This project that has received funding from the European Union's Horizon 2020 - Research and Innovation Framework Programme, H2020-FCT-2015, under grant agreement no 700381.

Analysis System for GAthered Raw Data

ASGARD

Instrument: Research and Innovation Action proposal

Thematic Priority: FCT-1-2015

D12.1 ASGARD Data Protection Guideline

Deliverable number	12.1	
Version:	1.2	
Delivery date:	August 2018	
Dissemination level:	Public	
Classification level:	Non-classified	
Status	FINAL	
Nature:	Report	
Main author(s):	Maura Conway	DCU
	Monica Cappelletti	DCU
Contributor(s):		

DOCUMENT CONTROL

Version	Date	Author(s)	Change(s)
0.1	16/03/2017	Maura Conway (DCU) Monica Cappelletti (DCU)	
0.2	27/03/2017	Maura Conway (DCU) Monica Cappelletti (DCU)	Annexes III and IV have been divided into two dedicated files
0.3	17/05/2017	Maura Conway (DCU) Monica Cappelletti (DCU)	According to Reviewers' suggestions: minor changes in paragraph 1; new concept in paragraph 2; new paragraph 5.
0.4	30/05/2017	Romaios Bratskas (ADI)	Quality Review of the deliverable
1.0	31/05/2017	Maura Conway (DCU) Monica Cappelletti (DCU)	Finalizing the v1.0 of the deliverable
1.1	30/07/2018	Maura Conway (DCU) Monica Cappelletti (DCU)	Update version M24 Rewording, new paragraph 6, updated annexes.
1.2	29/08/2018	Romaios Bratskas (ADI)	Quality review of the deliverable

DISCLAIMER

Table of Contents

1. Introduction: Data protection regulation in the EU 4
2. Core concepts 5
3. Fundamental Principles 7
4. Notification process and Data Protection Impact Assessment 9
5. Novelties in the EU Data Protection Law 10
6. ASGARD Data Protection Policy 11

Annexes

ANNEX I. DATA PROTECTION AUTHORITIES (DPA) 13
ANNEX II. ASGARD DATA PROTECTION IMPACT ASSESSMENT TEMPLATE 14
ANNEX III. ASGARD Informed Consent Form 21
ANNEX IV. ASGARD DATA PROTECTION FLOWCHART 25
ANNEX V. ASGARD Code of Conduct Scheme 26

1. Introduction: Data protection regulation in the EU

The ASGARD project must comply with all EU laws regarding data protection. The purpose of this guideline is to explain core principles and concepts of the right to **protection of personal data in scientific research**.[1]

In the 1990s, the European Union started a process of codification of data protection and privacy rights in order to harmonise different national legislation. Directive 95/46/EC[2] ("Data Protection Directive") and Directive 2002/58/EC[3] ("E-Privacy Directive") were the first legal provisions that referred to define the legal framework, considering also the EU Charter of Fundamental Rights[4] and the appropriate national legislation that transposed these EU directives.

This multilevel legal environment has changed in 2018, when in May a new European Regulation came into force: the General Data Protection Regulation, GDPR.[5] Although the new Regulation confirms the main principles of both the above-cited Directives, it substitutes them and all national legislation on data protection and privacy rights.

This Guideline is divided into six sections: section 1 provides a short description of the EU legal framework, section 2 addresses the main concepts used in data protection legislation, section 3 provides the main principles of data protection rights, paragraph 4 supplies a short description of notification and data protection impact assessment (DPIA) processes, paragraph 5 outlines briefly the new EU Regulation novelties, and section 6 describes the Data Protection Policy in ASGARD that all research partners have to comply with.

The Guideline has five annexes: Annex I contains the list of ASGARD partner countries' National Data Protection Authorities (DPA) with links to their websites and national legislation; Annex II is the Data Protection Impact Assessment (DPIA) Template; Annex III is the Informed Consent Sheet template; Annex IV is the ASGARD Data Protection Flowchart that seeks to make it easier for partners to determine what dataset they can use in the project; Annex V is the code of conduct template.

---

[1] According to article 19 Regulation(EU) n. 1291/2013 (Horizon 2020): "all the research and innovation activities carried under Horizon 2020 shall comply with ethical principles and relevant national, Union and international legislation, including the Charter of Fundamental Rights of the European Union and the European Convention on Human Rights and its Supplementary Protocols. Particular attention shall be paid to the principle of proportionality, the right to privacy, the right to the protection of personal data, the right to the physical and mental integrity of a person, the right to non-discrimination and the need to ensure high levels of human health protection."

[2] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[3] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on Privacy and Electronic Communications). Later this Directive was amended with Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009.

[4] Article 8 (Protection of Personal Data) of the EU Charter of Fundamental Rights: "1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. 3. Compliance with these rules shall be subject to control by an independent authority."

[5] 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).

Directive 2016/680/EU[6] specifically addresses privacy constraints and requirements for Law Enforcement Agencies (LEAs), for more on which please consult ASGARD Deliverable 12.2. and Deliverable 12.6.

