D2.5 PRIVACY RISK ASSESSMENT FOR ENVISION

Project: Monitoring of Environmental Practices for Sustainable Agriculture Supported by Earth Observation

Acronym: ENVISION

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 869366.

Document Information

Grant Agreement Number	869366	**Acronym**		ENVISION
Full Title	Monitoring of Environmental Practices for Sustainable Agriculture Supported by Earth Observation			
Start Date	1st September 2020	**Duration**		36 months
Project URL	https://envision-h2020.eu/			
Deliverable	D2.5 Privacy Risk Assessment for ENVISION			
Work Package	WP2 Commercial Service Requirements			
Date of Delivery	**Contractual**	30/06/2021	**Actual**	
Nature	Report	**Dissemination Level**		Public
Lead Beneficiary	ETAM SA			
Responsible Author	Maroulla Schiza			
Contributions from	Yiorgos Gadanakis, UREAD			

Document History

Version	Issue Date	Stage	Description	Contributor
D0.1	23.06.2021	Draft	Draft version sent to reviewers for comments and input	Ms. Maroulla Schiza (ETAM)
D0.2	29.06.2021	Draft	Reviewer's comments & input	Yiorgos Gadanakis (UREAD)
F1.0	29.06.2021	Final	Incorporation of comments, finalisation of document	Ms. Maroulla Schiza (ETAM)

Disclaimer

This document and its content reflect only the author's view, therefore the EASME is not responsible for any use that may be made of the information it contains!

The ENVISION project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 869366

CONTENT

The ENVISION project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 869366

LIST OF TABLES

The ENVISION project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 869366

Terms & Definitions

data subject: an identified or identifiable natural person

personal data: any information relating to an identified or identifiable natural person (data subject)

sensitive data: personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or 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

processing: any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means (e.g., collection, recording, organisation, structuring, storage, dissemination, erasure)

controller: the natural or legal person which, alone or jointly with others, determines the purposes and means of the processing of personal data.

processor: a natural or legal person which processes personal data on behalf of the controller.

profiling: 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.

consent: any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, signifies agreement to the processing of personal data relating to him or her.

personal data breach: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

supervisory authority: a supervisory authority which is concerned by the processing of personal data.[1]

[1] https://www.privacy-regulation.eu/en/article-4-definitions-GDPR.htm

The ENVISION project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 869366

1 Introduction

Privacy and data protection is major challenge that needs to be addressed by EU funded projects given their collaborative nature. The General Data Privacy Regulation (GDPR) defines personal data as any information which is related to an identified or identifiable natural person. To this end any information that could individually or collectively lead to the identification of a natural person directly or indirectly (i.e., name, address or location data, identification number, commercial identity, IP address, etc.) are personal data.

All data collected must be kept secure and inaccessible to unauthorized persons. These data need to be handled with appropriate confidentiality and technical security, as required by National and European Union (EU) legislation and recommendations.

A privacy risk assessment is performed to safeguard that possible privacy breaches can be detected and facilitate informed decision-making that will minimize possible privacy risks and problems. Since the early stages of the ENVISION project, a proactive approach was adapted in minimizing possible negative impacts on the level of privacy and data protection, as well to consider the necessary measures to mitigate the identified risks.

The deliverable at hand presents an Overview of the Personal Data Framework presenting the basic EU and National legislation, as well as the personal data handled within the project. The next chapter presents the privacy risk assessment definition and characteristics and the methodological framework used to perform the privacy risk assessment. Finally, risks and mitigation measures are presented in detail.

The ENVISION project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 869366

2 Overview of the Personal Data Framework

2.1 The European Legislation

Common EU rules have long been established to safeguard that personal data receive a high level of protection across the EU. Several principles have been introduced over time including lawfulness, consent, purpose binding, necessity and data minimization, transparency and openness, accountability and privacy by design.
The European Directive 95/46/EC was the governing law on the processing of personal data in the EU that was replaced by the GDPR as of May 25, 2018. The Directive 95/46/EC envisaged that organisations which collect and further process personal data were obliged to ensure that technical and organisational measures are undertaken, to protect the data with an appropriate level of security. These minimum standards had to be implemented by national legislation in each EU Member State. This gave Member States the option to extend the scope of the Directive, retain pre-existing higher standards, or opt out of taking full advantage of derogations, which explains why different data protection standards that applied across European Countries2.

