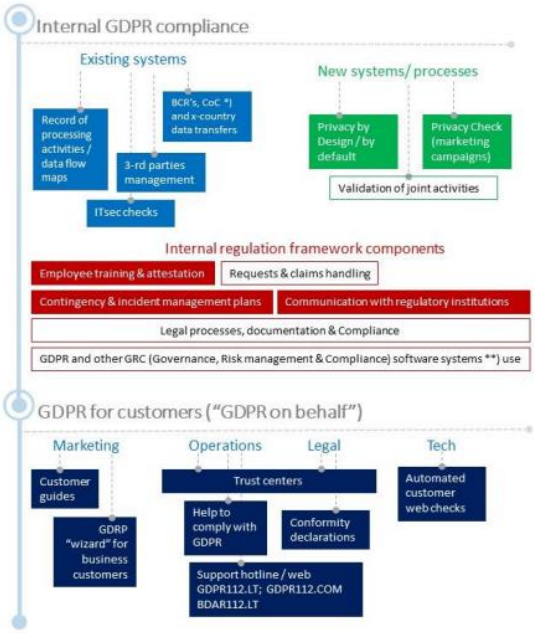
Privacy operational framework helps to ensure proper implementation of personal data protection aspects. GDPR compliance efforts for FinTech organizations should be around those dimensions:



- **CUSTOMER:** main focus to customer: be transparent, customer centric, build trust in interactions with customer's personal data and help to build lasting relationship;
- **INTERNAL**: Ensure that inside processes are well structured from personal data protection perspective, necessary tools and procedures are implemented and regularly followed (not „one time" activity);
- **REGULATORY**: have all necessary controls and proof about implemented requirements. Align to requirements from EU countries data protection authorities, in cases with international operations – there may be other requirements of local privacy legislations to comply as well

Funded by the European Union under the Grant Agreement No 101100509.
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Innovation Council and SMEs Executive Agency (EISMEA).
Neitherthe European Union nor the granting authorities can be held responsible for them.

- **Privacy by Design (PbD) reviews:** for the newly developed systems we carry out PbD review according structured methodology (Privacy Management Reference Methodology, 7 Privacy by Design principles, etc.);
- **Customer Privacy and GDPR – related questions process**: designing process how customers can properly approach Your organization for any privacy or personal data issues and in case of necessity integrate it with the other helpdesk / service desk "engines";
- **Process Privacy check** - taking one isolated business process and checking it for GDPR compliance according our GDPR methodology and existing GDPR framework;
- **Data Protection Impact Assessment** (formal review of any given IT / Cloud system to define risk level, necessity and proportionality of personal data collected, quantifying the risks involved);
- **Detail review of web / mobile assets** – review of existing or planned applications or portals from GDPR perspective;



- **Supporting all external Data Protection Officer operations** (Data subject access requests, customer claims and requests, supervision of GDPR implementation, risks assessment, incidents resolution, communication with Personal Data Protection authorities;
- **Regular training and attestation of employees:** including web-based video trainings and online testing;
- **Legal documents review** – depending on the preparedness of organization, legal documents can be already implemented, or just in preparation phase. Review from the practical applicability viewpoint, advice in cases we see best practices from real data protection operations.
- *(if needed)* **Advice on third party GDPR solutions** for internal compliance (OneTrust, iTrust, TrustHub, etc.)[1];
- *(if needed)* – review of non – EU customers data protection requirements and legislation if such are applicable.

1.2 Information security standards and methodologies

Any organization in finance business should have

- **IT and Cloud technologies strategy** and development roadmap;
- **Information Security risks management framework** and ISMS, aligned with business risks and continuity management;
- Proper **Governance** of all IT operations;
- Well managed **relations with third parties** – business partners, customers, regulatory authorities.

[1] *Short review of Privacy software / cloud services vendors can be found here:* https://iapp.org/resources/article/2018-privacy-tech-vendor-report/

Funded by the European Union under the Grant Agreement No 101100509.
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Innovation Council and SMEs Executive Agency (EISMEA).
Neitherthe European Union nor the granting authorities can be held responsible for them.