2. Core concepts

European Data Protection legislation is based on some core concepts concerning the subjects who are going to acquire, collect, process, profile, and use data; the different types of data; and notification procedures. Below are listed the most important definitions for scientific research activities. These definitions have been extrapolated from EU legislation, EU and Member State (MS) official documents, or other legal documents.

SUBJECTS IN DATA PROCESS	**Data Controller**[7]: The natural or legal person, which alone or jointly with others determines the purposes and means of the processing of personal data.
	Data Processor[8]: A natural or legal person, which processes personal data on behalf of the controller.
DIFFERENT TYPES OF DATA	**Personal Data**[9]: Any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number, location data, an online identifier or to one or more factors specific to his physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Personal data may be processed if the data subject has unambiguously given his consent ("prior consent").
DIFFERENT TYPES OF DATA	**Special Categories of Personal Data or "Sensitive Personal Data"**[10]: Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. "Sensitive personal data" may be processed if the data subject has given his explicit consent to the processing of those data ("prior written consent").
	Genetic Data[11]: personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.

[6] Directive 2016/680/EU 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.
[7] Art. 4, n. 7), Regulation (EU) 2016/679.
[8] Art. 4, n. 8), Regulation (EU) 2016/679.
[9] Art. 4, n. 1), Regulation (EU) 2016/679.
[10] Art. 9, Regulation (EU) 2016/679.
[11] Art. 4, n. 13), Regulation (EU) 2016/679.

DIFFERENT TYPES OF DATA	**Biometric Data**[12]: personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.
	Anonymisation (**Anonymised Data**)[13]: Processing of data with the aim of removal of information that could lead to an individual being identified. Data can be considered anonymised when it does not allow identification of the individuals to whom it relates, and it is not possible that any individual could be identified from the data by any further processing of that data or by processing it together with other information which is available or likely to be available. Use of anonymised data does not require the consent of the "data subject."
	Simulated Data: Imitation or creation of data that closely matches real-world data, but is not real world data. For these data, consent is not necessary since it is not possible to identify the "data subject."
	Pseudonymous data: "subset of personal data that cannot be attributed to a specific data subject without the use of additional information provided such additional information is kept separately and is subject to technical and organisational measures to ensure that remains separate"[14].
	Pseudonymisation[15]: The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.
	Big Data[16]: High-volume, high-velocity, high-value and high-variety information (4Vs) assets that demand innovative forms of information processing.
	Open Data[17]: Data that can be freely used, re-used, and redistributed by anyone – subject only, at most, to the requirement to attribute and share-alike.

[12] Art. 4, n. 14), Regulation (EU) 2016/679.

[13] For the definition of, for example, the Irish Data Protection Authority, see https://www.dataprotection.ie/docs/Anonymisation-and-pseudonymisation/1594.htm and the UK Information Commissioner, see https://ico.org.uk/for-organisations/guide-to-data-protection/anonymisation/.

[14] *Data Protection. A practical Guide to UK and EU Law*, Carey, Peter [2015], 34.

[15] Art. 4, n. 5), Regulation (EU) 2016/679.

[16] For the 4Vs theory see *Big Data to Smart Data,* Iafrate Fernando [2015]. The UK Data Protection Authority refers to Gartner's definitions "Big data is high-volume, high-velocity and high-variety information assets that demand cost-effective, innovative forms of information processing for enhanced insight and decision making", Information Commissioner's Office, *Big Data and Data Protection*, 6 [2014].

[17] Definition of Open Data Handbook, http://opendatahandbook.org/guide/en/what-is-open-data/

PROCESSES	**Processing of Personal Data**[18]: Any operation (or set of operations) that is performed upon personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.
	Profiling[19]: Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location, or movements.

3. Fundamental Principles

European Data Protection legislation provides that personal data must be collected, used, and processed fairly, stored safely, and not disclosed to any other person unlawfully. From this perspective we can outline the following fundamental principles regarding personal data use[20]:

1. Personal data must be obtained and processed **fairly, lawfully, and in a transparent way**[21]: according the DP legislation the data controller has to respect certain conditions, for example to obtain prior consent from the natural person (the "data subject") before collecting his/her personal data;
2. Personal data should only be collected for **specified, explicit, and legitimate purposes** and not further processed in any way incompatible with those purposes: personal data must be collected for specific, clear, and lawfully stated purposes, which the data controller has to specify to the "data subject";
3. Personal data should be used in an **adequate, relevant, and not excessive way** in relation to the purposes for which they are collected and/or further processed: processing of personal data should be compatible with the specified purposes for which it was obtained (data minimisation principle);
4. Keep personal data **accurate, complete**, and, where necessary, **up-to-date**;
5. **Retain** personal data for **no longer** than is necessary: personal data should not be kept for longer than is necessary for the purposes for which it was obtained;
6. Keep personal data **safe and secure**: the data controller must assure adequate technical, organisational, and security measures to prevent unauthorised or unlawful processing, alteration, or loss of personal data;
7. **No transfer of personal data overseas**: it is prohibited to transfer personal data to any country outside of the European Union and European Economic Area.

[18] Art. 4, n. 2), Regulation (EU) 2016/679.
[19] Art. 4, n. 4), Regulation (EU) 2016/679.
[20] These principles are extrapolated from Regulation (EU) 2016/679.
[21] New EU regulation has required also that personal data are processed in a transparent manner (article 5, Regulation (EU) 2016/679.

