


Project Acronym:

Hydroptics

 Ref. Ares(2021)7383097 - 30/11/2021

Grant Agreement number:

871529 (H2020-ICT-2019-2)

Project Full Title:

Photonics sensing platform for process optimisation in the oil industry



## DELIVERABLE

### D2.2 – Report on GDPR and legal aspects: First

<b>Dissemination level</b>	PU – Public
<b>Type of Document</b>	Report
<b>Contractual date of delivery</b>	30/11/2021
<b>Deliverable Leader</b>	George Athanasiou (DBC)
<b>Status &amp; version</b>	V2.0
<b>WP / Task responsible</b>	DBC
<b>Keywords:</b>	GDPR compliance, legal issues

<b>Deliverable Leader:</b>	DBC
<b>Contributors:</b>	George Athanasiou, Sara Nabaraoui, George Sidiras (DBC)
<b>Reviewers:</b>	Sargis Hakobyan (ALPES)
<b>Approved by:</b>	Sargis Hakobyan (ALPES)

Document History			
Version	Date	Contributor(s)	Description
V1.0	10/11/2021	DBC	First complete version
V1.1	20/11/2021	ALPES, DBC	Internal review
V2.0	30/11/2021	ALPES, DBC	Final version, after review by the Coordinator

*This document is part of a project that has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 871529. It is the property of the HYDROPTICS consortium and shall not be distributed or reproduced without the formal approval of the HYDROPTICS Management Committee. The content of this report reflects only the authors' view. EC is not responsible for any use that may be made of the information it contains.*

## Executive Summary

The document outlines the common legal framework for HYDROPTICS's consortium to take into consideration during research and realization phases of the project. It provides a first guidance on compliance with privacy and data protection issues that might arise during the project. The deliverable also identifies and describes the risks in the above-mentioned areas that might arise out of the project and the measures to mitigate the risks. Additionally, the deliverable presents the methodology to deal with impact, ethical and liability in order to generate a framework to be used in the project as baseline for the HYDROPTICS's project.

Finally, the document describes requirements of conducting impact assessment with regard to data protection and privacy issues. Requirements of GDPR framework and how Data Protection Impact Assessment (DPIA) is going to address them for the specific needs of HYDROPTICS project are addressed, starting from the definition of the DPIA. Furthermore, criteria and specific situations that will require DPIA to be conducted in the HYDROPTICS project are addressed.

## Table of Contents

Executive Summary .....	2
Table of Contents .....	3
1. Introduction .....	4
1.1. The Right to the Protection of Personal Data .....	4
1.1.1. Background Information .....	4
1.1.2. Key Points .....	5
2. Principles, Rights and Obligations under the General Data Protection Regulation .....	6
2.1. Core definitions .....	6
2.2. General Principles .....	6
2.2.1. Seven Principles .....	7
2.3. Legal grounds for the processing of personal data .....	8
2.4. Rights of data controllers .....	10
2.5. Obligations of data processors .....	12
2.6. Data controllers and data processors .....	14
3. Relevant Regulatory Frameworks in Turkey & Switzerland .....	16
3.1. Turkish Data Protection Law (DPL) .....	16
3.2. Switzerland, the Federal Act on Data Protection (FADP) .....	17
4. Data Management Measures in HYDROPTICS .....	19
5. Ensuring HYDROPTICS components GDPR compliance .....	21
6. Consent within HYDROPTICS .....	24
6.1. Data collection activities .....	24
6.2. Consent processes within HYDROPTICS .....	24
6.3. Voluntary participation in pilots .....	24
6.4. Consent requirements for the HYDROPTICS pilots .....	25
6.5. Data lifecycle .....	26
7. Data Mapping .....	27
8. Data Protection Impact Assessment (DPIA) .....	29
8.1. When the DPIA is required .....	29
8.2. DPIA process key elements .....	32
8.3. Why DPIA in HYDROPTICS .....	37
9. Preliminary identified risks .....	38
Conclusion .....	45
Annex I: Regulatory compliance specifications for each component in HYDROPTICS .....	46
Annex II: Informed consent form for participation in research .....	49
Annex III: Compliance Questionnaire .....	50

## 1. Introduction

The main objective of HYDROPTICS project is to develop a set of integrated sensors, making use of advanced photonics subsystems, aimed at optimizing the processes of the oil industry. The device will be validated in real industrial settings, for oil extraction and oil refining processes. The HYDROPTICS platform will perform: 1) oil in water measurements, 2) corrosion inhibitor concentration measurements, 3) oil droplets and suspended solids in water measurements, 4) industrial process optimization, based on simulation of processes through digital twins, as well as data assimilation from the readings coming from the sensors.

Moreover, a key vision of HYDROPTICS is to elaborate how data provided by these advanced photonic sensors can be combined with readily available process data, and a digital twin of the process apparatus to gain in-depth process understanding. Digitalization of process data, data fusion, machine learning and artificial intelligence shall enable a new level of process optimization yielding high and constant product quality despite fluctuating process conditions.

Use of human-related data in HYDROPTICS project will not be multilevel and throughout the development of the project there will be specific conditions where human data will be used, however, all necessary measures must be taken to ensure that the risk is minimized and HYDROPTICS project is compliance with all EU regulation and best practice approaches relevant to the safety and privacy of data.

The right to personal data protection can be affected by collecting and processing of some types of data in HYDROPTICS project that might fall under the scope of GDPR. This would require that HYDROPTICS's partners carefully and anticipatory define the types of data, means and purposes of processing, the roles of every partner applied in the project. Based on that, the legal grounds for processing and respective obligations of HYDROPTICS's partners will be established. While the project involves the use of different innovative technologies, a Data Protection Impact Assessment will likely be required (or recommended to demonstrate the compliance with GDPR) by HYDROPTICS partners who may be likely to process personal data.

### 1.1. The Right to the Protection of Personal Data

#### 1.1.1. Background Information

As privacy, the protection of natural persons in relation to the processing of personal data is a fundamental right.<sup>1</sup> Article 8 of the ECHR<sup>2</sup> provides a right to respect for one's "private and family life, his home and his correspondence"<sup>3</sup>. Article 8 is considered to be one of the convention's most open-ended provisions.<sup>4</sup> Additionally the Council of Europe has modernized its Convention 108 for the protection of individuals with regard to automatic processing of personal data: in 2018 it adopted Convention 108+. The modernized version of Convention 108 seeks to respond to the challenges posed, in terms of human rights, by the use of new information and communication technologies.<sup>5</sup> Moreover, Article 8(1) of the Charter and Article 16(1) of the Treaty on the Functioning of the European Union ("TFEU") provide that everyone has the right to the protection of personal data concerning him or her.<sup>6</sup>

---

<sup>1</sup> 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). OJ L 119, Recital 1 ['GDPR']

<sup>2</sup> Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols No. 11 and No. 14, Rome, 4 November 1950, ETS No. 5. <http://conventions.coe.int/treaty/en/treaties/html/005.htm>

<sup>3</sup> Article 8 of the European Convention on Human Rights - Wikipedia

<sup>4</sup> Elizabeth Wicks; Bernadette Rainey; Clare Ovey (12 June 2014). *Jacobs, White and Ovey: the European Convention on Human Rights*. Oxford University Press. p. 334. ISBN 978-0-19-965508-3.

<sup>5</sup> [Council of Europe convention 108+: A modernised international treaty for the protection of personal data - ScienceDirect](#)

<sup>6</sup> Ibid



Data protection is closely linked to privacy. The notion of data protection originates from the right to privacy, and both are instrumental in preserving and promoting fundamental values and rights and to exercise other rights and freedoms - such as free speech or the right to assembly.<sup>7</sup> However, these rights are commonly recognized all over the world as two separate rights.<sup>8</sup> The two rights differ in their formulation and scope. The right to respect for private life consists of a general prohibition on interference, subject to some public interest criteria that can justify interference in certain cases.<sup>9</sup> The protection of personal data is viewed as a modern and active right,<sup>10</sup> putting in place a system of checks and balances to protect individuals whenever their personal data are processed. The processing must comply with the essential components of personal data protection, namely independent supervision and the respect for the data subject's rights.<sup>11</sup>

### 1.1.2. Key Points

Under Article 8 of the ECHR, a person's right to protection with respect to the processing of personal data forms part of the right to respect for private and family life, home and correspondence.

CoE Convention 108 is the first and, to date, the only international legally binding instrument dealing with data protection. The Convention underwent a modernization process, completed with the adoption of amending Protocol CETS No. 223.

Under EU law, data protection has been acknowledged as a distinct fundamental right. It is affirmed in Article 16 of the Treaty of the Functioning of the EU, as well as in Article 8 of the EU Charter of Fundamental Rights.

Under EU law, data protection was regulated for the first time by the Data Protection Directive in 1995.

In view of rapid technological developments, the EU adopted new legislation in 2016 to adapt data protection rules to the digital age. The General Data Protection Regulation became applicable in May 2018, repealing the Data Protection Directive.

Together with the General Data Protection Regulation, the EU adopted legislation on the processing of personal data by state authorities for law enforcement purposes. Directive (EU) 2017/680 establishes the data protection rules and principles that govern personal data processing for the purposes of preventing, investigating, detecting and prosecuting criminal offences or executing criminal penalties.

---

<sup>7</sup> European Data Protection Supervisor. Data Protection. Available at: accessed July 29, 2019

<sup>8</sup> Ibid

<sup>9</sup> e Handbook on European data protection law, above fn. 15. P.19

<sup>10</sup> Advocate General Sharpston described the case as involving two separate rights: the "classic" right to the protection of privacy and a more "modern" right, the right to data protection. See CJEU, Joined cases C-92/09 and C-93/02, *Volker und Markus Schecke GbR v. Land Hessen*, Opinion of Advocate General Sharpston, 17 June 2010, para. 71. Cross-reference from the Handbook on European data protection law, above fn. 15. P.19

<sup>11</sup> Hustinx, P., EDPS Speeches & Articles, EU Data Protection Law: the Review of Directive 95/46/EC and the Proposed General Data Protection Regulation, July 2013. Cross-reference from the Handbook on European data protection law, above fn. 15. P.19

## 2. Principles, Rights and Obligations under the General Data Protection Regulation

### 2.1. Core definitions

In the course of this project, it will be important to consider a number of important definitions. This is because their application will often determine which data protection provisions apply and how they do so.

#### “Personal data”

Any information relating to an identified or identifiable natural person (data subject).

#### “Identifiable natural person”

Anyone who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier (e.g., IP addresses) or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

#### “Data subject”

Any natural person whose personal data is being processed.

#### “Data controller”

A natural or legal person who, alone or jointly, determines the purposes and means of processing.

#### “Data processor”

A natural or legal person who processes personal data on behalf on the controller.

#### “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, 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.

#### “Pseudonymization”

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 organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

#### “Consent of the data subject”

Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

#### “Personal data breach”

Breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

### 2.2. General Principles

The GDPR has two main objectives: protection of natural persons regarding the processing of personal data and ensuring free movement of personal data within the EU.<sup>12</sup> These objectives are above all other principles specified in the GDPR and should be always taken into consideration during processing of personal data. Besides objectives, the GDPR provides seven principles of personal data processing as explained further. These principles must be observed in most instances of processing. This is particularly where the legal base relied upon is consent, for which

---

<sup>12</sup> GDPR, Art.1

few exemptions of foreseen. HYDROPTICS declares compliance with all EU regulation and best practice approaches relevant to the safety and privacy of data.

### 2.2.1. Seven Principles

#### Lawfulness, fairness, and transparency<sup>13</sup>

The principle means that the personal data shall be processed lawfully, fairly and in a transparent manner. What is more important, these requirements should be fulfilled in relation to the data subject. Lawfulness means that personal data should be processed under one of the legal grounds specified in article 6 of the GDPR.<sup>14</sup> Legal grounds potentially applicable to HYDROPTICS are: prior and informed consent of data subject, when processing is necessary to protect vital interest of the data subject or another natural person, when processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. The principle of fair processing governs primarily the relationship between the controller and the data subject.<sup>15</sup> Controllers should notify data subjects and the public that they will process data in a lawful and transparent manner and must be able to demonstrate the compliance of processing operations with the GDPR. Processing operations must not be performed in secret and data subjects should be aware of potential risks.<sup>16</sup> Transparency principle establishes an obligation for the controller to take any appropriate measure in order to keep the data subjects informed about how their data are being used in a concise, transparent, intelligible and easily accessible form, using clear and plain language.<sup>17</sup> Transparency may refer<sup>18</sup> to the information given to the individual before the processing starts,<sup>19</sup> the information that should be readily accessible to data subjects during the processing,<sup>20</sup> but also to the information given to data subjects following a request of access to their own data.

