

ZDMP: Zero Defects Manufacturing Platform



WP2 Business Challenge: Vision, Market, Use Cases, and Interlinking

D2.5a: Regulation and Trustworthy System - Vs: 1.0.1

Deliverable Lead and Editor: Alvaro Moreton, ROOT

Contributing Partners: IKER, UOS-ITI, ICE

Date: 2020-02-10

Dissemination: Confidential

Status: EU Approved

Abstract

The purpose of deliverable D2.5a: “Regulation and Trustworthy System”, is to provide a first approach to the main legal issues related to data management in smart manufacturing by identifying them, whilst providing an outline on collateral aspects such as the ownership of machine-generated data and cyber security measures in the field of manufacturing industry.

Grant Agreement:
825631



Document Status

Deliverable Lead	Alvaro Moreton, ROOT
Internal Reviewer 1	Ronal Bejarano, TAU
Internal Reviewer 2	Eduardo Vila, MRHS
Internal Reviewer 3	Stuart Campbell, ICE
Type	Deliverable
Work Package	WP2: Business Challenge: Vision, Market, Use Cases, and Interlinking
ID	D2.5a: Regulation and Trustworthy System
Due Date	2019-09
Delivery Date	2019-09 (v1.0.0) & 2020-02 (v1.0.1) Due to Review request
Status	EU Approved

Project Partners:

For full details of partners go to www.zdmp.eu/partners



Executive Summary

This deliverable is the first of three corresponding to the Task 2.5 “Regulation and Trustworthy system”. This first deliverable offers a preliminary overview and study of the legal issues arising from the data management in relation to manufacturing industry and, more specifically, in relation to smart factories. To illustrate this, the different use cases developed for ZDMP have been analysed, and potential legal issues have been identified.

Additionally, a classification of the various types of data / information is provided and analysed with the aim of assessing which regulations should apply. Furthermore, collateral aspects such as the ownership of machine-generated data or cyber security measures in the field of the manufacturing industry, are analysed as well as other potential topics which may impact the ZD environment.

The contents of this document are:

- Overview of data management in smart manufacturing environments, focusing on the analysis of data lifecycle and types of data in this kind of environment, as well as on the identification of possible legal issues related to data management
- Analysis of the privacy issues that may arise in a smart manufacturing environment and an overview of the GDPR requirements, as well as the provision of general recommendations for its compliance
- Analysis of possible legal issues that may arise as a consequence of data sharing among organisations that collaborate in a smart manufacturing ecosystem
- Analysis of the use cases provided in D2.3: “Industry Scenario and Use Cases” to identify possible legal issues that may arise regarding the processing and sharing of data
- Overview of other legal issues that may arise in smart manufacturing
- Overview of the potential cybersecurity challenges faced in smart manufacturing and security recommendations for ZDMP
- Recommendations for implementing a trust model for ZDMP to manage risks

In the following versions of this deliverable, the different legal issues identified (especially the ones related to data protection), as well as the recommendations provided to be compliant with the applicable regulations, will be further developed in line with the partners’ needs that may arise as the project develops. Additionally, other collateral aspects such as recommendations related to cybersecurity will be extended. All these contents will be adapted to the project’s needs and to the information provided in the upcoming deliverables from the different WPs.

