FUDGE-5G

FUlly DisinteGrated private nEtworks
for 5G verticals

Deliverable 6.3

GDPR Handbook

Version 1
Work Package 6

Main authors	João Henriques, António Borges, Luís Rosa, André Gomes, Luís Cordeiro
Distribution	Internal
Delivery date	31 August 2021 (M12)
Delivered date	31 August 2021 (M12)

Partners

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957242

Disclaimer

Project details

Project title: FUlly DisinteGrated private nEtworks for 5G verticals
Acronym: FUDGE-5G
Start date: September 2020
Duration: 30 months
Call: ICT-42-2020 Innovation Action

For more information

Project Coordinator
Prof. David Gomez-Barquero
Universitat Politecnica de Valencia
iTEAM Research Institute
Camino de Vera s/n
46022 Valencia
Spain

http://fudge-5g.eu
info@fudge-5g.eu

Acknowledgement

FUDGE-5G has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement Nº 957242. The European Union has no responsibility for the content of this document.

Abstract

The present document covers the underlying issues related to the GDPR Handbook, in the scope of the FUDGE-5G project, and provides practical guidelines for members of the project to manage personal data in a compliant manner. This handbook gathers the best practices according to the requirements of the General Data Protection Regulation (GDPR) and individual rights to attain. It also includes the best practices on processing personal data providing a practical approach to comply with data privacy regulations aligned to the requirements of the GDPR. This deliverable also includes the templates of the consent forms and the ethical and legal frameworks to be used throughout the project.

Versioning and contributions

Versioning

#	Description	Contributors
0.1	First Release	ONE
1.0	Submitted Version	ONE, O2M

Contributors

Partner	Authors
ONE	João Henriques, António Borges, Luís Rosa, André Gomes, Luís Cordeiro, Paulo Simões
O2M	Peter Sanders

Reviewers

Reviewer	Partner
Peter Sanders	O2M
Paulo Simões	ONE

Abbreviations

BCRs	Binding Corporate Rules
CoC	Codes of Conduct
DMP	Data Management Plan
DPO	Data Protection Officer
EU	Europe Union
ePD	ePrivacy Directive
GDPR	General Data Protection Regulation

Executive Summary

The present document covers the underlying issues related to the GDPR Handbook, in the scope of the FUDGE-5G project, and provides practical guidelines for members of the project to manage personal data in a compliant manner. This handbook gathers the best practices according to the requirements of the General Data Protection Regulation (GDPR) and individual rights to attain. It also includes the best practices on processing personal data, providing a practical approach for consortium members to comply with data privacy regulations aligned to the requirements of the GDPR. This deliverable also includes the templates of the consent forms and the ethical and legal frameworks to be used throughout the project.

This deliverable starts by presenting an overview of the domain and introduces key definitions, such as data privacy, personal data, processing, data controller, data processor, accountability, and liability.

Principles providing guidance for FUDGE-5G for data processing activities are addressed, such as lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality and accountability.

This deliverable also presents a roadmap with the steps to follow, aiming to contribute with the best practices to be undertaken by FUDGE-5G, to implement an effective data privacy programme.

Finally, the GDPR Handbook discusses the operational key activities in terms of data protection procedures to be performed by FUDGE-5G partners. Those steps include team member's administration, datasets administration, communications, supporting platforms, remote work, cookie compliance, research, third-party data, data encryption, privacy and code of conduct.

Table of contents

Disclaimer 2

Abstract 3

Versioning and contributions 4

Versioning 4

Contributors 4

Reviewers 4

Abbreviations 5

Executive Summary 6

Table of contents 7

Table of figures 10

Table of tables 10

1. Introduction 11

1.1. GDPR Overview 11

1.2. ePrivacy Directive 12

1.3. Key Concepts 12

1.3.1. Data Privacy 12

1.3.2. Personal Data 12

1.3.3. Processing 13

1.3.4. Data Controller 13

1.3.5. Data Processor 13

1.3.6. Data Sub-Processor 13

1.3.7. Organization 14

1.3.8. Accountability and Liability 14

1.3.9. Fines 14

1.3.10. Data Protection Officer 15

1.3.11. Privacy Notice 15

1.4. Structure of the Document 15

2. Individual's Rights 16

3. Data Processing Principles 18

3.1. Lawfulness, Fairness and Transparency 18

3.2. Purpose Limitation 18
3.3. Data Minimisation 18
3.4. Accuracy 18
3.5. Storage limitation 18
3.6. Integrity and Confidentiality 19
3.7. Accountability 19
4. Data Privacy Programme 20
4.1. Appoint a Data Protection Officer (DPO) 20
4.2. Maintain a personal data register 21
4.3. Notify purpose and seek consent 21
4.4. Response to individuals requesting information about their personal data 22
4.5. Enforce security mechanisms 23
4.6. Embed data privacy into systems, processes and services 24
4.7. Data breaches notification 24
4.8. Management of third parties 25
4.9. Personal data protection when transferring overseas 26
4.10. Communicate data protection policies, practices and processes 27
5. Key activities and data protection procedures 28
5.1. Team members administration 28
5.2. Administration of datasets 28
5.3. Data Processing for Deliverables and Reports 29
5.4. Communications 29
5.5. Supporting platforms 29
5.6. Remote work 29
5.7. Cookie compliance 30
5.8. Research 30
5.9. Subcontracts 30
5.10. Third-party data 31
5.11. Data encryption 31
5.12. Privacy 31
5.13. Code of Conduct 31
6. References 32
Annex A: Informed Consent Template for FUDGE-5G Trials 33
Annex B: General Informed Consent Template 35

Annex C: Data Processing Agreement Template 39
Annex D: Template for Website Data Privacy Policy 45
Annex E: Code of Conduct 50

Table of figures

FIGURE 1 - DATA MANAGEMENT METHODOLOGY 28

Table of tables

TABLE 2 – INDIVIDUAL RIGHTS 16
TABLE 1 – FUDGE-5G DPOS 20
TABLE 3 – PERSONAL DATA PROTECTION MECHANISMS WHEN TRANSFERRING OVERSEAS 26

1. Introduction

The purpose of this handbook is to provide practical guidelines for members of the project so they can manage personal data in a compliant manner. This document consists of a "GDPR Handbook" (Deliverable D6.3) to help FUDGE-5G in the preparation of the trials and to be gradually updated during the project's lifetime, according to new findings and new requirements discovered along the project. This handbook gathers the best practices according to the General Data Protection Regulation (GDPR) (EU, 2016) requirements and practices. It also provides guidance in following the best practices on processing personal data, providing a practical approach to comply with data privacy regulations aligned to the requirements of the GDPR. This deliverable also includes the templates of consent forms, as well as ethical and legal frameworks to be used throughout the project.

1.1. GDPR Overview

GDPR (EU, 2016) represents a first step toward giving EU citizens and residents more control over how their data is used by organizations. Any company handling personal data of people in the EU must comply with the GDPR, no matter where it is located. Collecting personal data must be done subject to the EU's GDPR. All data related to an identified or identifiable person (e.g., name, birthdate, email address, telephone number) is considered as personal data.

As of May 25th, 2018, the European Data Protection Regulation is applicable in all MEMBER STATES to harmonize data privacy laws across Europe. Data management activities comprising personal information must comply with the seven principles of the GDPR.

That compliance with the legislation can assume different perspectives, including personal, professional, and reputational (PWC, 2021). The personal perspective corresponds to the personal data to be processed. The professional perspective comprises the compliance with GDPR daily activities for managing the personal data. The reputational perspective refers to the reputation of the project in case of breach of the legislation, which negatively affects credibility and trust (besides possible legal implications).

Data protection regulators may enforce mandatory audits, request access to documentation and evidence, or even mandate that an organization stops processing personal data. Organizations failing to protect personal data or not complying with data privacy regulations aren't just risking financial penalties. Violating people's privacy rights can result in fines of up to 4% of the global revenue or €20 million, whichever is higher. They also risk operational inefficiencies, intervention by regulators and, most important, permanent loss of trust. In terms of reputation, non-compliance with the law may also result in brand damage and loss of trust from consumers, customers and employees.