#### Purpose limitation

Purpose limitation principle means that personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.<sup>21</sup> The purpose of processing data must be defined before processing is started.<sup>22</sup> For example, if the data initially collected in HYDROPTICS for conducting research and further is processed for marketing activities without any additional legal grounds, this would be incompatible with the purpose limitation principle. This principle is also important, where the original legal basis for the collection and processing of data was consent, for limiting the scope for further research using personal data where such a purpose was not outlined in the original consent materials.

#### Data minimization

Data minimization principle means that personal data shall be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.<sup>23</sup>

#### Accuracy

Accuracy principle means that personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for

---

<sup>13</sup> GDPR, Article 5(1)(a)

<sup>14</sup> GDPR, Art. 6

<sup>15</sup> See Handbook on European data protection law, P. 118

<sup>16</sup> Ibid

<sup>17</sup> GDPR, Art. 12

<sup>18</sup> Handbook on European data protection law,. P.120

<sup>19</sup> GDPR, Art. 13 and 14

<sup>20</sup> Article 29 Working Party, Opinion 2/2017 on data processing at work, P. 23. Cross-reference from the Handbook on European data protection law, above fn. 15. P. 120

<sup>21</sup> Ibid

<sup>22</sup> See Handbook on European data protection law, above fn. 15. P.122

<sup>23</sup> Ibid

which they are processed, are erased, or rectified without delay.<sup>24</sup> In the HYDRPOPTICS project it will therefore be important to ensure that data are collected a processed in an accurate manner. This will require using suitable devices and recording equipment.

### Integrity and confidentiality

Integrity and confidentiality principle means that that personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organizational measures.<sup>25</sup>

### Accountability<sup>26</sup>

Accountability principle means that the controller shall be responsible for and be able to demonstrate compliance with all the previously mentioned principles. To facilitate the compliance with this requirement, controllers can i) record the processing activities, making them available to the supervisory authority upon request (Article 30 GDPR); ii) adhere to approved codes of conduct or certification mechanism; iii) designate a Data Protection Officer; iv) undertake a Data Protection Impact Assessment; iv) ensure data protection by design and by default; v) adopt policies and procedures, and implement them, to allow the exercise of the rights of data subjects.<sup>27</sup>

## 2.3. Legal grounds for the processing of personal data

To comply with the lawfulness principle of GDPR, any processing of personal data shall be based on one or several legal grounds stipulated in Article 6 of GDPR.<sup>28</sup> It should be noted that whilst several may be applicable in a real-world context where a HYDROPTICS like prototype might be deployed they are unlikely to be applicable within the context of a research project such as HYDROPTICS given the conditions for their use will not exist. This may include the existence of legislation at the national level.

To define the appropriate legal basis for processing of personal data in HYDROPTICS project, the purposes of processing should be specified, types of processed personal data and the nature, circumstances, other features of processing should be assessed. The most relevant ground for the HYDROPTICS project is that of consent (or explicit consent where sensitive data is involved). This is because the conditions necessary for the utilization of the other legal bases are not likely to exist within the context of a research project.

---

<sup>24</sup> Ibid

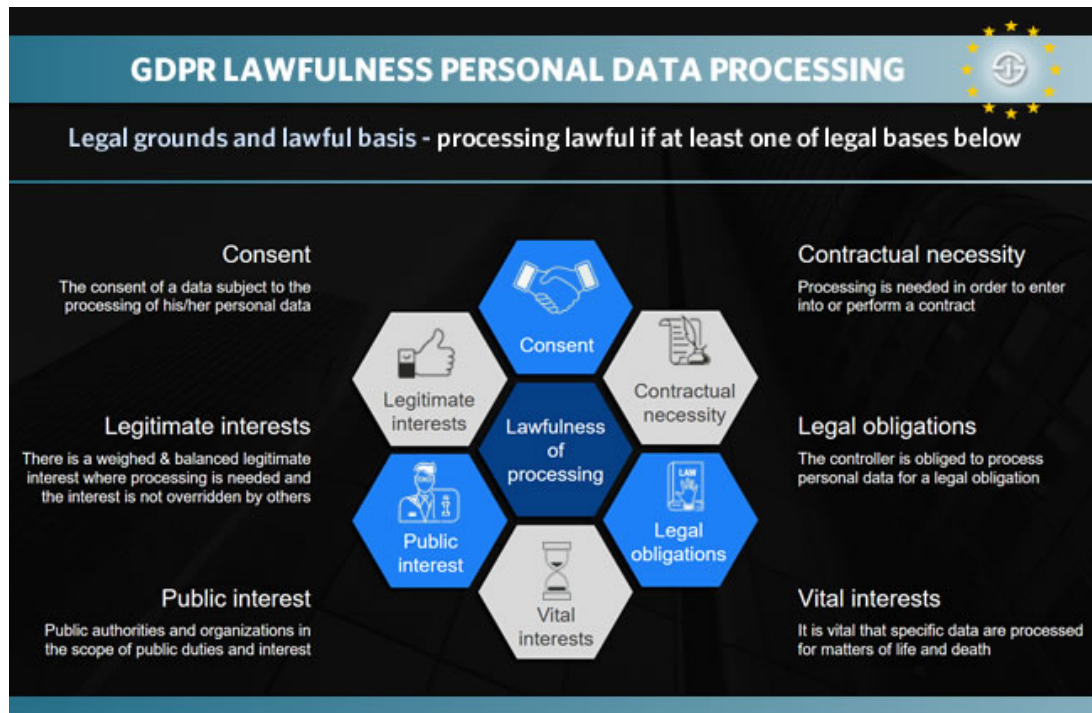
<sup>25</sup> Ibid

<sup>26</sup> GDPR, Art. 5(2)

<sup>27</sup> See HR-Recycler, P. 19

<sup>28</sup> [Article 6: Lawfulness of processing \(gdpr.org\)](#)





As mentioned above for the HYDROPTICS project the consent of data subject is likely to be the most important legal base for the processing of personal data. **The data subject has given consent to the processing of his or her personal data for one or more specific purposes.**<sup>29</sup>

The GDPR provides that the consent should be:

### Freely given:

Consent can be deemed freely given “if the data subject is able to exercise a real choice and there is no risk of deception, intimidation, coercion or significant negative consequences if he/she does not consent.”<sup>30</sup> The GDPR specifies that “when assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.”<sup>31</sup>

### Informed:

Informed consent will usually comprise a precise and easily understandable description of the subject matter requiring consent.<sup>32</sup> The individual concerned must be given, in a clear and understandable manner, accurate and full information of all relevant issues, such as the nature of the data processed, purposes of the processing, the recipients of possible and the rights of the data subject.<sup>33</sup>

### Specific:

For consent to be valid, it must also be specific to the processing purpose, which must be described clearly, and in unambiguous terms. This goes hand-in-hand with the quality of information given about the purpose of the consent. In this context, the reasonable expectations of an average data subject will be relevant.<sup>34</sup>

### Unambiguous indication of wishes:

<sup>29</sup> GDPR, Art. 6(1)(a)

<sup>30</sup> Article 29 Working Party (2011), Opinion 15/2011 on the notion of consent, WP 187, Brussels, 13 July 2011, P. 12

<sup>31</sup> GDPR, Art. 7 (4)

<sup>32</sup> See Handbook on European data protection law P.146

<sup>33</sup> See Article 29 Working Party (2007), Working Document on the processing of personal data

<sup>34</sup> See Handbook on European data protection law P.147

Consent requires a statement from the data subject or a clear affirmative act which means that it must always be given through an active motion or declaration. It must be obvious that the data subject has consented to the particular processing.<sup>35</sup> A “clear affirmative act” means that the data subject must have taken a deliberate action to consent to the particular processing. Consent can be collected through a written or (a recorded) oral statement, including by electronic means.<sup>36</sup>

## 2.4. Rights of data controllers

The data controllers in HYDROPTICS project should be informed about the rights of data subjects because they correspond with the relevant obligations of any controller (and of any processor if applicable). In the HYDROPTICS project these rights must be facilitated by all data controllers. The rights of data subjects under the GDPR are as follows:

### Right to be informed:<sup>37</sup>

The controller shall take appropriate measures to provide to data subject information about data controller (identity, contact detail, contacts of Data Protection Officer (DPO)), the purposes of the processing, the recipients of data and other information. It should be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language.<sup>38</sup>

### Right of access:<sup>39</sup>

The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

- the purpose of processing,
- the categories of personal data concerned,
- the recipients of personal data,
- where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period,
- the existence of the right to request from the controller rectification or erasure of personal data,
- the right to lodge a complaint with a supervisory authority,
- where the personal data are not collected from the data subject, any available information as to their source,
- the existence of automated decision-making, including profiling.<sup>40</sup>

The controller shall provide a copy of the personal data undergoing processing. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.<sup>41</sup>

---

<sup>35</sup> Article 29 Working Party. Guidelines on consent under Regulation 2016/679 17/EN WP259 rev.01. As last Revised and Adopted on 10 April 2018

<sup>36</sup> Ibid

<sup>37</sup> GDPR, Art. 12, 13, 14

<sup>38</sup> GDPR, Art. 12

<sup>39</sup> GDPR, Art. 15

<sup>40</sup> Ibid

<sup>41</sup> Ibid

### Right to rectification:<sup>42</sup>

The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.<sup>43</sup>

### Right to erasure ('right to be forgotten'):<sup>44</sup>

The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay where one of the following applies:

- the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed,
- the data subject withdraws consent on which the processing is based and where there is no legal ground of processing,
- the data subject objects to the processing and there is no other legitimate ground of processing,
- the personal data have been unlawfully processed,
- the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject,
- the personal data have been collected in relation to the offer of information society services.<sup>45</sup>

### Right to restriction of processing:<sup>46</sup>

The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies:

- the accuracy of the personal data is contested by the data subject,
- the processing is unlawful, and the data subject opposes the erasure of the personal data and requests the restriction of their use instead,
- the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims,

the data subject has objected to processing when the processing is based on public interest or legitimate interest of data controller by pending the verification whether the legitimate grounds of the controller override those of the data subject.<sup>47</sup>

### Right to data portability:<sup>48</sup>

The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where the processing is based on a consent of data subject or performance of the contract and the data processed by automated means.<sup>49</sup>

---

<sup>42</sup>GDPR, Art. 16

<sup>43</sup>Ibid

<sup>44</sup>GDPR, Art. 17

<sup>45</sup>Ibid

<sup>46</sup>GDPR, Art. 18

<sup>47</sup>Ibid

<sup>48</sup>GDPR, Art. 20

<sup>49</sup>Ibid

**Right to object:<sup>50</sup>**

The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on public interest or legitimate interest of data controller, including profiling based on those provisions and marketing purposes. The controller shall no longer process the personal data unless some exceptions are applied.<sup>51</sup>

**Right to lodge a complaint with a supervisory authority:<sup>52</sup>**

Every data subject shall have the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement if the data subject considers that the processing of personal data relating to him or her infringes this Regulation.<sup>53</sup>

**Right to an effective judicial remedy against a supervisory authority and to receive compensation:<sup>54</sup>**

Whenever the data subject considers that his or her rights under the GDPR have been infringed as a result of the processing of his or her personal data in non-compliance with the GDPR, he or she has the right to an effective judicial remedy and the right to receive compensation.<sup>55</sup>

**2.5. Obligations of data processors**

Besides the controllers' obligations corresponding to the rights of data subjects specified above in section 2.3 the GDPR specifies the other requirements for data controllers and processor. While demonstration of compliance reflects the accountability principle of data processing, the HYDROPTICS's partners shall be aware of the relevant obligations. Thus, the GDPR specifies the following obligations of data controllers:

**Demonstration of compliance**

The GDPR establishes the general obligation of data controllers to implement appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with GDPR. The measures shall be implemented taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, be updated and reviewed where necessary.<sup>56</sup> The examples of the measures to be taken are the implementation of data protection policies; codes of conducts, certification.<sup>57</sup>

**Data protection by design and by default<sup>58</sup>**

The data protection by design obligation requires data controllers both at the time of the determination of the means for processing and at the time of the processing itself implement appropriate technical and organizational measures, which are designed to comply with data-protection principles, such as data minimization, in an effective manner and to integrate the necessary safeguards.<sup>59</sup> The implementation shall take into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing.