The GDPR was adopted as a Regulation (EU) 2016/679 of the European Parliament and of the Council on April 27, 2016. More specifically, in contrast to the Data Protection Directive, the GDPR is intended to apply directly in each EU Member State without the need for implementing legislation, and to create a framework within which more detailed rules can be made. This harmonizes the legislation across Europe. The GDPR, strengthens obligations both for the data controllers and processors, following a risk-based and impact-driven approach. Such an approach should enable organizations to identify and assess the risks, likelihood, and impact of potential breaches of confidentiality, integrity, and availability of personal data, and support them in adopting the necessary security measures.

The GDPR has been effective on a European level since the 25th of May 2018 and EU countries were required to implement it in the National Legislation. National legislation in the consortium countries relative to personal data protection is presented in the following[3]:

BELGIUM: Act of 30 July 2018 on the Protection of Natural Persons with Regard to the Processing of Personal Data.
CYPRUS: Law 125(I) of 2018 Providing For The Protection of Natural Persons with respect to the Processing of Personal Data and for the Free Movement of Such Data.
GREECE: Law 4624/2019 on the Personal Data Protection Authority, Implementing the General Data Protection Regulation (Regulation (EU) 2016/679) and Transposing into National Law Data Protection Directive with Respect to Law Enforcement (Directive (EU) 2016/680) and Other Provisions.
LITHUANIA: Law No XIII-1426 of 30 June 2018 amending Law No I-1374.
SERBIA: Law on Protection of Personal Data (Official Gazette of the Republic of Serbia, No. 87/2018 (9-11-2018).

2 https://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf
3 https://www.dataguidance.com/

The ENVISION project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 869366

SLOVENIA: The Personal Data Protection Act 2004 is presently enforced. Slovenia has not yet adopted the new Personal Data Protection Act that fully implements the GDPR.
UK: The Data Protection Act 2018.

2.2 Personal data within ENVISION

According to the Data Management Plan, the ENVISION project handles the following types of Data presented in Table 1.

Table 1: Types of data per Work Package

WP	Types of data	Legal Restrictions
WP1	Personal data of consortium	GDPR
WP2	Personal data of users & consortium	GDPR
WP3	Farmers' data personal data, declaration, farm information EO Data Vector Data Laboratory Analyses	GDPR Open data Legal licenses
WP4	Personal data of users Testing procedures related data EO Data Vector Data	GDPR Open data Legal licenses
WP5	Personal data of users	GDPR
WP6	Foreground knowledge	Consortium Agreement
WP 7	Personal data of users & consortium	GDPR

All data produced in the project will be available to the Consortium throughout its lifetime. Appropriate licensing agreements will be required for data reuse after the project's conclusion, which will be defined through the business model report during the course of the project.

The following table maps the personal data processed by the ENVISION project per processing operation. Their analysis is based on Articles 4 and 9 of the General Regulation on Personal Data Protection (EU) 2016/679.

The ENVISION project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 869366

Table 2: Data mapping per processing operation

No	PROCESSING OPERATION	TYPE OF DATA	DATA SUBJECTS	DATA SOURCE	ACCESS	STORAGE PERIOD	PROCESSING PURPOSE	EXISTING PROTECTIVE MEASURES
1	Personal data of users - **PROJECT MANAGEMENT**	Contact Information	CONSORTIUM MEMBERS	CONSORTIUM MEMBERS	CONSORTIUM MEMBERS (ALL)	PROJECT LIFETIME	PROJECT MANAGEMENT	TECHNICAL & ORGANISATIONAL SECURITY MEASURES PRIVACY POLICY CONSORTIUM AGREEMENT
2	Personal data of users & consortium - **COMMERCIAL SERVICE REQUIREMENTS**	Contact Information of users and digital recordings, anonymized gender data	CONSORTIUM PARTNERS, USERS	END USERS OF ENVISION SERVICES CONSORTIUM MEMBERS	WP2 TASK LEADERS (UREAD, ETAM)	PROJECT LIFETIME	USER STORIES GENDER CONSIDERATIONS	TECHNICAL & ORGANISATIONAL SECURITY MEASURES PRIVACY POLICY CONSENT FORMS IMPLEMENTATION OF INFORMATION SECURITY MANAGEMENT SYSTEM DATA ANONYMISATION
3	Farmers' personal data, declaration, farm information - **EARTH OBSERVATION DATA PRODUCTS**	Farmers' personal data, declaration forms, farm information	FARMERS	PAs & CBs - FARMERS	TASK 3.2 LEADERS (NOA, EL ILVO, Agroapps) & Pas / CBs	PROJECT LIFETIME	IMPLEMENTATION AND VALIDATION OF BUSINESS CASES	PRIVACY POLICY (project, PAs & CBs) IMPLEMENTATION OF INFORMATION SECURITY MANAGEMENT SYSTEM DATA ANONYMISATION
4	Personal data of users - **ENVISION SERVICE**	Users contact data including emails and passwords	PLATFORM USERS	END USERS OF ENVISION SERVICES	TASK 4.2 LEADER (DRXS)	PROJECT LIFETIME	OPERATION OF ENVISION PLATFORM	TECHNICAL & ORGANISATIONAL SECURITY

