Food Systems in European Cities

Deliverable 8.2

POPD-Requirement No.2

Project Acronym and Name	FoodE – Food Systems in European Cities
Type of action	IA – Innovation Action
Grant Agreement No.	862663
Work package	8
Dissemination level	Confidential
Document type	Ethics
Lead partner	UNIBO
Authors	Antonella Samoggia, Francesco Orsini, Francesca Monticone, Matteo Vittuari, Fabio De Menna, Mara Petruzzelli, Francesco Cirone, Rachele Del Monte
Contributors	All partners
Planned delivery date	31/05/2020
Actual delivery date	29/05/2020
Project website	www.foode.eu
Project start date	01/02/2020
Duration	48 months
Version	1.0

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 862663

Project Consortium

No.	Institution Short name	Institution Full name	Country
1	UNIBO	ALMA MATER STUDIORUM – UNIVERSITÀ DI BOLOGNA	IT
2	APT	INSTITUT DES SCIENCES ET INDUSTRIES DU VIVANT ET DE L'ENVIRONNEMENT - AGRO PARIS TECH	FR
3	RMN	COMMUNE DE ROMAINVILLE	FR
4	SWUAS	FACHHOCHSCHULE SUDWESTFALEN	DE
5	ILS	INSTITUT FUR LANDES- UND STADTENTWICKLUNGSFORSCHUNG gGMBH	DE
6	FLY	FLYTECH SRL	IT
7	NOL	NOLDE ERWIN	DE
8	BOL	COMUNE DI BOLOGNA	IT
9	NAP	COMUNE DI NAPOLI	IT
10	UNINA	UNIVERSITA DEGLI STUDI DI NAPOLI FEDERICO II	IT
11	HCA	HAGUE CORPORATE AFFAIRS BV	NL
12	LAN	GEMEENTE LANSINGERLAND	NL
14	WR	STICHTING WAGENINGEN RESEARCH	NL
16	POL	POLAR PERMACULTURE SOLUTIONS AS	NO
17	TAS	TASEN MICROGREENS AS	NO
18	MBI	ASOCIATIA MAI BINE	RO
19	ARC	ARCTUR RACUNALNISKI INZENIRING DOO	SI
20	BEE	DRUSTVO URBANI CEBELAR	SI
21	SBD	AJUNTAMENT DE SABADELL	ES
22	ISL	ORGANIZACION DE PRODUCTORES DE TUNIDOS Y PESCA FRESCA DE LA ISTA DE TENERIFE	ES
23	ULL	UNIVERSIDAD DE LA LAGUNA	ES
24	UAB	UNIVERSITAT AUTONOMA DE BARCELONA	ES
25	METAINST	STICHTING METABOLIC INSTITUTE	NL
26	NBL AS	NABOLAGSHAGER AS	NO

Document Control Sheet

Version	Date	Summary of changes	Author(s)
0.1	05/05/2020	First draft	UNIBO
1.0	29/05/2020	Final version filled in with the partners' contributions	All partners

Table of contents

Introduction

This deliverable contains the information and documents required by the European Commission in order to ensure compliance with ethic requirement no. 2:

- Confimation that beneficiaries have appointed a Data Protection Officer (DPO) and that the contact details of the DPO are made available to all data subjects involved in the research. For beneficiaries not required to appoint a DPO under the General Data Protection Regulation (GDPR) a detailed data protection policy for the project must be kept on file and submitted to the Agency upon request.
- The beneficiary must explain how all of the data they intend to process is relevant and limited to the purposes of the research project (in accordance with the 'data minimisation' principle).
- A description of the technical and organisational measures that will be implemented to safeguard the rights and freedoms of the data subjects/research participants.
- A description of the security measures that will be implemented to prevent unauthorised access to personal data or the equipment used for processing.
- In case personal data are transferred from the EU to a non-EU country or international organisation, confirmation that such transfers are in accordance with Chapter V of the General Data Protection Regulation 2016/679.
- In case personal data are transferred from a non-EU country to the EU (or another third state), confirmation that such transfers comply with the laws of the country in which the data was collected.
- In case of further processing of previously collected personal data, an explicit confirmation that the beneficiary has legal grounds for the data processing and that the appropriate technical and organisational measures are in place to safeguard the rights of the data subjects.

The following sections contain the details of the DPO for each beneficiary and provide, among others, a description of procedures for the processing of data used for the research, for procedures that will be implemented for the safeguarding the rights and freedoms of the data subjects/research participants, for security measures to prevent unauthorized access to personal data, for the further processing of previously collected personal data.

1 General overview

The General Data Protection Regulation (GDPR) provides a common legal framework for all EU Member states and sets guidelines for the collection and processing of personal information of individuals within the European Union (Regulation 2016/679 EU). It applies to all companies processing the personal data of data subjects residing in the Union, regardless of the company's location. The GDPR makes its applicability very clear – it applies to the processing of personal data by controllers and processors in the EU, regardless of whether the processing takes place in the EU or not. The GDPR also applies to the processing of personal data of data subjects in the EU by a controller or processor not established in the EU, where the activities relate to: offering goods or services to EU citizens (irrespective of whether payment is required) and the monitoring of behavior that takes place within the EU. Non-EU businesses processing the data of EU citizens also have to appoint a representative in the EU.

The GDPR has also an impact on research activities. International research consortium must implement a data processing compliant with the GDPR (artt. 6, 7, 8, 9, 13, 14 of the GDPR), releasing a proper information sheet and consent form.

2. Contact details of Data Protection Officers for Beneficiary

According to the art. 37 of GDPR, "the controller and the processor shall designate a data protection officer in any case where:

1. the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
2. the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale […]".

Beneficiaries of the FoodE consortium required to appoint a DPO. The details can be found in the table below:

Beneficiary	DPO contact details
UNIBO	privacy@unibo.it - scriviunibo@pec.unibo.it
APT	tahar.zouzou@agroparistech.fr
RMN	dpo@ville-romainville.fr
SWUAS	datenschutzbeauftragte@fh-swf.de
ILS	m.boden@boden-rechtsanwaelte.de
NOL	e.nolde@nolde-partner.de
UNINA	uff.privacy@unina.it
HCA	privacy@hague.company, atanasov@hague.company
LAN	marijke.schep@lansingerland.nl
WR	functionarisgegevensbescherming@wur.nl
ARC	tristan.pahor@arctur.si
SBD	protecciodades@ajsabadell.cat - dpd@ajsabadell.cat
ULL	dpd@ull.es ; https://www.ull.es/servicios/dpd/
UAB	proteccio.dades@uab.cat
NBL AS	adam@nabolagshager.no

3 Processing of data

3.1 Data Minimization principles

The data minimization principle is set out in art.5 (1)(c) of the GDPR, and it states that:

"1. Personal data shall be:
(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation)"

The data processing is done within the research activities framework and after the collection of data subject's consent.