---

<sup>50</sup> GDPR, Art. 21

<sup>51</sup> Ibid

<sup>52</sup> GDPR, Art. 77

<sup>53</sup> Ibid

<sup>54</sup> GDPR, Art. 78 and Art.82

<sup>55</sup> See HR-Recycler, P. 23

<sup>56</sup> GDPR, Art. 24(1)

<sup>57</sup> GDPR, Art. 24(2) and 24 (3)

<sup>58</sup> GDPR, Art. 25

<sup>59</sup> GDPR, Art. 25(1)

The example of the measure is pseudonymization. The data protection by default obligation is the reflection of data minimization and purpose limitation principles. It requires data controllers to implement appropriate technical and organizational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed.<sup>60</sup> “That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.”<sup>61</sup> As an element to demonstrate compliance with the obligations of data protection by design and by default controllers might apply an approved certification mechanism.<sup>62</sup>

### Records of processing activities<sup>63</sup>

The obligation requires data controllers (and processors, if any) to record in writing (including the electronic form) the information about data controller and details about data processing, including, inter alia, the categories of data subjects and categories of data, the purpose of processing.<sup>64</sup> The obligation has some exceptions, however, it is applied when the processing of sensitive data takes place.

### Cooperation with the supervisory authority<sup>65</sup>

“The controller and the processor and, where applicable, their representatives, shall cooperate, on request, with the supervisory authority in the performance of its tasks.”<sup>66</sup>

### Security of processing<sup>67</sup>

The data controller, and data processor (if applicable), shall implement the appropriate technical and organizational measures to ensure a security of data processing.<sup>68</sup> The examples of the measures to be taken are:

- the pseudonymization and encryption of personal data,
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services,
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident,
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.<sup>69</sup>

The Handbook on European data protection law suggests the following organizational measures to ensure privacy:

- regular provision of information to all employees about data security rules and their obligations under data protection law, especially regarding their confidentiality obligations,
- clear distribution of responsibilities and a clear outline of competences in matters of data processing, especially regarding decisions to process personal data and to transmit data to third parties or to data subjects,

---

<sup>60</sup> GDPR, Art. 25(2)

<sup>61</sup> Ibid

<sup>62</sup> GDPR, Art. 25(3)

<sup>63</sup> GDPR, Art. 30

<sup>64</sup> Ibid

<sup>65</sup> GDPR, Art. 31

<sup>66</sup> Ibid

<sup>67</sup> GDPR, Art. 32

<sup>68</sup> Ibid

<sup>69</sup> GDPR, Art. 32(1)

- 💧 use of personal data only according to the instructions of the competent person or according to generally laid down rules; - protection of access to locations and to hard- and software of the controller or processor, including checks on authorization for access,
- 💧 ensuring that authorizations to access personal data have been assigned by the competent person and require proper documentation,
- 💧 automated protocols on electronic access to personal data and regular checks of such protocols by the internal supervisory desk (therefore requiring all data processing activities to be recorded),
- 💧 careful documentation for other forms of disclosure than automated access to data so as to demonstrate that no illegal data transmissions have taken place.<sup>70</sup> The measures are defined on the basis of the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.<sup>71</sup>

### Notification of a personal data breach <sup>72</sup>

The controller shall notify about a personal data breach to the supervisory authority without undue delay and where feasible, not later than 72 hours after having become aware of it.<sup>73</sup> Moreover, data controller shall document the breach and the remedial measures taken. The exception from the notification obligation is the ability of controllers to demonstrate that the breach is unlikely to result in a risk to the rights and freedoms of natural persons.<sup>74</sup> Moreover, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.<sup>75</sup>

### Prior consultation<sup>76</sup>

The controller shall consult the supervisory authority prior to processing where a DPIA (Data Protection Impact Assessment) indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.<sup>77</sup>

### Stakeholders' consultation<sup>78</sup>

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.<sup>79</sup>

## 2.6. Data controllers and data processors

If a HYDROPTICS partner processes personal data, the scope of its obligations and responsibilities will greatly depend on its status under the GDPR – data controller or data processor. The main entity responsible for compliance with data protection rules is the data controller while it defines the purposes and means of processing. In other words, the first and foremost role of the concept of controller is to allocate responsibility.<sup>80</sup> The data processor processes the personal data on behalf of the controller and on the basis of the controller's instructions.

---

<sup>70</sup> See Handbook on European data protection law, above P.167

<sup>71</sup> Ibid

<sup>72</sup> GDPR, Art. 33

<sup>73</sup> Ibid

<sup>74</sup> Ibid

<sup>75</sup> GDPR, Art. 34

<sup>76</sup> GDPR, Art. 36

<sup>77</sup> Ibid

<sup>78</sup> GDPR, Art. 35(9)

<sup>79</sup> Ibid

<sup>80</sup> Article 29 Data Protection Working Party. Opinion 1/2010 on the concepts of "controller" and "processor". 00264/10/EN WP 169. Adopted as of February 16, 2019.

“Therefore, two basic conditions for qualifying as processor are on the one hand being a separate legal entity with respect to the controller and on the other hand processing personal data on his behalf. This processing activity may be limited to a very specific task or context or may be more general and extended.”<sup>81</sup> While data processor acts on behalf of data controller, the lawfulness of the processor's data processing activity is determined by the mandate given by the controller. “A processor that goes beyond its mandate and acquires a relevant role in determining the purposes or the essential means of processing is a (joint) controller rather than a processor.”<sup>82</sup>

The controllers shall use only processors providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that processing will meet the requirements of the GDPR and ensure the protection of the rights of the data subject.<sup>83</sup> Moreover, the controller and processor shall enter into the agreement that specifies the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller.<sup>84</sup>

Therefore, when different HYDROPTICS's partners are involved into the processing of personal data in one process (for example, with the use of one technology), their respective roles must be defined prior to processing.

---

<sup>81</sup> Ibid

<sup>82</sup> Ibid

<sup>83</sup>GDPR, Art. 28(1)

<sup>84</sup> GDPR, Art. 28(3)

### 3. Relevant Regulatory Frameworks in Turkey & Switzerland

The present chapter provides the overview of national legislations in non-EU Member States of HYDROPTICS's partners.

#### 3.1. Turkish Data Protection Law (DPL)



Turkish Data Protection Law (DPL) was enacted in 2016. Turkey's supervisory authority, The Personal Data Protection Board (DPB), is still publishing assorted regulations and communiqués relating to it, as well as draft versions of secondary legislation.

Although it stems from EU Directive 95/46/EC, DPL features several additions and revisions. It does, however, contain almost all of the same fair information practice principles, except that it does not allow for a “*compatible purpose*” interpretation and any further processing is prohibited. Where the subject gives consent that data may be compiled for a specific purpose, the controller can then use it for another purpose as long as further consent is obtained, or if further processing is needed for legitimate interests.

The grounds for processing under DPL are similar to GDPR – saving that explicit consent is needed when processing sensitive and non-sensitive personal data. Inevitably, this is much more time-consuming. Such a burdensome obligation would initially make it seem that DPL provides a higher level of data protection compared to GDPR, but DPL's definition of explicit consent also has to be compared to GDPR's regular consent. *‘Freely given, specific and informed consent’* is common to both, while GDPR further requires *‘unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her’*.

While DPL consent might appear to be less onerous than GDPR, no DPB enforcement action has yet occurred: interpretation of explicit consent therefore remains uncertain. Under DPL, the processing grounds for sensitive personal data are notably more limited than under GDPR – with the exception of explicit consent, the majority of sensitive personal data can be processed, but only if it is currently permitted under Turkish law. The sole exception is data relating to public health matters.

Equally burdensome under DPL is the cross-border transfer of personal data to a third country. As determined by the DPB, the country of destination must have sufficient protection – either that, or parties must commit to provide it. DPL also states that: *“In cases where interests of Turkey or the data subject will be seriously harmed, personal data shall only be transferred abroad upon the approval of the Board by obtaining the opinion of relevant public institutions and organizations”*. Under this provision, data controllers must decide whether a transfer could cause serious harm, and if it does, they need to obtain DPL approval. However, it is unclear how these interests might be determined.

Controllers have to maintain internal records under GDPR, whereas DPL does not make any general requirement to register with the data protection authorities. Instead, it has one notable point, DPL and GDPR are in harmony:



just as not complying with GDPR requirements carries substantial penalties, so does any breach of Turkish provisions.<sup>85</sup>

### 3.2. Switzerland, the Federal Act on Data Protection (FADP)



In Switzerland, the Federal Act on Data Protection (FADP) protects the privacy and the fundamental rights of natural and legal persons when their data is processed. It sets out the requirements for permissible data processing in accordance with the rule of law and therefore protects against possible abuses.<sup>86</sup>

Although Switzerland is not a member state of the European Union (EU), the country has been traditionally connected to the European legislation, in order to ensure a free flow of capital between the two regions. Following the provisions of the General Data Protection Regulation (GDPR), applicable at the level of the EU starting with 25th of May 2018, Switzerland had to modernize its national legislation concerning the protection of data.

The FDAP first passed in 1992 and is currently undergoing review to bring it closer to the standards set out in the GDPR. While the FDAP and the GDPR share many similarities, there are some important differences.

Perhaps most notably, while the GDPR only recognizes natural persons to be "data subjects" the FDAP recognizes both natural and legal persons.

The EU's proposed ePrivacy Regulation, would extend privacy rights to legal persons in much the same way as the FDAP.

Some of the other key differences between the GDPR and the FDAP are set out below:<sup>87</sup>

---

<sup>85</sup> [Turkish Data Protection vs. GDPR: Spot the Difference \(finance-monthly.com\)](#)

<sup>86</sup> [GDPR and Switzerland - TermsFeed](#)

<sup>87</sup> [DPR and Switzerland - TermsFeed](#)

	GDPR	FDAP
<b>Scope</b>	All private persons, businesses, charities, and local, national and EU-level public organizations processing personal data in the EU.	All private persons, businesses, charities, and federal government organizations <b>based in Switzerland</b> . Public bodies at the cantonal (regional) level are subject to local data protection laws.
<b>Data subject</b>	Natural persons only.	Natural persons <b>and legal persons</b> (e.g. corporations).
<b>Standard of consent</b>	Must be freely given, specific, informed, unambiguous, and given via a clear, affirmative action.	Must be " <b>given voluntarily on the provision of adequate information.</b> " Must be given expressly when the processing concerns "sensitive personal data or personality profiles."
<b>Maximum fine</b>	4% of annual global turnover or €20 million.	250,000 Swiss Francs (CHF) (approximately €235,000).
<b>Data subject rights</b>	<ul style="list-style-type: none"> <li>Right to be informed</li> <li>Right of access</li> <li>Right to rectification</li> <li>Right to erasure</li> <li>Right to restrict processing</li> <li>Right to data portability</li> <li>Right to object</li> <li>Rights related to automated decision-making</li> </ul>	<p>Only "<b>the right to information</b>" is explicitly set out in the FDAP. This is similar in scope to the "right of access" under the GDPR.</p> <p>Data subjects can also <b>request the rectification and erasure</b> of their personal data through Swiss civil law.</p>
<b>Data breach notification requirements</b>	<p>For a serious data breach likely to risk the "rights and freedoms" of individuals: inform the <u>Data Protection Authority</u> within 72 hours at the latest.</p> <p>For a very serious data breach that is likely to cause "high risk to the rights and freedoms" of individuals: inform the affected individuals without undue delay.</p>	No formal data breach notification requirements.