No	PROCESSING OPERATION	TYPE OF DATA	DATA SUBJECTS	DATA SOURCE	ACCESS	STORAGE PERIOD	PROCESSING PURPOSE	EXISTING PROTECTIVE MEASURES
								MEASURES PRIVACY POLICY CONSENT FORMS ENCRYPTION MECHANISMS
5	Personal data of users - **BUSINESS CASES IMPLEMENTATION AND EVALUATION**	Users contact data + digital recordings	END USERS	END USERS OF ENVISION SERVICES	WP5 LEADER (ILVO)	PROJECT LIFETIME	ENALUATION OF ENVISION SERVICE / PRODUCTS	TECHNICAL & ORGANISATIONAL SECURITY MEASURES PRIVACY POLICY CONSENT FORMS
6	Personal data of newsletter recipients & project stakeholders- **DISSEMINATION AND COMMUNICATION**	Subscribers and project stakeholders contact data	PROJECT NEWSLETTER SUBSCRIBERS AND STAKEHOLDERS	PROJECT NEWSLETTER SUBSCRIBERS AND STAKEHOLDERS	WP7 LEADER (ITC)	PROJECT LIFETIME	DEVELOP AND IMPLEMENT EFFECTIVE DISSEMINATION AND COMMUNICATION	TECHNICAL & ORGANISATIONAL SECURITY MEASURES PRIVACY POLICY CONSENT FORMS

The ENVISION project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 869366

The Project involves personal data collection and/or processing mainly of contact information. The data will be collected for internal use in the project, and not intended for long-term preservation. The data retention period is defined as the project's lifetime and all original data will be erased after the end of the project. Furthermore, the Consortium partners handling personal data pay special attention to security and respect the privacy and confidentiality of the natural persons by fully complying with the applicable national, European, and international framework, and the European Union's GDPR 2016/679. It needs to be noted that partners are implementing technical and organisational measures that enable information security.

The participation of users / data subject in ENVISION project is voluntary but nonetheless, informed consent will be sought from each individual user before his or her data is even stored. All data subjects are adults and therefore no issues on handling data of children are raised. The general framework by which data collection, storage, protection, retention and destruction is performed by Partners complies with consortium countries national legislation and the GDPR. This applies in all processing operations and consent is collected by the partners responsible for each task whilst the rights of the data subjects are clearly communicated.

The ENVISION consortium provides precise information on what type of personal data they process, how it is processed and which data-flows they enable. Owners of personal data will be able to withdraw their consent for processing their personal data. All partners carry out a personal information assessment in their own context concerning their own collection, storage and/or processing of personal data, prior to the collection of personal data in the frames of the project. They additionally take measures that assure information systems safety. Each partner is liable for inappropriate security at its own premises.

In terms of data retention and destruction, data will be deleted or fully anonymised as soon as the relevant purpose as stated in the DoA is fulfilled. Regarding data processing, the collected data are immediately pseudonymised and aggregated, and the original data will not be stored whatsoever. Furthermore, ENVISION has prepared a "Personal Data Protection Policy" and "Terms and Conditions" documents, in order to inform the users of the purposes of data collection.

Processing of 'special categories' of personal data takes place in WP2, and specifically for the elaboration of the Gender Situation Analysis and Needs Assessment and concerns the consortium's personal data. The necessary data were collected in an anonymised form to minimise risk. These data were not stored but were used upon receiving to produce statistical results. The data produced by the input provided cannot divulge the personal information of a specific member of the Consortium. Additionally, the collection of data had received clearance and were monitored by the Information Security Officer that had been appointed.

Databases owned by PAs & CBs that are to be used for the development of the ENVISION service need to be investigated further. Within these databased there is clear distinction between data that do not contain personal data (pure parcel data) or data that do (farmer data that can lead to farmer identification). Farmer data are considered sensitive mainly due to the size of the databases. To this end the PAs and CBs that are owners of these databases will need to conduct a "Privacy Risk Analysis" that will examine the types of data that will be needed for the project, the scope of processing, the size of the databases, the anonymization / pseudonymization methodologies and the residual risks and mitigation measures. This process will require partners' DPOs (Data Protection Officer) approval following GDPRs requirements.