During the project, participants' personal data collected in the FoodE app will be used for research purposes. Data will be used for reports, articles, infographics. Participants' personal data will be analysed through third party services and softwares. Personal data, such as socio-economic information and food habits, will be used for app user profiling, dissemination of information, promotion of CRFS products and services, promotions of events at the CRFS level, engage in environmentally-oriented loyalty programme, engage in promoting special benefits and awards, share FoodE research findings.

Data collected from dissemination activity involving school pupils, will be used to support research activity in awareness creation in young people. Data will be used in public events, among MyLocalFoodE initiatives, with the purposes to: i) return a feedback of the in-class experience to kid families; ii) engage school pupils in presenting sustainable CRFS concepts; and iii) developing (within Hackatons) innovative strategies for developing innovative CRFS in their regions. Awareness creation activities in school pupils will be included in the European Guidebook to Sustainable CRFS.

As a first step to develop an operational methodology for the assessment of CRFS, FoodE will identify and evaluate which are the main features of CRFS initiatives contributing to deliver environmental, societal, and economical sustainable actions.To do so, a survey will be delivered to participants and managers of sustainable food related initiatives across Europe. No personal data will be collected but only generic data pertaining to the core activities of the CRFS initiative (e.g. size, type of operation, market channels, products, etc.). Data will be used for reports, articles, infographics.

In addition, the questionnaire will allow each CRFS initiative to be included in the largest comprehensive European database of sustainable City/Region food systems. A second data collection will regard the environmental, economic, and social impacts of selected CRFS. No personal data will be collected. The subsequent analysis will be used for a simplified assessment of the impacts and the creation of an innovative tool for the social, environmental and economic assessment of initiatives that will be made available after the end of the project. The data collected will stay confidential, will be used only for research and will not be sold.

Each partner partitipating, in order to determine their respective responsabilities for compliance with the obligations under GDPR, will meet their respective duties to provide the information referred to in article 13.

As regards the exercising of the rights, the data subjects can adress the DPO of each partner.

3.2 Technical and organisational measures implemented to safeguard the rights and freedoms of the data subjects/research participants and to prevent unauthorised access to personal data

First of all, all the people involved in personal data processing within the research project will be informed before starting research activities and they will receive a detailed information (see art. 13 of the GDPR) and they will explicitly consent to the personal data processing (see Del. 8.1). Relating to personal data not obtained directly from the data subject, the information relating to the processing of personal data will not be provided in case of impossibility of the provision to the data

subject, or involvement of a disproportionate effort, or the provision is likely to render impossible or seriously impair the achievement of the objectives of that processing, pursuant to Art. 14, par. 5 of the GDPR.

Moreover, the GDPR introduces the principles of accountability, privacy by design and by default. It determines controller and processor's responsibilities and requires the implementation of appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation (artt. 23-25 and Chapter IV of the GDPR). Controller is responsible for setting out data processing procedures according to the GDPR.

Each Partner participating in the project, as an independent Data controller of the personal data processed in its research is fully compliant with the principles and standards sanctioned by the GDPR and, in particular, implemented organizational and technical measures, pursuant to art. 32 of the GDPR, as detailed below.

FLY, BOL, NAP, POL, TAS, BEE, ISLATUNA, METAINST confirm that they do not process personal data in relation to the research H2020-FoodE.

3.2.1. Alma Mater Studiorum, Università di Bologna (UNIBO)

Alma Mater Studiorum-Università di Bologna has a complex security system for its IT infrastructure (server, personal computer, storage cloud etc.), involving the whole university staff according to Decreto Rettorale n. 271/2009 del 23.02.2009 (Testo unico sulla privacy e sull'utilizzo dei sistemi informatici di Ateneo).

Alma Mater Studiorum-Università di Bologna subscribed the archival system Titulus97, which determines the management, archival, storage rules of the whole administrative paper and digital University's documentation and is the core system on which actions (by design) are implemented to guarantee the protection of personal data.

With regards to personal data protection in the framework of research projects, in particular, Alma Mater Studiorum-Università di Bologna implements organizational and technical security actions:

a) it organizes training courses for administrative staff supporting research teams. Some training workshops involve also researchers in the wider framework of research integrity. These workshops are certified by the University Human Resources Department;
b) it promotes policies to strengthen personal data protection actions (e.g. university staff can access to online resources only after the authentication; passwords must be periodically modifie – every six months – on the basis of an identity management system; authorized personnel only can access to online resources on the basis of the activities carried out);
c) it promotes security policies through its IT Systems and Services Division (Area Sistemi e Servizi Informatici – CESIA);
d) it provides research teams with IT tools for the data processing and storage. Research teams, for example, can access to university data storage tool in cloud (OneDrive) using the institutional password;
e) it realizes, under the GDPR provisions, a data processing register with risk analysis, impact evaluation and organizational and technical tools to protect personal data. If the data controller considers necessary it, it will contact the national authority dedicated to the personal data protection;

f) it activates, under GDPR provisions, the procedures to inform about data breach and in serious cases can also inform the data subjects involved;
g) it defines the data storage procedures for paper documentation stored in the university archives ("Titulus97") with limited and controlled access;
h) before the submission of a research project, the research team consults the DPO in order to guarantee data minimization and to provide procedures in compliance with the GDPR.

Storage, retention and destruction of data: in compliance with EU and national legislation, research data (files containing questionnaire data for statistical analysis, transcripts of interviews and focus groups, transcripts of field observations, photos, minutes, videos, action diaries, etc.) are stored in computers, laptops, intranet directories, hard-drives, cloud storage systems (i.e. Microsoft OneDrive) of the research institutions accessible through institutional password modified periodically (every 3 months in case of storage of sensitive data), and protected by regularly updated antiviruses.
None of the project data will be left inadvertently available by being left on desks or in unlocked rooms.
All the research materials stored in computers are subjected to back up regularly (according to each institutions' regulations) in order to safeguard them from accidental losses.
As a general principle, all materials that could lead to an identification of the person (e.g., informed consent, names/codes list of participants of the longitudinal study) are stored separately from actual data (questionnaires, transcripts, data files, etc.) and handled by different members of the research team.
All the files containing confidential information and personal details of the research participants are stored in University repository, in compliance with CESIA - IT Systems and Services Division security policies.
In particular the data are password protected (see above), accessible only to authorized team members (authorized and controlled by the team or research leader) when they are no more necessary for the research, they are destroyed in according with art. 5 par. 1 letter "e" of GDPR (storage elimination).
The research data are contained on a separate file and do not contain any personal data. Files containing "special categories of personal data (art. 9 GDPR)" will be stored in researchers' laptop, University network folders, cloud systems.
All these resources are managed in compliance with University security policies, regularly subjected to backup procedures, and are accessible only to authorized members of the research teams, protected with University authentication credentials (see above).