In this context, FUDGE-5G is “the legal entity which, alone or with others, determines the processing and use of the personal data”. FUDGE-5G consortium members collect and process personal data on behalf of the project. Thus, they must comply with the FUDGE-5G data management plan procedures to protect the privacy rights of individuals, to protect the project's reputation, and to avoid breaching the legislation.

1.2. ePrivacy Directive

The GDPR is complemented by Directive 2002/58/EC on privacy and electronic communications ePrivacy Directive (ePD), amended by Directive 2009/136 (EU, ePrivacy Directive, 2002) (SUPERVISOR, 2021), which concerns the protection of privacy in the electronic communications sector and covers some data not classed as “personal”, such as some communications metadata. As a Directive, it is transposed into EU nations’ laws rather than being imposed in a unified way as regulation *per se*.

1.3. Key Concepts

This section introduces the key definitions, such as data privacy, personal data, processing, data controller, data processor, accountability, and liability.

1.3.1. Data Privacy

Data privacy corresponds to what that people need to know concerning their personal data that organizations are collecting about them and how they are using it (GDPR, 2021).

1.3.2. Personal Data

Personal data comprises any information that can be used to directly or indirectly identify a living person (PWC, 2021). Individuals can be directly identified from data being processed, such as name, address, email address, contact details, or photos. Examples of the data that can directly identify the name or account number or could be a digital identifier such as IP address, username, or location data such as GPS coordinates.

Personal data also refers to the data that can be used for indirectly identifying an individual, for instance from online identifiers, IP addresses or GPS location data. Indirect identification can be achieved by combining different data sets from different sources (e.g., gender, birth date, and license plate number).

Personal data may be classified as sensitive in case of leaking or misusing sensitive personal data may harm individuals, such as in the following cases:

- Political or religious beliefs.
- Racial or ethnic origin.
- Sex life or sexual orientation.
- Physical or mental health.
- Criminal offences and court proceedings.
- Project Membership.

It is important to differentiate personal data from sensitive personal data, since processing sensitive personal data may require additional safeguards. Examples of sensitive personal data include, for instance:

- Voice recording.
- Health records.
- Political affiliations.
- Biometrics.

1.3.3. Processing

Processing refers to the manual and automated operations that can be performed on data, such as collecting, recording, organizing, classifying, storing, modifying, amending, retrieving, using, or revealing such data by broadcasting, publishing, transmitting, making available to others, integrating, blocking, deleting, or destroying.

GDPR recognizes that not all those involved with the processing of personal data have the same responsibilities. Therefore, a distinction is made between Data Controllers and Data Processors.

1.3.4. Data Controller

Data Controllers are the accountable organizations responsible for collecting and controlling data by following data protection principles. They also respond to individuals' rights and enforce security measures and manage data breaches. They take the responsibility of contracting Data Processors and assessing their compliance, by evaluating the guarantees on protecting any data or information the Data Controller or Data Processor may have access to.

1.3.5. Data Processor

Data Processors take the responsibility for processing personal data on behalf of a Data Controller, according to its instructions. They also decide about the information to be collected and take responsibility for recording a justification. As main responsibilities, they should be compliant with Data Controllers' instructions. Such compliance can be enforced with third-party contracts by including security measures and notifying controllers about personal data breaches. Data Processors respond to the Data Controller regarding the compliance of (possible) Data Sub-processors.

1.3.6. Data Sub-Processor

Data sub-processors are those (from another organization) the Data Processor subcontracts and assigns processing activities. Data Sub-processors require previous approval from Data Controllers before being engaged. The responsibilities of Data Sub-processors to the Data Processors and the responsibilities of Data Processors to the Data Controllers are similar. Therefore, a Data Sub-Processor has the same level of responsibility in case of damage

resulting from its processing actions, in case of non-compliance with legal obligations, or even in case of non-compliance with the instructions of the Data Controller.

1.3.7. Organization

In the context of this handbook, the term organization refers to the various entities whose members are performing personal data processing activities. It is important to note that an organization may act as Data Processor in some scenarios and act as Data Controller in other scenarios, according to the specific purpose of processing personal data.

1.3.8. Accountability and Liability

Despite the FUDGE-5G Project having ultimate responsibility in terms of compliance, all consortium members collecting and processing personal data on the project's behalf also need to be aware of their responsibilities under the Data Protection legislation. This Handbook provides guidance to all FUDGE-5G project members, to ensure they are aware of their obligations under the legislation.

In certain circumstances, FUDGE-5G team members can be held individually responsible and liable for breaches of the Data Protection legislation, if a breach has been found in consequence of their direct involvement, negligence, or even as result of their 'connivance'.

The FUDGE-5G project should also advise its members about the appropriate procedures to follow in terms of data acquisition, storage, disclosure, and processing.

1.3.9. Fines

GDPR fines are designed to make non-compliance a costly mistake for both large and small businesses. Each EU country's data protection regulator acts as an authority and administers the GDPR fines. The less severe infringements could result in a fine of up to €10 million, or 2% of the firm's worldwide annual revenue from the preceding financial year, whichever amount is higher. The severity of the penalty will be determined by authorities. The following list contains the criteria an authority may use to determine the amount for fines:

- Gravity and nature.
- Intention.
- Mitigation.
- Precautionary measures.
- History.
- Cooperation with the supervisory authority.
- Data category.
- Notification.
- Certification.
- Aggravating and mitigating factors.

1.3.10. Data Protection Officer

The concept of Data Protection Officer (DPO) is introduced by GDPR as a leadership role for overseeing the organization's data protection programme and ensuring compliance with the applicable laws.

1.3.11. Privacy Notice

A privacy notice corresponds to a public document from an organization, explaining how personal data is processed and how data protection principles are applied. GDPR provides detailed instructions on how to create a privacy notice, placing an emphasis on making them accessible and easy to understand. In the case of collecting data directly from someone, the organization should provide the data subject with the privacy notice.

If FUDGE-5G is directly collecting information from an individual, the following information must be included in its privacy notice:

- The identity and contact details of FUDGE-5G representatives, and its DPO.
- The purpose of processing an individual's personal data and its legal basis.
- The legitimate interests or a third party, if applicable.
- Any recipient or categories of recipients of an individual's data.
- The details regarding any transfer of personal data to a third country and the adopted safeguards.
- The retention period or the criteria used to determine the data retention period.
- The existence of each data subject's rights.
- The right to withdraw consent at any time, in case of being relevant.
- The right to lodge a complaint with a supervisory authority.
- Whether the provision of personal data is part of a statutory or contractual requirement or obligation, and the possible consequences of failing to provide the personal data.
- The (possible) existence of an automated decision-making system, including profiling, and information about how this system has been set up, its significance, and the consequences.

1.4. Structure of the Document

This document is organized as follows. This section presented the purpose of GDPR handbook, a GDPR overview and its key concepts. Section 2 introduces the rights of individuals. Section 3 presents the data processing principles. Section 4 provides the roadmap to be followed to achieve an effective data privacy programme in the project. Finally, Section 5 presents the key activities and data protection procedures.

2.Individual's Rights

The GDPR covers, as part of their objectives, the ownership and control over the individual's personal data. Therefore, individual rights are usually related to the protection of personal data of individuals. Despite this, all those rights are being classified as absolute, even though some of them are applied just in specific circumstances. Those rights are presented in Table 2, presented next.