3 Privacy Risk Assessment

3.1 Definition and characteristics

A Privacy Risk Assessment may be defined as a systematic process that provides an early warning system to detect privacy risks. A Privacy Risk Assessment can enhance the information available internally to facilitate informed decision-making, avoid costly mistakes in privacy compliance, and provide evidence that an organization is taking measures to minimize its privacy risks and problems.

The GDPR requires the conduction of a Data Privacy Risk or/and Impact Assessment where processing is likely to result in a high risk to the rights and freedoms of natural persons. This includes cases of automated processing, large scale processing of special data, and systematic, large scale monitoring of a public area.

The GDPR though cannot guarantee though the elimination of possible risks if it is not properly implemented, monitored and enforced. At the same time state-of-the-art technology plays an integral role by offering practical privacy protection tools that support the application of legal provisions.

The Data Protection Risk Assessment (DPRA) and the Data Protection Impact Assessment (DPIA) process are distinct parts of the Risk-based approach. "Risk" means "a working hypothesis that describes an event and its consequences, which have been assessed in terms of severity and probability of occurrence". According to the GDPR, attention should be paid to risks that are presented by processing, i.e., accidental or unlawful destruction, loss, alteration, unauthorised disclosure, or access to personal data transferred, stored or otherwise processed which could lead to in physical, material or non-material damage to the data subjects.
With a risk assessment we identify at a first stage the potential risks and evaluate them in terms of their degree, i.e. the severity of the impacts on the subjects and the likelihood of occurrence of the identified risks.

In cases where the processing operations pose a low risk to the data subjects, the controller must consider whether the risk is managed in accordance with existing measures and whether to take further mitigation measures. On the other hand, in the event that the risk assessment identifies acts that may pose a "high risk" to the rights and freedoms of the subjects, the controller must, after consulting the Data Protection Officer (DPO), conduct an impact assessment (DPIA).
In accordance with the GDPR regulatory framework and the Article 29 Working Group guidelines, an Impact Assessment is not necessary if the Risk Assessment shows that the processing operations are unlikely to pose a "high risk" on the rights and freedoms of data subjects. As the Working Party of Article 29 points out, based on paragraph a.35, risk is assessed on the basis of nine criteria out of which at least two must be met at the same time (see next chapter) to pose a high risk. As ICO (Information Commissioner's Office - UK) points out, especially in cases where the processing is based on the legal obligation the DPIA is not necessary once a Risk Assessment (RA) has proceeded.

The ENVISION project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 869366

3.2 Methodological framework

According to the GDPR, typical "high risk" incidents are processing operations that include:

- systematic and comprehensive evaluation of personal aspects of natural persons, which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person,
- large-scale processing of specific categories of data (sensitive personal data) referred to in Articles 9 and 10 of the GDPR (i.e., political views, religion, sex, genetic data, health, criminal offences, etc.),
- systematic surveillance (video recordings) of publicly accessible space on a large scale (i.e., workplace surveillance, external security cameras, etc.) and
- processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or (c) a systematic monitoring of a publicly accessible area on a large scale.

To clarify the "high risk" incidents of Article 35 of the GDPR, the “Article 29 Working Group” has developed nine (9) criteria that indicate the cases where processing may pose a high risk to the rights and freedoms of subjects. These criteria refer to processing operations that include:

1. Evaluation or rating of customers, employees and other individuals in relation to job performance, creditworthiness, financial situation, health, preferences and so on.
2. Making automated decisions that may lead to exclusion or discrimination against individuals.
3. Systematic monitoring for the observation or control of data subjects through networks, which may be collected without the subjects being aware of who collects them and how they will use them, or it is impossible for the subjects to avoid processing because they receive country in a publicly accessible area.
4. Sensitive data related to privacy activities such as electronic communications or affecting the exercise of fundamental rights by subjects such as freedom of movement or because their violation may have serious consequences for the subject's daily life such as financial data that could be used in payment fraud.
5. Large-scale processing of data based on the number of subjects, the volume or range of data, the duration of the activity and the geographical extent of the processing.
6. Assigning or combining data sets resulting from more than one processing operation, for different purposes or from different controllers in a way that exceeds the subject's reasonable expectations regarding their use.
7. Vulnerable data subjects who are in an unequal power relationship with the controller in the sense that the subjects may not be able to consent or easily oppose the processing (i.e., children, employees, patients, the elderly, etc.).
8. New technologies that may have an impact on the underlying personal and social implications, such as the combined use of fingerprints, the use of smart technology systems, face recognition for improved physical access control, internet of things applications, etc.
9. When the processing itself is intended to allow, modify or deny data subjects access to a service or contract (i.e., loans).