Qualtrics, Microsoft forms and a tool developed by Arctur (see 3.2.17) will be used for data gathering. Each project survey will have its own password and username that allows restricted access to researchers.

Online forms (e.g. Qualtrics and/or Microsoft forms) will be used for data gathering. Each project survey will have its own password and username that allows restricted access only to authorized members of the research team.

3.2.2. Agro Paris Tech (APT)

AgroParisTech's IT network comprises inidividual computers linked to servers (including back-up servers) which are maintenance by a dedicated IT team onsite. INRAe uses the AgroParisTech network to link it to the internet and its cloud-working capacity via VPN. The IT team of AgroParisTech integrates a person dedicated to network security and data protection. Individual computers connect to the network via a DHCP connection after a MAC address authorization process. Each user also signs an user chart including security rules.

Access to the individual computers have several security levels: badge access to the site, locked individual offices and session login/password on the computers. Once on the computer all online services of AgroParisTech and INRAe are based on login/password accesses. Computer OS for this study will be Windows 10 using the Windows Defender antivirus with a daily update. The maintenance of the computers are done by two proximity IT persons of the INRAe lab and the IT team of AgroParisTech. Each computer is inventoried in the AgroParisTech GLPI database.

Research data will be stored in individual computers of the researchers in charge (Agnès Lelièvre, APT and Véronique Saint Ges INRAe) and will temporarily available to interns for specific studies on institutional individual computers. Internship contract includes security and confidentiality rules. Access to the data will be negated at the end of the contract. The data might also be stored on the INRAe cloud (access by institutional login) and external hard drives as a back-up kept in secured offices and closets. A weekly back-up will be done during the study. Data will be kept for 7 years thus and will then be anonymised and archived.

The right to access for personal data can be sent by mail with an accompanying identity paper to the researchers in charge or AgroParisTech DPO according to the « Informatique et Libertés » law.

	Création	*Reading*	*Modification*	*Suppression*	*Administration*
Visitor		*x*			
User		*x*	*x*		
Team leader	*x*	*x*	*x*	*x*	
Functional Administrator	*x*	*x*	*x*	*x*	*x*

3.2.3 Commune de Romainville (RMN)

The city of Romainville has a complex security system for its IT infrastructure (servers, personal computers, storage, etc.), involving the whole city staff.
With regards to the Food-e H2020 project, The city of Romainville will conduct activities/studies in the framework of the project, involving human subjects, however the IT infrastructure implements organizational and technical security actions made to secure all data used by its staff:

i) it regularly promotes policies to strengthen personal data protection actions (e.g. city staff can access to resources and data only after the authentication; passwords must be periodically modifies – every six months – on the basis of an identity management system; authorized personnel only can access to resources on the basis of the activities carried out);
j) it promotes security policies through its IT Systems and Services Division (Direction des systèmes d'information - DSI);
k) it realizes, under the GDPR provisions, a data processing register with risk analysis, impact evaluation and organizational and technical tools to protect personal data. If the data controller considers necessary it, it will contact the national authority dedicated to the personal data protection;
l) it activates, under GDPR provisions, the procedures to inform about data breach and in serious cases can also inform the data subjects involved;
m) before creating any personal database, the staff consults the DPO in order to guarantee data minimization and to provide procedures in compliance with the GDPR policy of the city of Romainville.

Storage, retention and destruction of data: in compliance with EU and national legislation, All data (files, emails, photos, minutes, videos, action diaries, etc.) are stored in computers, laptops, intranet directories, hard-drives of the IT infrastructure only accessible through institutional password modified periodically (every 6 months), and protected by regularly updated antiviruses.
None of the project data will be left inadvertently available by being left on desks or in unlocked rooms.
All the data stored in the IT infrastructure are subjected to back up regularly (daily, weekly, monthly) in order to safeguard them from accidental losses.
In particular the data are password protected, accessible only to authorized team members (authorized and controlled by the team or research leader) when they are no more necessary, they are destroyed in according with art. 5 par. 1 letter "e" of GDPR (storage elimination).
All these resources are managed in compliance with city of Romainville security policies, regularly subjected to backup procedures, and are accessible only to authorized members of the staff teams, protected with the city authentication credentials (see above).

3.2.4. FACHHOCHSCHULE SUDWESTFALEN (SWUAS)

Each questionnaire and video recording is marked with a participant ID. The participant ID is assigned by the Department of Agriculture of the University of Applied Sciences Südwestfalen (Fachhochschule Südwestfalen) and consists of letters and numbers that have no relation to the person (i.e. in particular no names, initials or similar). The assignment of the participant ID to the person is listed. The receipt does not contain any information about the participant ID, so that the research data cannot be assigned to your person via the receipt. After the transcripts for all video/interview recordings have been prepared, the list with the assignment of the participant ID to the person is deleted. From this point on, the research data collected for this project will no longer contain any data that directly relate to the person. Nevertheless, persons are of course recognizable through the video recordings. An ano-nymization of the recordings (e.g. by pixelation

of the faces) is not possible for the research project, since the expression of the face is what matters. Scientific publications are made in such a way that it is no longer possible to draw conclusions about individual persons.

3.2.5. INSTITUT FUR LANDES- UND STADTENTWICKLUNGSFORSCHUNG gGMBH (ILS)

In Germany the processing of personal data is regulated by the General Data Protection Regulation (GDPR). The GDPR is completed by the Federal Data Protection Act (BDSG) as of 25 May 2018 and the Data Protection Acts in all German Federal States in order to ensure the protection of the fundamental right to informational self-determination.

The North-Rhine Westphalia (NRW) Data Protection (of 25 May 2018) builds the regulatory framework for the processing of data by ILS. Especially paragraph 17 regulates the processing of data for scientific purposes with regard to requirements for collection, processing, transfer and publication of data. In addition, the ILS has its own "Data Security Concept" as of 01/2019. ILS gGmbH takes appropriate technical and organisational measures to ensure compliance with the obligations under data protection law in accordance with Art. 32 DSGVO.