## 4. Data Management Measures in HYDROPTICS

Data collection and management in HYDROPTICS will be guided through the following principles/measures:

- 💧 Data will be generated only in an **anonymized form**. Therefore, the questionnaires, interview guidelines and other used instruments must not contain questions, which answers could lead to the participant's identity – alone or in combination with other answers.
- 💧 The **anonymity and privacy of participants** must be respected. Personal information must be kept confidential. Guarantees of confidentiality and anonymity given to the participants must be honoured, unless there are clear and overriding reasons to do otherwise.
- 💧 In case that the participants must be registered at the HYDROPTICS platform, they must not be registered with their name. E.g. an ID-code will be applicable instead of it. That **guarantees the anonymity** of the participant and further, the ID-code helps to match answers of questionnaires and the data collected at the platform by the user.
- 💧 The participants themselves have their **data sovereignty**. In case the participant wants the deletion of their data, this has to be done without any undue delay.
- 💧 The participant is allowed to change/ limit the access authorization of their data collected at the HYDROPTICS platform.
- 💧 Only information pertinent to piloting activities is permitted to be collected.
- 💧 All researchers have the duty of confidence in regard to collected data.
- 💧 The integrity of stored, processed and published data must be ensured by the researchers and the project consortium.
- 💧 Data that are collected by the participant at the HYDROPTICS platform must be treated with care:
  - 💧 Participants must be informed that the data could be used for the project.
  - 💧 Participants must be informed in which way the data could be used.
  - 💧 The participants must be informed who has the data sovereignty.
  - 💧 The participants must be informed when the collected data will be deleted.
  - 💧 Appropriate measures, namely cryptography and physical security measures, must be taken by the researcher to protect the collected data.
  - 💧 Appropriate measures, namely cryptography and physical security measures, must be taken by the researcher to store and process data in secure manner.
  - 💧 In case the participant withdraws from the pilot, the collected data at the platform must be deleted or the access to them must be impossible for others, without any undue delay.

Pseudonymization/Anonymisation is a technique that is used to reduce the chance that personal data records and identifiers lead to the identification of the natural person (data subject) whom they belong too. Identifiers make identification of a data subject possible.

Pseudonymisation/Anonymisation enhances privacy by replacing most identifying fields within a data record by one or more artificial identifiers, or pseudonyms. There can be a single pseudonym for a collection of replaced fields or a pseudonym per replaced field.

Specifically, the GDPR defines pseudonymization in Article 3, as “the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information”. To pseudonymise a data set, the “additional information” must be “kept separately and subject to technical and organisational measures to ensure non-attribution to an identified or identifiable person”.

HYDROPTICS will consider the implementation of the following techniques<sup>88</sup>:

- **Directory replacement:** A directory replacement method involves modifying the name of individuals integrated within the data, while maintaining consistency between values, such as “postcode + city”.
- **Scrambling:** Scrambling techniques involve a mixing or obfuscation of letters. The process can sometimes be reversible. For example: “Annecy” could become Yneanc
- **Masking:** A masking technique allows a part of the data to be hidden with random characters or other data. For example: Pseudonymisation with masking of identities or important identifiers. The advantage of masking is the ability to identify data without manipulating actual identities.
- **Personalised anonymization:** This method allows the user to utilise their own anonymisation technique. Custom anonymisation can be carried out using scripts or an application.
- **Blurring:** Data blurring uses an approximation of data values to render their meaning obsolete and/or render the identification of individuals impossible.

While the project evolves the consortium will compare the proposed techniques and decide to implement one or more techniques according to the needs of the project.

---

<sup>88</sup> <https://www.enisa.europa.eu/news/enisa-news/enisa-proposes-best-practices-and-techniques-for-pseudonymisation>

## 5. Ensuring HYDROPTICS components GDPR compliance

In order to properly map the roles and obligations of each stakeholder, it is first necessary to understand the ecosystem of actors across HYDROPTICS use cases. The main stakeholders that can be immediately identified include:

- 💧 The HYDROPTICS service provider
- 💧 The service developer that offers their products to the infrastructure provider,
- 💧 Natural persons that purchase services from a provider
- 💧 Organisations (legal persons) that purchase services from a provider,
- 💧 The Data Protection Authorities, Law Enforcement, CERTs etc. and all organisations that might interface with the Data Controllers in case of a cyber security incident, data breach etc.

The first step is to identify which actors take up the role of the Data Controller, the Data Processor, the Data Protection Officer and the data subject, as well as their specific obligations.

### Obligations of the Data Controller:

The GDPR considers data subjects that are natural persons. Across all use cases that role is assumed by the users that connect to a network protected by HYDROPTICS components. When a service provider utilises HYDROPTICS components, it is their obligation to obtain **consent** from their clients (i.e. the data subjects). Consent can be given in the form of the contract between e.g. an ISP and the client purchasing services for a home network. Article 7 of the GDPR states that in this case all information “must be presented in a form that is easily distinguishable and comprehensible, otherwise the declaration will not be considered binding.” The service provider thus takes up the role of the **Data Controller** and appoints the **Data Processor** and **Data Protection Officer**, whose contact information should be accessible to the data subjects. When a private or public organisation purchases Security-as-a-Service from a provider, **both the client and the provider take up the role of the Data Controller**. The data subjects are the natural persons using the client organisation’s network (e.g. employees etc.). This use case falls under the case of **Joint Controllers**. The way that statutory processes are being implemented by the Data Controller, should overlap with the component, hence the Data Controller should remain in control of the reporting. The Data Controller is also obligated to refer to the Data Protection Authority to obtain consultation, authorisations or to report a data breach.

### Obligations of the service developer:

The developer that offers their products through the Catalogue or directly to the provider, is obligated to provide the full specifications regarding how data processing is performed within the component, as well as all the APIs and interfaces that allow data sharing. Using data minimisation practices within the component, data encryption or anonymisation/pseudonymisation is the obligation of the developer. It is the obligation of the service provider that purchases and instantiates the component to provide information on how it is used (i.e. which data sharing APIs are being used, etc.) to their clients. If data outputs from the component are being used for further processing by the HYDROPTICS provider, it is the obligation of the provider to release the specifications for the additional processing. The component developer is required to analyse which types of personal information can be viewed by the component (e.g. packet headers, email accounts, device IDs etc.) and specify if identifiability of the data subject can arise from the processing within the component. In essence, the component developer should complete a Data Protection Impact Assessment for each component product.

### Obligations of the Data Processor and Data Protection Officer:

The system administrator that onboards, instantiates and manages the component acts as the **Data Processor**. The Data Processor should be able to ensure that the rights of the data subject are being respected. Hence, the Data Processor should have available interfaces to erase, rectify etc. personal data when asked, either through the Dashboard or directly through the management interfaces of the component. If the component device does not retain data, the existence of such an interface might be irrelevant. If the data retained within the component are

not identifiable, the GDPR states that the data subject must provide a way to identify their data. The **Data Protection Officer** should serve as a contact point between the Data Controller and the appropriate **Data Protection Authority**. In case of a data breach, both the data subjects and the Data Protection Authority should be notified.

### ePrivacy Compliance:

In the context of ePrivacy, the HYDROPTICS components do not utilise cookies to offer a user experience hence there is no obligation from the component developer or ISP to provide cookie disclaimers. The network traffic, however, that passes through the component might contain cookie information. In such a case, cookies receive the same level of protection as any identifiable personal data under the GDPR. HYDROPTICS can consider additional measures to protect cookies and other communication metadata, should the ePrivacy regulation require additional protections for cookies and other communication metadata.

### Non-discrimination:

The HYDROPTICS components do not profile the user based on their network traffic or look into personal communication contents (e.g. messages, emails etc.). Hence, the risk of discrimination on the grounds of the Amsterdam Treaty is minimal. There needs to be assurance that the profiling information is not being used to deny access to basic services to a natural person based on their gender, ethnicity, religious, political views etc. This extends to the provision of internet access, to employment practices such as termination of a contract etc. In case of a remediation action that denies access to a user due to a security event, there is a level of transparency since the security events attached to a remediation action are logged. HYDROPTICS and the service developer, however, are obligated to ensure that in case of a false positive detection of an attack (i.e. when a user has been denied access to a network due to a false identification of a cybersecurity incident), the remediation action can be rolled back and access to a user can be restored.

Based on the previous analysis, HYDROPTICS has adopted a project specifications template (please refer to Annex I for an example on how to utilise the specifications through the Store and for the full template) and will improve it to include various security and privacy metadata. HYDROPTICS will deliver full specifications as part of WP2. This template can of course be adapted to any components that store or process personal data (internal or external to HYDROPTICS). The information will be enhanced with HYDROPTICS data and risk factors, and already includes:

- **General Information:** This includes basic information on the service/component such as its name, its developer and a brief description of its key function. It also includes any certification or standardisation marks.
- **Interfaces and Formats:** This is a brief overview of all the inputs and outputs that are programmed in the component. This includes all interfaces and a mention of all standard and non-standard data formats.
- **Data Types (based on Article 4 & Article 11):** This section overviews the way that the GDPR applies to the component. It contains information on the types of personal data that can be parsed by the component (e.g. if it collects IP addresses, emails, cookies etc.), any data in special categories (e.g. medical, political, religious etc. This generally does not apply to the specific HYDROPTICS components, although it might be used in future developments). Identifiability refers to the possibility that the data help identify a specific data subject with processing that is internal to the component. This helps assess the impact of a data breach and the level of protection that must be applied, within the DPIA. It is the responsibility of the component developer to include which types of personal data can be parsed by the component. An example is IP addresses in L3 network data, HTTP Cookies in L7 Data, etc. An analysis per protocol might be required<sup>89</sup>.
- **Data Storage:** This section details how the component stores data, what is the retention period, if there are additional protection mechanisms. It is the responsibility of the component developer to apply data protection in the form of encryption/pseudonymisation/anonymisation.

---

<sup>89</sup> (e.g. the headers From, Authorization, Proxy-Authorization, User-Agent, X-ATT-DeviceId, X-Wap-Profile, X-UIDH, X-Csrft-Token, X-Request-ID, X-Correlation-ID, Set-Cookie could lead to identification of a person or device within HTTP traffic). This work should be applied (at minimum) to the application layer protocols used by the project.

- 💧 **Data Processing:** This section details the processing of personal data within the component. It includes purpose, if processing is monetized or profiles the individual, a description of the data processing algorithm, and a description of the obligations of the data processor etc. It includes a justification on the lawfulness of processing and what is considered to be legitimate use for the component.
- 💧 **Data sharing:** This section details the possible data recipients. It lists the APIs and interfaces that are available to the component for data sharing. It considers GDPR stipulations, as well as the needs of law enforcement and cybersecurity agencies. The component provider is responsible to make clear which APIs are available for a data sharing, but the service provider that chooses to on-board the component may opt-out from using them. It is the responsibility of the service provider to provide information to their clients on how their data are being shared and if they are being monetized or re-used.
- 💧 **Data Subject Rights:** This section is relevant if the component retains personal data (such as network flows, IPs etc.). If there is no retention, the data subject rights do not apply. If data are retained but are not identifiable, Article 11 states that the data subject should provide a way to identify subsets of data relating to them.
- 💧 **Open Internet:** This part is relevant to the Open Internet regulation and EU's net neutrality rules. If the component applies traffic classification or rate limiting, it should be justified as lawful according to the regulation's stipulations.
- 💧 **Non-discrimination:** This section applies only on components that perform any sort of behavioural profiling or process data in sensitive categories. In this case, there should be justification of the use of this processing and safeguards should be in place to ensure that the information cannot be misused against the data subject or lead to discriminatory practices of any kind.

ePrivacy (pending definition of the new regulation): This section regards processing of communication contents/metadata and the identifiability of the data subject. The provider needs to ensure that communications are safe and secure and that no unwarranted processing takes place (with the exception of Lawful Interception).

## 6. Consent within HYDROPTICS

### 6.1. Data collection activities

The data collection activities that will be performed within HYDROPTICS events, will strictly adhere to EC regulation as well as the legislation of individual Member States and Associated Countries. The following specific cases for data collection are immediately identified:

- 💧 **The collection of personal, non-sensitive data within the HYDROPTICS public events (workshops, pitstops etc.).** WP1 foresees the organization of the HYDROPTICS advisory board workshops, demonstrations and public dissemination events, as a means to receive valuable stakeholder and end-user feedback within the project's lifecycle. Should the collection of data via questionnaires or surveys be required within the HYDROPTICS workshops, **it will only entail the collection of personal, non-sensitive data.** In such cases, participants will be presented **with a consent form, available both in English and the local languages** of the locations where each HYDROPTICS event will be held. The data will be **appropriately anonymised prior to any processing.**
- 💧 **Written and Audio/Visual documentation of the HYDROPTICS demos/pilots & dissemination events.** The HYDROPTICS demos will be extensively documented by means of collecting written and photographic evidence, as well as audio/video capture. As previously stated, the participants of the project's pilots will be debriefed and fully notified of all the pilot-related activities, including the documentation activities. Consent forms will be made available to the participants available both in English and the local language in the event location. Volunteers will be able to withdraw from these activities at any given time.