The ENVISION project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 869366

Following the aforementioned criteria, the identification of potential risks for each processing operation is based on:

- ☑ the category of data: it is examined whether the processing operation contains "sensitive" personal data or other data resulting from their processing out of which risks may arise for the subjects[4].
- ☑ data subjects: regarding whether processing includes "sensitive" data subjects[5].
- ☑ the source of the data: it is assessed whether the source of the data is the subjects themselves or not, in order to assess whether the processing is in line with the reasonable expectations they have for the processing of their data and to determine the obligations of the Controller to the subjects[6].
- ☑ data access: the number and status of people who have access to the data is looked into. Restricting access to data by the controller reduces the likelihood of risks occurring.
- ☑ data retention period: assesses whether a specific data retention period has been set. This aspect affects the processing scale[7].
- ☑ the purpose of the processing: it is examined whether the purpose of the processing is in line with the reasonable expectations of the data subjects in conjunction with the legality and necessity of the processing[8].
- ☑ its legal basis: the legality of the processing is examined and its necessity is assessed[9].
- ☑ existing data protection measures: the adequacy of the existing protection measures taken by the controller and the need for additional risk mitigation measures are assessed.

Once the potential processing risks have been identified, they are examined on the basis of the nine (9) criteria of the Article 29 Working Group to determine whether a processing operation poses a high risk to the data subjects and to assess the **severity** of the impacts on the subjects. At the same time, from the assessment of the vulnerability of the existing protection measures as well as the nature of the threat, the likelihood and the consequence of the risk occurring is estimated. Finally, considering the consequences and likelihood of the risk, the degree of risk of the respective processing operation is determined and, if necessary, the risk mitigation measures are determined.

4 Article 9-10 and recitals 51, 53, 71 and 75, GDPR.
5 Recital 75, GDPR and Article 29 Working Group, 9. 12.
6 Article 13, 15 and Recital 50, GDPR.
7 ICO, p. 23.
8 Recital 50, GDPR.
9 Article 6, GDPR.

The ENVISION project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 869366

The methodological framework to determine risks' consequence and likelihood is presented in the following:

1. **Assessing the Consequence of risk on data subjects**

The severity of risk is assessed using three criteria, which were developed in reference to the content of article 83 of the GDPR on risk assessment. These criteria are:

- Threat to life (bodily harm)
- Financial Loss (material damage)
- Damage to reputation (non-tangible damage)

For each of the above criteria the scale Low = 1, Medium = 2 and High = 3 is defined and evaluated as indicated in the table below:

Table 3: Determinants of Risk Consequence

Consequence	Threat to life	Financial Loss	Damage to reputation
High	Death	Destruction of assets	Non-monetary damage at an international level Disclosure of sensitive data (health, sexuality, political and religious beliefs, etc.)
Medium	Serious accidents Physical injury	Loss of assets	Moral damage at national level. Disclosure of financial data.
Low	Annoyance of the subject	Unauthorized disclosure of data	Moral damage at the local level. Disclosure of identity data.

<u>The consequence of the risk is considered:</u>

High (= 3) if at least 2 criteria are assessed as highly consistent
Medium (= 2) if at least 2 criteria are rated as of medium consistency, or one criterion is rated as high consistency regardless of whether the other two are medium or low
Low (= 1) if all criteria are evaluated as of low consistency or only one criterion is of medium consistency

The ENVISION project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 869366

2. **Assessing the likelihood of risks occurring**

Respectively, the likelihood of occurrence of the risk is evaluated using the following criteria:

- Limited access
- Limited storage period
- Adequate Security Measures

For each of the above criteria the scale Low = 1, Medium = 2 and High = 3 is again defined and the criteria are assessed as indicated in the table below:

Table 4: Determinants of Risk Likelihood

Likelihood	Limited access	Limited storage period	Adequate Security Measures
High	Not set	Not set	They do not exist
Medium	Possibility of access by persons outside the permanent staff of the Controller (external collaborators, contractors, subcontractors, etc.)	Some but long lasting	There are some measures
Low	Access by a few authorized persons	Limited period	Adequate Measures

The likelihood of the risk occurrence is considered:

High (= 3) if at least 2 criteria are assessed as highly consistent
Medium (= 2) if at least 2 criteria are rated as of medium consistency, or one criterion is rated as high consistency regardless of whether the other two are medium or low
Low (= 1) if all criteria are evaluated as of low consistency or only one criterion is of medium consistency

3. **Determination of final risk (risk possibility)**

The final risk is evaluated by combining the severity, consequence and likelihood of occurrence of each risk, multiplying the number corresponding to each characterization (High = 3, Medium = 2, Low = 1).