Table 1 – Individual Rights

Right	Details
Right of access personal data	Individuals have the right to access and request copies of their personal data.
Right to request rectification	Allows individuals to have their personal data rectified (if inaccurate) or completed (if it is incomplete).
Right to request erasure or deletion of data	The right of individuals to request erasure of their personal data, without undue delays. Despite being an absolute right, there are specific circumstances where this right is not mandatory.
Right to impose a restriction on processing	Empowers the individuals to limit personal data processing and introduce restrictions on processing of their data.
Right to data portability	Individuals must be able to receive their personal data in an organized, commonly used machine-readable form.
Right to object to the processing	It is related with automated and mechanical decision-making and profiling. Individuals can object to having those decisions made about them by means of such processing frameworks.

At least one of the following bases should be attained by FUDGE-5G for processing data according to the principle that all personal data be processed lawfully and fairly:

- Consent of the individual to the processing of their personal data.
- Legitimate interest of FUDGE-5G or the third parties engaged.
- When it is needed in order to proceed with a contract.
- Legal obligation exists to process personal data for.
- Under a vital interest for individuals to protect their lives.
- When a public interest exists.

Because different kinds of data require also different levels of protection, different conditions are specified for processing sensitive and personal data. Usually, sensitive data can be processed only in case of explicit consent, unless the data are required for filing legal proceeding or claims, or if there is any legal, public interest or regulatory requirement. For instance, personal data related to convictions and criminal offences can usually only be processed if they are carried out under the control of a certain government authority or in accordance with local laws.

3. Data Processing Principles

Data processing must be performed by following a set of principles, such as lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity, confidentiality and accountability.

3.1. Lawfulness, Fairness and Transparency

Fair, lawfulness and transparency on personal data should always be followed. Therefore, it is expected from the FUDGE-5G project members to obtain and process personal information fairly, with the clear knowledge and awareness of the personal data. The organization should be prepared to explain about their plans related with the data, and they should be able to justify the processing activities in case they are asked.

3.2. Purpose Limitation

Personal data should only be processed for a specified and lawful purpose. In that sense, the FUDGE-5G project members must keep the data only for one or more specified and lawful purposes, avoiding using the data for anything other than these purposes.

3.3. Data Minimisation

Data processing should use the less possible personal data according to effective needs. Thus, project members must only use and disclose data according to agreed purposes of the project, and to the minimum extent necessary to achieve those purposes. Typically, this will include the datasets, correspondence, notifications, and information concerning events and use case demonstrations.

3.4. Accuracy

Personal data should be maintained accurate, up to date and complete. To that aim, the necessary measures should be introduced to update data in case they are inaccurate. Therefore, the project should follow procedures to achieve the high levels of data accuracy and that personal data are kept up-to-date and fit for purpose.

3.5. Storage limitation

Personal data should not be retained beyond the strict time that is required to satisfy the specified purposes in a format that allows the identification of the individuals. After that period of time, data should be anonymized or destroyed in a verifiable, appropriate and secure manner .

3.6. Integrity and Confidentiality

Personal data can be lost, destructed or damaged. To avoid that, security measures should be introduced to ensure unlawful or unauthorised access, disclosure, modification or deletion. The project team members should leverage a continuous process to keep the data safe and secure.

3.7. Accountability

Accountability refers to the appropriate measures and records that should be provide the evidence to demonstrate the compliance with GDPR. It requires, from project members, associated service providers and Data Processors, a culture of compliance supported by evidence of embedded processes, data management protocols and the involved structures in their governance.

4. Data Privacy Programme

The roadmap to be followed by FUDGE-5G to achieve an effective data privacy programme, considering the best practices in the domain (PWC, 2021), entails the following steps:

- Appoint a Data Protection Officer (DPO).
- Maintain a personal data register.
- Notify purpose and seek consent.
- Respond when individuals ask about their personal data.
- Enforce security mechanisms.
- Embed data privacy into your systems, processes, and services.
- Notify data breaches.
- Manage third parties.
- Protect personal data when transferring overseas.
- Communicate data protection policies, practices, and processes.

These steps will be further discussed next.

4.1. Appoint a Data Protection Officer (DPO)

The DPO role can be assigned to an existing employee within the project, or alternatively, someone else can be recruited for that role. The FUDGE-5G DPO role should be assigned to an expert in data protection, enabled with the appropriate resources. The DPO must report to the highest management level. Moreover, the DPO provides assistance in monitoring internal compliance with the applicable data protection laws. He also advises on data protection obligations, providing expert advice when needed, and acting as a point of contact for individuals and data protection authorities.

The DPO main role is to ensure that personal data are processed in compliance with the data protection rules. Table 2 identifies the FUDGE-5G project DPO and the DPO of each consortium partner, in the scope of the project.

Table 2 – FUDGE-5G DPOs

#	Partner	DPO	Email
FUDGE-5G		Luís Cordeiro, ONE	cordeiro@onesource.pt
1	UPV	Carlos Barjau	carbare1@iteam.upv.es
2	TNOR	Kashif Mahmood	kashif.mahmood@telenor.com
3	ATH	Alan Dahi	dpo@athonet.com
4	CMC	Mika Skarp	mika.skarp@cumucore.com
5	FHG	Pousali Chakraborty	pousali.chakraborty@fokus.fraunhofer.de
6	O2M	Peter Sanders	peter.sanders@one2many.eu

7	UBI	Eleonora Papatsoutsou	epapatsoutsou@ubitech.eu
8	ONE	Luís Cordeiro	cordeiro@onesource.pt
9	5CMM	Manuel Fuentes	manuel.fuentes@fivecomm.eu
10	IDE	Sebastian Robitzsch	sebastian.robitzsch@interdigital.com
11	HWDU	Joerg Thomas	joerg.thomas@huawei.com
12	THA	Candice Zimmermann	candice.zimmermann@thalesgroup.com

4.2. Maintain a personal data register

In order to protect personal data, it is necessary to know what data could be collected, how it will be used and where it will be stored. The first step to achieve this is to identify all the processing activities comprising personal data that take place in the project. A 'Personal data register' will document how and why data is used. Maintaining a personal data register represents a key requirement for most data privacy regulators.

As a first step, the document should identify the personal data being held and processed in a data discovery evaluation:

- Where it is located.
- Who has access to it.
- For how long it is retained.

GDPR requires identifying and documenting the following information for every processing activity taking place within FUDGE-5G:

- DPO Name/Contact and contact details of any other third-party, in case it applies.
- The lawful basis and purpose of processing the data.
- The different categories of personal data involved.
- The systems and locations where the personal data is being processed.
- Where the data is transferred to and the list of recipients.
- The retention period and enforced technical and security measures.

4.3. Notify purpose and seek consent

Consent should be given freely, specific, informed, throughout an unambiguous agreement, provided by individuals through a statement or a clear affirmative action to the processing of their personal data. Consent gives control and choice to the individuals over how their personal data is being processed. It represents a key legal aspect for lawfully processing personal data. Despite this, conditions should be met to ensure the consent is valid. This is an important principle in GDPR when collecting individuals' personal data. Therefore, the organization should provide a detailed and clear information intended to explain the processing when requested. To that aim, it should be able to explain why, what and how

data are being processed. The information to be included in the privacy information shared with individuals is the following one:

- Contact details of the project and DPO.
- Purpose and lawful basis for processing, including details of legitimate interests (if applicable).
- Recipients of collected/processed personal data and details of cross-border transfers.
- Retention period of personal data.
- Existence of automated decision-making.
- Details on individuals' rights, process for withdrawing.
- How to file complaints.

Privacy information should be provided to individuals prior to or at the time of collecting their personal data. Alternatively, if collected from other sources, It should be provided within a reasonable timeframe. Privacy information must use clear and plain language and be concise, intelligible, transparent and easily accessible.

Individuals may consent in writing or in any other form. In case the consent is given in writing, it should be distinct from any other agreement for terms and conditions and written using simple and clear language. Anytime, individuals can also withdraw their consent and the withdrawal procedures should be as easy as those followed for giving the consent.

The FUDGE-5G research comprising data processing activities such as surveys should be undertaken by consent. Consent templates are annexed to this document for specific purposes of trials ("Annex A: Trial Informed consent template") or more general purposes ("Annex B: General Informed consent template").

