CYBERHIMPREX
Cybersecurity of Healthcare Improved in a X-border perspective

Project Title	**Cyber**security of **H**ealthcare **Impro**ve**d** in a **X**-border perspective
Project Acronym	CYBERHIMPREX
Project Number	101101322
Type of instrument	DIGITAL-SME Digital SME Support Actions
Topic	DIGITAL-2022-CYBER-02-SUPPORTHEALTH-Support To Cybersecurity In The Health Sector
Starting date of Project	01/01/2023
Duration of the project	24
Website	https://cyberhimprex.policlinicogemelli.it

D1.4 Approach to Data Protection Impact

Work Package	WP 1 Project Coordination
Lead author	Lorenzo Marchesi (UCSC)
Contributors	Fabio Rizzoni (FPG), Pasquale Mari (FPG), Salvatore Agnes (UCSC), Mariano Alberto Pennisi (UCSC), Justyna Karolina Kielar (UCSC)
Peer reviewers	Saverio Caruso (FPG), Aimilia Magkanaraki (7HCR), Diana Navarro Llobet (FPHAG)
Version	V1.0
Due Date	30/06/2023
Submission Date	30/06/2023

Dissemination Level:

x	PU — Public
	SEN — Sensitive
	R-UE/EU-R — EU Classified
	C-UE/EU-C — EU Classified
	S-UE/EU-S — EU Classified

The work described in this document has been conducted within the CYBERHIMPREX project. This project has received funding by the European Union Digital Europe Programme (DIGITAL) under grant agreement No. 101101322.

Version History

Revision	Date	Editor	Comments
0.1	20/06/2023	Lorenzo Marchesi (FPG)	
0.2	25/06/2023	Pasquale Mari (FPG)	Quality check
1.0	30/06/2023	Lorenzo Marchesi (UCSC)	Acquisition of Quality Check and Peer Review indications, Document Closed

List of Contributors

The list of contributors to this deliverable are presented in the following table:

Section	Author(s)
All (1, 2, 3, 4, 5, 6, 7, 8, 9, 10)	Lorenzo Marchesi (UCSC)
5 – The datasets, Quality Check	Pasquale Mari (FPG)
6 – Analysis of the datasets in the CYBERHIMPREX Project	Fabio Rizzoni (FPG)
6 – Analysis of the datasets in the CYBERHIMPREX Project	Salvatore Agnes (UCSC)
6 – Analysis of the datasets in the CYBERHIMPREX Project	Mariano Alberto Pennisi (UCSC)
4. The DPIA regulatory framework and 8. Roadmap and DPIA methodology	Justyna Karolina Kielar (UCSC)
Peer review	Aimilia Magkanaraki (7HCR)
Peer review	Diana Navarro Llobet (FPHAG)
Peer review	Saverio Caruso (FPG)

Keywords

Cybersecurity, Data Protection Impact Analysis, General Data Protection Regulation, Privacy-by-design, Secure Information Sharing Platform, Regulatory Framework

Disclaimer

Executive Summary

The datasets contemplated by the CYBERHIMPREX project are ten. An assessment - based on the Regulatory Framework for the DPIA and the underlying principles for this instrument which are set forth in Regulation 679/2016 GDPR - has narrowed down the sets to scrutinize for DPIA to the datasets n. 1 (relevant to the SISP) and n. 2,3,4,5 and 6 (relevant to people interventions and organizational interventions).

For dataset n.1, the authors have ascertained that in a first phase only mock-data will be used (which does not contain personal data) and that "real" personal data will be used only in a second phase, if the first tests are successful. Nonetheless, a DPIA is not required because, as analyzed in this deliverable, the use of such data does not fall within the data management criteria for which a DPIA is required. The very limited quantity of data and limitations to the use and the consent policy are among the elements at the basis of the conclusion, as well as the Privacy-by-design approach used by the developer. The outcomes will be produced in compliance with GDPR and with articles of the GDPR determining specifications for the DPIA instrument. The instrument, when the project's duration is concluded, will be ready-to-use in a compliant way if the users adhere to privacy best practices.

For datasets n. 2, 3, 4, 5 and 6, likewise, a DPIA is not required because the features of such collection of personal data does not fall within the elements indicated in art. 35 of GDPR (limited number of data subjects, non-systematicity of the collection, no innovative methods involved, voluntariness of participation, administration of informed consent).