The ENVISION project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 869366

The following table is used to assign the above values to the final risk category:

Table 5: Final Risk Determination Matrix

Severity X Consequence			
9	9	18	27
6	6	12	18
4	4	8	12
3	3	6	9
2	2	4	6
1	1	2	3
	1	2	3
	Likelihood		

The final risk is considered:

High: if the product is equal to or greater than 18 and immediate risk management measures need to be taken.
Medium: if the product is equal to or greater than 8 and less than 18, further organizational and technical measures must be taken to limit the degree of the risk.
Low: if the product is less than 8 and further risk mitigation measures may be taken.

The ENVISION project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 869366

3.3 ENVISION Privacy Risk Assessment

Following the aforementioned methodology Table 6 presents in detail the procedure for determining the degree of risk for each processing operation of ENVISION that carries personal data.

Table 6: ENVISION Privacy Risk Assessment

PROCESSING OPERATION	SEVERITY											CONSEQUENCE					LIKELIHOOD					FINAL RISK	
	Evaluation or grading of personal aspects	Making automated decisions with legal or significant results for the subjects	Systematic monitoring	Sensitive data	Large-scale data processing	Assign or combine data sets	Data concerning vulnerable subjects	Application of new technologies	Processing that prevents subjects from exercising a right or using a service or contract	TOTAL SEVERITY	SEVERITY ASSESSMENT (H_3 - M_2 -L_1)	Threat to life	Financial Loss	Damage to reputation	TOAL RISK CONSEQUENCE SCORE	RISK CONSEQUENCE ASSESSMENT (H_3 - M_2 - H_1)	Limited access	Limited storage period	Adequate Technical Safety Measures	TOTAL RISK LIKELIHOOD SCORE	RISK LIKELIHOOD ASSESSMENT (H_3 - M_2 -L_1)	TOTAL SCORE	FINAL RISK (H_3 - M_2 -L_1)
Personal data of users - **PROJECT MANAGMENT**	1	1	1	1	1	1	1	1	1	9	1	1	1	1	3	1	1	2	1	4	1	1	LOW
Personal data of users & consortium - **COMMERCIAL SERVICE REQUIREMENTS**	1	1	1	2	1	1	2	1	1	11	2	1	1	1	3	1	2	2	1	5	2	4	LOW
Farmers' personal data, declaration, farm information - **EARTH OBSERVATION DATA PRODUCTS**	1	1	1	2	2	1	1	1	1	11	2	1	2	1	4	1	2	2	1	5	2	4	LOW
Personal data of users - **ENVISION SERVICE**	1	1	1	1	1	2	1	2	1	11	2	1	1	1	3	1	1	2	1	4	1	2	LOW
Personal data of users - **BUSINESS CASES IMPLEMENTATION AND EVALUATION**	1	1	1	1	1	1	1	1	1	9	1	1	2	1	4	1	1	2	1	4	1	1	LOW
Personal data of users & consortium - **DISSEMINATION AND COMMUNICATION**	1	1	1	1	1	1	1	1	1	9	1	1	1	1	1	1	1	2	1	4	1	1	LOW

From the results (final risk) of the Privacy Risk Assessment, it becomes clear that the processing operations carried out by the project do not correspond to the above criteria and therefore do not seriously threaten the rights and freedoms of their subjects. However, in the event of changes affecting the nature, scope and purposes of the existing processing operations, the ENVISION project and more specifically partners that own personal data will have to reassess the risks that such changes pose and consequently re-evaluate the need for an DPIA for some of them.

4 Risks and mitigation measures

This chapter presents possible privacy risk events and their mitigation measures. For every potential risk event the possibility and mitigation measures are specified. Risk events are also assigned to the project's processing operations.