Table of Contents

0	Introduction.....	1
1	Data Management in Smart factories	6
	1.1 Data Lifecycle in Smart Manufacturing	6
	1.2 Types of Data in Smart Manufacturing.....	7
	1.3 Techniques for Data Management.....	8
	1.4 Overview of the Legal Issues Affecting the Use of Data	8
	1.5 ZDMP Liaising with other Data Oriented Projects	9
	1.5.1 Boost 4.0	9
	1.5.2 International Data Spaces	10
	1.6 Blockchain in Smart Manufacturing.....	10
2	Data Protection.....	12
	2.1 Personal Data Processing in Smart Manufacturing.....	12
	2.1.1 Personal Data Concept	13
	2.1.2 Manufacturing Companies' Employees Personal Data Processing.....	14
	2.1.3 Business partners and suppliers	15
	2.1.4 Customer Personal Data Processing	15
	2.1.5 Platforms' Marketplace and Personal Data Processing.....	15
	2.2 GDPR Compliance.....	16
	2.2.1 Scope	16
	2.2.2 Data Controller and Data Processor.....	16
	2.2.3 Data Protection Officer	21
	2.2.4 Principles Relating to the Processing of Personal Data	22
	2.2.5 Data-Subjects Rights.....	25
	2.2.6 Automated Individual Decisions Making, Including Profiling.....	27
	2.2.7 International Transfer of Personal Data.....	27
	2.2.8 Cloud Storage and Data Protection.....	28
3	Legal Issues Related to the Sharing of Data	30
	3.1 Data Ownership and IP Protection of Data	30
	3.2 Confidential Information and Trade secrets	33
4	Use Cases Analysis	35
	4.1 UC1.1: Engine Block Manufacturing: Defects Detection and Prediction in Aluminium Injection Operations	36
	4.2 UC1.2: Engine Block Manufacturing: Defects Detection and Prediction in Machining Operations	37
	4.3 UC1.3: Engine Block Manufacturing: Defects Reduction by Optimization of the Machining Process.....	38
	4.4 UC2.1: Moulds Manufacturing: Process alert System for Machine Tool Prevention.....	40
	4.5 UC2.2: Moulds manufacturing: Smart process parameter tuning.....	41
	4.6 UC2.3: Moulds Manufacturing: In-Line 3D Modelling.....	43
	4.7 UC3.1: Electronic Products Manufacturing: Component inspection	44
	4.8 UC3.2: Assembly line: AI-supported optical defects detection	45
	4.9 UC3.3: Assembly line: Monitoring and Control System.....	47
	4.10 UC4.1: Steel Tubes: Productor Monitor	48
	4.11 UC4.2: Stone Tiles: Equipment Wear Detection	49
	4.12 UC4.3: Supply Chain: Quality Control at Construction Site.....	50
	4.13 UC4.4: Supply Chain: Quality Traceability	52
	4.14 Use Cases Summary Table	53

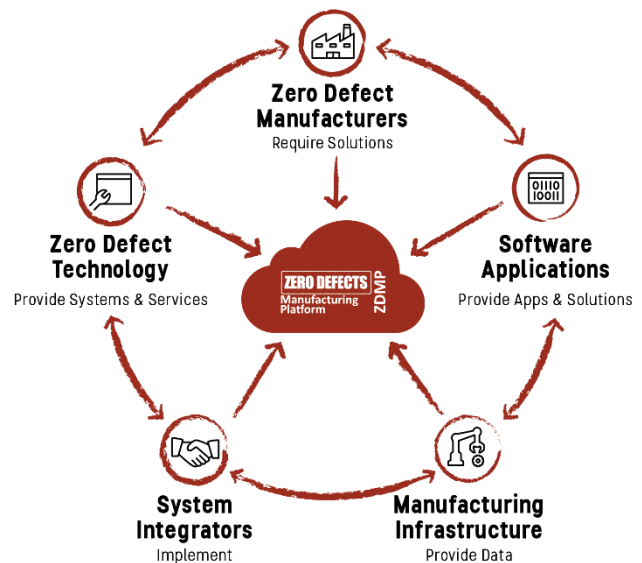
5	Other Legal Issues Related to Smart Manufacturing	55
5.1	Liability	55
5.2	Labour Laws	56
6	Cybersecurity	57
6.1	Cybersecurity in Smart Manufacturing Systems	57
6.1.1	Cybersecurity challenges	57
6.1.2	Security Measures.....	58
6.2	General Guidelines to Implement a Robust ZDMP Platform.....	60
6.2.1	International Electrotechnical Commission (IEC-62443)	61
7	Trust and Trustworthiness in Complex Systems	63
7.1	Trust, Trustworthiness, and Risks.....	63
7.1.1	Definitions.....	63
7.1.2	Trust Related Literature.....	64
7.2	Trust Modelling	64
8	Recommendations	67
9	Conclusions.....	74
10	Implementation Actions	75
10.1	Data Management Planning within ZDMP	75
10.1.1	Data Summary	75
10.1.2	FAIR Data.....	80
10.1.3	Allocation of resources	82
10.1.4	Data Governance and Security	82
10.2	Ethics Forum.....	83
10.3	Data Protection Implementation Plan.....	84
10.4	Data Exchange Implementation Plan.....	91
	Annex A: History	94
	Annex B: References.....	95
	Annex C: Consent form.....	100

0 Introduction

0.1 ZDMP Project Overview

ZDMP – Zero Defects Manufacturing Platform – is a project funded by the H2020 Framework Programme of the European Commission under Grant Agreement 825631 and conducted from January 2019 until December 2022. It engages 30 partners (Users, Technology Providers, Consultants, and Research Institutes) from 11 countries with a total budget of circa 16.2M€. Further information can be found at www.zdmp.eu.

In the last five years, many industrial production entities in Europe have started strategic work towards a digital transformation into the fourth-industrial revolution termed Industry 4.0. Based on this new paradigm, companies must embrace a new technological infrastructure, which should be easy to implement for their business and easy to implement with other businesses across all their machines, equipment, and systems. The concept of zero-defects in the management of quality is one of the main benefits deriving from the implementation of Industry 4.0, both in the digitalisation of production processes and digitalisation of the product quality.