These are:
Access control. These are measures that are suitable to prevent data processing systems from being used by unauthorised persons.
Measures taken:
-Access to the server is only possible with a key.
- Firewall installed, managed by an external IT service partner , firewall rules are documented.
In case of more than 15 minutes of inactivity, access is automatically blocked on the workstations.
- Access is only granted individually, administrator rights are limited to the most necessary.

Protection against unauthorized reading, modification and deletion, measures to ensure that those authorised to use a data processing system can only access the data subject to their access authorisation and that personal data cannot be read, copied, modified or removed without authorisation during processing, use and after storage.

Measures taken:
- There is an authorization concept that regulates the creation, modification and deletion of user profiles. The administration of rights is carried out by obligated system administrators
The ILS itself does not log firewall accesses, an external IT service partner from Münster, who manages the ILS firewall, logs them. The log data has not been checked/controlled in the past.

Transfer control, measures to ensure that personal data cannot be read, copied, changed or removed by unauthorized persons during electronic transmission or during its transport or storage on data carriers, and that it is possible to check and determine to which locations personal data is to be transferred by data transfer equipment.

- Data is only transmitted in encrypted form (SSL or VPN)

Availability control, measures to ensure that personal data are protected against accidental destruction or loss

Measures taken:
There is a data backup concept, but the backed up data is not encrypted
The recoverability of the backups is tested once a week. The result of the backups or their successful execution is constantly monitored.

Organization within the company

There is a data protection concept with guidelines for the handling of hardware and software by employees, rights of users to information, regulations for order processing and the behaviour in the event of data breaches. The employees have been trained and are obliged to maintain data secrecy.

3.2.6 NOLDE ERWIN (NOL)

The engineering office Nolde & Partner has 2 employees of which only the managing director Dipl.-Ing. Erwin Nolde has access to the project files for the project "FoodE". All project data is saved daily on a separate server and can be quickly restored after physical or technical incidents. The data backup is checked at regular intervals for proper functioning.
The company server can only be accessed from outside via a Virtual Private Network, for which there are only two access points. The passwords are changed every six months.

Sensitive documents in paper form, are kept locked.

The measurement data collected for the project are only recorded as a whole and cannot be traced back to individual persons.

We do not carry out surveys on specific groups or individuals.
The collection of personal data is also reduced to the required minimum.
Contact data is only stored locally without using a cloud and is protected against unauthorized access by password authentication.

3.2.7 UNIVERSITA DEGLI STUDI DI NAPOLI FEDERICO II (UNINA)

Università degli Studi di Napoli Federico II has a personal data security system, that involves university staff according to Decreto Rettorale n. 2019/2088 del 29.05.2019 (Regolamento dell'Università degli Studi di Napoli Federico II in materia di trattamento dei dati personali).
Università degli Studi di Napoli Federico II subscribed the archival system UGOV, defining the management, archival, storage rules of administrative papers and digital University's documentation and is the core system on which actions (by design) are implemented to guarantee the protection of personal data.
Personal data protection in the framework of research projects are implemented by Università degli Studi di Napoli Federico II through security actions, such as use of ID based access to on line stored resources limited to quthorized personnel, application of security policies under CSI (Centro servizi informatici) control, availability of institutional data storage tools (One Drive), etc.

Storage, retention and destruction of data: in compliance with EU and national legislation, research data (files containing questionnaire data for statistical analysis, transcripts of interviews and focus

groups, transcripts of field observations, photos, minutes, videos, action diaries, etc.) are stored in computers, laptops, intranet directories, hard-drives, cloud storage systems (i.e. Microsoft OneDrive) of the research institutions accessible through institutional password modified periodically (every 3 months in case of storage of sensitive data), and protected by regularly updated antiviruses.

None of the project data will be left inadvertently available by being left on desks or in unlocked rooms.

All the research materials stored in computers are subjected to back up regularly (according to each institutions' regulations) in order to safeguard them from accidental losses.

As a general principle, all materials that could lead to an identification of the person (e.g., informed consent, names/codes list of participants of the longitudinal study) are stored separately from actual data (questionnaires, transcripts, data files, etc.) and handled by different members of the research team.

All data are password protected accessible only to authorized team members (authorized and controlled by the team or research leader) when they are no more necessary for the research, they are destroyed in according with art. 5 par. 1 letter "e" of GDPR.

The research data are contained on a separate file and do not contain any personal data. Files containing "special categories of personal data (art. 9 GDPR)" will be stored in researchers' laptop, University network folders, cloud systems.

All these resources are managed in compliance with University security policies, regularly subjected to backup procedures, and are accessible only to authorized members of the research teams, protected with University authentication credentials (see above).

3.2.8 HAGUE CORPORATE AFFAIRS BV (HCA)

With regards to personal data protection in the framework of research projects, Hague Corporate Affairs (HCA) and its linked third party Hague Belgium BVBA (Hague BE) implement organisational and technical security actions. Concretely, they:

- undertake an analysis of the risks presented by data processing and assesses the appropriate level of security to put in place;
- have established and implement an information security policy;
- regularly review the information security policies and, where necessary, improve it;
- apply pseudonymisation where it is appropriate to do so;
- have the capacity to restore access to personal data in the event of any incidents. The organisations work with a cloud (e.g. Dropbox, Office 365) and have an established backup process to ensure data safety and availability.

The personal data collected and processed within the project (photos, minutes, videos, stakeholder mappings, etc.) are stored in computers, laptops, intranet directories, hard-drives, cloud storage systems (i.e. Dropbox, Office 365) of the organisations accessible through passwords. Only authorised personnel can access the project-related data, based on the activities carried out.