Those tasks are universal across any organization and do not depend on specific infrastructure, systems or business models. At strategic level this may sound too simplistic, however full implementation of those tasks is very broad task critically important for overall business success.

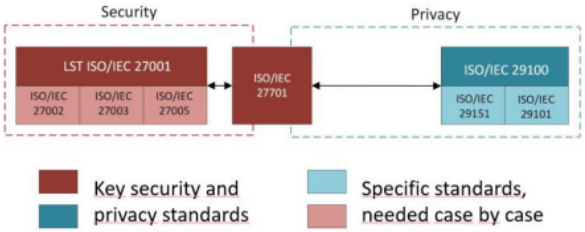
To fully achieve end-to-end effectiveness, there should be deep alignment from strategy level to the smallest systems implementations, employee work rules and procedures. For that detail knowledge of situation is needed, which is typically achieved through audits (as „snapshot picture" in time), experienced broad knowledge internal or external IT Security specialists who know and document situation regularly („chronicle") and well equipped and trained experts on specific systems in operations or implementation („masters"). Organizations can use completely different project and organization development methodologies (e.g. Agile vs. Waterfall), however good governance and management is key to success or failure in both approaches.

To optimize process and minimize probability for errors and other risks we do use structured approaches based on internationally recognized standards together with best practices and other expert insights.

Use of standards: IT governance, use of standards for security and privacy should be well planned. Overall use of ISO 27001/27002 (Information Security Management System) standards, or NIST standards in US along with other good IT governance practices (ITIL, CoBIT and other) is necessary for bigger organizations.

It should be taken into account that use of such standards and frameworks is very time and resources consuming and intensive task, e.g. ISO 27001 alone has 114 „controls" to ensure good control over IT security situation. Application of standards should be wise and aligned with organization size and needs (applicability)

We do apply Information Security standards along with most recent additions (so called „Privacy Extensions", as those standards and frameworks are used by EU countries personal data protection supervisory authorities along with GDPR and other legislation. Various recommendations issued for good practices by European Data Protection Board[2], and consecutively – by local EU countries data protection authorities (e.g. Lithuanian State Data Protection Inspectorate – VDAI[3]).



Privacy Partners use simplified version of ISO 27001 audit methodologies which allows to indicate key importance issues in organization systems, processes, IT and cloud environment without going too deep into unnecessary details. Worth to mention that most of regulatory authorities (e.g. Bank of Lithuania or central banks of other EU countries do require detail documentation on IT security policy and overall IT development strategy, however this does not mean formal certification for IT security standards, which would mean unnecesary regulatory and financial load for smaller agile fintech companies.

[2] *List of variuos EU Data Protection Board recommendations: https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en*

[3] *Lithuanian State Data Protection Inspectorate recommendations: https://vdai.lrv.lt/lt/informacija-visuomenei/rekomendacijos-gaires-ir-kt*

Funded by the European Union under the Grant Agreement No 101100509. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Innovation Council and SMEs Executive Agency (EISMEA). Neitherthe European Union nor the granting authorities can be held responsible for them.

1.3 Resourcing models

Full scope of Privacy and Security compliance activities should be managed by specialist team. To ensure independence DPO (Data Protection Officer) can not be at the same time IT manager or CISO. Smaller organizations do have challenges to appoint all necessary personnel both due to the cost and scarce resources in the market of experienced specialists with proven track record and experience in specific industry.

For our customers we do:

- Appoint dedicated specialist who is aware about all infosec and privacy questions going on in organization;
- Depending on need – adding experts form our IT and legal teams and experienced DPO's;
- Have helpdesk / hotline communication channels open for organizations to be able to request advice anytime;
- For bigger organizations – embedding Data Protection Officers into organizations as part-time specialist, also deploying internal org compliance portals;
- Supporting internal organization DPO's and IT managers in "co-pilot" mode, allowing them concentrate on strategic tasks and at the same time bringing top notch latest knowledge form DPO and CISO domains.