HYDROPTICS **does not foresee the need to collect sensitive information of any kind.** The consortium has also set in place a plan for ensuring the consent of every participant in the case of data collection activities.

### 6.2. Consent processes within HYDROPTICS

The Consortium has already identified certain cases when consent of individual participants to project activities (that might require data collection) is needed. Four forms of consent are identified:

- 💧 When not expressly granted, **Implied Consent** can be inferred by participation to the HYDROPTICS workshops and public events by persons that are willing observants, without their participation in data collection and feedback activities,
- 💧 **Express Consent** in written or verbal form will be required of participants to HYDROPTICS workshops and events that participate in activities that require feedback and data collection through questionnaires etc. for the purposes of collecting User Requirements etc.,
- 💧 **Informed Consent** in written form will be required for participation in the HYDROPTICS demos,
- 💧 **Unanimous Consent**, or general consent, by a group of several parties is consent given by all parties and is currently unforeseen.

Templates for Consent forms for audio/visual recording, participation in HYDROPTICS pilots or feedback collection will be made available as part of T1.3. The involved partners, under the supervision of the Technical Coordinator, will be responsible to collect and anonymise the information prior to any processing, and the Project Coordinator will be in charge of maintaining an archive with the consent forms and documenting the related activities in the annual WP1 reports.

### 6.3. Voluntary participation in pilots

Participants for the HYDROPTICS pilots will be identified and selected among:

- 💧 End-user partner organizations



- 💧 Other invited end-user representatives,
- 💧 Other partner organizations,
- 💧 Research and Academia,
- 💧 General public, if necessary.

The Consortium will not discriminate among volunteers on basis of their race, ethnicity, religious, or political beliefs etc. but will exercise caution in order to maintain demographic diversity in terms of age and gender balance among volunteers. Participants unable to give consent will be excluded from participating in the HYDROPTICS pilots. Minors, the elderly, and persons that are mentally impaired (e.g. intoxicated, sleep-deprived, showing signs of high stress, etc.) are thus excluded. The Consortium also retains the right to exclude a volunteer from participation or interrupt her/his participation in case of conflict of interest (such as participation to other relevant studies). HYDROPTICS states that there are no foreseeable risks to participants to project activities (physical or otherwise).

#### 6.4. Consent requirements for the HYDROPTICS pilots

Informed Consent requires three elements: (i) **voluntary participation**, (ii) **competence** and (iii) **comprehension**. In order to conform to the requirements, set in place by the Nuremberg Code, the Declaration of Helsinki, the APA Ethics Code and relevant EU legislation, the Informed Consent forms need to include, at minimum, the following information:

- 💧 A statement that HYDROPTICS involves research subjects and an explanation of the main purpose.
- 💧 The expected duration of the subject's participation in the pilot activity.
- 💧 A description of the procedures to be followed with focus on the experimental procedures.
- 💧 A statement that participation is voluntary.
- 💧 Information about who is organising and funding the research.
- 💧 A description of any reasonably foreseeable risk, discomfort or disadvantages. (First Aid and medical care will be available during the demonstration.)
- 💧 A description of any benefits to the subject or to others, which may reasonably be expected from the research, thus avoiding inappropriate expectations.
- 💧 A statement describing the procedures adopted for ensuring data protection/confidentiality/privacy including duration of storage of personal data and curation procedures.
- 💧 A description of handling of incidental findings.
- 💧 A reference to whom to contact for answers to pertinent questions about the research and research subjects' rights, and whom to contact in the event of a research-related injury to the subject.
- 💧 A statement offering the subject the opportunity to ask questions and to withdraw at any time from the research without consequences.
- 💧 An explanation of what will happen with the data or samples at the end of the research period and if the data/samples are retained or sent/sold to a third party for further research.
- 💧 Information about what will happen to the results of the research.

Finally, the participants will have to date, sign and initial the form, declaring that:

- 💧 They understand the purpose of the pilot,
- 💧 They have been given all the information that they have asked for,
- 💧 They agree to participate to the pilot,

- They understand that they reserve the right to ask for clarifications during the pilot and that they can withdraw at any given time.

Prior to the pilots, participants will be guided through the consent form and all pilot activities by qualified research staff.

## 6.5. Data lifecycle

Furthermore, participants will be fully informed about information handling during all the stages of the data lifecycle, including:

- Where and how this information it will be stored. The partner responsible for the data collection and processing will also be responsible to ensure the security of the facilities and the confidentiality of the data, with support from the Project Coordinator and the Technical Coordinator.
- Who will have access rights to it. Qualified research personnel will have access to the data gathered from the participants after they have been anonymised. Consent forms will only be accessed by the Coordinator and/or the Data Protection Officer of the organisation collecting and processing data.
- How long it will be stored. Only during the project lifecycle. The related partner and the Coordinator will be responsible to delete and destroy data sets after the project's conclusion.
- How it will be anonymised and processed. The Data Protection Officer of the partner involved in these activities, will be responsible to anonymise any collected data sets. Only the Coordinator or a certified Data Protection Officer will have access to non-anonymised sets, in order to facilitate the removal of a user's data, should it be requested by the user. Any processing (automatic or manual) will be performed only on anonymised sets.

The signed consent statements will be held on archive by the Project Coordinator and the involved partner, and will be relayed to the Project Officer (all relevant documents will be part of the annual project management reports). Furthermore, **participants will be able to withdraw their consent forms and data at any given time.** Any partner involved in data collection and data processing will be required to **provide assurance that the data will not be mishandled or utilized outside the expected scope of the project, along with the verification of their respective national Data Protection Authorities, when deemed necessary.**

## 7. Data Mapping

For the purposes of monitoring project activities to ensure GDPR compliance, DBC has already provided the partners and project participants with a questionnaire (see Annex III) and has conducted interview with all the project partners. As already indicated in the Grant Agreement HYDROPTICS adopts a specific template for the definition of the regulatory compliance specifications for each component. The template will relate to any components that store or process personal data (internal or external to HYDROPTICS) and add security metadata.

The questions included in the questionnaire, aimed to help document processing activities which relate to personal data processing. The partners were asked to fill in the questionnaire and provide the following information:

- 💧 Work packages and tasks, for the implementation of which, they need to process personal data.
- 💧 Type of personal data processed (e.g. name, surname, data of birth, address, health information, IP address, race, occupation, etc.).
- 💧 Type of processing (e.g. collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction etc.).
- 💧 Automatic or manual way of processing.
- 💧 Role in the processing, either as data controllers or data processors.
- 💧 Identification of possible data processors.
- 💧 Source of personal data (directly from the individual or from another source).
- 💧 Categories of data subjects.
- 💧 Purpose of processing.
- 💧 Legal basis of processing (e.g. consent or other).
- 💧 Means to gain consent by a data subject.
- 💧 Place where personal data are stored and retained.
- 💧 Third parties which may offer hosting services for personal data.
- 💧 Retention time.
- 💧 Technical and organizational measures applied by the partners.

It is important that partners and the DBC team understand and maintain a record of their processing activities. In such a way, the partners have spotted the critical parts/ aspects of their activities which relate to personal data. Thus, monitoring legal and ethical compliance proves to be transparent and more effective. In addition, the answers provided by the partners will be regularly updated (approx. every 6 months) so that they provide any additional information as the project progresses. As will be mentioned below, the need for a regular update has arisen by the careful study and review of the answers of the partners in relation to the work packages descriptions contained in the Grant Agreement.

The partners have completed the questionnaire by considering their activities so far. As a result, their answers indicate that for the time being, personal data processing for working on the project deliverables does not appear so often. Most of the partners do not process personal data, rather anonymized data. It shall be mentioned that besides processing of personal data of third parties, within the project processing of the personal data of the partners and the data subjects working for them takes place.

From careful and thorough review of the answers provided by the partners, we can infer that processing of personal data takes or will likely take place in the cases mentioned below. It is noteworthy that the list is not restrictive, rather subject to changes and updates as the project proceeds.

- 💧 **Project management:** Personal data are processed for the purposes of the project management. Personal data refer mainly to data of the participants and data subject which work for the partners and who are part of the consortium. The legal basis for the processing of such data is mainly the performance of a contract, that would be the performance of the obligations agreed upon in the Grant Agreement.
- 💧 **Trials:** For the purposes of working on some deliverables (e.g. validation of results, testing etc.) the partners may engage real users and perform use case trials. In such a case, it is imperative that the data subjects shall give their informed consent as indicated by the current legislation.

During the HYDROPTICS public events, workshops, public dissemination events: During such events, the organizing committee will have to collect and process personal data of participants. The data may include information about the name, profession, contact details etc. of individuals and photographs of the events, which may include data subjects. It shall be noted that no public events have taken place so far. However, it is noted that processing of personal data during such events, will be subject to a strong data protection policy. Individuals will be informed beforehand about the way their data are processed and will consent to participating in written form. In addition, if the events will be photographed or videotaped, the appropriate signs/ notices will be placed. It shall be noted that the Data protection information sheet which will be given to the participants will contain all essential information indicated by the GDPR (including but not limited to, name of data controller and/ or data processor, scope of processing, legal basis of processing, retention time of data, rights of data subjects, recipients of data, etc.). It shall be mentioned that the processing of data during such events will follow the guidelines set in the Grant Agreement – Ethics and Societal Impact Section (pg. 238-243).

## 8. Data Protection Impact Assessment (DPIA)

One of main elements of GDPR, introduced in article 35, is the need to perform the Data Protection Impact Assessment (DPIA) in specific situations.

Although not specifically described in GDPR, DPIA is considered as a process designed to describe the data processing and assess its necessity and proportionality. DPIA is designed to help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data by assessing them and determining the measures to address them. DPIAs are important tools for accountability, as they help controllers not only to comply with requirements of the GDPR, but also to demonstrate that appropriate measures have been taken to ensure compliance with the Regulation<sup>90</sup>. In other words, a DPIA is a process for building and demonstrating compliance and to avoid possible consequences of non-compliance which can cause a fine up to 4% of worldwide turnover for a company.

The GDPR places obligations on both:

- 💧 the 'data controller', which 'alone, or jointly with others, determines the purposes and means of the processing of personal data'; and
- 💧 the 'data processor', which 'processes personal data on behalf of the controller'.

However, the subject responsible for carrying out of DPIA is data controller.<sup>91</sup> If the processing is wholly or partly performed by a data processor, the processor should assist the controller in carrying out the DPIA and provide any necessary information.

The HYDROPTICS project team is applying the regulation defined by the Commission "Ethics and data protection" as mandatory for all H2020.

### 8.1. When the DPIA is required

A Data Protection Impact Assessment (DPIA) is required under the GDPR any time a new project is beginning that is likely to involve "a high risk" to other people's personal information.<sup>92</sup>

The variety of discussion running nowadays related to Impact Assessment and the related GDPR direction around DPIA demonstrate the difficulties to define borders which separate the need to do mandatory assessment (DPIA), from the simple adherence to GDPR principles. In general, the suggestion received by authorities is to run the assessment if not sure to be directly or indirectly involved in one of the cases which require that.

Furthermore, it is important to maintain the compliance during processes so assessment will be a periodic action to be performed. The aim of this document is to provide evidence of methodology, procedures and related outcomes that will be part of the compliance process activated by HYDROPTICS project partners to provide their specific assessments related to Legal, Social, Ethics and Liability issues.

In line with the risk-based approach embodied by the GDPR, carrying out a DPIA is not mandatory for every processing operation.<sup>93</sup> The GDPR demands that a DPIA be carried out "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."

---

<sup>90</sup>See also recital 84: "The 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".

<sup>91</sup> WP29.