Table of Contents

1. Introduction

1.1 Scope and purpose of the document

The present deliverable has the scope of assessing if the use of personal data during the progress of the project requires a DPIA or not. The authors have concluded that a DPIA is not applicable and this is analytically documented in these pages.

1.2 Structure of the document

The document is structured in the following manner:

- Section 4 – The regulatory Framework (which redirects to Annex 1)
- Section 5 – Containing a table with information on the datasets relevant for the Project
- Section 6 – Assessment of the datasets and explanation of DPIA non-applicability
- Section 7 – Privacy-by-design and GDPR compliance specifications by the SISP developer

2. Applicable documents and sources

The following documents contain requirements applicable to the generation of this document:

Reference	Document Title	Document Reference	Version	Date
Reg EU 679/2016	General Data Protection Regulation	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:2016:119:TOC	OJEU Vol 56	May 4,2016
Recitals to Reg EU 679/2016		https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:2016:119:TOC	OJEU Vol 56	May 4,2016
DPIA template on gdpr.eu		https://gdpr.eu/data-protection-impact-assessment-template/		
DPIA guidelines of the Italian privacy authority		https://www.garanteprivacy.it/valutazione-d-impatto-della-protezione-dei-dati-dpia-		

Table 1-Applicable documents

The following sources of information/data have been used to draft this document:

Reference	Document Title	Document Reference	Version	Date
Reg EU 679/2016	General Data Protection Regulation	Official Journal of the European Union https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:2016:119:TOC	Vol 56	May 4,2016
Recitals to Reg EU 679/2016		https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:2016:119:TOC	Vol 56	May 4,2016
DPIA guidelines of the Italian privacy authority		https://www.garanteprivacy.it/valutazione-d-impatto-della-protezione-dei-dati-dpia-		
DPIA utility of the French privacy authority		https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/8581268		

Table 2-Sources

3. Glossary of Acronyms

Acronym	Description

DPIA	**Data Protection Impact Assessment**
DPO	**Data Protection Officer**
GDPR	**General Data Protection Regulation (Re. EU 679/2016)**
HCO	**Health Care Organization**
SISP	**Secure Information Sharing Platform**

Table 3-Acronyms

4. The DPIA regulatory framework

The Regulatory Framework for the DPIA-Data Protection Impact Assessment and the underlying principles for this instrument are set forth in Regulation 679/2016 GDPR-General Data Protection Regulation (articles 35-Data Protection Impact Assessment and art. 36-Prior Consultation) and in the recitals to the Regulation (nos. 79, 84, 89-96). The regulation and recitals are reproduced in Annex 1.

5. The datasets

The following table describes and specifies the datasets which will be used in the 10 interventions to be carried out within the CYBERHIMPREX project.

CYBERHIMPREX intervention		Activity that uses or accesses the data	Data	Data belong to	Data are treated by	Notes
Cross border Data/Knowledge sharing interventions						
1	**Set-up an inter-organizational (including cross-border) secure data sharing capability via a new tool (SISP)**	An FPG clinical department will securely transfer clinical and personal of patients data to an FPHAG clinical department using a tool (SISP-Secure Information Sharing Platform) and vice versa.	Personal Identification Clinical data (including images)	Patients	2 Clinical departments at FPG (e.g. dialysis centre, emergency room) 2 Clinical departments at FPHAG	The activity will be performed in a limited span of time, in two pilots No more than 10 patients are expected to be involved at each hospital Patients will be involved only if they sign a consent form The data will not be circulated outside the participating clinical departments The SISP tool has been designed to be GDPR compliant
People interventions						
2	**Improve cybersecurity skills of technical staff, via multi-method training (NCSF, CyberRange Training)**	The activity consists in training ICT and clinical engineering staff using a variety of methods (in presence, on line, e-learning)	Personal Identification	Participants	FPG and 7HRC employees that organize/participate the training	≅25 participants at FPG ≅25 participants at 7HRC Persons will be involved only if they sign a consent form.
3	**Raise cybersecurity staff awareness via customized nudging and education pills (SBNT, TECT, CH)**	The activity will include: - an on line survey (questionnaires autonomously and anonymously filled by the respondents) - a phishing	Personal Identification (+ **relevant attributes**)	Staff	FPG employees that organize and manage the survey, the phishing and the focus groups	Selected staff members at FPG are planned to be targeted by the survey and by the phishing simulation. We expect that the survey will not require answers that may damage or discriminate the respondents; therefore, it will be considered if anonymization can be avoided. If not, the platforms delivering the