WORK PRINCIPLES AND CERTIFICATES

Privacy and security do encompass any organizational aspect and process. In our activities we do stick to those principles:

- **Specialization**: IT should be analyzed by experienced IT manager, legal – lawyer with GDPR / Privacy specialization, overall organization processes – experienced manager;
- **Regularity of processes:** audit, inventory or review always propose recommendations or actions which should be implemented and tracked;
- **Proactive and preventive approach**: Solution of problems and crisis always is more costly and resources consuming than timely preparation;
- **4 (or more) eyes principle**: in tough and unknown situations we do discuss internally, in case of necessity – externally in DPO / Infosec community and implement Quality Assurance processes;
- **Strict process isolation and internal IT security:** we do practice what we sell. Strict confidentiality, no details for non-involved specialists, technical isolation and access rights management, working with customer documents in customer infrastructure allow us to ensure necessary confidentiality;
- **Responsibility and accountability:** any work done is logged in our systems in detail and are accessible for customers;
- **Worst case scenario coverage:** we do guarantee quality of our work. At the same time, we are covered by insurance up to 1 M EUR per incident (unlimited number of incidents per year)

Funded by the European Union under the Grant Agreement No 101100509. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Innovation Council and SMEs Executive Agency (EISMEA). Neitherthe European Union nor the granting authorities can be held responsible for them.

KEY CERTIFICATIONS

Detail certifications, links to the issuer online resources confirming certification or translations to Lithuanian language are available upon request.

Membership in professional organizations: Privacy Partners are member of Lithuanian Data Protection Officers (LDAPA) association - http://ldapa.lt/ , Martynas Bieliūnas holds membership in European Association of Data Protection Professionals (www.eadpp.eu)

Main Privacy Partners experts, participating in projects, qualification proven by international and local certifications.

- **Martynas Bieliūnas** (CIPP/E (Certified Information Privacy Professional/Europe), CIPM (Certified Information Privacy Manager), ISO/IEC 27001 Lead Auditor);
- **Mantas Kapočius** (CompTIA, ITIL project and process management certificates);
- **Vytautas Krekys** (CISO, Fintech compliance qualifications, physical and IT security, risk management specialist);
- **Ingrida Stankevičienė** (IT Governance GDPR Fundamentals, CIPP/E);
- **Mantas Sebeika** (IT technical specialist);
- **Šarūnas Virbickas** (Information security and privacy law expert (LL.M. Stockholm University, Law and IT), Data Protection Officer (ECPC-B), Prince 2 Foundation project management, Transnational law certified);
- **Artūras Jankauskas** (IT security specialist).
- **Matas Adomavičius** (system analyst);

Funded by the European Union under the Grant Agreement No 101100509. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Innovation Council and SMEs Executive Agency (EISMEA). Neitherthe European Union nor the granting authorities can be held responsible for them.

QUALIFICATION DOCUMENTS: METHODOLOGY, CERTIFICATES, INSURANCE

The Chairperson and Directors of the

International Association of Privacy Professionals

decree that in recognition of the successful demonstration of the requisite knowledge of information privacy with advanced concentration in European data protection laws, standards and practices, we do confer upon:

Martynas Bieliunas

the designation of

Certified Information Privacy Professional/Europe (CIPP/E)

With all rights, privileges and distinction thereunto appertaining. In witness hereof we have caused this certificate to be signed by the duly authorized officers of the Association.

CIPP

ANSI

0003053541
August 1, 2022
July 31, 2024

The Chairperson and Directors of the

International Association of Privacy Professionals

decree that in recognition of the successful demonstration of the requisite knowledge of information privacy management, we do confer upon:

Martynas Bieliunas

the designation of

Certified Information Privacy Manager (CIPM)

With all rights, privileges and distinction thereunto appertaining. In witness hereof we have caused this certificate to be signed by the duly authorized officers of the Association.