To remain competitive and keep its leading manufacturing position, European industry is required to produce high quality products at a low cost, in the most efficient way. Today, the manufacturing industry is undergoing a substantial transformation due to the proliferation of new digital and ICT solutions, which are applied along the production process chain and are helping to make production more efficient, as in the case of smart factories. The goal of the ZDMP Project is to develop and establish a digital platform for connected smart factories, allowing to achieve excellence in manufacturing through zero-defect processes and zero-defect products.

ZDMP aims at providing such an extendable platform for supporting factories with a high interoperability level, to cope with the concept of connected factories to reach the goal of zero-defect production. In this context, ZDMP will allow end-users to connect their systems (ie shop-floor and Enterprise Resource Planning systems) to benefit from the features of the platform. These benefits include product and production quality assurance amongst others. For this, the platform provides the tools to allow following each step of production, using data acquisition to automatically determine the functioning of each step regarding the quality of the process and product. With this, it is possible to follow production order status and optimise the overall processes regarding time constraints and product quality, achieving the zero defects.

0.2 Deliverable Purpose and Scope

The purpose of this document “D2.5 Regulation and Trustworthy System”, is to offer a preliminary overview of the legal issues for data management in relation to manufacturing industry and, more specifically, in relation to smart factories. This is the first of three deliverables, and its content is will be updated and extended in the future based on the needs that may arise during the project and in particular once ZDMP Limited (ZDL) starts its activity.

This first deliverable identifies possible legal issues that may arise in a smart manufacturing environment such as ZDMP, particularly regarding data management. It provides an overview of the possible regulations that may apply as well as recommendations to comply with such regulations. Further aspects such as data management, cybersecurity, and the creation of trustworthy systems in smart manufacturing environments are also addressed in a general way in this deliverable and will be extended in following updates.

Specifically, the DOA states the following regarding this Deliverable:

T2.5	Regulation and Trustworthy System/Data Management	ROOT		M7-9, 16-18, 46-48
D2.5abc	Regulation and Trustworthy System/Data Management Document	R	CO	9, 18, 48 RD11, 4, & 6
<p>This task will offer a preliminary overview and study of the legal issues arising from the data management in relation to manufacturing industry and, more specifically, in relation to smart factories. Hence, a classification of the different types of data and / or information will be provided and analysed with the aim at assessing which regulations should apply on subjects such as intellectual or industrial property, trade secrecy, data protection, among others. Furthermore, collateral aspects such as the ownership of machine-generated data or cyber security measures in the field of the manufacturing industry, will be evaluated as well as other potential topics which may impact the ZD environment. After identifying a set of propositions and barriers, recommendations will be provided to resolve them. Automatic processing systems will also be based on smart contracts to facilitate the processing of information most-likely utilising advances in block chain technology.</p> <p>One of the focus points of the study will be to address the requirements a proper data processing structure shall observe in terms of governance, to be compliant with GDPR and other regulations and industry standards, while increasing proficiency, traceability, user-control over their data and maximising security. This will include liaising with experts like International Data Spaces and Data orientated projects, especially manufacturing ones, such as project Boost 4.0.</p> <p>This report will be used as a basis for RTD WPs 4-8, as well as other applicable WPs to ensure that a system for Data Management and Governance is both holistic and mandatory (where applicable).</p>				

0.3 Target Audience

Whilst primarily aimed at all the ZDMP project partners, this deliverable is of particular interest for those partners involved in WPs 4 to 8.

Additionally, it provides the European Commission and its reviewers a view on the possible legal issues arising from data management in a smart manufacturing environment that might be faced during the project.

0.4 Deliverable Context

This report is used as a basis for Research and Technical Development (RTD) WPs 4 to 8, as well as other applicable WPs to ensure that the system for Data Management and Governance is both holistic and mandatory (where applicable):

- WP4: Technical Challenge: Requirements, Specifications, and Standardization
- WP5: ZDMP Core Services and Middleware
- WP6: ZDMP Platform Building

- WP7: Process Quality Assurance
- WP8: Product Quality Assurance

Primary Preceding documents:

- **D2.3 “Industry Scenarios and Use Cases”:** Is a reference document focused on defining the top-level requirements associated with the industrial pilots that will be the validation scenarios of the ZDMP project

Primary Dependant documents:

- None

0.5 Document Structure

This deliverable is broken down into the following sections:

- **Section 1: Data Management in Smart factories:** This provides an overview of data management in smart factories. Data life cycle and types are analysed in general terms as well as data management related legal issues
- **Section 2: Data Protection:** Identifies the different scenarios in which personal data are collected and processed in smart manufacturing. Additionally, it provides an overview of the main requirements of GDPR, as well as some general recommendations to comply with this regulation
- **Section 3: Legal Issues Related to the Sharing of Data:** Analyses the different issues related to the sharing of data in smart manufacturing ecosystems such as determining the ownership of data or the sharing of confidential data
- **Section 4: Use Cases Analysis:** Each of the use cases provided in D2.3 is analysed to identify possible situations that should be taken into consideration from the legal point of view or that may generate legal risks
- **Section 5: Other Legal Issues Related to Smart Manufacturing:** Provides an overview of other legal issues that may arise in smart manufacturing, such as liability, labour law, or algorithm-related legal issues
- **Section 6: Cybersecurity:** Addresses the main cybersecurity challenges in smart manufacturing and provide general recommendations to assure security
- **Section 7: Trust and Trustworthiness in Complex Systems:** Provides recommendations for implementing a trust model for ZDMP that can help stakeholders to manage risks
- **Section 8: Recommendations:** Primary recommendations based on this report
- **Section 9: Conclusions:** Concludes and Summarises the document as well as identifies the next steps
- **Section 10: Implementation Actions:** In this section are briefly described the actions already implemented and the ones that will be implemented during the upcoming months regarding data management, data protection and data sharing within the project activities
- **Annexes:**
 - **Annex A:** Document History
 - **Annex B:** References
 - **Annex C:** Consent Form

0.6 Document Status

This document is listed in the Description of Action as “confidential” since it may relate to some specific data aspects which should not be visible to a public audience due to eg security concerns.

0.7 Document Dependencies

This document has two further iterations that are to be submitted in months eighteen and forty-eight.

0.8 Glossary and Abbreviations

A definition of common terms related to ZDMP, as well as a list of abbreviations, is available at <http://www.zdmp.eu/glossary>.

0.9 External Annexes and Supporting Documents

Annexes and Supporting Documents:

- None

0.10 Reading Notes

- None

0.11 Document Updates

Following the M9 Review comments the original document (v1.0.0) was requested to be resubmitted (v1.0.1) and the issues raised were addressed as follows:

Issue	How/Where addressed
DPO for the project should be named	A DPO for ZDMP project has been named (Oscar Garcia from ICE) (See Section 10.2)
An ethic advisor/board was not yet identified and installed	An Ethics Forum (composed by, the project’s DPO, the legal coordinator, and the members of the Executive Board) has been created (See Section 10.2)
A clear data management plan has not been forwarded to the Commission	An advancement of the first Data Management Plan (including highlights) have been included in this updated version of D2.5a (See Section 10.1). The plan was/will be to complete this in D2.5b
Analysis of which operations across all aspects of the project (from use cases, sub calls down to everyday consortium management) entail the collection, manipulation, transmission, or storage of personal data	This was already performed in the D2.5a (regarding use cases) and is now extended in this updated version of the deliverable in the Section 10.3.1.2 (personal data processed within the project administration and the dissemination activities) and in Section 10.3.1.3 (personal data processed within the subcalls activities)
Analysis of all instances of personal data should be conducted, not only in use cases but also in Dissemination, to ensure compliance to GDPR	This has been included in Section 10.3.1.2
The document should provide a concise chapter called privacy and intellectual property implementation plan	The new chapter can be found in Section 10
There is a strong focus on GDPR, however less on intellectual property. The data a	A preliminary analysis has been provided in this D2.5a (Section 3) in which due to the fact that the protection of

<p>company uses to reduce time to manufacture, defects, preventive maintenance etc, is clearly offering that company a competitive advantage. It is unclear why any larger manufacturer would put this kind of data at the disposal of a large grouping of actors like ZDMP especially since machine generated data lack many distinguishing factors that would allow it to be covered by copyright legislation.</p>	<p>data under copyright and trade secrets fall short in scope the via of the contractual agreement to protect datasets and regulate data sharing between the different stakeholders operating in ZDMP is recommended as the best option to cover all the necessary aspects. The next steps are described in this updated version of the deliverable (Section 10.4). The statement also supposes that manufacturers MUST put their data at the disposal of ZDMP. This is a misunderstanding. Providers will provide zApps, potentially to specific manufactures (possibly including their supply chain), potentially as generic solutions. It will be up to the providers to decide the features and what is best for their business (sales etc) which may or may/not include the sharing of data with the ZDMP central platform (eg storage) or not. The buyers of applications will seek to purchase based on their needs – for example in the field of data sharing. Indeed, as identified in WP3 deliverables larger manufacturers are more likely to host their own platforms because of the issues.</p>
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