<sup>92</sup> [Data Protection Impact Assessment \(DPIA\) - GDPR.eu](https://www.gdpr.europa.eu/data-protection-impact-assessment-dpia-gdpr)

<sup>93</sup> Article 29 Data Protection Working Party. 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. 17/EN WP 248 rev.01. ["DPIA Guidelines"] Adopted on 4 April 2017. As last Revised and Adopted on 4 October 2017. P.5

However, there is no ‘silver bullet’ method for carrying out impact assessments.<sup>94</sup>

***“What matters is the choice of an appropriate assessment method allowing for the best understanding and treatment of possible consequences of the envisaged initiative. These methods can range from qualitative or quantitative risk management to scenario planning, to scientific foresight, supported by a compliance check with relevant legal and otherwise regulatory requirements (e.g., technical standards).”***<sup>95</sup>

The GDPR sets out the minimum features of a DPIA:<sup>96</sup>

- a description of the envisaged processing operations and the purposes of the processing,
- an assessment of the necessity and proportionality of the processing,
- an assessment of the risks to the rights and freedoms of data subjects,
- the measures envisaged to:
  - “address the risks.”
  - “demonstrate compliance with this Regulation”.<sup>97</sup>

DPIA may concern a single data processing operation or could be used to assess multiple processing operations that are similar in terms of nature, scope, context, purpose, and risks.<sup>98</sup> Depending on the specific implementation of HYDROPTICS project, it should be decided what processing operation falling into the DPIA requirement can be deemed similar. Moreover, A DPIA can also be useful for assessing the data protection impact of a technology product, for example a piece of hardware or software, where this is likely to be used by different data controllers to carry out different processing operations.<sup>99</sup> Starting from May 25th, 2018, GDPR<sup>100</sup> applies to all EU countries. One of main elements of GDPR, introduced in article 35, is the need to perform the Data Protection Impact Assessment (DPIA) in specific situations.

Article 35 of the GDPR covers Data Protection Impact Assessments. The DPIA is a new requirement under the GDPR as part of the “protection by design” principle. According to the law:

***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.***

While this passage makes it clear that a DPIA is required by law under certain conditions, it is unhelpfully light on specifics. To help clarify the situation, here are some concrete examples of the types of conditions that would require a DPIA.<sup>101</sup>

- If you’re using new technologies,
- If you’re tracking people’s location or behavior,
- If you’re systematically monitoring a publicly accessible place on a large scale,

---

<sup>94</sup> D. KLOZA, Niels VAN DIJK, R.GELLERT, I. BÖRÖCZ, A. TANAS, E. MANTOVANI , P. QUINN. Data protection impact assessments in the European Union: complementing the new legal framework towards a more robust protection of individuals. d.pia.lab Policy Brief No. 1/2017. Available at: accessed July, 30, 2019

<sup>95</sup> Ibid

<sup>96</sup> GDPR, Art. 35 (7) and Recitals 84 and 90

<sup>97</sup> See DPIA Guidelines, P. 4

<sup>98</sup> See DPIA Guidelines, P. 4

<sup>99</sup>Ibid

<sup>100</sup> 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).

<sup>101</sup> [Data Protection Impact Assessment \(DPIA\) - GDPR.eu](https://www.gdpr.eu/Data-Protection-Impact-Assessment-DPIA)

- 💧 If you're processing personal data related to "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",
- 💧 If your data processing is used to make automated decisions about people that could have legal (or similarly significant) effects,
- 💧 If you're processing children's data,
- 💧 If the data you're processing could result in physical harm to the data subjects if it is leaked.

GDPR Article	Details	What this means
Art. 35(7)(a)	A systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the DC	Use visualisations (flow diagrams), cover the complete data lifespan, don't use techno-babble as many in the Supervisory Authority won't understand this!
Art. 35(7)(b)	An assessment of the necessity and proportionality of the processing operations in relation to the purposes	To observe data minimisation and purposes limitation principles in the GDPR, exact documentation is key to demonstrate compliance to the satisfaction of the Supervisory Authority.
Art. 35(7)(c)	An assessment of the risks to the rights and freedoms of the Data Subject	Assessment means not only description but also evaluation in terms of likelihood and severity!
Art. 35(7)(d)	The measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of the Data Subject and other persons concerned.	This is about effectiveness of what's been done that creates outcomes. This is what the Supervisory Authority will be looking for.

In other cases, where the high-risk standard is not met, it may still be prudent to conduct a DPIA to minimize your liability and ensure best practices for data security and privacy are being followed in your organization.

Additionally, the WP29 Guidelines provide the following criteria that shall be considered to define the need for DPIA:21 1. Evaluation or scoring 2. Automated decision-making with legal or similar significant effect 3. Systematic

monitoring 4. Data processed on a large scale 5. Sensitive data or data of a highly personal nature 6. Matching or combining datasets 7. Data concerning vulnerable data subjects 8. Innovative use or applying new technological or organizational solutions 9. When the processing in itself “prevents data subjects from exercising a right or using a service or a contract”.<sup>102</sup>

## 8.2. DPIA process key elements<sup>103</sup>

A DPIA should begin early in the life of a project, before processing commences, and run alongside the planning and development process. The UK's Information's Commissioner Officer diagram<sup>104</sup>, shown in the following figure - DPIA assessment process, illustrates the main actions:



A more detailed description of the steps is provided below:

STEP	COPLIANCE CHECK	
1: Identify for each single partner the need for a DPIA	The criteria to define whether the DPIA is applicable to HYDROPTICS are described in sections 3.1. The consultation of the organisation's GDPR compliance structure (a DPO if appointed), is also strongly suggested.	
	Partners' law compliance and transparency	Conduct an information audit to determine what information is processed and who has access to it.  Each HYDROPTICS partner has a legal justification for any data processing activities.  Each partner provides clear information about data processing and legal justification in the privacy policy.

<sup>102</sup> WP29 Guidelines

<sup>103</sup> <https://ico.org.uk/>

<sup>104</sup> <https://ico.org.uk/>



	<p>Data security managed by each single HYDROPTICS partner</p>	<p>Take data protection into account at all times, from the moment organisations begin developing a product to each time it processes data appointing a proper monitoring procedure.</p> <p>Encrypt, pseudonymize, or anonymize personal data wherever possible.</p> <p>Each partner creates an internal security policy for research team members, and build awareness about data protection.</p> <p>Know when to conduct a data protection impact assessment, and have a process in place to carry it out.</p> <p>Have a process in place to notify the authorities and your data subjects in the event of a data breach.</p>
	<p>Accountability and governance</p>	<p>Each partner should designate someone responsible for ensuring GDPR compliance across the organization.</p> <p>Appoint, if necessary, a Data Protection Officer</p>
	<p>Privacy rights</p>	<p>It's easy for HYDROPTICS stakeholders (internal/external):</p> <ul style="list-style-type: none"> <li>💧 to request and receive all the information you have about them.</li> <li>💧 to correct or update inaccurate or incomplete information.</li> <li>💧 to request to have their personal data deleted.</li> <li>💧 to ask you to stop processing their data.</li> <li>💧 to receive a copy of their personal data.</li> <li>💧 For partners process their data.</li> </ul> <p>If one of HYDROPTICS's module makes decisions about people based on automated processes, stakeholders have a procedure to protect their rights.</p>
	<p>When HYDROPTICS partners do this screening and decide a DPIA is not needed, they should document their decision and the reasons for it. In case of doubt, completing a DPIA is suggested.</p>	
	<p>In order to provide a clear view of processes as required by art. 35 . 7<sup>105</sup>, and to enhance the compliance with GDPR principles a DPIA should be carried out before</p>	

<sup>105</sup> Art.35(7)(a): a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller.

<p>Step 2: Each partner should describe the processing</p>	<p>processing data due the lack of that could generate high risks for the organisation. See Recitals 84<sup>106</sup>, 90<sup>107</sup> and 94<sup>108</sup></p>	
	<p>The nature of the processing</p>	<p>how data are</p> <ul style="list-style-type: none"> <li>💧 collected;</li> <li>💧 stored;</li> <li>💧 used</li> </ul> <p>Who</p> <ul style="list-style-type: none"> <li>💧 has access to the data;</li> <li>💧 you share the data with;</li> </ul> <p>whether partner uses any processors; retention periods; security measures;</p> <p>whether partner is using any new technologies; novel types of processing; and which screening criteria has been flagged as likely high risk.</p>
	<p>The scope of the processing</p>	<p>Related to personal data:</p> <ul style="list-style-type: none"> <li>💧 the nature of them;</li> <li>💧 the volume and variety;</li> <li>💧 The sensitivity.</li> </ul> <p>Related to their processing:</p> <ul style="list-style-type: none"> <li>💧 extent and frequency; duration;</li> <li>💧 number of data subjects involved;</li> </ul> <p>Geographical area covered.</p>
	<p>The context of the processing</p>	<ul style="list-style-type: none"> <li>💧 the source of the data;</li> <li>💧 the nature of partner relationship with the individuals;</li> <li>💧 how far individuals have control over their data;</li> <li>💧 how far individuals are likely to expect the processing;</li> </ul>

106 Recital 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.

107 Recital 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

108 Recital 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.

		<ul style="list-style-type: none"> <li>💧 whether these individuals include children or other vulnerable people;</li> <li>💧 any previous experience of this type of processing;</li> <li>💧 any relevant advances in technology or security;</li> <li>💧 any current issues of public concern;</li> </ul> <p>In due course, whether you comply with any GDPR codes of conduct (once any have been approved under Article 40 109 ) or GDPR certification schemes;</p> <p>Whether compliance with relevant codes of practice has been considered.</p>
	The purpose of the processing	<ul style="list-style-type: none"> <li>💧 Partner legitimate interests, where relevant;</li> <li>💧 the intended outcome for individuals;</li> <li>💧 the expected benefits for the partner, the project or for society as a whole</li> </ul>
Step 3: Partners should consider consultation	During HYDROPTICS's lifetime, and starting from the release of D2.3, this step will achieve a very high importance and the methodology provided herein could facilitate the identification of potential issues to be addressed by DPIA.	
Step 4: Each partner should assess necessity and proportionality	<p>In case of doubts, each partner can consult his country privacy agency to receive suggestions and be supported in the assessment procedures.</p> <p>A timeline and justification of data use should be provided compared with the evidence of possible alternative ways to conduct the data collection and its analysis.</p> <p>Anyhow data collected should be adequate, relevant and limited to what is strictly necessary in relation to the purposes for which the data are processed (data minimisation principle), see Art. 5 of the GDPR<sup>110</sup></p> <p>Data should also be accurate and kept up to date (accuracy principle).</p>	
Step 5: Each partner should identify and assess risks	<p>At this stage, it is necessary to consider the potential impact on individuals and any harm or damage the processing may cause - whether physical, emotional or material. HYDROPTICS will apply the following methods to identify and assess risks (also described in more detail in chapter 4 herein).</p> <p>Baseline security criteria: the minimum set of defences to fend off risks;</p> <p>Risk scale: a universal way of quantifying risk;</p> <p>Risk appetite: the level of risk the organisation is willing to accept; and</p>	

109 Art. 40 - <http://www.privacy-regulation.eu/en/article-40-codes-of-conduct-GDPR.htm>

<sup>110</sup> Art. 5 - Principles relating to processing of personal data.

	<p>Scenario- or asset-based risk management: the strategies to reduce the damage caused by certain incidents or that can be caused to certain parts of the organisation.</p> <p>Furthermore Art. 32 requires risks "from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data" to be identified and mitigated.</p>
<p>Step 6: Each partner should identify measures to mitigate the risks</p>	<p>All the sources of the identified risks shall be recorded. Moreover, for all the risks the measures to avoid or minimize them shall be considered. At this stage of the HYDROPTICS project at least the following measures might be identified: Take measures to pseudonymise and encrypt personal data;</p> <p>Ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;</p> <p>Restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and/or Implement a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of processing.</p>
<p>Step 7: Final step, process closing, and outcomes recorded</p>	<p>The primary aim of conducting a DPIA is to identify and minimise the data protection risks involved in a project. However, as has been emphasised throughout this guide, keeping a record of all steps taken as part of the DPIA will help to ensure that the process is completed thoroughly, and to reassure stakeholders that all data protection risks have been considered. This written record should also form the basis of putting into effect the data protection solutions which have been identified, and can be used to check off the implementation of each solution. HYDROPTICS project is providing a dynamic tool to manage DPIA evolution during project lifecycle.</p>
<p>Step 8: Integrate outcomes into plan and keep under review</p>	<p>After completing the process, each partner should integrate the outcomes from his DPIA back into HYDROPTICS project plan and keep his DPIA under review using the wiki tool provided by the HYDROPTICS team. Throughout this process, each partner should consult individuals and other stakeholders as needed.</p>

The methodology proposes an innovative approach, based on the use of a dedicated monitoring online tool, to DPIA that is closely related to processes in place in executing the HYDROPTICS project and considering<sup>111</sup> the expected outcomes and risks associated to those actions.