CIPM

ANSI

0003053541
August 1, 2022
July 31, 2024

The Chairperson and Directors of the

International Association of Privacy Professionals

decree that in recognition of the successful demonstration of the requisite knowledge of information privacy with advanced concentration in European data protection laws, standards and practices, we do confer upon:

Ingrida Stankeviciene

the designation of

Certified Information Privacy Professional/Europe (CIPP/E)

With all rights, privileges and distinction thereunto appertaining. In witness hereof we have caused this certificate to be signed by the duly authorized officers of the Association.

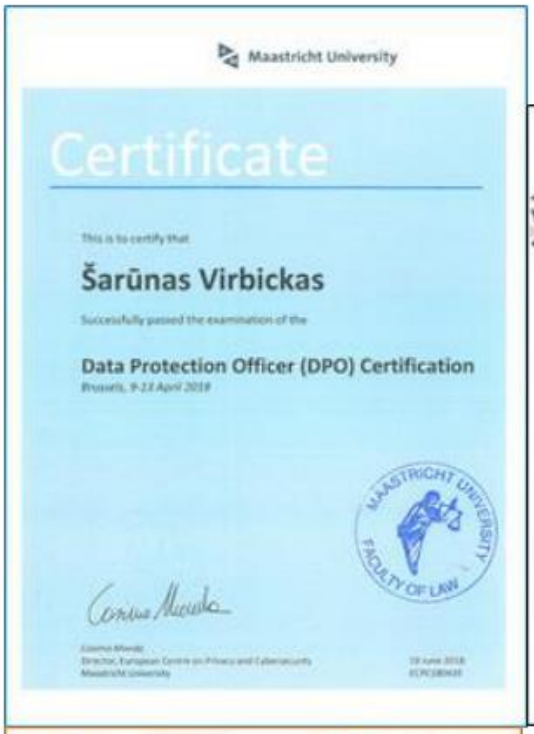
CIPP

ANSI

0003316831
June 1, 2021
June 30, 2023

Funded by the European Union under the Grant Agreement No 101100509. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Innovation Council and SMEs Executive Agency (EISMEA). Neitherthe European Union nor the granting authorities can be held responsible for them.

QUALIFICATION DOCUMENTS: METHODOLOG


Maastricht University

Certificate

This is to certify that

Šarūnas Virbickas

Successfully passed the examination of the

Data Protection Officer (DPO) Certification

Brussels, 9-13 April 2018

MAASTRICHT UNIVERSITY FACULTY OF LAW


EXAMENSBEVIS

DEGREE CERTIFICATE

Sarunas Virbickas

Juris magisterexamen

Stockholms universitet


APMG International

AXELOS

GLOBAL BEST PRACTICE

This is to certify that

Sarunas Virbickas

Has achieved the

PRINCE2® Foundation certificate in Project Management

Effective from 19 October 2016 Expiry date N/A

Certificate number 04053244-01-KKWG Candidate number 200050153O

Funded by the European Union under the Grant Agreement No 101100509.
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Innovation Council and SMEs Executive Agency (EISMEA).
Neitherthe European Union nor the granting authorities can be held responsible for them.

QUALIFICATION DOCUMENTS: METHODOLOGY, CERTIF

Maastricht University
ECPC
European Centre on Privacy & Cybersecurity

Attn. Šarūnas Virbickas
42 Rue du Tivoli
67000 Strasbourg
France

Maastricht, 19 July 2021

Dear Šarūnas Virbickas,

Following your participation in the Emerging Issues and Challenges Course from 9 – 11 June 2021, we are pleased to confirm that with this letter your ECPC-B Professional Data Protection Officer Certification is re-validated.

Šarūnas Virbickas
Certificate number: ECPC180435
Date of obtaining certification: 19 June 2018
Date of revalidating certification: 11 June 2021

This certification is valid until: 11 June 2023

We would like to thank you very much for your confidence in the European Centre on Privacy and Cybersecurity and look forward to staying in touch.