4.4. Response to individuals requesting information about their personal data

Individuals are empowered by GDPR to have control over their personal data and to know how their data is being used. Therefore, they have the right to request about their personal information and it will be particularly important to provide an answer in a reasonable time bound. Answering to the requests will include authenticating the requester, verifying the request and preparing an appropriate response, including information concerning:

- Identification of the personal data being stored/processed.
- The purposes for processing the data.
- Whom, within the project, maintains the personal data and to whom the data will be disclosed.
- If personal data is being used in automated decision-making processed and how that automated decision-making works.
- How long will data be retained and which criteria are being used for retention.

The following list enumerates the steps to be taken for providing a response to a data subject request:

- Receive the data subject request and forward it to the responsible team member.

- Verify if the request is self-raised or on behalf of others.
- Check the identity of the individuals.
- Assess the request and verify if an extension time or charges are involved. In that case the response to the individuals should include further details.
- Identify the location of the individual's personal data, as well as the specific systems or physical documents where it is present.
- Proceed according to the type of data subject request, and take the required actions (e.g., data erasure, introduce restrictions on processing, copying data).
- Compile the details about the data subject to the DPO, to formulate the most appropriate response.
- Send and record the response to the individual.

4.5. Enforce security mechanisms

Organizations should introduce the means, processes and the guarantees to have personal data protected. To achieve that, organizations should be aware of the distinct nature and amount of data being processed, adapting their processes, controls and systems to secure personal data. To that aim, organizational and technical measures are needed to secure and protect personal data.

Organizational measures include for instance:

- Audits.
- Risk assessments.
- Policies.
- Procedures.
- Awareness.
- Training.
- Business continuity.

Technical security measures comprise the technological aspects to be implemented as controls, such as:

- Awareness.
- Training.
- Audits.
- Risk assessments.
- Policies and procedures.
- System security.
- Physical security.
- Anonymization of personal data.
- Encryption of personal data.
- Data disposal.
- Two-factor passwords authentication.
- Remote access.
- Controls for bring-your-own-device scenarios.

- Business continuity.

Moreover, frameworks such as ISO 27001 can also contribute to assess and develop adequate measures. The following steps can help in the identification of the measures to be implemented:

- Review the personal data being held and carry out an information security risk assessment about how they are being used, and the risks presented when processing.
- Perform technical vulnerability assessments on devices and systems presenting high risk concerning the personal data being processed, such as penetration tests.
- Assess and select the most adequate security measures to mitigate the identified risks.
- Ensure information security programme and latest security best practices are available are kept up to date.

4.6. Embed data privacy into systems, processes and services

The concepts of privacy by design and privacy by default are being introduced by data privacy laws. Privacy by design concerns the design of a new process or applications. A set of key principles will contribute for guidance of FUDGE-5G members to be informed about the overall approach, as follows:

- New processes and applications should attend to privacy and data protection concerns by developing a corporate culture where privacy and data protection are in the top of those priorities.
- Support accountable processes by conducting internal audit reviews targeting data privacy and practices.
- Establish and maintain a transparency approach where privacy notices are regularly updated to reflect privacy practices and processing activities.
- Define and enable safeguards by enforcing encryption and data minimisation mechanisms over the personal data.

Privacy by design requires introducing the organizational and technical measures able to implement the data privacy principles and to embed controls into the processing activities to meet the legal requirements and protect individuals' rights.

Privacy by default ensures that only the strictly necessary personal data is stored or processed to achieve a specific purpose. Data privacy by default links to the fundamental data protection principles of data minimization and purpose limitation. Committed organizations include the safeguards for personal data to embed data privacy into the design and overall lifecycle of any technology, business process, product, or service.

4.7. Data breaches notification

Because data breaches can occur for different reasons, it is important to be aware of the risks and introduce the preventive actions to minimize them. It is particularly important to be aware of the data privacy regulations and their strict reporting timelines, being prepared to comply with those timelines in case of breach. Therefore, after a data breach has been

identified, the authority should be notified without undue delay (and no later than 72 hours), with the following information:

- Description of the nature of the breach:
  - Identification of the persons who have accessed what and when.
  - Lookup for the root cause of the breach.
  - Detailed information about how data is being used.
  - Identification of the individuals being affected.
- Analysis of the estimated impact and possible effects.
- Contact details for data protection supervisors.
- Procedures taken by the FUDGE-5G project to investigate and remediate the incident.

Moreover, the following actions can be considered:

- Prepare a response plan and communicate it to all team members and third parties, such as stakeholders.
- Assign the responsibility and time to a person or team for managing breaches.
- Regularly test the plan to minimise the disruption that typically follows a breach.
- Verify if personal data is involved.
- Identify what personal data has been impacted and how.
- Evaluate the impact of the breach and evaluated if rights and freedoms of individuals are in risk.
- Determine if other authorities and the individuals concerned should be notified.
- Carry out a thorough investigation to identify the source of the breach.

4.8. Management of third parties

Third-party risk management is considered a requirement by data privacy regulations. Therefore, the contractor has the responsibility in case an engaged third party violates data privacy laws when processing personal data. Any contractual agreement with a service provider should specify clauses defining the measures to ensure compliance with requirements of data privacy laws. Therefore, the following points should be considered:

- Subject.
- Duration of processing.
- Nature and purpose of processing.
- Personal data.
- Terms or clauses required by the processor.
- Rights and obligations of the controller.

Enhancing the third-party risk management programme is particularly important, and contracts *per se* are not enough. Thus, the following aspects should be considered:

- Conduct a due diligence assessment to ensure that the third-party has the required controls to protect personal data.

- Clearly define the roles, responsibilities and liabilities of both parties, updating the existing contracts or drafting new ones.
- Continue to improve ongoing monitoring through risk assessments and audits to ensure that third parties are maintaining adequate controls to protect personal data.

4.9. Personal data protection when transferring overseas

Cross-border data transfers occur when personal data is transferred to a third country, with the receiver corresponding either to a different organization or to a company in the same corporation group.

Personal data protection faces important challenge for data being transferred across several countries as organizations develop their activity in a global economy. Even for considered safe in terms of offered guarantees of data protection (and thus to where data can potentially be transferred), one should adopt proper safeguards.

A number of different mechanisms recognized by GDPR can be adopted to have protection when transferring data to a different country, such as Binding Corporate and request Binding Corporate Rules (BCRs), instruction of standard contractual clauses, code of conduct or request for certification, as described in Table 3.

Table 3 – Personal data protection Mechanisms when transferring overseas

Right	Description
BCR	Requires approval from the authority to legally enforce corporate internal rules and policies for data transfers within multinational group companies that allow intragroup data transfers to countries not providing an adequate level of protection for personal data.
Standard contractual clauses	Clauses can include a set of standard clauses, provided by a relevant Authority, to be used in contracts.
Code of Conduct	Demonstrate the application of self-regulatory programmes to demonstrate to regulators and consumers that an organization follows certain data privacy standards.
Certification	Can be granted to the receiver, under a scheme approved by the authority. The certification scheme must include appropriate and directly enforceable safeguards to protect the rights of individuals whose personal data is transferred.

A specific exception may be required regarding the application of GDPR in the case of cross-border transfers, relying on the individual to explicitly consent or even introducing the contractual clauses for the individual.

4.10. Communicate data protection policies, practices and processes

Complying with GDPR requires that everyone in FUDGE-5G is aware of its responsibilities on the protection of personal data. It will be important to communicate the data privacy policies and practices to ensure everyone knows how to process and protect personal data.