The new European Regulation has also added some other principles to correctly manage privacy and data protection rights. These new principles provide as follows:

- Data Controller **accountability**: taking into account the nature, scope, context, purposes, and risks of processing, the Data Controller has to implement **appropriate technical and organisational measures**.[22]
- **Principles of data protection by design and by default**[23] must be applied:
    - **Privacy by design**[24]: The Data Controller, before starting collection and processing of personal data as well as during the processing itself ("the whole life cycle of data"), has to implement **appropriate technical and organisational measures**, such as pseudonymisation, which are designed to implement data protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing. In other words, before starting "working" with personal data, the entire process from the start has to be designed in compliance with the required technical and legal safeguards of data protection regulations (e.g. adequate security);
    - **Privacy by default**: The Data Controller has to implement appropriate technical and organisational measures for **ensuring that, by default, only personal data that are necessary for each specific purpose of the processing are processed**.[25]

More specifically "Privacy by design's" (PbD) core concepts[26] are:

1. Being **proactive not reactive**, preventative not remedial: The "PbD approach is characterized by proactive rather than reactive measures. It anticipates and prevents privacy invasive events before they happen. PbD does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred — it aims to prevent them from occurring. In short, Privacy by Design comes before-the-fact, not after";
2. Having **privacy as the default** setting: "PbD seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice. If an individual does nothing, their privacy still remains intact. No action is required on the part of the individual to protect their privacy — it is built into the system, by default";
3. Having **privacy embedded into design**: "PbD is embedded into the design and architecture of IT systems and business practices. It is not bolted on as an add-on, after the fact. The result is that privacy becomes an essential component of the core functionality being delivered. Privacy is integral to the system, without diminishing functionality";
4. Avoiding the **pretence of false dichotomies**, such as privacy vs. security: "PbD seeks to accommodate all legitimate interests and objectives in a positive-sum win-win manner, not through a dated, zero-sum approach, where unnecessary trade-offs are made. PbD avoids the pretence of

[22] Art. 24, Regulation (EU) 2016/679.
[23] Art. 25, Regulation (EU) 2016/679.
[24] The "privacy by design" approach was developed by the Information and Privacy Commissioner of Ontario, Canada in the mid-1990s, see https://www.ipc.on.ca/wp-content/uploads/2013/09/pbd-primer.pdf and https://www.iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf. Some European Data Protection Authorities directly referred to this approach, even before "Privacy by design" was explicitly provided for in the new European regulation.
[25] For a practical guide on how privacy by design and by default principles can be made concretely and effectively see European Union Agency for Network and Information Security (ENISA), *Privacy and Data Protection by Design: From Policy to Engineering*, December 2014, https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design.
[26] Concepts are extrapolated from PbD approach of the Information and Privacy Commissioner of Ontario, see https://www.ipc.on.ca/wp-content/uploads/2013/09/pbd-primer.pdf.

false dichotomies, such as privacy vs. security – demonstrating that it is possible to have both";

5. Providing **full life-cycle management of data**: "PbD, having been embedded into the system prior to the first element of information being collected, extends securely throughout the entire lifecycle of the data involved — strong security measures are essential to privacy, from start to finish. This ensures that all data are securely retained, and then securely destroyed at the end of the process, in a timely fashion. Thus, PbD ensures cradle to grave, secure lifecycle management of information, end-to-end";
6. Ensuring **visibility and transparency of data**: "PbD seeks to assure all stakeholders that whatever the business practice or technology involved, it is in fact, operating according to the stated promises and objectives, subject to independent verification. Its component parts and operations remain visible and transparent, to users and providers alike. Remember, trust but verify";
7. Being **user-centric and respecting user privacy**: "PbD requires architects and operators to protect the interests of the individual by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options. Keep it user-centric".

It is worth underlining here that for **Law Enforcement Agencies (LEAs)** there are **other requirements and constraints** provided for in Directive 2016/680/EU on processing of personal data for the purposes of the prevention, investigation, detection, or prosecution of criminal offences.[27] ASGARD Deliverable 12.2 should be consulted regarding these privacy constraints and requirements.

4. Notification process and Data Protection Impact Assessment

According to previous legal framework (Directive 95/46/EC), each data controller had to notify its national Data Protection Authority (DPA) of its decision to start collection of personal data before starting this process. This notification aimed at communicating in advance the creation of a new "database," explaining the reasons for and purposes of this, and the technical and organisational safeguards in place to protect the personal data. Consequently, DPAs were enabled to verify the legal and technical safeguards required by EU legislation.

The **new European Regulation** introduces a different way to manage data protection issues, following PbD principles, and not requiring to be registered or notified to data protection authorities[28]. However, Member States can add or specify additional legal requirements or derogations to processing for scientific research purposes.[29] Annex I of this Guide is a list of ASGARD partner countries' national Data Protection Authorities (DPA) with links to their websites and national legislation.

According to the GDPR, each Data Controller has to carry out an assessment of the impact of processing operations on the protection of personal data before starting the processing itself to evaluate the origin,

[27] Directive 2016/680/EU 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA. For security of processing principles for LEAs see article 29.