Table 7: Risk events and mitigation measures

Risk Event	Possibility	Processing Operation	Mitigation measure
Breach of the Responsibility of the controller	LOW	Project Management Commercial Service Requirements Earth Observation Products ENVISION Service Business Cases Implementation and Evaluation Dissemination and Communication	The Consortium implements appropriate technical and organisational measures to ensure information security and to be able to demonstrate that processing is performed in accordance with legislation. The project's Privacy Policy summarises the Consortium's responsibilities. Partners comply with GDPR and national legislation and follow appropriate procedures.
Failure to protect data by design and by default	LOW	Project Management Commercial Service Requirements Earth Observation Products ENVISION Service Business Cases Implementation and Evaluation Dissemination and Communication	The project partners have implemented appropriate technical and organisational measures for ensuring that, by design and default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. A number of partners of the consortium have implemented an approved certification scheme (ISO 27001) that demonstrates compliance with the requirement. Partners comply with GDPR and national legislation and follow appropriate procedures.

The ENVISION project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 869366

Risk Event	Possibility	Processing Operation	Mitigation measure
Personal data retained longer than necessary	LOW	Project Management Commercial Service Requirements Earth Observation Products ENVISION Service Business Cases Implementation and Evaluation Dissemination and Communication	Personal data are stored for a specific period that is already defined as the lifetime of the project. The need for a limited retention period is communicated to the partners and the data controllers have taken proper measures. All partners are fully compliant to the applicable National and European legislation.
Data accessed by unauthorized personnel	LOW	Project Management Commercial Service Requirements Earth Observation Products ENVISION Service Business Cases Implementation and Evaluation Dissemination and Communication	Partners assign access rights to specific team members. Partners that handle sensitive personal data have appointed an Information Security Officer or a DPO to safeguard access rights. All partners are fully compliant to the applicable National and European Union legislation.
Lack of data subjects' consent	LOW	Commercial Service Requirements ENVISION Service Business Cases Implementation and Evaluation Dissemination and Communication	All partners processing personal data have the responsibility to collect consent forms from the data subject. The consent forms clearly present the data collected and the scope of the process, informing data subjects on their rights according to the GDPR (e.g., right to withdraw consent, erasure, data portability).

The ENVISION project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 869366

Risk Event	Possibility	Processing Operation	Mitigation measure
Failure to satisfy the data subjects rights	LOW	Commercial Service Requirements ENVISION Service Business Cases Implementation and Evaluation Dissemination and Communication	Data subjects' rights to Information, Access, Rectification, Erasure, Restriction of Processing, Data Portability, Object, Avoid Automated Decision-Making are safeguarded. The consortium and specifically partners that process personal data in the frames of the tasks they participate have taken proper technical and organizational measures that ensure such a risk is mitigated. Naming conventions are used to easily trace data files containing personal data, access is given to data controllers, data are safely stored and can be located with appropriate keywords to facilitate processing for exercising the users' rights. All data subjects are informed of their rights.
The technical systems of the partners lead to a security breach	LOW	Project Management Commercial Service Requirements Earth Observation Products ENVISION Service Business Cases Implementation and Evaluation Dissemination and Communication	Partners are compliant to the technical measures necessary to safeguard the security of information. Different processes and controls like user access management, network security management, protection from malware, system and application access control mitigate the possible risks of a security breach.

The ENVISION project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 869366

Risk Event	Possibility	Processing Operation	Mitigation measure
The platform design or the technical systems of the partners lead to a security breach	LOW	ENVISION Service	The platform will protect personal data by design and by default. Data registered on the platform will not be accessible from outside. The database will not be discoverable to other network machines operating ton the same LAN, VLAN with the database server or other networks. Only ENVISION technical team members will be granted access rights. Access to the platform will only be granted to registered users. The data produced by the platform are personal and will not be shared with others without users' permission. A Privacy Policy, Terms of Use and Consent form will be applicable for the platform.
Unlawful data transfer	LOW	Project Management Commercial Service Requirements Earth Observation Products ENVISION Service Business Cases Implementation and Evaluation Dissemination and Communication	In cases of transfer of personal data (i.e., databases) the controller examines risks through a DPIA. The controller provides the data subject the identity and the contact details of the controller and the data protection officer, as well as the purposes of the processing for which the personal data are intended and the legal basis for the processing. The rights of the data owner are also communicated.