3.2.9 GEMEENTE LANSINGERLAND (LAN)

The Lansingerland municipality sees the protection of personal data as a matter of good governance. The aim is to securely exchange and share personal data when this is desirable, useful and necessary. Residents and employees must be able to trust that personal data will be processed lawfully, carefully and securely. The Municipal Executive creates the conditions for a privacy-conscious organizational culture and pursues an adequate privacy policy in that context. We are transparent about our data processing and the way we protect personal data. In dilemmas with regard to the processing of personal data, we enter into a dialogue with those involved and, where possible, seek solutions together. Within the Municipality of Lansingerland, the Commission is ultimately responsible for the careful and responsible handling of personal data entrusted to the organization by citizens, employees and third parties. The following principles apply:

Board of Mayor & Aldermen (BM&A)
1) The BM&A provides a team of professionals who support the BM&A and the process owners ((the team managers) in privacy policy.
2) The BM&A facilitates privacy awareness and training for all employees.
3) The Municipality of Lansingerland has mechanisms for privacy incident management.
4) The Municipal Executive keeps a register of data processing that takes place under its responsibility as referred to in Article 30 of the General Data Protection Regulation (GDPR).
5) The Commission is responsible for compliance with privacy legislation and pursues a proactive privacy policy that fits within this policy framework.
6) The Municipal Executive will include the subject of Privacy and Information Security in the planning and control cycle of the Municipality of Lansingerland.
7) The Municipal Executive can provide explanations (social and legal) about privacy policy and management measures and therefore provides good documentation.
8) The Municipal Executive ensures that the information security of the Municipality of Lansingerland is organized in accordance with the applicable standard and uses the oath of office and, where necessary (ie if it concerns high-risk information), other confidentiality regulations that must be signed by employees. .
9) The Municipal Executive informs the Council about privacy policy.
10) The Municipal Executive has appointed a DPO that supervises compliance with privacy legislation.
11) The Commission evaluates the topicality and effectiveness of this policy framework every two years.

Scope
This privacy policy framework has the following scope:
• The Privacy Policy Framework of the Municipality of Lansingerland applies to all business operations of the Municipality of Lansingerland insofar as it uses personal data and the municipality has control over this.
• The Privacy Policy Framework Municipality of Lansingerland contains generic privacy principles

for the processing operations carried out by the municipality. The privacy policy framework is the stepping stone for the design of process-related privacy policy, which is elaborated in process plans. In addition, it provides principles for municipal-wide regulations such as a procedure for facilitating privacy rights.

• The privacy policy of the Municipality of Lansingerland includes both business processes and the underlying facilities for information processing and data storage. Paper or digital information processing makes no difference.

• The council is responsible for the functioning of the registry. The Registry also processes personal data, for example in incoming letters addressed to the Council. This Privacy Policy Framework therefore also applies to the Registry. In this context, the registrar can be regarded as a process owner.

• The privacy policy of the Municipality of Lansingerland applies to processes that the municipality outsources, purchases or otherwise organizes, such as participation in a legal entity that provides information services for the Municipality of Lansingerland.

• The privacy policy of the Municipality of Lansingerland applies to data exchange with third parties such as the Tax Authorities, the Council for Child Protection, the police and healthcare providers.

• The privacy policy covers the entire "data life cycle": from the generation or collection of data, its daily use and data storage through to its archiving and destruction.

• The privacy policy applies to the processing of statistical and / or anonymised data, insofar as it cannot be excluded that persons can be identified or profiled.

• The privacy policy applies to information security issues.

Privacy compliance

Lansingerland Municipality is aware of the social responsibility associated with the processing of personal data. For this reason:

• the Municipality of Lansingerland pursues a proactive privacy policy based on this privacy policy framework;

• the Municipality of Lansingerland facilitates the exercise of individuals' rights;

• The Municipality of Lansingerland monitors the proper compliance with laws and regulations in the field of privacy protection.

Necessary data processing

Process owners process personal data only for specified purposes that have a legal basis in law, insofar as this falls within their mandate and is necessary or desired. Depending on the situation, there may be different bases of data processing:

1. the performance of public duties;
2. the fulfillment of legal obligations;
3. safeguarding of vital interests for the person (s) involved;
4. the formation or implementation of an agreement to which a data subject is a party;
5. the representation of a legitimate interest of the Municipality of Lansingerland or a third party to whom data are provided, unless the right to the protection of privacy prevails.

Process owners
Process owners provide appropriate organizational and technical solutions to ensure the legality, proportionality, accuracy, security of data processing ("privacy safeguards") and document those measures in process plans.
The privacy officer will keep a "Article 30 register" (see §4.4) of the data processing that falls under the ultimate responsibility of the Commission. Process owners help to keep the registry complete and up-to-date through "Article 30 forms," which provide the required attributes for the registry and update as necessary. The Municipal Executive is transparent about business operations, data processing and privacy policy and facilitates the exercise of rights by persons about whom the municipality processes data. Process owners cooperate in this by making the necessary data that they process according to existing procedures available. The Commission and process owners promote the importance of privacy policy and set a good example themselves. They make privacy negotiable. In dilemmas, they enter into a dialogue with target groups about whom information is processed.

Content of the process plan
Each process owner is responsible for drawing up process plans for the data processing that takes place. The following topics are documented in a process plan:
1) Privacy analysis / PIA report
2) Concrete privacy management measures
3) Critical Performance Indicators (KPIs)
4) (possibly) FG statement
4.1.1 Design of the process plan

A process plan is based on an initial risk assessment, followed by a privacy analysis or PIA (Privacy Impact Assessment). The privacy analysis or PIA is instrumental in determining appropriate control measures. The extent to which and the way in which business processes and data processing require attention are related to the results of the privacy analysis or PIA.
In order to provide a complete picture, the Municipality of Lansingerland uses a system in which both potential personal impact on those involved and potential administrative impact on the organization are estimated. The higher the estimated impact, the more robust the control measures (privacy guarantees). These scores are determined on the basis of the matrix shown opposite. Process owners follow the advice of PIT when determining their risk score.

Design of the process plan
A process plan is based on an initial risk assessment, followed by a privacy analysis or PIA (Privacy Impact Assessment).The privacy analysis or PIA is instrumental in determining appropriate control measures. The extent to which and the way in which business processes and data processing require attention are related to the results of the privacy analysis or PIA. In order to provide a complete picture, the Municipality of Lansingerland uses a system in which both potential personal impact on those involved and potential administrative impact on the organization are estimated. The higher the estimated impact, the more robust the control measures (privacy

guarantees). These scores are determined on the basis of the matrix shown opposite. Process owners follow the advice of PIT when determining their risk score. PIA reports are drawn up in accordance with Article 35 (7) GDPR, which means that the following aspects are documented:

a) A systematic description of the intended processing operations and the processing purposes (formulate categories of data subjects and categories of personal data in Annex 1);
b) An assessment of the necessity and proportionality of the processing operations with regard to the purposes;
c) An assessment of the risks to the rights and freedoms of data subjects;
d) The measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with privacy laws.