		simulation targeting one or more groups of staff members - some meetings with selected staff members to perform focus groups				questionnaires and the simulated phishing will ensure that the responses will be anonymized. However, in order to analyse the data, some **relevant attributes** will be used (e.g. professional group, sex, range of age).
4	**Set-up the new cybersecurity "angel" role via dedicated training**	The activity consists of an in-presence training of staff from clinical departments. The in-presence training may be complemented by on-line or e-learning training.	Personal identification	Staff	FPG employees that organize/participate to the training	≅100 FPG staff members Persons will be involved only if they sign a consent form.
Organization interventions						
5	**Improve cybersecurity orientation of the procurement process via alignment with ENISA guidelines**	The activity will include meetings with staff and managers to perform interviews or workshops. Also suppliers could be interviewed (other than the consultants that will be contracted to for executing the intervention)	Personal identification	Staff Suppliers	FPG and FPHAG employees that organize/participate to the meetings	≅15 FPG mangers and staff members, and suppliers and ≅15 FPHAG managers and staff members, and suppliers are expected to be involved in interviews/workshops Persons will be involved only if they sign a consent form.
6	**Improve the cybersecurity**	The activity will include meetings	Personal identification	Staff Suppliers	FPG employees that organize the meetings	≅25 FPG managers and staff members, and suppliers are expected to be involved in

	governance organization and system via a stakeholder involvement approach and new tools (RGT)	with staff and managers to perform interviews or workshops. Also suppliers could be interviewed (other than the consultants that will be contract to execute the intervention)				interviews/workshops ≅200 FPG staff considered as potential cybersecurity "angels" Persons will be involved only if they sign a consent form.
Technology						
7	**Improve web navigation system security via *web proxy*.**	**NA**				
8	**Improve business continuity via an immutable backup system.**	**NA**				
9	**Reduce the Attack Surface via Operating Systems (OS) update**	**NA**				
10	**Improve Security by Design capability via new supporting tools (SDSP, CST)**	**NA**				

6. Analysis of the datasets in the CYBERHIMPREX project

This evaluation applies to the use of personal and sensitive data in the framework of tasks set forth in this project.
Of the datasets described above, only datasets n.1 ((intervention 1, regarding the use of a software application named Secure Information Sharing Platform-SISP) and 2,3,4,5 and 6 (people interventions and organization interventions) need to be assessed in order to conclude if the data controller is required to perform a DPIA.

Dataset n. 1 Cross border Data/Knowledge sharing interventions
The scenarios under assessment are three:

1) A mock data driven scenario (in the first phase) of the project, with no relevance to personal data management issues and not subject to protective measures prescribed by regulatory.
2) A second phase where a very limited number of real time data will be potentially used for testing purposes for which protective measures are also described in the chapter of the present deliverable named "Privacy-by-design and GDPR compliance of the SISP"
3) As far as the third scenario is concerned - that of a potential real-time use of the system, as an outcome beyond the duration of the project - the effort of the developers is centred on the privacy-by-design aspect of the system so that future users under whose "jurisdiction" it will serve will have the necessary instruments to implement a secure use wherever the protection of personal data is concerned.

The following elements concur to the definition of the operational framework and relevant risks.

- The dataset would be deployed in the set-up operations of a Health Care Organization inter-organizational (including cross-border) secure data sharing capability via a new tool (SISP).
- An FPG clinical department will securely transfer clinical and personal patients' data to an FPHAG clinical department using a tool (SISP-Secure Information Sharing Platform) and vice versa.
- The data will be clinical data (including images) belonging to the patient.
- Data will be of patients from two clinical departments at CYBERHIMPREX partner FPG and two Clinical departments at FPHAG
- The activity will be performed for a limited span of time, in two pilots
- No more than 10 patients are expected to be involved in each hospital
- Patients will be involved only if they sign a consent form
- The data will not be circulated outside the involved clinical departments
- The SISP tool has been designed to be GDPR compliant (see next section 7.)