[28] In particular see Recital n. 89, Regulation (EU) 2016/679.

[29] Art. 89, Regulation (EU) 2016/679.

nature, particularity, and severity of risk[30] attaching to their proposed processing. Such Data Protection/Privacy Impact Assessments (DPIA) can then be utilised to define appropriate measures to assure data protection and compliance with EU legislation.

A DPIA is required in case of:

- Systematic and extensive evaluation of personal aspects in automated processing (e.g. profiling);
- Processing on a large scale of sensitive data or of personal data relating to criminal convictions and offences;
- Systematic monitoring of a publicly accessible area on a large scale.

The main aspects of DPIAs are:

a) Systematic description of processing operations and the purposes of the processing;

b) Assessment of the necessity and proportionality of the processing operations in relation to the purposes;

c) Assessment of the risks to the rights and freedoms of data subjects;

d) Measures to deal with the risks, including safeguards, security measures, and mechanisms to ensure data protection and to demonstrate compliance with EU legislation.[31]

In the event that a DPIA indicates a high risk in terms of data protection and privacy rights, the Data Controller must consult the National Data Protection Authority prior to the processing.[32] Annex II to this Guideline is the ASGARD Data Protection Impact Assessment Template.

5. Novelties in the EU Data Protection Law

Unlike Data Protection Directive[33], the new European Regulation has introduced a novel system of DP rights, where the data subject is the main point around which different guarantees (for data subject) and obligations (for data controller/processor) are set up. The general aim is to avoid data profiling.

There are, at least, four principal novelties:

1. **Profiling**: the EU Regulation has not only defined the term "profiling"[34], but it has also included various restrictions on this activity. Firstly, there is the data subject's right to be informed of "the existence of automated decision making including profiling" and "the significance and the envisaged consequences of such processing"[35]. Secondly, the data subject has the right to restriction of

[30] Art. 35, Regulation (EU) 2016/679.
[31] See Article 29 Data Protection Working Party Group, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, adopted 4 April 2017.
[32] Art. 36, Regulation (EU) 2016/679.
[33] According to Data Protection Directive, data subjects have a general rights "not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work , creditworthiness, reliability, conduct, etc", see article 15, Directive 95/46/EC
[34] See definition above.
[35] Art. 13, 14 and 15, Regulation (EU) 2016/679.

processing[36], to object to processing of personal data[37], and "the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her"[38].

2. **Data Protection Impact Assessment**: in order to better guarantee the protection of these data subject rights, the EU Regulation has introduced the Data Protection Impact Assessment[39], that, with particular reference to profiling, should "be made where personal data are processed for taking decisions regarding specific natural persons following any systematic and extensive evaluation of personal aspects relating to natural persons based on profiling those data"[40].
3. **Anonymisation/Pseudonymisation**: the EU Regulation strongly encouraged data processor and data controller in using anonymisation and pseudonymisation to better protect personal data and retain it[41].
4. **Data Security**: the EU Regulation has defined different obligations for data controller and data processor regarding data security. First of all, they have to assure "sufficient guarantees to implement appropriate technical and organisational measures" to comply with EU DP Regulation and specific measures for "security of processing"[42], using also i.e. anonymisation or pseudonymisation. Moreover, in case of personal data breach, data controller MUST "without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach" to national DP authority[43].

6. ASGARD Data Protection Policy

ASGARD Data Protection Policy is described in Deliverable D.1.1. In this section it is worthy highlighting briefly the main aspects concerning the research activities and the data protection actions put in place in the project.

Whenever an ASGARD research Unit decides to collect **new data and personal data**, after consulting the Societal Ethical Legal Privacy (SELP) Unit, the research Unit:

- (*Eventually*) conducts the **Data Protection Impact Assessment (DPIA)** to identify the risks and adopt the right solution to minimise them. Annex II to this Guideline contains the ASGARD Data Protection Impact Assessment Template.
- In case of collection of personal data, the researcher will explain the purpose and all the information related the process to data subjects. These data subjects, if they agree to participate, can sign the consent and receive copy of the **information notice and the informed consent**. Annex III contains a sample of the information statement for the ASGARD research activities.

In the ASGARD project, the research partners can also use to train and test their tool **datasets already available** in the research community. However, in order to comply with the EU DP rules, each proposed dataset MUST BE verified by the SELP in advance or authorised by the Ethical and Societal Impact Review

[36] Art. 18, Regulation (EU) 2016/679.
[37] Art. 21, Regulation (EU) 2016/679.
[38] Art. 22, Regulation (EU) 2016/679.
[39] See above.
[40] Recital 91, Regulation (EU) 2016/679.
[41] For the definition of anonymisation and pseudonymisation, see above.
[42] Art. 32, Regulation (EU) 2016/679.
[43] Art. 33, Regulation (EU) 2016/679.

Board (ESIRB). SELP will colour each dataset in one of the following **colour-code**:

- Green datasets: low DP risks, these datasets can be used in the ASGARD project;
- Yellow datasets: medium DP risks, these datasets can probably be used after going through the formal ASGARD Ethical Review Process or satisfying other legal requirements (i.e. IPR);
- Red datasets: high DP risks, these datasets CANNOT be used in ASGARD.