Also, it will be important to develop a culture of privacy awareness within FUDGE-5G, by highlighting the importance of data privacy values and how to translate them into practice. Moreover, data protection policies and practices should be communicated to make everyone is familiar with its roles and responsibilities when processing personal data. The use of posters, emails and other means can help to communicate the importance of personal data protection. Privacy notices must be updated to ensure that everyone understands what personal data is being processed and how such processing must be done, so everyone makes informed decisions about it. Therefore, some aspects must be met regarding privacy notices:

- Conciseness and transparency.
- Written in clear and plain language.
- Delivered in a timely manner.
- Made publicly available and easy to access.

Moreover, it will be particularly important to involve the key team members and distribute information in order they can attend regular data privacy training to ensure they are kept up to date about internal processes and latest developments in the domain of privacy.

5. Key activities and data protection procedures

This section presents the key activities and data protection procedures to be followed by FUDGE-5G. It includes procedures for team member's administration, datasets administration, communications, supporting platforms, remote work, cookie compliance, research, third-party data, and data encryption.

5.1. Team members administration

As new partner employees are involved as members in the project, it is requested from them to sign a contract covering the processing of personal information, sensitive information and transferring this data in the delivery of services such as payroll, insurances and for advice. At the end of the retention period within the employee privacy statement, data should be securely disposed. Employees have the responsibility that the information provided in their data is up to date.

5.2. Administration of datasets

The FUDGE-5G datasets contain all the results of research activities in terms of publications, as well as data collection on the website and social networks. These results also involve white papers and promotional materials, including brochures, flyers, newsletters, posters, press releases and videos produced during the FUDGE-5G project. Also, tests and trials will result in datasets requiring administration.

To ensure the compliance with the GDPR and the Data Management Plan (DMP), each dataset lifecycle will follow the methodology depicted in Figure 1, composed of the following key steps:

- Step 1: The data will be collected from the experiment (or from the partner producing the data).
- Step 2: Each partner collecting/generating datasets is responsible for following this document rules. The partner's DPO must ensure that all required procedures are properly implemented.
- Step 3: The FUDGE-5G DPO reviews the datasets collected/generated and ensures they are in accordance.
- Step 4: The generated and processed data will be stored following the established DMP procedures.

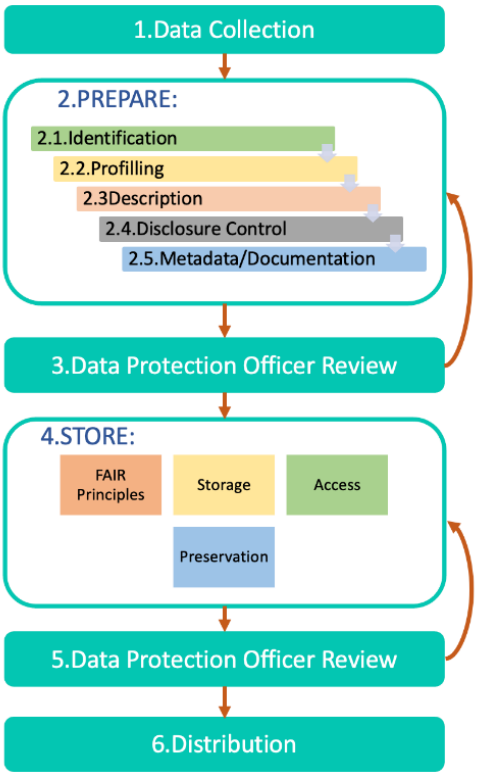

Figure 1 - Data management methodology

- Step 5: The FUDGE-5G DPO reviews the storage procedure and ensures that the DMP procedures were properly implemented.
- Step 6: The partner responsible for the dataset follows the DMP procedures for dataset distribution, in order to make it available.

5.3. Data Processing for Deliverables and Reports

All deliverables (or any other way of reporting comprising data possessing) require a written note by the FUDGE-5G DPO and the consortium partners' DPOs, according to Table 2. The note must explicitly corroborate and explain the compliance with the consortium privacy policy and GDPR EU regulations.

5.4. Communications

GDPR states that the processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest. Because all email addresses are personal data, if someone informs that he no longer wants to be contacted via email or text, his/her name and contact details must be removed from the distribution list, and a note made that they no longer consent to receive emails or texts. Thus, those Individuals whose option was to not receive emails should not be included in the mailings or bulk text messages. Also, an unsubscribe option must be included at the bottom of the email or text message.

5.5. Supporting platforms

The communications team is responsible for providing, maintaining and monitoring the platforms which facilitate the communication both between project members and towards external stakeholders. Many of FUDGE-5G communication and dissemination platforms gather visitors tracking data that will be exploited by the project to correlate and assess the project visibility to the community in general and the specifically targeted audiences. The following support platforms follow that purpose and may store personal data:

- https://fudge-5g.atlassian.net
- https://cloud.fudge-5g.eu
- https://fudge-5g.eu
- https://zenodo.org/communities/fudge-5g
- https://twitter.com/fudge5geu
- https://www.linkedin.com/company/fudge-5g/
- https://www.youtube.com/channel/UCeL-7ukTWMczPkYhBrO1sCg

5.6. Remote work

Remote working is a paradigm that has leveraged since the COVID-19 pandemic broke out. Since then, large portions of the population have been confined to their homes by local and national directives. Despite this, most companies have continued operating using a distributed workforce, and some even made remote working permanent. Such

circumstances demand a different security approach, which may be significantly different from work in centralized offices, due to the physical dispersion of the places where data is stored and processed.

5.7. Cookie compliance

Cookies are small text files that websites place on devices being used for browsing. They are processed and stored by web browser and usually are harmless and serve crucial functions for websites. Cookies are an important tool that can give businesses a great deal of insight into their users' online activity. Regulations concerning cookies are split between the GDPR (GDPR, 2021) and the ePrivacy Directive (SUPERVISOR, 2021).

Cookies can potentially identify someone without consent. They are the primary tool that advertisers use to track users' activity online. Therefore, they can be classified as personal data in certain circumstances and, consequently, they are subject to the GDPR. To comply with the regulations governing cookies under the GDPR and the ePrivacy Directive, it is required to:

- Receive users' consent before any cookies are used, except strictly necessary cookies.
- Provide accurate and specific information about the data each cookie tracks and its purpose, in plain language, before consent is received.
- Document and store the consent received from users.
- Allow users to access services even if they refuse to allow the use of certain cookies.
- Provide a manner for users to withdraw their consent for cookies, as easily accessible as it was for them to give their consent in the first place.

For the purpose of compliance of cookie usage, a template for website data privacy policy is included in this document as "Annex D: Website Data Privacy Policy template".

5.8. Research

Unless anonymised, records of individual's views are considered personal data and, as such, are subject to the privacy rights detailed in this handbook. Published data must not identify any individual person without his/her explicit consent. However, anonymised data from datasets can be processed and published for statistical purposes. Data should only be collected through the agreed platforms and by authorised individuals. As with all forms of data collection, a retention period must be clearly defined, and data should be securely deleted when this period expires.

The FUDGE-5G research comprising data processing activities such as surveys should be undertaken by consent. Consent templates are annexed to this document for the specific purpose of trials, in "Annex A: Trial Informed consent template" and in "Annex B: General Informed consent template".

5.9. Subcontracts

In case of FUDGE-5G partners planning to subcontract certain services that imply processing of personal data, the sub-contractors should follow the responsibilities of Data Processors.

"Annex C: Data Processing Agreement template" provides an agreement template for governing that kind of activities.

5.10. Third-party data

When third-party data is used internally, a declaration should present its use to the individuals whose data is being processed. This must be delivered within one month of obtaining the data, at the point of first communication or prior to disclosure to any further parties. If the third-party notifies the project (or if the project becomes aware) of any errors in data, these errors must be rectified within one month after notification. Third parties requiring the erasure of data or applying restrictions in processing are required to notify the DPO, that will undertake all reasonable procedures to comply with those requests. Whenever the DPO advises of a request for restriction or erasure, project partners are required to comply with this notice.