The data that will be processed to implement this task will be "mock" data, that is non personal data artificially created for testing purposes.
If the test is successful, real personal data may be potentially used for a second pilot but the elements assessed lead to consider that a DPIA is not applicable to the case for the following reasons, based on the indications provided in art. 35 and 36 of GDPR and relevant recitals.

- Advice was sought from the DPO office of FPG who agreed that at the time of writing, also considering the description of action and the project's roadmap, the risks do not require a DPIA to be performed.
- The processing does not imply a systematic and extensive evaluation of personal aspects relating to 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.
- Processing does not imply the use of a large scale of special data categories or of personal data relating to criminal convictions and offences.

- Processing does not imply a systematic monitoring of a publicly accessible area on a large scale.
- An information sheet will be administered to all participants signing consent, operation which will be closely monitored.

The scopes do not appear to present a risk to the freedoms and rights of citizens nor are any risks for the security of personal data. Scopes are summarized as follows:

- Set-up a cross-border inter-organizational HCO secure data sharing capability via a new tool,
- Set-up a process to manage cross-border knowledge sharing in view of improving security collectively, also via new tools,
- Improve cybersecurity orientation of the procurement process via alignment with ENISA guidelines (by using 11 out of 15 solutions developed in H2020 projects).

Datasets n. 2, 3 and 4 (People interventions) and 5 and 6 (Organizational interventions)

In such a project operational framework the possible data collected is acquired by personal contact and affiliation data of staff or involved experts. Eventually these may participate in surveys on the scopes of the project (e.g. secure sharing platforms, cyber-security environments etc.). Such collection and processing of personal data, likewise, will not require a DPIA because of the limited numbers of involved data subjects, the lack of a systematic nature in the personal data collection and the lack of innovative aspects in such working methods, as well as the voluntary feature of participation and of the administration of information sheets and consent forms.

7. Privacy-by-design and GDPR compliance of the SISP

The developer (RHEA Group, incorporated in Belgium) has provided the following specification of the Privacy-by-design of the SISP and of GDPR compliance:

When developing the SISP (Secure Information Sharing Platform) software application, our team prioritized incorporating good privacy-by-design practices and ensuring compliance with the European General Data Protection Regulation (GDPR). We followed a risk analysis approach that incorporated certain aspects of a Privacy Impact Assessment (PIA) to identify and evaluate potential privacy risks associated with the software's functionalities and data processing activities. This risk analysis allowed us to understand the data flows, processing activities, and potential privacy implications of the application.

Throughout the development process, we adhered to the following privacy-by-design practices:

***Data Minimization**: We designed the SW to only collect the minimum amount of personal data necessary to fulfil the intended purpose of the SISP software, thereby reducing potential privacy risks.*

***Lawful Basis for Data Processing**: We ensured that we had a lawful basis for processing personal data within the SISP software, such as obtaining user consent, fulfilling contractual obligations, complying with legal requirements, or pursuing legitimate interests.*

***User Consent**: Where applicable, we implemented mechanisms to obtain user consent for data processing activities. We provided clear and easily understandable consent requests, informing users about the specific purposes of data processing and their rights under GDPR.*

***Data Security**: We implemented robust data security measures (see below), including encryption, access controls, and regular security audits, to protect personal data within the SISP software and prevent unauthorized access, disclosure, or alteration.*

By incorporating these privacy-by-design practices and considering privacy risks through the risk analysis process, we aimed to develop the SISP software application with privacy as a fundamental consideration. Adhering to European GDPR rules, we prioritized the protection of individuals' rights and privacy while using the software, contributing to a more secure and privacy-respecting environment for our users.

Security Controls implemented into SISP:

Data Confidentiality	• *Encryption of data* • *Encryption of connections* • *Access rules*
Data Integrity	• *Data Integrity checks* • *Monitoring to avoid unauthorized modification*
Data Availability	• *Monitoring to avoid unauthorized deletion*
Regularly testing, assessing and evaluating the effectiveness of technical and organisational measures	• *Regular vulnerability assessment*
Identification and authorization	• *Best practices*
Events Logging	• *Monitoring requirements to account for the who, what, where, when, target, source, and success/failure of the logged event*
Secure Configuration	• *Privacy-by-design and by default*
IT Governance	• *Risk Assessment*
Certifications	• *Security-related certifications (ISO27001)*

8. Ethical and Data Privacy aspects relevant to this Deliverable

The present deliverable has been submitted to the internal Ethics Advisory Board and, subsequent to review, no ethics issues or data privacy aspect have been recorded in the contents and conclusions.