The ENVISION project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 869366

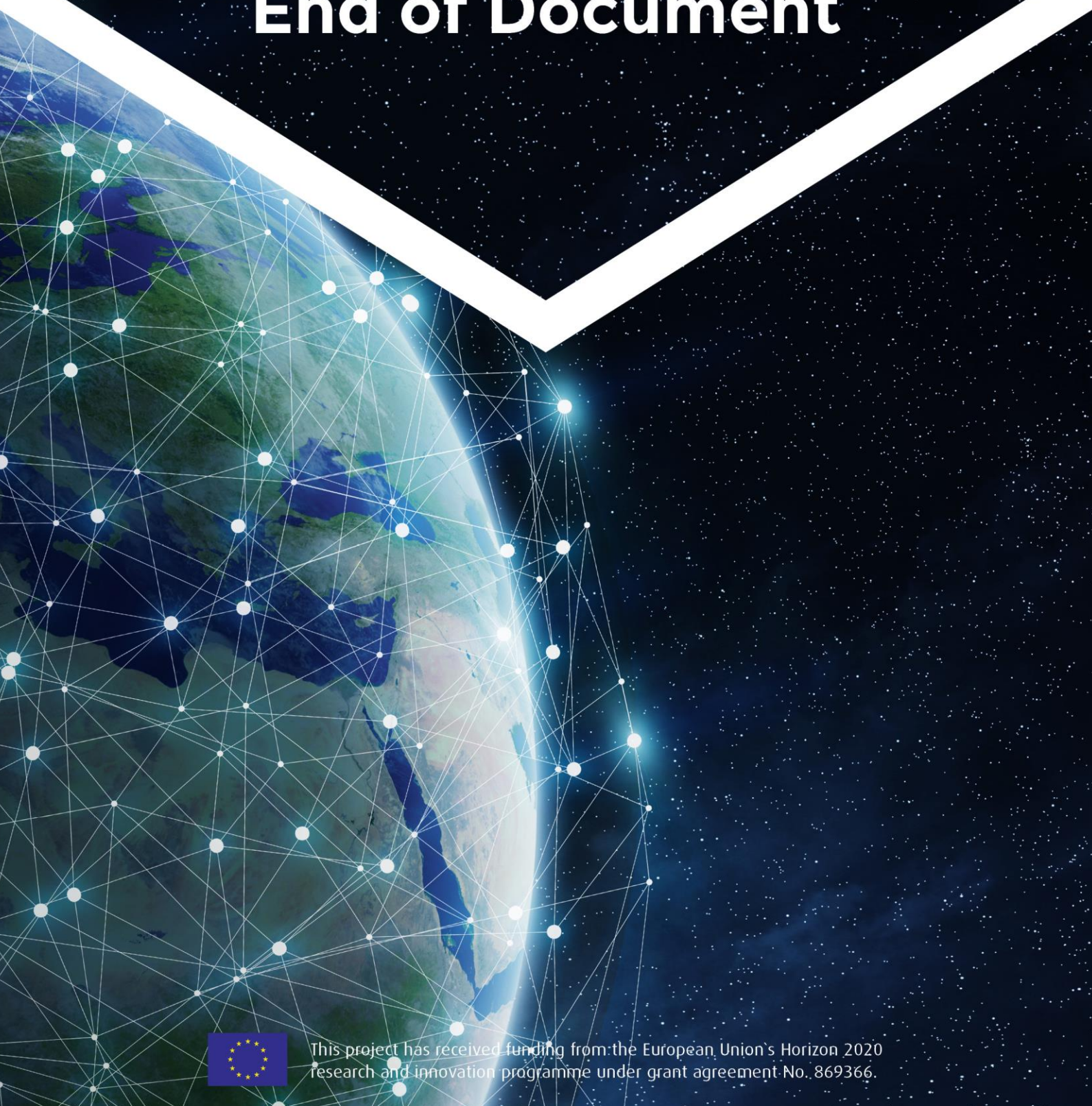
Risk Event	Possibility	Processing Operation	Mitigation measure
Personal data breach	LOW	Project Management Commercial Service Requirements Earth Observation Products ENVISION Service Business Cases Implementation and Evaluation Dissemination and Communication	The controller follows the procedure described in the GDPR and without undue delay and not later than 72 hours after having become aware of it, notifies the personal data breach to the supervisory authority, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. The controller documents any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken.
Improper storage, publishing, and re-use of personal data	LOW	Project Management Commercial Service Requirements Earth Observation Products ENVISION Service Business Cases Implementation and Evaluation Dissemination and Communication	Personal data will be stored in secure servers and will not be published or re-used under any circumstances, whilst anonymisation and cryptographic controls are implemented. Access rights to personal data are awarded to trained personnel and technical security measures are in place.

The ENVISION project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 869366

The ENVISION project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 869366

envision

End of Document



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 869366.