5.11. Data encryption

Organization-sensitive data should be encrypted both in transit and at rest. GDPR explicitly mentions "encryption" when discussing appropriate technical and organizational security measures. Encryption is important since encrypted data will be illegible and useless (or at least much more difficult to use) in case of breach.

5.12. Privacy

The FUDGE-5G project activities will design, develop, trial and showcase novel solutions that greatly rely on electronic communications. New or improved products will emerge from these activities, as well as research outputs to be published and shared open and freely. Thus, the project will follow the ePD regulations regarding the protection of users' data and their informed consent.

5.13. Code of Conduct

Codes of Conduct (CoC), under the GDPR, are voluntary sets of rules that assist members of that Code with data protection compliance and accountability in specific sectors or relating to specific processing operations. GPRP recommends the use of approved CoC.

CoC can help organizations ensuring they follow best practices and rules designed specifically for their sector or processing operations, thus enhancing compliance with data protection laws. They are developed and managed by a "Code Owner" with the expertise and knowledge of how to enhance data protection in that specific domain.

A GDPR "Code of Conduct" is more than just a documented guidance or best practice. It must materially specify or enhance the application of data protection laws to a certain sector or processing activity, rather than being just a restatement of the GDPR.

Annex E provides a template for a FUDGE-5G CoC, but it takes more time and effort to have it developed, discussed, approved, and implemented.

6. References

EU. (2002). *ePrivacy Directive*. Retrieved 7 2021, from https://edps.europa.eu/data-protection/our-work/subjects/eprivacy-directive_en

EU. (2016). *GDPR*. Retrieved 7 2021, from http://data.europa.eu/eli/reg/2016/679/2016-05-04

GDPR. (2021). *Cookies, the GDPR, and the ePrivacy Directive*. Retrieved 7 2021, from https://gdpr.eu/cookies/

NIST. (2021). *Cybersecurity Framework*. Retrieved 7 2021, from https://www.nist.gov/industry-impacts/cybersecurity-framework

PWC. (2021). *Data Privacy Handbook - A starter guide to data privacy compliance.* Retrieved 7 2021, from https://www.pwc.com/m1/en/services/assurance/risk-assurance/documents/data-privacy-egypt-what-you-need-know-en.pdf

SUPERVISOR, E. D. (2021). *ePrivacy directive*. Retrieved 7 2021, from https://edps.europa.eu/data-protection/our-work/subjects/eprivacy-directive_en

Annex A: Informed Consent Template for FUDGE-5G Trials

Please tick the appropriated boxes
Participating in the trial

	Yes	No
I have read and understood the trial information dated [DD/MM/AAAA], or it has been read to me. I have been able to ask questions and my questions were answered clearly and to my satisfaction.	☐	☐
I consent to voluntary participate in this trial and I understand that I can refuse to answer questions and withdraw from the trial, with having to provide a justification.	☐	☐
I understand that taking part in this trial involves what the participant [has to do / will be subject to].	☐	☐
I understand that taking part in this trial has [risks] as potential risk.	☐	☐

Use of information

	Yes	No
I understand that the information and data that I will provide will be used for [list the planned outputs].	☐	☐
I understand that personal information collected that can identify me will only share among the trial team.	☐	☐
I agree that my information can be quoted in research outputs.	☐	☐

Future use or reuse of the information by others

	Yes	No
I give permission to [specify the data] that I provide to be deposited in Zenodo so it can be used for future research and learning.	☐	☐
I understand that all my data that will be publicly available is anonymized, thus I cannot be identified as the data provided.	☐	☐

Signatures

_____

Name of the participant [IN CAPITALS]

_____

Signature of the participant

_____

Date

I have read, in detail, the information sheet to the potential participant, and ensured that the participant understands to what he is giving consent.

_____

Name of the trial responsible [IN CAPITALS]

_____

Signature of the trial responsible

_____

Date

Annex B: General Informed Consent Template

RESEARCH CONSENT FORM
PROCESSING PERSONAL DATA OF
EUROPEAN UNION (EU) / EUROPEAN ECONOMIC AREA-BASED (EEA) PERSONS

This consent form provides information for potential research participants to understand how the processing of their personal data will be conducted for the purpose of this research project, which is subject to the General Data Protection Regulation (GDPR). Please sign at the bottom to indicate that you have read and understood how your personal data will be processed, your related rights, and that you consent to this processing as described below.

You can find information related to the purpose of the research project, how it will be conducted and by whom from the project consent form, which you should receive as a separate document. We are conducting the processing of personal data related to this research project on the basis of your consent.

NOTE: all instructions are highlighted in grey. Please delete the instructions before submitting the form to the IRB for review.

Choose one of the two options, depending on whether you intend to use the same dataset for other related research, or you know you will only use it for the current research. Delete the other option from the form you submit to potential subjects. Also, please delete the "Option" header for each section that is used, complete any other areas that are highlighted in yellow, and remove the highlighting before submitting the form to the IRB for review.

Option 1:

We will only use your personal data for the purposes of this research project.

Option 2:

We will use your personal data primarily for the purposes of this research project. If the results of this research will indicate that further studies are beneficial for [include topic/field/area of study/benefit for society], we may process your personal data for the purpose of extending our research in the field/area of [include specific area/field]. You will be informed before processing takes place.

PERSONAL DATA USED

Fill out the categories of data you will use for the research project, aiming to be as detailed as possible; the categories of data mentioned are just examples and they should be replaced depending on the project.

In addition to the information you will directly submit to us, these are the categories of personal data we will use:

genetic data (in particular……..)
data related to health (in particular blood type, heart rate…….)
behavioral data (in particular)……..

Rev. 9/30/2019

……..

Only include this if you obtain personal data from other sources than what you observe directly and what the subject is providing to you. Otherwise, delete this paragraph:

We obtain additional personal data related to you from third party sources, as follows:

Data related to your social interactions from your Facebook account;
Data related to your school performance from your student file;
…….

Include if this is the practice, otherwise delete this sentence:
As a safeguard to protect your privacy, we pseudonymize (key-code) your personal data. [Optionally, include information of who has access to the key-coded data and who has access to the key, as well as the circumstances when re-identification can occur].

RECIPIENTS OF YOUR PERSONAL DATA

Include information about all entities that have access to the personal data, including service providers that are contracted for, handling data or any other service on your behalf (ex: cloud service providers). Please indicate the name of the service provider.

Option 1:
We will not share your personal data with any third party. We will only disclose the personal data to authorities for those situations where we will receive a lawful order to do so.

Option 2:
We will share your personal data with the following recipients:

…the Supervisory Body for X (US based)……

…Processors that act on our behalf: a cloud service provider, an image processor…….
Public authorities, for those situations where we will receive a lawful order to do so.

YOUR RIGHTS

Under the GDPR and its implementing laws at national level, you have the following rights, with the conditions and limitations set out in Chapter III of the GDPR:

To obtain confirmation that your data is being processed, as well as access to and a copy of your personal data;
To obtain correction of your personal data;
To obtain erasure of your data, if you submit a reasoned request;
To obtain portability of your data;
To obtain restriction of your data (which means we limit the access to your dataset) if you submit a reasoned request;
To withdraw your consent at any time.

When you withdraw your consent, we will not collect additional information related to you. We may also erase the personal data we already collected. This will happen only if its erasure does not render impossible or seriously impair the achievement of the objectives of the research project.

To exercise your rights, please use the contact information below to submit a request. When you submit a request, please indicate your name, the name of this project, your reasons for making the request, if necessary, and other details you think will be useful for us to comply with your request.

ADDITIONAL INFORMATION

Include the retention period (how long will you keep the data for after the end of the project). If the retention period depends on other factors, you don't have to mention an exact period of time, but you will have to mention the factors that influence the establishment of the period. Choose one of the two options and delete the other.

Option 1:

We retain your personal data for [insert retention time] after the project is completed.

Option 2:

The period of time for which we retain your personal data depends on [include the factors that influence this period of time].