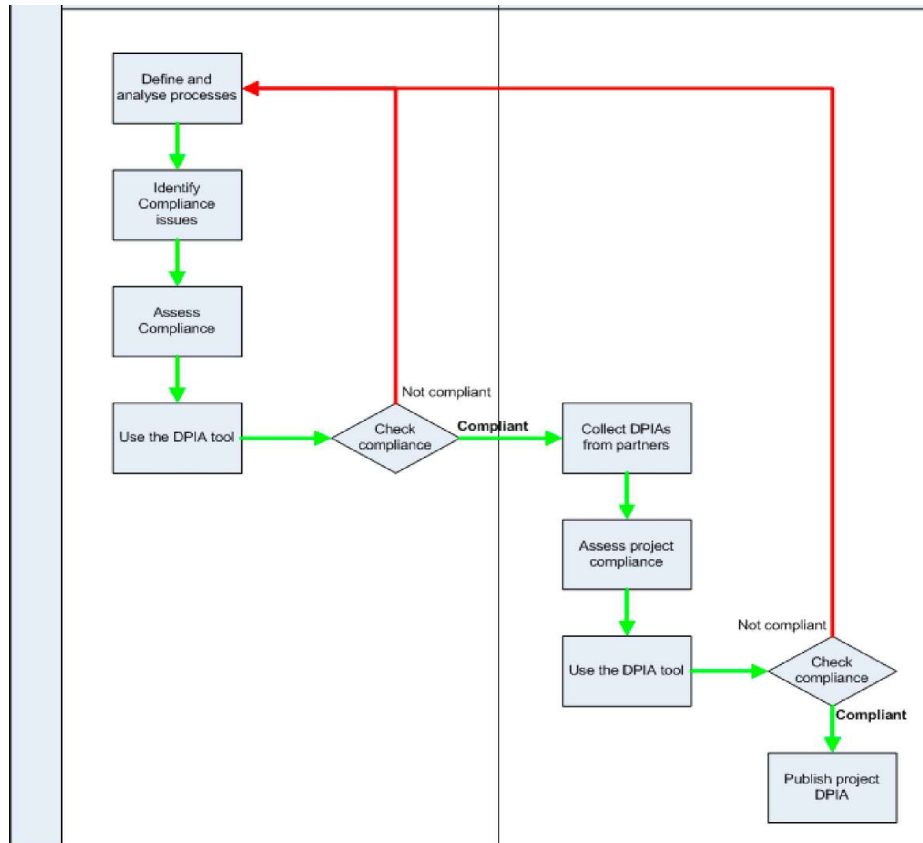
The main goal is to provide HYDROPTICS's partners with tools to conduct effective Data Protection Impact Assessments (DPIA).

Once the first Impact assessment and the related DPIA has been completed, the dynamic compliance process will start, supported by the wiki tool provided by the HYDROPTICS project.

Being a research project HYDROPTICS, needs to have a harmonised view to drive its overall impact. In view of that, here an extension of single partner compliance assessment process is proposed.

The following graph presents the various steps each partner should follow to achieve the compliance assessment.

<sup>111</sup> Duricu, A. (2019). Data Protection Impact Assessment (DPIA) and Risk Assessment in the context of the General Data Protection Regulation (GDPR).



### 8.3. Why DPIA in HYDROPTICS

Although the project is not running “systematic” actions as described in GDPR regulation, and no sensitive personal data are expected, being a research project in which some pilots will run for a limited period of time in a contained space, some actions carried out (e.g piloting activities, dissemination, etc.) could partially go under some of criteria specified bellow. Similarly, analyzing twitter posts related to a specific event in a specific area will have a tweet coverage close to 100%. In view of these, we suggested all partners involved as data controller to complete a dynamic DPIA. In the early months of the project this is considered to be preliminary, as there is not yet a detailed view of data use along the project. The GDPR makes it clear (Article 35 and recitals 89<sup>112</sup> and 91<sup>113</sup>) that the use of a new technology, defined in “accordance with the achieved state of technological knowledge” (recital 91), can trigger the need to carry out a DPIA. This is because the use of such technology can involve novel forms of data collection and usage, possibly with a high risk to individuals’ rights and freedoms. Indeed, the personal and social consequences of the deployment of a new technology may be unknown. A DPIA will help the data controller to understand and to treat such risks.

<sup>112</sup><https://gdpr-info.eu/recitals/no-89/>

<sup>113</sup><https://gdpr-info.eu/recitals/no-91/>

## 9. Preliminary identified risks

The table below presents the identified data protection risks and measures to mitigate them.

RISKS RELATED TO THE PROTECTION OF PERSONAL DATA						
Risk ID	Name	Description	Probability of occurrence	Impact	Risk response plan	Responsible partner
LAWFULNESS, FAIRNESS AND TRANSPARENCY						
DP.1	Consent lacks informativeness	<p>HYDROPTICS involves a wide range of technologies developed and operated by different partners. The technologies are connected to each other and operated both separately and commonly.</p> <p>Additionally, the project involves different data subjects and different pilots. The variety of all these elements as well as the complexity of technologies might create difficulties for a data subject to understand the flows of their personal data and subjects involved in the</p>	Possible	Severe	<p>For different groups of subjects and for different pilots, the processing activities and the roles of the processing entities will be defined in advance. The consent forms will vary depending on the data subjects and their role in the project (pilot, activities). Informational sheets will be provided in addition to consent forms. At the stage of signing the informed consent, the data subject will be asked if they fully understand its content.</p> <p>In case of non-understanding, the missing information will be provided and any issues clarified. For example, the project's technology developers will explain to the data subject how the technology in question</p>	DBC + all partners

		processing. This affects both lawfulness and transparency of data processing.			works and how it processes their data. All this will be monitored during the whole period of processing of data at every stage of their participation in the project. Moreover, material on the website and media about the project will serve as additional source of information/clarification for data subjects.	
<b>PURPOSE LIMITATION</b>						
DP.2	Purpose of data processing is not clearly defined	The purpose of personal data processing is conducting the research activities in the project. However, due to the complexity of the project, the mentioned purpose is deemed to be too wide and might lack sufficient specification.	Possible	Severe	The general purpose will be layered to sub-purposes and accompanied with clear description of the project and its goals (in informational sheets, on the website). This will ensure that the purpose is detailed enough to determine what kind of processing is and is not included within the specified purpose, and to allow that compliance with the law can be assessed and data protection safeguards applied.	DBC
DP.3	Processing of personal data outside the scope of the purpose it	The project's pilots will engage end users working at end user HYDROPTICS partners. In this case, some	Probable	Severe	While engaging end users in pilots or other project activities, the conditions of their data processing (including purpose, legal basis,	DBC + all partners

	was collected for	of their personal data is already being processed by the respective partners. Depending on the description of initial purposes of data processing, it might be incompatible with processing activities in the project.			processing activities) will be defined separately from the existing processing activities in their organisation. This will enable compatibility with the purpose.	
<b>DATA MINIMIZATION</b>						
DP.4		Hydroptics will collect data via different means and different technologies, which will be processed by different partners. It might happen that data collected by one partner for its purposes is provided to another partner but this data is not needed to achieve the goals of those partners	Possible	Severe	For every processing activity the scope of the data necessary to achieve the purpose of processing will be defined. Additionally, the list of partners involved in that processing activity as well as their respective roles will be specified. The filtering and cleaning of data at the will be applied. Moreover, the data that is processed for aggregation purposes will be pseudonymized and anonymized.	DBC + all partners
<b>INTEGRITY AND CONFIDENTIALITY</b>						



DP.5	Insufficient security of data processing, transfer and storage	Hydroptics's technical architecture is complex and will include different layers and several means of processing data (several types of devices, hardware, middleware). This all might create the security risks such as risks of data loss, breach of confidentiality.	Possible	Severe	The measures to ensure security of processing include data pseudonymisation and anonymization, secure middleware, data filtering and cleaning, encryption.	All partners
------	--	---	----------	--------	--	--------------

**STORAGE LIMITATION**

DP.6	Different periods of data storage	Hydroptics includes different partners processing different types of data and with regards to different processing activities. Partners might store the data for different periods of time.	Probable	Severe	The Hydroptics partners shall agree on the minimum and maximum periods for storing personal data (might vary for different processing purposes)	DBC + all partners
------	-----------------------------------	---	----------	--------	---	--------------------

**ACCOUNTABILITY**

DP.7	The roles of partners are not clearly defined	Involvement of almost all partners in processing of data with respect to different	Probable	Severe	All partners shall define their role (controller/processor of personal data), the partners they cooperate with and how. They will	DBC + all partners
------	---	--	----------	--------	---	--------------------

		purposes and activities creates the risk of lack of accountability ('everyone is responsible for everything'='no one is responsible')			specify the purposes of data processing, types of data and relevant activities.	
DP.8	Access to data by unauthorized subjects	HYDROPTICS includes different companies, organisations and universities. While some representatives are continuously involved in the project activities and are informed on the necessary procedures, other employees might get access to the data not being aware of the rules of its protection.	Probable	Severe	The HYDROPTICS partners will provide the information on the person responsible for data protection in their organization (name and contact details). In compliance with art. 30 of the GDPR, HYDROPTICS partners shall keep the record of processing activities describing the type of data processed, by whom (including the person within organization) and for which purpose. The scope and amount of people having access to the personal data shall be limited.	All partners
<b>RESPECT OF DATA SUBJECTS' RIGHTS</b>						
DP.9	Limited right to erasure of personal data	HYDROPTICS will apply technologies similar to blockchain that make the erasure of data of a specific data subject	Probable	Severe	To solve this issue, HYDROPTICS will use the type of technology that allows to delete the pieces of the information from the chain without deleting the whole chain (e.g., IOTA). It proposes the use of	All partners

		technically challenging			structure digital identities to store all information gather for a data subject in a private tangle of sorts. What this means is that when TensorFlow pre-processors identify private information related to any known data subject, the information is placed on a special private tangle that belongs to the data subject. This private tangle is analogous to the IOTA SSI structure in that it stores private information about the data subject. The data subject to which the data belongs has then the ability to keep or delete the whole private tangle, without affecting the integrity of the main tangle, thus allowing it to forget the private data, in an efficient manner. This will enable compliance with the requirement of data erasure.	
DP.10	Limited data portability	It is not defined if the data processed within HYDROPTICS might be technically transferred to another data controller under the	Remote	Severe	The control of data portability shall be carried out at the development and validation stages of HYDROPTICS's technical architecture.	All partners

		request of data subject				
--	--	-------------------------	--	--	--	--

## Conclusion

The deliverable is the first report of our activities in GDPR compliance and legal issues management in Hydroptics project. The defined methodology (compliance framework of Hydroptics) will be followed in the next period of the project where mature results will be available by the project beneficiaries and the pilot tests will be realised.

## Annex I: Regulatory compliance specifications for each component in HYDROPTICS

Based on consortium analysis, HYDROPTICS will adopt the following template for the definition of the regulatory compliance specifications for each component, showcased in the following Tables. This template will be evolved to any components that store or process personal data (internal or external to HYDROPTICS) and add security metadata. HYDROPTICS will provide the Data Protection Impact Assessment and related specifications for all data collecting/processing components. An example is then provided for the existing ORION vDPI (at TRL5).

**General Information:** This includes basic information on the component such as its name, its developer and a brief description of its key function. It also includes any certification or standardisation marks.

**Table 1: Component general information.**

1	General Information	component Name	<component name>
		component version	<component version number>
		component Developer	<component developer>
		component Description	<description of component>
		Certification & Standardisation	<any existing certification or standardisation marks>

**Interfaces and Formats:** This is a brief overview of all the inputs and outputs that are programmed in the component. This includes all interfaces and a mention of all standard and non-standard data formats.

**Table 2: Overview of interfaces and data formats.**

2	Interfaces and Formats	Data Inputs	<description of data inputs>
		Data Outputs	<description of data outputs>
		Data Formats	<description of data types and formats>

**Data Types (based on Article 4 & Article 11):** This section overviews the way that the GDPR applies to the component. It contains information on the types of personal data that can be parsed by the component (e.g if it collects IP addresses, emails, cookies etc.), any data in special categories (e.g. medical, political, religious etc). Identifiability refers to the possibility that the data help identify a specific data subject with processing that is **internal** to the component. This helps assess the impact of a data breach and the level of protection that must be applied, within the DPIA. It is the responsibility of the component developer to include which types of personal data can be parsed by the component. An example is IP addresses in L3 network data, HTTP Cookies in L7 Data, etc. An analysis per protocol might be required<sup>114</sup>.