Process owners record in their process plans how they provide appropriate organizational and technical privacy protection measures in a practical way - avoiding the following errors as much as possible:
1. Illegal / unlawful data processing: use, storage or exchange of information is prohibited by law (by direct prohibition or limitation of permitted use).
2. Disproportionate data processing: use, storage or exchange of information is (a) inadequate or excessive or (b) the organizational interest in data processing is disproportionately small while the impact on individuals may be disproportionately detrimental.
3. Irrelevant data processing: the information used, stored or exchanged serves no business purpose, is irrelevant or outdated.
4. Inaccurate data processing: the information used, stored or exchanged is not an accurate representation of reality.
5. Unsafe data processing: the used, stored or exchanged information threatens to be too easily accessible to unauthorized persons, to be manipulated or to be unavailable.
6. Failure to observe special legal requirements: formal obligations are neglected when using, storing or exchanging information.
7. Unsupervised data processing: the process owner fails to check whether the privacy-safeguarding measures have actually been implemented or to evaluate the extent to which his process plan needs adjustment.

Generic solutions are sufficient for A1 processes. As long as a process is qualified as A1, less attention is required. To inform process owners, PIT publishes a list of A1 processes. Reality should be consistent with the process plan. Changes in business operations necessitate adjustment of process plans, which may require another PIA.

3.2.10 STICHTING WAGENINGEN RESEARCH (WR)

On this issue, Stichting Wageningen Research (WR) refers to the public “Policy document on the processing of Personal data at Wageningen University & Research”, available at: https://www.wur.nl/upload_mm/7/1/6/d773c3d6-ba4f-4a52-8346 9376376cf53a_Regulations%20for%20the%20protection%20of%20personal%20data%20WUR.pdf

The processing of personal data includes appropriate security measures. WUR's starting point is NEN-EN-ISO/IEC 27002:2017 to make sure that personal data is optimally secured. In our security policy you can read more about the type of measures we take (https://www.wur.nl/nl/Waardecreatie-Samenwerking/Informatiebeveiliging.htm)

3.2.11 ASOCIATIA MAI BINE (MBI)

Organizational and technical security actions: Given the small size of our organisation and the relative small amount of data that we collect and process we use an encrypted Wi-Fi Network updated to the latest firmware for our Internet connection in our office. We use a paid account on Gsuite by Google as our mailling server.

Storage, retention and destruction of data: in compliance with EU and national legislation, research data (files containing questionnaire data for statistical analysis, transcripts of interviews and focus groups, photos, minutes, videos, etc.) are stored in laptops, hard-drives, cloud storage systems (Google Drive – paid account) of the organization accessible through passwords modified periodically (every 6 months), and protected by regularly updated antiviruses.
None of the project data will be left inadvertently available by being left on desks or in unlocked rooms.
We use Google Forms for the gathering of data of surveys with respect to the GDPR regulations.
We back up all of our data on a regular basis on password encrypted portable hard drives accessible only to authorized team members.

3.2.12 ARCTUR RACUNALNISKI INZENIRING DOO (ARC)

Arctur Računalniški inženiring has always carefully addressed the matter of correct processing of personal data. The protection of personal data processed by Arctur is an ethical priority, before a regulatory obligation; that personal data shall be »processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency'); ...« (General Data Protection Regulation EU 2016/679, Article 5(1)).

The personal data we collect on the basis of user/partner explicit consent is stored in an electronic or physical database of personal data (depending on the form of the acquired personal data) that are adequately insured and accessible only to authorized employees of Arctur d.o.o. The personal information provided to us is stored only within the European Union and is not transmitted to third countries or international organizations. Collected personal data may be kept in a personal data collection until there is a legitimate basis, until user/partner consent is revoked in the processing of personal data, the fulfilment of a contractual obligation, or for as long as is necessary to achieve the purpose for which they are processed or meet legal requirements.

The Arctur privacy organizational model provides that each Arctur employee processes only the data necessary to offer the requested service, according to the internal organization and above all the purposes indicated and proposed to the interested party. Therefore, for this purpose, Data Protection Officer with reference to the individual service, has appointed each collaborator of the company as "processor", binding him to a specific area of treatment. To this end, by design, the company information system is also made up of "watertight compartments". The collaborator can

access from his computer station only the data necessary to perform his duties. Together with the appointment, each subject receives an internal regulation on the use of IT tools and rules of conduct, including ethical ones, on all information that the collaborator accesses by virtue of his specific job. To implement the information security that each collaborator processes, Arctur provides training and updating courses on the processing of personal data to its assigned collaborators.

Arctur gained a system certification ISO/IEC 27001:2013- System certificate SI20/30223176, valid from 14 April 2020 until 13 April 2023.

- **IT security guarantees provided by Arctur**

The analysis on IT risks and on corporate hardware and software infrastructures and IT adaptation measures was carried out by our System Administrators with specific tools and check lists. The results of the investigation allowed our technicians to further improve the protection measures against cyber-attacks and cyber threats, gradually and proportionally to the risk for the rights and freedoms concerned. Arctur guarantees the maximum reliability and security of its systems, here are some of the characteristics related to IT security:

- Arctur data center is designed, built and managed to offer our customers maximum security and best performance;
- The data center is located within our headquarters on Slovenian territory;
- Data center is configured in such a way to offer load balancing, fault tolerance and backup functions of the most critical systems;
- Diesel generator is able to intervene in support of the UPSes, to guarantee the power supply to the data center and all of its services even if the power supply from the grid is interrupted;
- The electrical emergency systems (generators) are located outside the datacenter and offices. The support UPSes are located in a room separate from the server room and are separated by fire walls;
- Data carriers (three different ISPs) reach the data centers from three physically distinct optical lines. Each data line that allows the connection to the Internet is configured in fault tolerance with the others, for an automatic mutual intervention if one of the ISPs no longer provides the service;
- Each site is equipped with an external video surveillance system and alarm system. Access is possible only with badge and access code;
- The server rooms are also delimited by a perimeter defence system and physical access is allowed only to people with authorized badges;
- Each data room is equipped with a redundant conditioning system which guarantees its cooling and the correct temperature in all conditions. The air conditioning systems are equipped with free cooling to allow maximum energy and wear savings of the systems during the colder months;
- Data center is equipped with a series of sensors that detect its temperature, humidity, the presence of smoke and all these sensors are connected to an operational center (NOC);
- A video surveillance system controls both access and operation within the rooms;

- **Outputs developed within the project**

Arctur´s role in the FoodE project is to provide ICT support on all tasks, especially on T3.2: FoodE App and T7.1.4. The FoodE interactive website.

1. FoodE App

The main structure of the FoodE App is described in section 1.3.5 Project methodology.