Your personal data is transferred to the United States, which has not sought nor obtained an adequacy decision from the European Commission. This means that there may be risks to your personal data under this jurisdiction. However, we adopt and implement sufficient safeguards to protect your personal data, as described in this form. We transfer your data on the basis of your explicit consent, under Article 49 GDPR.

If you have any concerns about how your personal data is being handled, use the address below to contact us. If you will not be satisfied with our reply and how we protect your personal data, you can contact the data protection authority in your home country or in another relevant jurisdiction for this processing activity, pursuant to the conditions of Article 77 GDPR.

CONTACT INFORMATION IF YOU HAVE QUESTIONS OR CONCERNS REGARDING GDPR

Name:
Address:
Post Code:
Phone: :
Email:

CONSENT SIGNATURE and DATE

Rev. 9/30/2019

Print Name:

_____

Signature:

_____

Date:

_____

Annex C: Data Processing Agreement Template

This Data Processing Agreement ("**Agreement**") forms part of the Contract for Services ("**Principal Agreement**") between

_____
_____
_____
(the "**FUDGE-5G Partner**") and

_____
_____
_____
(the "Data Processor")
(together as the "**Parties**")

WHEREAS

(A) The FUDGE-5G Partner acts as a Data Controller.

(B) The FUDGE-5G Partner wishes to subcontract certain Services, which imply the processing of personal data, to the Data Processor.

(C) The Parties seek to implement a data processing agreement that complies with the requirements of the current legal framework in relation to data processing and with the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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).

(D) The Parties wish to lay down their rights and obligations.

IT IS AGREED AS FOLLOWS:

1. Definitions and Interpretation

1.1 Unless otherwise defined herein, capitalized terms and expressions used in this Agreement shall have the following meaning:

1.1.1 "Agreement" means this Data Processing Agreement and all Schedules;

1.1.2 "FUDGE-5G Partner Personal Data" means any Personal Data Processed by a Contracted Processor on behalf of FUDGE-5G Partner pursuant to or in connection with the Principal Agreement;

1.1.3 “Contracted Processor” means a Sub-Processor;

1.1.4 “Data Protection Laws” means EU Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other country;

1.1.5 “EEA” means the European Economic Area;

1.1.6 “EU Data Protection Laws” means EU Directive 95/46/EC, as transposed into domestic legislation of each Member State and as amended, replaced or superseded from time to time, including by the GDPR and laws implementing or supplementing the GDPR;

1.1.7 “GDPR” means EU General Data Protection Regulation 2016/679;

1.1.8 “Data Transfer” means:

1.1.8.1 a transfer of FUDGE-5G Partner Personal Data from the FUDGE-5G Partner to a Contracted Processor; or

1.1.8.2 an onward transfer of FUDGE-5G Partner Personal Data from a Contracted Processor to a Subcontracted Processor, or between two establishments of a Contracted Processor, in each case, where such transfer would be prohibited by Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Data Protection Laws);

1.1.9 “Services” means the _____ services the FUDGE-5G Partner provides.

1.1.10 “Sub-Processor” means any person appointed by or on behalf of Processor to process Personal Data on behalf of the Company in connection with the Agreement.

1.2 The terms, “Commission”, “Controller”, “Data Subject”, “Member State”, “Personal Data”, “Personal Data Breach”, “Processing” and “Supervisory Authority” shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly.

2. Processing of FUDGE-5G Partner Personal Data

2.1 Processor shall:

2.1.1 Comply with all applicable Data Protection Laws in the Processing of FUDGE-5G Partner Personal Data; and

2.1.2 Cot Process FUDGE-5G Partner Personal Data other than on the relevant FUDGE-5G Partner ’s documented instructions.

2.2 The FUDGE-5G Partner instructs Processor to process FUDGE-5G Partner Personal Data.

3. Processor Personnel
Processor shall take reasonable steps to ensure the reliability of any employee, agent or contractor of any Contracted Processor who may have access to the FUDGE-5G Partner Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know / access the relevant FUDGE-5G Partner Personal Data, as strictly necessary for the purposes of the Principal Agreement, and to comply with Applicable Laws in the context of that individual's duties to the Contracted Processor, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

4. Security

4.1 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Processor shall in relation to the FUDGE-5G Partner Personal Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR.

4.2 In assessing the appropriate level of security, Processor shall take account in particular of the risks that are presented by Processing, in particular from a Personal Data Breach.

5. Sub-Processing

5.1 Processor shall not appoint (or disclose any FUDGE-5G Partner Personal Data to) any Sub-Processor unless required or authorized by the FUDGE-5G Partner.

6. Data Subject Rights

6.1 Taking into account the nature of the Processing, Processor shall assist the FUDGE-5G Partner by implementing appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the FUDGE-5G Partner obligations, as reasonably understood by FUDGE-5G Partner , to respond to requests to exercise Data Subject rights under the Data Protection Laws.

6.2 Processor shall:

6.2.1 promptly notify FUDGE-5G Partner if it receives a request from a Data Subject under any Data Protection Law in respect of FUDGE-5G Partner Personal Data; and

6.2.2 ensure that it does not respond to that request except on the documented instructions of FUDGE-5G Partner or as required by Applicable Laws to which the

Processor is subject, in which case Processor shall to the extent permitted by Applicable Laws inform FUDGE-5G Partner of that legal requirement before the Contracted Processor responds to the request.

7. Personal Data Breach

7.1 Processor shall notify FUDGE-5G Partner without undue delay upon Processor becoming aware of a Personal Data Breach affecting FUDGE-5G Partner Personal Data, providing FUDGE-5G Partner with sufficient information to allow the FUDGE-5G Partner to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.

7.2 Processor shall co-operate with the FUDGE-5G Partner and take reasonable commercial steps as are directed by FUDGE-5G Partner to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

8. Data Protection Impact Assessment and Prior Consultation Processor shall provide reasonable assistance to the FUDGE-5G Partner with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which FUDGE-5G Partner reasonably considers to be required by article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law, in each case solely in relation to Processing of FUDGE-5G Partner Personal Data by, and taking into account the nature of the Processing and information available to, the Contracted Processors.

9. Deletion or return of FUDGE-5G Partner Personal Data

9.1 Subject to this section 9 Processor shall promptly and in any event within

10 business days of the date of cessation of any Services involving the Processing of FUDGE-5G Partner Personal Data (the “Cessation Date”), delete and procure the deletion of all copies of those FUDGE-5G Partner Personal Data.

10. Audit rights

10.1 Subject to this section 10, Processor shall make available to the Co FUDGE-5G Partner mpany on request all information necessary to demonstrate compliance with this Agreement, and shall allow for and contribute to audits, including inspections, by the FUDGE-5G Partner or an auditor mandated by the FUDGE-5G Partner in relation to the Processing of the FUDGE-5G Partner Personal Data by the Contracted Processors.

10.2 Information and audit rights of the FUDGE-5G Partner only arise under section 10.1 to the extent that the Agreement does not otherwise give them information and audit rights meeting the relevant requirements of Data Protection Law.

11. Data Transfer

11.1 The Processor may not transfer or authorize the transfer of Data to countries outside the EU and/or the European Economic Area (EEA) without the prior written consent of the FUDGE-5G Partner. If personal data processed under this Agreement is transferred from a country within the European Economic Area to a country outside the European Economic Area, the Parties shall ensure that the personal data are adequately protected. To achieve this, the Parties shall, unless agreed otherwise, rely on EU approved standard contractual clauses for the transfer of personal data.

12. General Terms

12.1 Confidentiality. Each Party must keep this Agreement and information it receives about the other Party and its business in connection with this Agreement ("Confidential Information") confidential and must not use or disclose that Confidential Information without the prior written consent of the other Party except to the extent that:
(a) disclosure is required by law;
(b) the relevant information is already in the public domain.

12.2 Notices. All notices and communications given under this Agreement must be in writing and will be delivered personally, sent by post or sent by email to the address or email address set out in the heading of this Agreement at such other address as notified from time to time by the Parties changing address.