This approach is visually described in the ASGARD DATASETS FLOWCHART, available in the Annex IV.

Finally, Data Protection issues could emerge even in some specific events organised by the ASGARD community, such as the hackathons. During these events, not only ASGARD partners can participate, since some external participants could be invited. In this perspective, in order to:

1. Remind all ASGARD partners the importance of guarantee data protection and privacy rights to individuals;
2. and to let be aware of it also the external participants

specific **code of conduct** MUST be signed before the starting of the event. Annex V is a sample of this code of conduct.

ANNEX I. DATA PROTECTION AUTHORITIES (DPA)

EU / MEMBER STATES	EUROPEAN/NATIONAL DATA PROTECTION AUTHORITY WEBSITE	REGULATIONS
European Union	https://edps.europa.eu/edps-homepage_en	**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), available here.
Austria (BMI; AIT; ZRK)	https://www.dsb.gv.at/	Data Protection Act ("ADPA"), available here
Belgium (BFP; NICC)	https://www.dataprotectionauthority.be/	*New regulation under discussion.*
Cyprus (ADITESS)	http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/home_en/home_en?opendocument	*New regulation under discussion.*
Finland (POHA)	https://tietosuoja.fi/etusivu	*New regulation under discussion.*
France (PP; CEA)	https://www.cnil.fr/professionnel	*New regulation under discussion.*
Germany (UKON; L1S)	https://www.bfdi.bund.de/DE/Home/home_node.html	Data Protection Amendment Act ("GDPAA"), available here. However, each German Federal States ('Bundesländer') are approving their federal regulations.
Greece (KEMEA; CERTH)	http://www.dpa.gr/	*New regulation under discussion.*
Ireland (DCU; UCD; IBM)	https://www.dataprotection.ie/docs/Home/4.htm	Data Protection Act 2018, available here
Italy (IT CC; UNIMORE; ENG)	https://www.garanteprivacy.it/	*New regulation under discussion.*
Netherlands (NFI; TNO; UVA)	https://autoriteitpersoonsgegevens.nl/en	GDPR Execution Act ("UAVG", Uitvoeringswet Algemene verordening gegevensbescherming), available here
Portugal (PJ; INOV; PDMFC)	https://www.cnpd.pt/	*New regulation under discussion.*
Spain (GUCI; BSC-CNS; VICOM; AIQ)	https://www.aepd.es/	*New regulation under discussion.*
Sweden (NFC; FOI)	https://www.datainspektionen.se/	Data Protection Act 2018, available here
United Kingdom (CAST; UU)	https://ico.org.uk/	Data Protection Act 2018, available here

ANNEX II. ASGARD DATA PROTECTION IMPACT ASSESSMENT TEMPLATE

FOR THE LASTEST VERSION OF THE ASGARD DATA PROTECTION IMPACT ASSESSMENT TEMPLATE CONSULT HERE.

The following version is a sample.

ASGARD Data Protection Impact Assessment Template (DPIA)

Each ASGARD Research UNIT must first consult the SELP Unit and then fill-in each section of this template before starting the collection of a new dataset.
Please refer to the ASGARD Data Protection Guideline before completing this form.
Remember this template aims to comply with EU Data Protection legislation.

SECTION A - General Information about the Research Unit

Name of ASGARD Research Unit	
Name of the Leader of the Research Unit	
List of people involved in the process	
DPIA Sent Date	
DPIA Date of Approval by SELP (WP12)	

SECTION B - Data Protection Impact Assessment

Step I: Identify the need for a DPIA

Please provide a brief description of the aim(s) of the Work Package or activity and data for processing:

Please identify and explain the purpose(s) of the data processing:

Purpose a: …… Purpose b: …… Purpose n: ……

Step II: Describe the information flow

A. Please identify and describe the provenance of data.

- Will the project involve the collection of **new** information/data about individuals?

YES	NO

****

If YES

a) Identify the type of personal data (See the definition of ASGARD Data Protection Guideline):

	YES	NO
Personal data		
Sensitive data		
Biometric data		
Genetic data		
Anonymised data		
Simulated data		
Open source data		
Linked Open Data		

b) Detail your procedures for data collection (when, how, information sheets, informed consent forms, other documents, etc.):

If NO

i. Will the project involve further processing of previously collected data?

YES	NO

ii. Details on the dataset(s) used or source of the data:

Identify the owner of the dataset(s) (name and important information)	
Is data openly and publicly accessible – open source? (Yes or no)	
Do you have the permission of the owner to use this dataset(s)? (Yes or no)	
Do you have informed consent forms, information sheets, other documents of the previous collection? (Yes or no)	

iii. Identify the type of personal data (See the definition of ASGARD Data Protection Guideline):

	YES	NO
Personal data		
Sensitive data		
Biometric data		
Genetic data		
Anonymised data		
Simulated data		
Open source data		
Linked Open Data		

****

B. Describe the data management process, specifying timelines:

PROCEDURE	SHORT DESCRIPTION	TIMELINE (BEGINNING & END DATES)
Storage		
Retention		
Exchange		
Transfer		
Destruction or re-use		
Data structure and preservation (encryption, etc.)		
Data-merging		
Data processing		

C. Detail your data safety procedures:

List who will have access, use, and process data	1. 2. 3. n.