**Table 3: Data types.**

3	Data types	Personal Data	Y/N	<description of personal data types processed>
		Special Categories	Y/N	<description of special/sensitive data processed>
		Identifiability	Y/N/P	<is the data identifiable within the component?>

<sup>114</sup> (e.g. the headers From, Authorization, Proxy-Authorization, User-Agent, X-ATT-DeviceId, X-Wap-Profile, X-UIDH, X-Csrf-Token, X-Request-ID, X-Correlation-ID, Set-Cookie could lead to identification of a person or device within HTTP traffic).

**Data Storage:** This section details how the component stores data, what is the retention period, if there are additional protection mechanisms. It is the responsibility of the component developer to apply data protection in the form of encryption/pseudonymisation/anonymisation.

**Table 4: Data storage.**

		Data Storage	Y/N	<description of local data storage>
4	Data Storage	Data Encryption	Y/N	<description of encryption scheme>
		Data Retention	Y/N	<retention period for data>
		Pseudonymisation	Y/N	<are the data decoupled or pseudonymised?>
		Anonymisation	Y/N	<are the data decoupled or anonymised?>

**Data Processing:** This section details the processing of personal data within the component. It includes purpose, if processing is monetized or profiles the individual, a description of the data processing algorithm, and a description of the obligations of the data processor etc. It includes a justification on the lawfulness of processing and what is considered to be legitimate use for the component.

**Table 5: Data processing activities performed by the component.**

		Purpose	<purpose of data processing>	
5	Data Processing	Monetisation	Y/N	<are the data being monetized?>
		Profiling	Y/N	< personal aspects relating to a natural person?>
		Data Processing	Y/N	<description of data processing algorithm>
		Data Processor	<who has access to the data & what are the obligations of the controller>	
		Data Protection Officer	<obligations of the Data Protection Officer>	
		Data Controller	<obligations of the Data Controller>	
		Consent processes	<Requirements for consent processes>	
		Lawfulness	<description of the lawful uses of the component>	

**Data sharing:** This section details the possible data recipients. It lists the APIs and interfaces that are available to the component for data sharing. It considers GDPR stipulations, as well as the needs of law enforcement and cybersecurity agencies. The component provider is responsible to make clear which APIs are available for a data sharing, but the service provider that chooses to on-board the component may opt-out from using them. It is the responsibility of the service provider to provide information to their clients on how their data are being shared and if they are being monetized or re-used.

**Table 6: Available APIs/interfaces for data sharing per recipient category.**

		HYDROPTICS components	Y/N	<which HYDROPTICS components get data from the component>
6	Data sharing	Third parties	Y/N	<which third parties get data from the component>
		Law enforcement	Y/N	<special API for law enforcement or national CERTs>
		Cross-border sharing	Y/N	<potential for cross border data sharing>
		CERT/CSIRT	Y/N	<access of CERT/CSIRTs to threat information>

**Data Subject Rights:** This section is relevant if the component retains personal data (such as network flows, IPs etc.). If there is no retention, the data subject rights do not apply. If data are retained but are not identifiable, **Article 11** states that the data subject should provide a way to identify subsets of data relating to them.

**Table 7: Data subject rights under the GDPR.**

7	Data Subject Rights	Right of access	Y/N	<is there an interface available from the component developer?>
		Right of rectification	Y/N	<is there an interface available from the component developer?>
		Right to be forgotten	Y/N	<is there an interface available from the component developer?>
		Restriction	Y/N	<is there an interface available from the component developer?>
		Notification	Y/N	<does the component generate notifications of a data breach?>
		Data portability	Y/N	<is there an interface available from the component developer to export data from the component?>

**Open Internet:** This part is relevant to the Open Internet regulation and EU’s net neutrality rules. If the component applies traffic classification or rate limiting, it should be justified as lawful according to the regulation’s stipulations.

**Non-discrimination:** This section applies only on components that perform any sort of behavioural profiling or process data in sensitive categories. In this case, there should be justification of the use of this processing and safeguards should be in place to ensure that the information cannot be misused against the data subject or lead to discriminatory practices of any kind.

**Table 8: Non-discrimination and misuse of data.**

9	Non-discrimination	Potential for misuse of data	Y/N N/A	<relevant only if data are special category, or if the component profiles the user>
---	--------------------	------------------------------	---------	---

**ePrivacy:** This section regards processing of communication contents and the identifiability of the data subject. The provider needs to ensure that communications are safe and secure and that no unwarranted processing takes place (with the exception of Lawful Interception).

**Table 9: ePrivacy compliance.**

10	ePrivacy	Protection of the contents of a communication	Y/N N/A	<relevant only if the component looks into the contents of the communications, i.e. the packet payloads>
		Use of cookies to provide a user experience and track user preferences	Y/N/ N/A	<relevant only if the processing includes cookies or tracks the users preferences>

Although the full specifications will be available at the Store level, an icon consent will be designed for easy visualization, since it is considered a best practice to avoid jargon and provide simple to understand instructions.



## Annex II: Informed consent form for participation in research

### [BEGINNING OF THE FORM]

I, undersigned [name] [date and place of birth – natural person] [contact details], hereby give my consent to take part in the research related to the pilot [name] carried out by the HYDROPTICS Consortium].

- 💧 I have been informed that the HYDROPTICS project (Photonics sensing platform for process optimisation in the oil industry) is a research project currently run under the Horizon 2020 Framework Programme under the grant agreement no. 871529. The coordinator of the project is Dr. Sargis Hakobyan, ALPES Lasers (ALPES) (sargis.hakobyan@alpeslasers.ch), who may be contacted with regard to any question regarding my participation.
- 💧 I have been informed about the nature and the purposes of the project, including the duration and the possible risks and benefits of participation. I have read and understood the Information Sheet dated [DD/MM/YYYY], or it has been read to me. I have had all my questions answered to my satisfaction.
- 💧 I understand that my participation in the research will include [describe briefly] as set out in the Information Sheet dated [DD/MM/YY].
- 💧 I have been informed that I can also address any ethical questions or concerns arising from this research to the Ethical and Legal Manager of the project, Ms. Sara Nabaraoui, DBC Europe (DBC and DIADIKASIA) (snabaraoui@diadikasia.gr).
- 💧 I understand [I will / I will not] be paid for my participation.
- 💧 I give this consent fully informed, freely and voluntarily and I understand that I am free to withdraw my consent and discontinue my participation at any time without any negative consequences.
- 💧 The relevant laws of [country] shall apply.

Done in two copies, of which one is for the HYDROPTICS Consortium and one for the participant.

Name of the participant: \_\_\_\_\_

Place / date: \_\_\_\_\_

Signature: \_\_\_\_\_

### Annex III: Compliance Questionnaire

GDPR QUESTIONNAIRE FOR PROJECT ACTIVITIES	
Work Package X	
<b>Partner Name:</b>	
<b>Contact Person:</b>	
<b>Contact information:</b>	
<b>Date:</b>	
Question(s)	Answer(s)
<p><b>For the purpose of working on the deliverables of the project, are you processing personal data?</b></p> <p>(personal data means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, <u>directly or indirectly</u>, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic,</p>	
<p><b>Identify the project work package(s) and specific task(s), for which you need to process data and the relevant deliverable.</b></p> <p>If you are processing personal data for more than one task(s), identify each specific task and relevant work package (WP).</p>	
<p><b>Identify the type of personal data you are processing <u>in relation to each respective task(s)</u>.</b></p> <p>(e.g. name, surname, data of birth, address,</p>	

<p><b>What is the type of processing? In other words, what do you do with the data?</b></p> <p>(e.g. collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction etc.)</p>	
<p><b>How do you process data?</b></p>	<p><b>Automatically:</b> (please specify, e.g. online questionnaires, website, platform, hosting, recordings, video taping etc.)</p> <p><b>Manually:</b> (please specify, e.g. printed questionnaires or copies, handwritten notes, etc.)</p> <p><b>Any other way:</b></p> <p><i>(Specify the above in accordance with each specific work-package and task)</i></p>
<p><b>What is your role in the processing of the data? Are you a <u>controller</u>?</b></p> <p>Do you alone or jointly with others, determine the <b>purposes and means</b> of the processing of personal data?</p> <p><b>Are you a <u>processor</u>?</b> Do you process the personal data <u>on behalf of another person</u> (controller)?</p> <p><b>If yes, who is the controller?</b></p> <p><b>Are you a <u>recipient</u>?</b> Are you a person, to which the personal data are disclosed, whether a third party or not?</p> <p>If yes, who is disclosing personal data to you?</p>	<p><i>(Answer in accordance with each specific work-package and task. For instance, you may be a controller for task 0.1 and a processor for task 0.2)</i></p>

<p><b>If you are a controller, do you engage ‘Data processors’ (a third party) to process data on your behalf?</b></p> <p><b>In other words, is there any third party that you have entered into an agreement with, to help you execute tasks which relate to data processing? (e.g. outsourcing etc.).</b></p> <p><b>Identify the tasks, which are outsourced.</b></p> <p><b>Have you a entered into <u>a written contract</u> with the data processor?</b></p>	<p><i>(Answer in accordance with each specific work-package and task.)</i></p> <p>By subscribing to the aforementioned third-party service, we have accepted its policy statement</p>
<p><b>Where do you collect the data from? Directly from the data subject?</b></p> <p><b>From another source?</b></p> <p><b>If yes, identify the other source?</b> (e.g. it would be another person, public office, open content databases, data mining etc.)</p>	<p><i>(Answer in accordance with each specific work-package and task.)</i></p>
<p><b>Describe the categories of data subjects. Are you processing children’s data?</b></p>	<p><i>(Answer in accordance with each specific work-package and task.)</i></p>
<p><b>Why do you process the data?</b></p> <p><b>What is the purpose of the processing?</b></p>	<p><i>(Answer in accordance with each specific work-package and task.)</i></p>
<p><b>What is the legal basis for the processing?</b> (If the legal basis is more than one, indicate this in the next column and provide relevant information.)</p>	<p><i>(Answer in accordance with each specific work-package and task.)</i></p>

<p><b>If the legal basis of processing is CONSENT, please identify HOW you receive consent of the individual.</b> (e.g. orally, in written form, electronically etc.)</p> <p><b>Provide information on the procedure you follow and a <u>copy of the information sheet and consent form.</u></b></p> <p><b>If consent is given electronically, provide a link to the relevant webpage.</b></p>	<p><i>(Answer in accordance with each specific work-package and task.)</i></p>
<p><b>Where do you store the personal data?</b></p>	<p><i>(Answer in accordance with each specific work-package and task.)</i></p>
<p>(e.g. on the cloud, on your own servers, on a third party’s servers, within EU, outside EU, in an office desk etc.)</p>	
<p><b>If personal data is hosted on a third party’s servers or the cloud, provide specific information on :</b></p> <p><b>A)</b> the name, type of entity that offers hosting services <b>and</b></p> <p><b>B)</b> whether the third party or cloud provider are GDPR compliant.</p>	<p><i>(Answer in accordance with each specific work-package and task.)</i></p>
<p><b>For how long do you store/ retain the data?</b></p> <p><b>Under what circumstances do you erase the data?</b></p>	<p><i>(Answer in accordance with each specific work-package and task.)</i></p>
<p><b>Do you implement technical and organizational security measures?</b></p> <p><b>Provide a description of the technical and organizational security measures you apply.</b> (e.g. security protocols, encryption, pseudonymization, CCTV, alarm, protection of premises, system security, cyber security, access control, transmission protocols, back ups, etc.)</p>	

**Do you keep a 'Record of Processing activities' for the project activities, which contains:**

- a) the name and contact details of the controller
- b) the purposes of the processing;
- c) a description of the categories of data subjects and of the categories of personal data;
- d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations
- e) where applicable, transfers of personal data to a third country or an international organisation,
- f) where possible, the envisaged time limits for erasure of the different categories of data
- g) a general description of the technical and

**The GDPR team reserves the right to ask for information in relation to the answers you provide and any other relevant GDPR issue.**