13. Governing Law and Jurisdiction

13.1 This Agreement is governed by the laws of _____.

13.2 Any dispute arising in connection with this Agreement, which the Parties will not be able to resolve amicably, will be submitted to the exclusive jurisdiction of the courts of _____, subject to possible appeal to _____.

IN WITNESS WHEREOF, this Agreement is entered into with effect from the date first set out below.

FUDGE-5G Partner
Signature _____
Name: _____
Title: _____
Date Signed: _____
Processor Company
Signature _____
Name _____

Title _____
Date Signed _____

Annex D: Template for Website Data Privacy Policy

This data privacy policy will explain how FUDGE-5G uses the personal data we collect from you when you use our website.

Topics:

- What data do we collect?
- How do we collect your data?
- How will we use your data?
- How do we store your data?
- Marketing
- What are your data protection rights?
- What are cookies?
- How do we use cookies?
- What types of cookies do we use?
- How to manage your cookies
- Privacy policies of other websites
- Changes to our privacy policy
- How to contact us
- How to contact the appropriate authorities

What data do we collect?

FUDGE-5G collects the following data:

- Personal identification information (Name, email address, phone number, etc.)
- [Add any other data yFUDGE-5G collects]

How do we collect your data?

You directly provide to FUDGE-5G with most of the data we collect. We collect data and process data when you:

- Register online or place an order for any of our products or services.
- Voluntarily complete a customer survey or provide feedback on any of our message boards or via email.
- Use or view our website via your browser's cookies.

- [Add any other ways FUDGE-5G collects data]

FUDGE-5G may also receive your data indirectly from the following sources:

- [Add any indirect source of data FUDGE-5G has]

How will we use your data?

FUDGE-5G collects your data so that we can:

- Process your order and manage your account.
- Email you with special offers on other products and services we think you might like.
- [Add how else FUDGE-5G uses data]

If you agree, FUDGE-5G will share your data with our partner companies so that they may offer you their products and services.

- [List organizations that will receive data]

When FUDGE-5G processes your order, it may send your data to, and also use the resulting information from, credit reference agencies to prevent fraudulent purchases.

How do we store your data?

FUDGE-5G securely stores your data at [enter the location and describe security precautions taken].

FUDGE-5G will keep your [enter type of data] for [enter time period]. Once this time period has expired, we will delete your data by [enter how you delete users' data].

Marketing

FUDGE-5G would like to send you information about products and services of ours that we think you might like, as well as those of our partner companies.

- [List organizations that will receive data]

If you have agreed to receive marketing, you may always opt out at a later date.

You have the right at any time to stop FUDGE-5G from contacting you for marketing purposes or giving your data to other members of the FUDGE-5G Group.

If you no longer wish to be contacted for marketing purposes, please click here.

What are your data protection rights?

FUDGE-5G would like to make sure you are fully aware of all of your data protection rights. Every user is entitled to the following:

The right to access – You have the right to request FUDGE-5G for copies of your personal data. We may charge you a small fee for this service.

The right to rectification – You have the right to request that FUDGE-5G correct any information you believe is inaccurate. You also have the right to request FUDGE-5G to complete the information you believe is incomplete.

The right to erasure – You have the right to request that FUDGE-5G erase your personal data, under certain conditions.

The right to restrict processing – You have the right to request that FUDGE-5G restrict the processing of your personal data, under certain conditions.

The right to object to processing – You have the right to object to FUDGE-5G's processing of your personal data, under certain conditions.

The right to data portability – You have the right to request that FUDGE-5G transfer the data that we have collected to another organization, or directly to you, under certain conditions.

If you make a request, we have one month to respond to you. If you would like to exercise any of these rights, please contact us at our email:

Call us at:

Or write to us:

Cookies

Cookies are text files placed on your computer to collect standard Internet log information and visitor behavior information. When you visit our websites, we may collect information from you automatically through cookies or similar technology

For further information, visit allaboutcookies.org.

How do we use cookies?

FUDGE-5G uses cookies in a range of ways to improve your experience on our website, including:

- Keeping you signed in
- Understanding how you use our website
- [Add any uses FUDGE-5G has for cookies]

What types of cookies do we use?

There are a number of different types of cookies, however, our website uses:

- Functionality – FUDGE-5G uses these cookies so that we recognize you on our website and remember your previously selected preferences. These could include what language you prefer and location you are in. A mix of first-party and third-party cookies are used.
- Advertising – FUDGE-5G uses these cookies to collect information about your visit to our website, the content you viewed, the links you followed and information about your browser, device, and your IP address. FUDGE-5G sometimes shares some limited aspects of this data with third parties for advertising purposes. We may also share online data collected through cookies with our advertising partners. This means that when you visit another website, you may be shown advertising based on your browsing patterns on our website.
- [Add any other types of cookies FUDGE-5G uses]

How to manage cookies

You can set your browser not to accept cookies, and the above website tells you how to remove cookies from your browser. However, in a few cases, some of our website features may not function as a result.

Privacy policies of other websites

The FUDGE-5G website contains links to other websites. Our privacy policy applies only to our website, so if you click on a link to another website, you should read their privacy policy.

Changes to our privacy policy

FUDGE-5G keeps its privacy policy under regular review and places any updates on this web page. This privacy policy was last updated on 9 January 2019.

How to contact us

If you have any questions about FUDGE-5G's privacy policy, the data we hold on you, or you would like to exercise one of your data protection rights, please do not hesitate to contact us.

Email us at:

Call us:

Or write to us at:

How to contact the appropriate authority

Should you wish to report a complaint or if you feel that FUDGE-5G has not addressed your concern in a satisfactory manner, you may contact the Information Commissioner's Office.

Email:

Address:

Annex E: Code of Conduct

1. Scope

This Statement of Code of Conduct (CoC) applies to all FUDGE-5G members, stakeholders and service providers.

2. Definitions

Board Member: a member of FUDGE-5G Board.

FUDGE-5G Party: a Board Member or any other member of FUDGE-5G project, stakeholders and service providers.

3. Principles

The FUDGE-5G members by virtue of their roles and responsibilities, represent the FUDGE-5G project to the larger society. They have a special duty to observe the highest standards of personal and professional conduct. The FUDGE-5G project requires all Parties to comply with the following CoC principles:

- Our words and actions embody respect for truth, fairness, free inquiry, and the opinions of others;
- We respect all individuals without regard to race, color, sex, sexual orientation, marital status, creed, ethnic or national identity, handicap, or age;
- We uphold the professional reputation of others and give credit for ideas, words, or images originated by others;
- We safeguard privacy rights and confidential information;
- We do not grant or accept favors for personal gain;
- We do not solicit or accept favors where a higher public interest would be violated;
- We avoid actual or apparent conflicts of interest and, if in doubt, seek guidance from appropriate authorities;
- We follow the letter and spirit of the laws and regulations affecting the Cloud Security
- Alliance;
- We actively encourage colleagues to join us in supporting these laws and regulations and the standards of conduct in these Ethics Principles.

4. Review and Acknowledgments

Upon the entry into force of this Statement of CoC , each FUDGE-5G Party shall be provided with and asked to review a copy of this Statement of Ethics and to acknowledge in writing that he/she has read, understood and agreed to abide by this Statement.

5. Entry into Force and Implementation

This Statement of CoC is approved by the FUDGE-5G Board.

This Statement of CoC will enter into force at ____.

The FUDGE-5G Board ensures that this Statement of CoC is given to and acknowledged by all FUDGE-5G Parties.

6. Oversight

The Board shall have direct responsibility for the oversight of this Statement of CoC and for the establishment of procedures to support this Statement of CoC .

7. Review and Changes

This Statement of Ethics shall be reviewed and updated as necessary, annually by the FUDGE-5G Board. Any changes to the Statement of CoC shall be communicated to all FUDGE-5G Parties.