List and describe briefly safeguards, security measures and mechanisms to ensure data protection.

D. Data transfer:

- Will the project involve further data transfer to **non-EU countries**?

YES	NO

If YES, please detail each data transfer (type of data transferred, country to which it will be transferred and purposes).

Step III: Identify Data Protection Risks

List potential Data Protection Risks:

Risks to individuals (for example damage caused by inaccurate data or a security breach, or upset caused by an unnecessary intrusion on privacy)	1. 2. n.
Risks to organisation/Data Processor (for example damage to reputation, or financial costs or a data breach, not completely compliant with EU regulation)	1. 2. n.

Step IV: Evaluate Data Protection Risks and solutions

Grade each risk (identified above) and describe the actions you could take to reduce the risks (identified above), and any future steps which would be necessary.

Risk	**Grade**: 0 = lower risk 1 = medium risk 2 = high risk	**Solution(s)**	**Result**: is the risk eliminated, reduced, or accepted?	**Evaluation**: is the final impact on individuals/organisation after implementing each solution a justified, compliant, and proportionate response to the aims of the project?

Step V: Check-list questions

Answer the following questions in order to check you have completed this DPIA template correctly. If you are not able to answer them, check what you have filled in the template above.

QUESTIONS		**YES**	**NO**
Have you identified the purpose(s) of the Work Package or activity?			
Have you identified the provenance of data?			
Are you collecting new information/data about individuals?			
If yes	How will you tell individuals about the use of their personal data?		
	If you are relying on consent to process personal data, how will this be collected and what will you do if it is withheld or withdrawn?		
Are you using previously collected data?			
If yes	Have you identified the owner of the datasets or the source of data?		
	(If it may occur) have you obtained the permission by the owner to use these datasets?		
Are you using personal data?			

Are you using anonymised data?			
Are you using simulated data?			
Have you identified the data management process?			
Have you identified the data safety procedures?			
Will the project require you transfer data outside the EU?			
If yes	How will you ensure that data is adequately protected?		
Have you identified Data Protection Risks?			
Have you identified lower risks?			
Have you identified medium risks?			
Have you identified high risks?			
Have you identified the solution(s) for each risk?			

ANNEX III. ASGARD Informed Consent Form

FOR THE LASTEST VERSION OF THE ASGARD Informed Consent Form CONSULT HERE.

The following version is a sample.

Information Sheet and Informed Consent Form of Participants

1. Information regarding the collection, data process and purpose of research

The purpose of this Information Sheet is to inform study participants of the process of collection and retention of his/her personal data for the purpose of this research project in accordance with the General Data Protection Regulation (EU GDPR).

Before signing the following Consent Form, study participants need to read the Information Sheet carefully and if they have any queries, to request additional information from ASGARD researchers.

The Data Controller of ASGARD (VICOMTECH, Spain) should retain one copy of the consent form signed by a representative of VICOMTECH organisation and the participant. The participant should also be given a copy of the consent form as a record of what they have signed.

1.1. Purpose of research

(1) The research project ASGARD (Analysis System for GAthered Raw Data) runs between 01 September 2016 and 29 February 2020, under the European Union's Horizon 2020 Research and Innovation Programme, under the Grant Agreement No. 700381 (*hereinafter*: Project).

(2) The successful conclusion of the Project requires the processing by ASGARD, of those Partners identified in the Grant Agreement, of data which might include personal data, to develop, test and evaluate of video, audio, and text analysis tools.

1.2. Collection Process

(3) In order to realise the deliverables of the research, study participants are invited to voluntarily participate in a recording, described below.

(4) Study participants will …….. (*ie. be recorded in a video, explain the process*) for research purposes only, in order to …….. (*explain the purposes of the research and the method of collection*).

(5) Study participants should be aware of the fact that in this recording the Data Controller is collecting is personal data.

(6) Study participants should be aware that in this recording, the Data Controller is collecting is categorised as sensitive data, such as biometrics - i.e. his/her picture, his/her voice.

1.3 Data Process

(7) The Data Controller is responsible for assuring the confidentiality of study participants. The Data Controller will assure the proper data security standard (technical and organisational) to prevent any data breach.

(8) The Data Controller will share this data only with those ASGARD Partners as identified in the Grant Agreement for research purposes.

(9) There will not be any data transfer to third parties outside the European Union. Data sharing between other European Researchers not involved in the ASGARD Consortium maybe be permitted if agreed under the terms of the Consortium Agreement.

(10) The Data Controller will store this data securely, where access can only be accessed by authorised persons engaged in official business of the Project; for this reason, the data will be password protected.

(11) In any report on the results of the ASGARD project, study participants' identities will remain anonymous.

(12) If any aspect of this Information is unclear, study participants may request additional information from Data Controller, before signing the Informed Consent Sheet and in any time after the participation of this recording. Study participants are entitled to access the information/data they have provided at any time.

(13) The current contact person of VICOMTECH is Juan Arraiza Irujo. His email is jarraiza@vicomtech.org.