- FoodE requires strict adherence to the protocols of data transfer safety and data integrity, personal data protection, access control, as well as compliance with legislation on EU and national levels. Arctur will develop novel application, its content will be provided by all partners. The implementation of the FoodE App will allow for easy accessibility and immediate interaction from users.
- Data Protection and compliance with national/EU legislation: Ethical standards and guidelines of Horizon 2020 will be rigorously applied. The use and transfer of participant data is covered by the EU *General Data Protection Regulation 2016/679* (GDPR), which ensures the protection of individuals.
- Data Standards: All incoming data will include metadata to enable cross-searching, etc. If (research) data is made available externally, we will comply with a standard used by Open Access data repositories.
- Privacy, dealing with sensitive data and guarantee compliance with *GDPR*. This will be ensured through strict monitoring of every user and administrative action. Every user will have the possibility to learn how her/his data is used.
- Data used for analytic purposes will be immediately anonymised and copied to separate storage, where necessary.
- App development and hosting: The app will be based on a modern data architecture hosted at a data centre held by Arctur. Proper governance and data stewardship carried out by Arctur personnel will enable data self-provision according to *GDPR* and *ISO/IEC 27001:2013*. The App will support full *GDPR* compliance through tracing of data access, manipulation and sharing with appropriate consent, secure storage and encryption mechanisms. Applications and external services will access data and information via rich and secure API interfaces tailored to their specific needs. We will explore, develop and include in the app various technological services, if viable.
- Data security: all data provided in app will be stored in Arctur data centre.

2. 4PM system (internal partner area)

Arctur provided its own project management tool, called 4PM. Tool is fully developed and licensed by Arctur. All partners will get credentials to enter this tool (data collected: partner´s email, name, surname, organisation name), password is created automatically and changed by system. The tool will provide documents repository and partner communication. Arctur will not process or analyse any (personal) data provided within 4PM. Exporting personal data from an application is done only on user/partner request as a system file (SQL, CSV ...). According agreement with FoodE coordinator,

data saved in 4PM will be stored and archived for 5 years (till 28. February 2025), after data will be deleted.

- For the implementation of remote user assistance, which is accessible from 4PM and on the website, we use the ISL Pronto system. When establishing a claim, the following personal information is collected in ISL Pronto: name, e-mail, location, IP address, conversation transcript.
- Log-in to 4PM: 4PM does not store users' user passwords. All passwords must be safe enough. The password must be complex enough: it consists of at least 8 characters and contains at least one large printed letter and at least one number.
- Registration of new users: Insights and access to data can be individually tailored. User group settings allow your administrators to customize their new users. User access is activated by the application administrator, which ensures that new users have the appropriate level of access to the data.
- User management and access control: Administrators have the ability to manage the rights of users to view and process personal data on three levels:

application (user groups)
projects (project applications)
groups of projects (project rights).

- Information security and compliance:

4PM is a cloud-based service (SaaS), hosted on Arctur's server infrastructure in the EU. With a number of security mechanisms, access control and technical solutions, data security is ensured.

- Organizational security:

protected premises, equipment and system software,
prevention from unauthorized access to the space where the technical equipment is located,
fire protection and counter-safety protection of technical equipment,
adequacy of the space in which the technical equipment is located,
regular reviews the operation of the technical equipment

- Technical security:

the implementation of the control of physical access and access to data located on technical equipment,
locking the rooms where the equipment is located,
preventing access to personal data located on technical equipment of premises maintenance, customers and other visitors,
preventing the use of passwords to people who have not been directly assigned a password or for a purpose not specified in this agreement.

- *ISO 9001: 2008* - Quality management system:

Security of user organization's data is a top priority in 4PM. State-of-the-art technologies, based on the security protocol SSL (Secure Socket Layer), protect user privacy and ensure that all user information, documents, and data is kept confidential.
Security mechanisms ensure that only authorized users from your organization can access information and data.
Each 4PM installation has its own virtual server, thereby eliminating the possibility of others gaining access to user data.

3. FoodE website

The website will be developed by May 2020 and will be constantly updated by Arctur, HCA and the project partners. It will also integrate the FoodE app. Arctur, as website ICT operator, does not process the collected information separately, nor does it connect this information to any other data.

- **Duration:** Data, collected through surveys, will be saved for one more year after project ends. All other data, uploaded on page, will be saved so long content is available online.
- **Personal data:** Arctur, as responsible for the maintenance and hosting of the FoodE website, will not process any personal data, nor will provide or sell personal data to any other subject. The data subject may request access to, revision or deletion of or a restriction processing of all related personal data, or object to personal data processing and the right to transfer data. Data subject's request shall be examined pursuant to provisions of the *GDPR*.
- **Cookie management:** On the FoodE website, notice about cookies settings will be displayed (website contains cookies and information about each cookie). Every user will have the choice to accept or refuse cookies. Data, gathered via cookies will be available in the system for 7-30 days, after are deleted permanently. Arctur will not process or analyse any data, collected via cookies.
- **CMS management:** Each webpage content administrator (Arctur, HCA, HAGUE BE Team) will be provided with unique user name and password.
- **Content:** All content on the website will be provided by all FoodE partners, who have to fully respect intellectual property rights. All visual materials provided by partners (photos, videos) have to be named accordingly to naming convention (in case partners provide own materials). Arctur is not responsible for copyrights and intellectual property for materials, provided by partners.
- **Survey and database management:** Partners, who will develop and manage surveys, which will appear on FoodE website domain: *foode.eu/survey*, will be provided with unique user name and password. Data, collected within survey will be stored in Arctur data centre till project ends (Feb 2024).

3.2.13 AJUNTAMENT DE SABADELL (SBD)

Sabadell City Council has appointed a data protection delegate, in accordance with the provisions of article 37.1.a. of the General Data Protection Regulation (EU) (2016/679) and Articles 34 and 36 of Organic Law 3/2018 on the protection of personal data and the guarantee of digital rights.

The contact email address of the Data Protection Officer is: dpd@ajsabadell.cat
Antivirus, and firewalls: Sabadell City Council has specific antivirus and firewall in order to proctect the inside network.
Backups: It will be done daily with the same access system.
Password policy: all authorizhed people access by the personal City Council username (provided by the Sabadell City Council) and password. City Council has specific rules for periods of mandatory modification of passwords and structure.

List of authorized persons: there is a list of authorized persons to access the information for each case and the scope of the authorization.
Security breaches: in the event of any incident that could jeopardize the security of the data, it must be recorded (record of security breaches) and reported to the data protection officer.
Rights protection: To exercise these rights, the interested party may contact Sabadell City Council by sending their application to the address of Sabadell City Council at Plaça Sant Roc 1, 08201 Sabadell (Barcelona), or delivering the forms completed with the corresponding documentation required at any Citizen Service Office or through the Sabadell City Council's procedures.