Kind regards,

Joyce Groneschild
Project Manager, ECPC


Certificate

Šarūnas Virbickas

Data Protection Officer (DPO) Certification

Funded by the European Union under the Grant Agreement No 101100509.
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Innovation Council and SMEs Executive Agency (EISMEA).
Neitherthe European Union nor the granting authorities can be held responsible for them.

QUALIFICATION DOCUMENTS: METHODOLOGY, CERTIFICATES, INSURANCE


EXIN

Mantas Kapocius

ITIL Foundation Certificate
in IT Service Management


CompTIA

ADVANCING THE GLOBAL IT INDUSTRY

Mantas Kapocius

has successfully completed the requirements to be recognized as

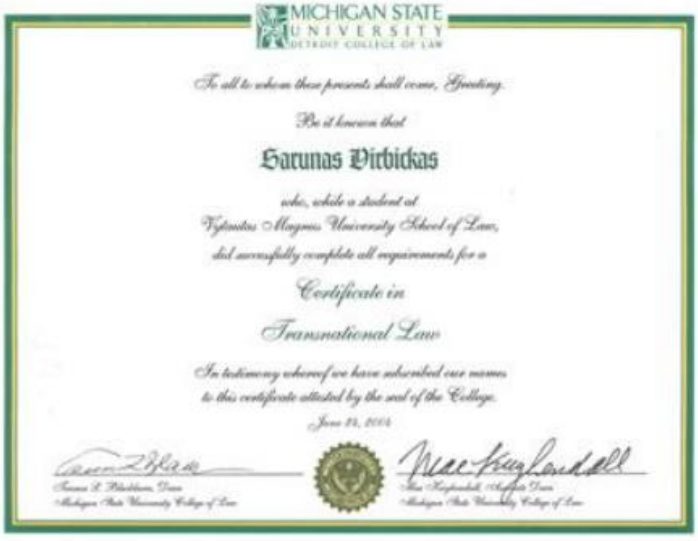
CompTIA Project+ CERTIFIED

COMP001020432475 — CAREER ID

TODD THIBODEAUX, President & CEO

June 28, 2012 — DATE CERTIFIED

Code:3FWR42E193R1299G
Verify at: http://verify.CompTIA.org


MICHIGAN STATE UNIVERSITY
DETROIT COLLEGE OF LAW

To all to whom these presents shall come, Greeting.

Be it known that

Šarunas Pirbickas

who, while a student at
Vytautas Magnus University School of Law,
did successfully complete all requirements for a

Certificate in
Transnational Law

In testimony whereof we have subscribed our names
to this certificate attested by the seal of the College.

June 23, 2014


IBITGQ

International Board for IT Governance Qualifications

Ingrida Stankeviciene

EU General Data Protection Regulation Foundation
(GDPR F)

GASQ

Funded by the European Union under the Grant Agreement No 101100509.
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Innovation Council and SMEs Executive Agency (EISMEA).
Neitherthe European Union nor the granting authorities can be held responsible for them.

QUALIFICATION DOCUMENTS: METHODOLOGY, CERTIFICATES, INSURANCE

TRECCERT

TRECCERT CERTIFICATE

This is to certify that

Martynas Bieliūnas

successfully fulfilled the certification requirements and is recognized as a

TRECCERT Certified ISO/IEC 27001 Lead Auditor

Date Certified: **22.12.2021**

Valid Until: **21.12.2024**

Certificate Number: **ISMS-30105-LA-TC-21**

TRECCERT CERTIFIED

Thilo Klein

Thilo Klein

Chief Executive Officer

Funded by the European Union under the Grant Agreement No 101100509.
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Innovation Council and SMEs Executive Agency (EISMEA).
Neitherthe European Union nor the granting authorities can be held responsible for them.