9. Conclusions

Having identified the relevant datasets that need to be assessed in order to establish if a DPIA is required, having acquired the privacy-by-design specifications of the developer of the SISP (RHEA, incorporated in Belgium), having assessed the datasets and their use within the Project and measured such information against the requirements for a DPIA set forth by GDPR (articles 35, 36 and relevant recitals), the authors have come to the conclusion that a DPIA is not required. Nonetheless monitoring shall continue throughout the Project's duration and measures will be adopted should they be required.

ANNEX 1

Relevant recitals to GDPR

(75) The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures; where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; where personal data of vulnerable natural persons, in particular of children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects.

(84) In order to enhance compliance with this Regulation where processing operations are likely to result in a high risk to the rights and freedoms of natural persons, the controller should be responsible for the carrying-out of a data protection impact assessment to evaluate, in particular, the origin, nature, particularity and severity of that risk. 2The outcome of the assessment should be taken into account when determining the appropriate measures to be taken in order to demonstrate that the processing of personal data complies with this Regulation. 3Where a data-protection impact assessment indicates that processing operations involve a high risk which the controller cannot mitigate by appropriate measures in terms of available technology and costs of implementation, a consultation of the supervisory authority should take place prior to the processing.

(89) Directive 95/46/EC provided for a general obligation to notify the processing of personal data to the supervisory authorities. While that obligation produces administrative and financial burdens, it did not in all cases contribute to improving the protection of personal data. Such indiscriminate general notification obligations should therefore be abolished, and replaced by effective procedures and mechanisms which focus instead on those types of processing operations which are likely to result in a high risk to the rights and freedoms of natural persons by virtue of their nature, scope, context and purposes. Such types of processing operations may be those which in, particular, involve using new technologies, or are of a new kind and where no data protection impact assessment has been carried out before by the controller, or where they become necessary in the light of the time that has elapsed since the initial processing.

(90) In such cases, a data protection impact assessment should be carried out by the controller prior to the processing in order to assess the particular likelihood and severity of the high risk, taking into account the nature, scope, context and purposes of the processing and the sources of the risk. That impact assessment should include, in particular, the measures, safeguards and mechanisms envisaged for mitigating that risk, ensuring the protection of personal data and demonstrating compliance with this Regulation.

(91) This should in particular apply to large-scale processing operations which aim to process a considerable amount of personal data at regional, national or supranational level and which could affect a large number of data subjects and which are likely to result in a high risk, for example, on account of their sensitivity, where in accordance with the achieved state of technological knowledge a new technology is used on a large scale as well as to other processing operations which result in a high risk to the rights and freedoms of data subjects, in particular where those operations render it more difficult for data subjects to exercise their rights. A data protection impact assessment should also 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 or following the processing of special categories of personal data, biometric data, or data on criminal convictions and offences or related security measures. A data protection impact assessment is equally required for monitoring publicly accessible areas on a large scale, especially when using optic-electronic devices or for any other operations where the competent supervisory authority considers that the processing is likely to result in a high risk to the rights and freedoms of data subjects, in particular because they prevent data subjects from exercising a right or using a service or a contract, or because they are carried out systematically on a large scale. The processing of personal data should not be considered to be on a large scale if the processing concerns personal data from patients or clients by an individual physician, other health care professional or lawyer. In such cases, a data protection impact assessment should not be mandatory.

(92) There are circumstances under which it may be reasonable and economical for the subject of a data protection impact assessment to be broader than a single Project, for example where public authorities or bodies intend to establish a common application or processing platform or where several controllers plan to introduce a common application or processing environment across an industry sector or segment or for a widely used horizontal activity.

(93) In the context of the adoption of the Member State law on which the performance of the tasks of the public authority or public body is based and which regulates the specific processing operation or set of operations in question, Member States may deem it necessary to carry out such assessment prior to the processing activities.