2. Consent Form for ASGARD Recording Dataset

[Copy for participant]

Participant Consent Form

Title of research	ASGARD Recording Dataset
Name of researcher	
Organisation	

I have read and understood the **Information Sheet** about this research project and data collection. This information has been fully explained to me and I have been able to ask questions, all of which have been answered to my satisfaction.	**YES** ☐	**No** ☐
I have understood that my participation is voluntary.	**YES** ☐	**No** ☐
I have understood that the ASGARD project will hold all information and data collected securely.	**YES** ☐	**No** ☐
I have understood the purpose of the research and data process and given my consent of collection my personal data.	**YES** ☐	**No** ☐
I have understood the purpose of the research and data process and given my express consent of collection my sensitive personal data.	**YES** ☐	**No** ☐
I have understood that I am entitled to access the information/data I have provided at any time.	**YES** ☐	**No** ☐
I have understood that I am free to contact the contact person identified in the **Information Sheet** to seek further clarification and information.	**YES** ☐	**No** ☐
I have been given a copy of the **Information Sheet** and this completed consent form for my records.	**YES** ☐	**No** ☐

Name and signature of the VICOMTECH representative		
Name and signature of the participant		
Date		

[Copy for ASGARD Consortium]

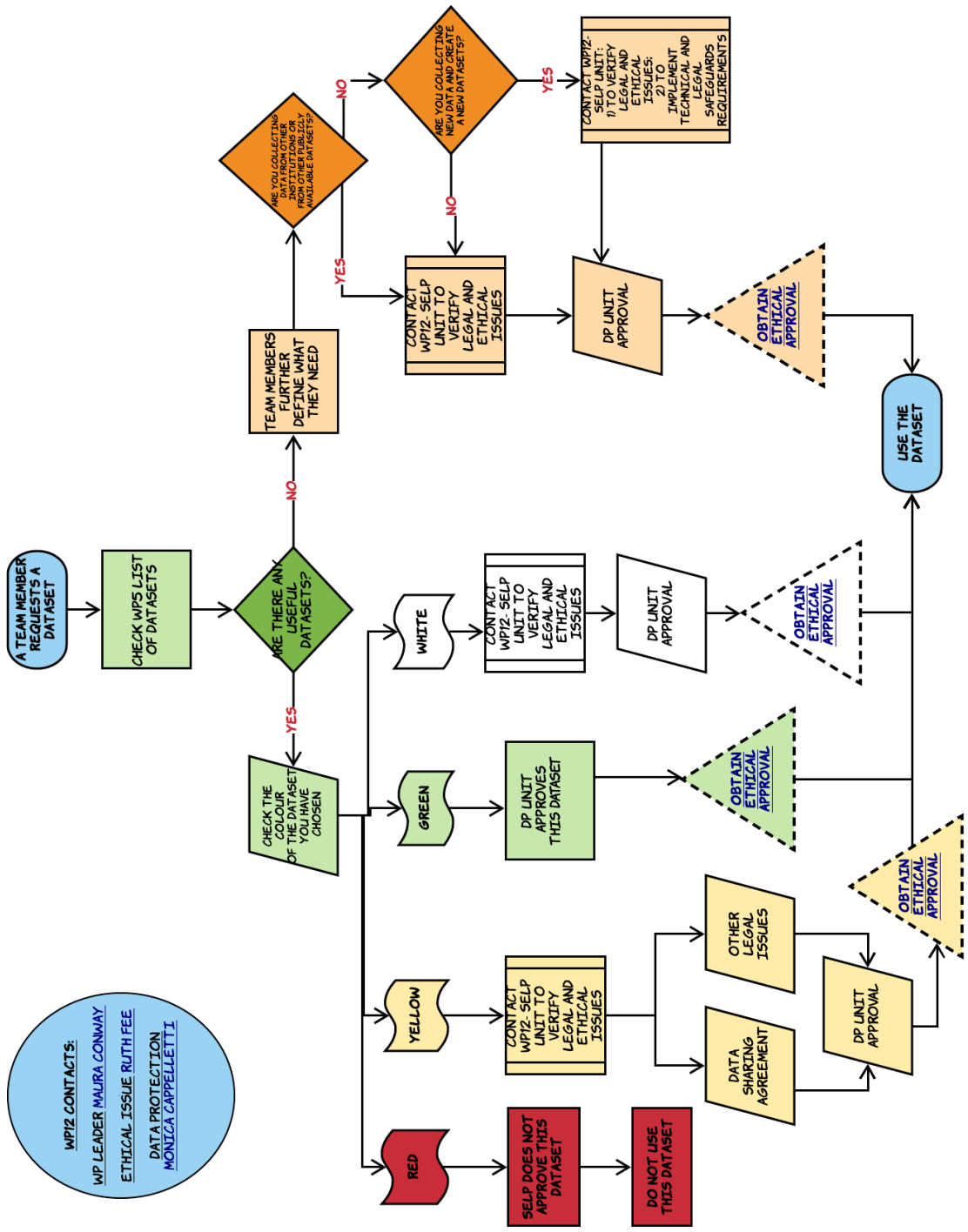
Participant Consent Form

Title of research	ASGARD Recording Dataset
Name of researcher	
Organisation	

I have read and understood the **Information Sheet** about this research project and data collection. This information has been fully explained to me and I have been able to ask questions, all of which have been answered to my satisfaction.	**YES** ☐	**No** ☐
I have understood that my participation is voluntary.	**YES** ☐	**No** ☐
I have understood that the ASGARD project will hold all information and data collected securely.	**YES** ☐	**No** ☐
I have understood the purpose of the research and data process and given my consent of collection my personal data.	**YES** ☐	**No** ☐
I have understood the purpose of the research and data process and given my express consent of collection my sensitive personal data.	**YES** ☐	**No** ☐
I have understood that I am entitled to access the information/data I have provided at any time.	**YES** ☐	**No** ☐
I have understood that I am free to contact the contact person identified in the **Information Sheet** to seek further clarification and information.	**YES** ☐	**No** ☐
I have been given a copy of the **Information Sheet** and this completed consent form for my records.	**YES** ☐	**No** ☐

Name and signature of the VICOMTECH representative		
Name and signature of the participant		
Date		

ANNEX IV. ASGARD DATA PROTECTION FLOWCHART



See ASGARD Data Protection flowchart here.

ANNEX V. ASGARD Code of Conduct Scheme

FOR THE LASTEST VERSION OF THE CODE OF CONDUCT CONSULT HERE.

The following version is a sample.

ASGARD Hackathon Code of Conduct

3. Code of Conduct

This Code of Conduct records the terms and conditions under which the ASGARD Consortium will make available the Data as defined herein during the *XXX* hackathon (*XXX, date XXX*).

All ASGARD Partners who will attend at the hackathon have to sign the Code of Conduct in order to participate at this event.

This Code of Conduct is governed by the CA and GA and that any breaches of the Code of Conduct will be dealt with in line with the penalties outlined therein.

1.3. Purpose of the data sharing