QUALIFICATION DOCUMENTS: METHODOLOGY, CERTIFICATES, INSURANCE

onetrust

THIS CERTIFICATE IS PROUDLY PRESENTED TO:

Mantas Sebeika

In acknowledgement of the successful practice of privacy, security, and governance.
The holder of this certificate has demonstrated the requirements to earn the designation of

OneTrust Certified Privacy Professional

This individual is now certified to serve as an administrator of the OneTrust Privacy Management Platform

Kabir Barday, CEO of OneTrust

3/22/2023 — DATE: *Valid One Year*

C79796 — Certification Number

QUALIFICATION DOCUMENTS: METHODOLOGY, CERTIFICATES, INSURANCE

onetrust

THIS CERTIFICATE IS PROUDLY PRESENTED TO:

Matas Adomavicius

In acknowledgement of the successful practice of privacy, security, and governance.
The holder of this certificate has demonstrated the requirements to earn the designation of

OneTrust Certified Privacy Professional

This individual is now certified to serve as an administrator of the OneTrust Privacy Management Platform

Kabir Barday, CEO of OneTrust

3/22/2023 — DATE: *Valid One Year*

C79802 — Certification Number

Funded by the European Union under the Grant Agreement No 101100509.
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Innovation Council and SMEs Executive Agency (EISMEA).
Neitherthe European Union nor the granting authorities can be held responsible for them.

QUALIFICATION DOCUMENTS: METHODOLOGY, CERTIFICATES, INSURANCE

INSURANCE POLICY

Colemont

Coverholder at LLOYD'S

CERTIFICATE OF INSURANCE

This is to Certify that insurance coverage have been effected to below named Insured under following terms:

POLICY NUMBER:	ESK0339434787
TYPE:	PROFESSIONAL INDEMNITY LIABILITY NETWORK SECURITY & PRIVACY LIABILITY CYBER INCIDENT RESPONSE
INSURED:	**Privacy Partners UAB** Legal entity code: 304846919
ADDRESS:	Smolensko g. 6, LT-03201 Vilnius
PERIOD:	From: 01st March 2022 (00:01 Local Standard Time) To: 01st March 2023 (00:01 Local Standard Time)
INTEREST:	To indemnify the Insured against liability incurred in connection with the business.
LIMIT OF LIABILITY:	EUR 1,000,000 each and every claim, including costs and expenses
DEDUCTIBLE(S):	EUR 0 each and every claim
TERRITORIAL LIMITS:	Worldwide
CONDITIONS:	**Wording:** Technology (RoW) v3.0
INSURER:	Underwritten by Lloyd's Insurance Company S.A. and other insurers

Authorised Signatory
for and on behalf of
UADBB "Colemont draudimo brokeris"
Legal entity code 124495055
Konstitucijos ave. 26, Floor 6, LT-08105 Vilnius
Lithuania

Date: 16-03-2022

Generalinis direktorius
Giedrius Ciunskas

UADBB „Colemont draudimo brokeris" | Konstitucijos pr. 26 | LT- 08105 Vilnius | Įm.kodas 124495055
AB bankas "Swedbank" a.s LT58 7300 0100 8556 0481 www.colemont.lt | el.p. info@colemont.lt Coverholder acting on behalf of Lloyd's Brussels (Lloyds's Insurance Company S.A.), a subsidiary of Lloyds' and authorised by the National Bank of Belgium.

Funded by the European Union under the Grant Agreement No 101100509.
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Innovation Council and SMEs Executive Agency (EISMEA).
Neitherthe European Union nor the granting authorities can be held responsible for them.

DOCUMENT VALIDITY

Documentation is actual and valid till June 1, 2023. There can be additions or customizations, if experts will pass additional exams or new employees are added.

Martynas Bieliūnas
Director / Managing Partner

Privacy Partners
Smolensko g. 6-407, Vilnius
Tel. +370 5 254 8240, Mob. +370 698 25292
Email: martynas@privacypartners.lt
https://privacypartners.lt

BDAR / INFOSEC (Privacy Partners support):
gdpr@privacypartners.lt; ph. +370 5 2548240

Funded by the European Union under the Grant Agreement No 101100509.
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Innovation Council and SMEs Executive Agency (EISMEA).
Neitherthe European Union nor the granting authorities can be held responsible for them.