(94) Where a data protection impact assessment indicates that the processing would, in the absence of safeguards, security measures and mechanisms to mitigate the risk, result in a high risk to the rights and freedoms of natural persons and the controller is of the opinion that the risk cannot be mitigated by reasonable means in terms of available technologies and costs of implementation, the supervisory authority should be consulted prior to the start of processing activities. Such high risk is likely to result from certain types of processing and the extent and frequency of processing, which may result also in a realisation of damage or interference with the rights and freedoms of the natural person. The supervisory authority should respond to the request for consultation within a specified period. However, the absence of a reaction of the supervisory authority within that period should be without prejudice to any intervention of the supervisory authority in accordance with its tasks and powers laid down in this Regulation, including the power to prohibit processing operations. As part of that consultation process, the outcome of a data protection impact assessment carried out with regard to the processing at issue may be submitted to the supervisory authority, in particular the measures envisaged to mitigate the risk to the rights and freedoms of natural persons.

(95) The processor should assist the controller, where necessary and upon request, in ensuring compliance with the obligations deriving from the carrying out of data protection impact assessments and from prior consultation of the supervisory authority.

(96) A consultation of the supervisory authority should also take place in the course of the preparation of a legislative or regulatory measure which provides for the processing of personal data, in order to ensure compliance of the intended processing with this Regulation and in particular to mitigate the risk involved for the data subject.

Art. 35 GDPR (Data protection impact assessment)

Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.
The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment.
A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of:

- a systematic and extensive evaluation of personal aspects relating to 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;
- 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
- a systematic monitoring of a publicly accessible area on a large scale.

The supervisory authority shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1. 2The supervisory authority shall communicate those lists to the Board referred to in Article 68.

The supervisory authority may also establish and make public a list of the kind of processing operations for which no data protection impact assessment is required. 2The supervisory authority shall communicate those lists to the Board.
Prior to the adoption of the lists referred to in paragraphs 4 and 5, the competent supervisory authority shall apply the consistency mechanism referred to in Article 63 where such lists involve processing activities which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union.
The assessment shall contain at least:

- a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;
- an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
- an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and

the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.
Compliance with approved codes of conduct referred to in Article 40 by the relevant controllers or processors shall be taken into due account in assessing the impact of the processing operations performed by such controllers or processors, in particular for the purposes of a data protection impact assessment.
Where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations.
Where processing pursuant to point (c) or (e) of Article 6(1) has a legal basis in Union law or in the law of the Member State to which the controller is subject, that law regulates the specific processing operation or set of operations in question, and a data protection impact assessment has already been carried out as part of a general impact assessment in the context of the adoption of that legal basis, paragraphs 1 to 7 shall not apply unless Member States deem it to be necessary to carry out such an assessment prior to processing activities.
Where necessary, the controller shall carry out a review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operations.

Article 36 GDPR (Prior consultation)

1. The controller shall consult the supervisory authority prior to processing where a data protection impact assessment under Article 35 indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.
2. Where the supervisory authority is of the opinion that the intended processing referred to in paragraph would infringe this Regulation, in particular where the controller has insufficiently identified or mitigated the risk, the supervisory authority shall, within period of up to eight weeks of receipt of the request for consultation, provide written advice to the controller and, where applicable to the processor, and may use any of its powers referred to in Article 58. That period may be extended by six weeks, taking into account the complexity of the intended processing. The supervisory authority shall inform the controller and, where applicable, the processor, of any such extension within one month of receipt of the request for consultation together with the reasons for the delay. Those periods may be suspended until the supervisory authority has obtained information it has requested for the purposes of the consultation.

3. When consulting the supervisory authority pursuant to paragraph 1, the controller shall provide the supervisory authority with:
(a) where applicable, the respective responsibilities of the controller, joint controllers and processors involved in the processing, in particular for processing within a group of undertakings;
(b) the purposes and means of the intended processing;
(c) the measures and safeguards provided to protect the rights and freedoms of data subjects pursuant to this Regulation;
(d) where applicable, the contact details of the data protection officer;
(e) the data protection impact assessment provided for in Article 35; and
(f) any other information requested by the supervisory authority.
4. Member States shall consult the supervisory authority during the preparation of a proposal for a legislative measure to be adopted by a national parliament, or of a regulatory measure based on such a legislative measure, which relates to processing.
5. Notwithstanding paragraph 1, Member State law may require controllers to consult with, and obtain prior authorization from, the supervisory authority in relation to processing by a controller for the performance of a task carried out by the controller in the public interest, including processing in relation to social protection and public health.