3.2.14 UNIVERSIDAD DE LA LAGUNA (ULL)

University of La Laguna has a complex security system for its IT infrastructure (server, personal computer, storage cloud etc.), managed by the STIC (Information and Communication Technology Service, https://www.ull.es/servicios/stic/)
Some key elements in the ethical advisory and data protection requirements are the Research Ethics and Animal Welfare Committee of the University of La Laguna (CEIBA, fully developed in this regulation: https://bit.ly/3c0GNHq) and the Data Protection Officer, the person who contributes to promoting adequate compliance with the General Data Protection Regulations at the University of La Laguna (https://www.ull.es/servicios/dpd/). To this end, the regulation attributes the following functions the Data Protection Officer: to inform and advise on the obligations deriving from the Regulation and from national legislation; to supervise compliance with the regulations and specific policies on data protection; to offer the advice requested on the impact assessment relating to data protection and to supervise its application and to cooperate and act as a contact point with the control authority (the Spanish Data Protection Agency). The data protection delegate is at the service of the university community, -administrative staff, students and research-teaching staff-, and of all persons related to the University of La Laguna, as an instrument and support for the adequate guarantee of the fundamental right to data protection.
With regards to personal data protection in the framework of research projects the University of La Laguna implements organizational and technical security actions:

n) it organizes training courses for administrative staff and research teams (https://bit.ly/2XsvNNR). Some training workshops involve researchers in the wider framework of research integrity. These workshops are certified by the University;
o) it promotes policies to strengthen personal data protection actions (e.g. university staff can access to online resources only after the authentication; passwords must be integrated on an identity management system; authorized personnel only can access to online resources on the basis of the activities carried out);
p) it promotes security policies through its Information and Communication Technology Service (https://www.ull.es/servicios/stic/),
q) it provides research teams with IT tools for the data processing and storage. Research teams, for example, can access to university data storage tool in cloud (OneDrive, Google Drive) using the institutional password;
r) it realizes, under the GDPR provisions, a Data Processing Activities Register. This register is an inventory of all processing of personal data managed by the University, and serves to organize

from it the organizational and technical measures to ensure the data, provide the rights of their owners, and generally comply with the RGPD and other applicable regulations. Being on the register means that the processing is duly controlled by the persons responsible for the organization.

s) it activates, under GDPR provisions, the procedures to inform about data breach and in serious cases can also inform the data subjects involved;
t) before the submission of a research project, the research team consults the DPD and the Ethics Committee (CEIBA, described previously) to guarantee data minimization and to provide procedures in compliance with the GDPR.

Storage, retention and destruction of data: in compliance with EU and national legislation, research data (files containing questionnaire data for statistical analysis, transcripts of interviews and focus groups, transcripts of field observations, photos, minutes, videos, action diaries, etc.) are stored in computers, laptops, intranet directories, hard-drives, cloud storage systems (i.e. Google Drive of the research institutions accessible through institutional password modified periodically, and protected by regularly updated antiviruses.

None of the project data will be left inadvertently available by being left on desks or in unlocked rooms.

All the research materials stored in computers are subjected to back up regularly (according to each institutions' regulations) in order to safeguard them from accidental losses.

As a general principle, all materials that could lead to an identification of the person (e.g., informed consent, names/codes list of participants of the longitudinal study) are stored separately from actual data (questionnaires, transcripts, data files, etc.) and handled by different members of the research team.

In particular the data are password protected (see above), accessible only to authorized team members (authorized and controlled by the team or research leader) when they are no more necessary for the research, they are destroyed in according with art. 5 par. 1 letter "e" of GDPR (storage elimination).

The research data are contained on a separate file and do not contain any personal data. Files containing "special categories of personal data (art. 9 GDPR)" will be stored encrypted in researchers' laptop, University network folders, cloud systems.

All these resources are managed in compliance with University security policies, regularly subjected to backup procedures, and are accessible only to authorized members of the research teams, protected with University authentication credentials (see above).

Microsoft forms, Google Forms will be used for data gathering. Each project survey will have its own password and username that allows restricted access to authorized members of the research team.

3.2.15 UNIVERSITAT AUTONOMA DE BARCELONA (UAB)

List of authorized personnel: there is a list of persons authorized to access the information, as well as the scope of this authorization.

Password policy: all people access by the university username (provided by the university) and password. University has specific rules for periods of mandatory modification of passwords and structure.

Antivirus, and firewalls: university has specific antivirus and firewall in order to proctect the inside network.
Backups: will be made on the university's Onedrive with the same access system
Security breaches: in the event of any incident that could jeopardize the security of the data, it must be recorded (record of security breaches) and reported to the data protection officer. It should be noted that, depending on the severity of the incident, the RGPD requires that it be communicated to the supervisory authority within a maximum of 72 hours.
The university has a procedure for reporting security incidents to the DPO.

3.2.16 NABOLAGSHAGER AS (NBL AS)

Nabolagshager AS has appointed Adam Curtis as their Data Proteciton Officer in the FoodE project. The organisation is currently using the Google Drive to store data with password protection on both Google Drive on the physical devices on which the data is accessed. Devices are installed with antivirus software. Staff are instructed to lock their devices when they step away from their desk. Only members of the staff working directly on the FoodE project have access to these files. Data that could lead to an identification of the person (e.g., informed consent, names/codes list of participants of the longitudinal study) will be stored separately from actual data (questionnaires, transcripts, data files, etc.).

3.3 Transfer to and from non EU-countries

EU data protection rules apply to the European Economic Area, which includes all EU countries and non-EU countries Iceland, Liechtenstein and Norway. When personal data is transferred outside the European Economic Area, special safeguards are foreseen to ensure that the protection travels with the data. These safeguards are defined by the Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation - GDPR).

GDPR applies also for partners based outside the European Union if data are collected in the European Union. It applies also to the case in which data are collected by a subject based in the European Union who transfer them to extra-EU third parties (see Chapter 5 “Transfers of personal data to third countries or international organizations” of the GDPR).

3.4 Further processing of previously collected personal data

The research project foresees the possibility to re-use data collected in research projects in similar scientific disciplines, pursuant to Recital 50 of the GDPR, which states that the processing of personal data for purposes other than those for which the personal data were initially collected is allowed where the processing is compatible with the purposes for which the personal data were initially collected, and that, in such a case, no legal basis separate from that which allowed the collection of the personal data is required. In any case, data subjects received specific information in the context of the past scientific research from which such data will be collected.