(1) In accordance with all EU laws concerning the protection of individuals with regards to the processing of personal data, the ASGARD Consortium retains control over Data used for the purpose of the research project.

(2) During the hackathon, ASGARD research partners will share Data with all ASGARD partners in order to test and evaluate different tools. This will serve to a) build a framework of best practice in developing and deploying procedures and techniques for data acquisition, processing, fusion, mining, and visualisation; and b) reprioritise and/or redefine the work to be done in the following development cycles (see paragraph 1.1.1 of the DoW).

1.4. Data sharing

(3) The Data to be utilised during the hackathon has been selected by ASGARD partners in compliance with EU legislation and will be used for the purpose of the research project.

(4) Subject to paragraph 2, references made to the use of Data in the hackathon preclude the use of said Data for any other purpose.

1.5. Duties of organisations involved in the data sharing

(5) Subject to paragraphs 3 and 4 above, ASGARD research partners will share the Data with all ASGARD partners in the hackathon contest for the purpose outlined in paragraph 2.

(6) ASGARD partners will use the Data in the hackathon contest for the purposes outlined in paragraph 2 above.

(7) Subject to paragraph 2, ASGARD partners are precluded from using the Data obtained during the course of the hackathon for any other purpose.

(8) Subject to paragraph 2, ASGARD partners will not transfer the Data to any other individual or entity, or permit its use outside the hackathon contest.

(9) In accordance with this Code of Conduct and subject to paragraph 2, ASGARD partners will not link the Data from the hackathon with any other dataset and will not attempt to identify any individual from the Data obtained during the hackathon.

(10) If a LEA partner does inadvertently identify any individual, they will neither record this information nor share the identification of that individual with any other person or entity and will inform the ASGARD Consortium as soon as possible if a breach of this Code of Conduct has occurred.

(11) In accordance with this Code of Conduct, all those participating in the hackathon, agree that Data are considered confidential information. The Data cannot be used, shared, or otherwise divulged outside the hackathon contest.

1.6. Information Governance

(12) Each ASGARD partner is required to sign this Code of Conduct and in so doing, agree to identify those individuals who will participate in the hackathon (see Annex I). For the purpose of this Code of Conduct, those individuals have to be recognised as Authorised Users.

(13) It is the responsibility of ASGARD partners to ensure that its Authorised Users are made aware of and will be bound by terms similar to those in this Code of Conduct so that each of the Authorised Users complies with all relevant duties, obligations and restrictions imposed, in particular, those outlined at paragraphs 6, 7, 8, 9, 10, 11.

(14) Individual **ASGARD partners are required to sign this Code of Conduct before starting the hackathon on *XXXXXX*.**

(15) ASGARD partners that have not signed this Code of Conduct in advance of the hackathon, will be precluded from participating in the hackathon.

For and on behalf of ASGARD partner	……
Signed	……

Print name	……
Position	……
Date	……

4. Annex I: AUTHORISED USERS TEMPLATE

Name of ASGARD partner	……
Name(s) and position(s) of person(s) who intend to participate at the ASGARD hackathon (Authorised Users)	1. …… 2. …… 3. …… 4. …… 5. …… 6. …… 7. …… 8. …… 9. …… 10. ……
Signed	……
Date	……