In addition, the following comments were made which will be addressed in the M18 version of this deliverable

Issue	Comment
<p>A clear data management plan has not been forwarded to the Commission</p>	<p>There was no DOA commitment or other obligation to provide at M9 which was seen as a preparatory deliverable although some information was given. However, an extended version of this is now included in this re-submitted deliverable and will be further enhanced in the D2.5b (M18).</p>
<p>The Use Case analysis to identify where data is affected is the right approach but there needs to be follow up PM</p>	<p>A follow up will be carried out through the questionnaire provided in this document (see Section 10.3.1.1) and will be reported in the D2.5b (M18)</p>
<p>There is a strong focus on GDPR, however less on intellectual property. The data a company uses to reduce time to manufacture, defects, preventive maintenance etc, is clearly offering that company a competitive advantage. It is unclear why any larger manufacturer would put this kind of data at the disposal of a large grouping of actors like ZDMP especially since machine generated data lack many distinguishing factors that would allow it to be covered by copyright legislation.</p>	<p>Next iteration of the deliverable (D2.5b) will focus mainly in the different aspects that should be covered in a data sharing agreement, as well as the good practices for a trustable data sharing between ZDMP stakeholders. Additionally, virtual data space models that supports the secure exchange, such as International Data Space will be analysed, and cooperative actions will be fostered.</p>
<p>Industrial intellectual property (all assets including data) needs to be detailed</p>	<p>Regarding the IP of datasets; in the next Data Management Plan (M18) will be included the licensing information of the datasets used in the project</p>

1 Data Management in Smart factories

Data management can be defined as an organization's management of information for a secure and structure storage and access [TEC19]. An overview of the data management in relation to smart factories is provided in this section. This includes a classification of the various types of data, as well as a first approach to the legal issues arising from the use of this data, and which will all be extended in the next sections.

1.1 Data Lifecycle in Smart Manufacturing

To understand the data lifecycle in a smart manufacturing environment, there are two concepts that should be explained initially [SPS+19].

- **Internet of Things (IoT):** Is the extension of the internet interconnectivity into everyday objects and interrelated physical devices such as sensors, smart applications, mechanical machines, computer devices, people, etc Physical devices become a source of data in industrial environments through IoT, these devices provide massive information about manufacturing processes
- **Industrial Internet of Things (IIoT):** The IIoT combines different technologies such as the IoT, Cyber-Physical Systems, Big Data, or Simulation used in the industrial environment to organise operations

The devices used in the manufacturing process are constantly generating huge volumes of data that provide valuable information to manufacturers [SPS+19]. In smart manufacturing, Big Data analytics is used to refine complicated processes [WIK19]. Big Data in manufacturing refers to enormous amounts of multi-source heterogeneous data that is typically generated during the product lifecycle [TQL+18].

The continuous increase in volume and velocity of data produced by IIoT sensors and devices results in an increased network traffic between device-cloud communication and in-network data transmissions, as well as additional efforts for data ingestion and processing. This is particularly challenging for the zero-defects manufacturing industry, since the amount of data and the required rates to enable real-time analysis are significantly higher than in other IoT applications. The ZDMP Platform, its applications, the interfaces, and the data must be secure and thus support of robust industrial networks is necessary as is privacy, security, and related trust services.

To better understand the different risks related to data management that may arise in smart manufacturing environments, it is necessary to understand the lifecycle of the industrial data which is exploited in the various stages:

- **Data Acquisition:** Comprises of the collection of data from sensors and IIoT technologies, common environments including associated physical localisation, chronological data, ERP systems, SCADA / MES systems / data, and existing databases, to assist, detect, and monitor production processes in real-time. The raw data collected during this stage is generated by different physical components of the smart factory
- **Data Storage:** The large volume of data obtained during the data acquisition phase is stored in available repositories for later use [SPS+1]
- **Data Processing:** Refers to the series of operations conducted to convert data to information and knowledge that manufacturers may use to make an informed decision. During this stage data is pre-processed (data cleaning reduction and simplification, harmonisation, etc) and exploited through data mining and data

analysis. This can be improved with analytic techniques such as machine learning, forecasting models, and large-scale computing [TQL+18]

- **Data transmission:** Data transmission is essential to maintain communications and interactions among different information systems, cyber-physical systems, partners, and human operators [TQL+18]
- **Data application:** Real-time data analysis provided to the manufacturer is used to make informed decisions to improve performance, responsiveness, and flexibility [SPS+1]

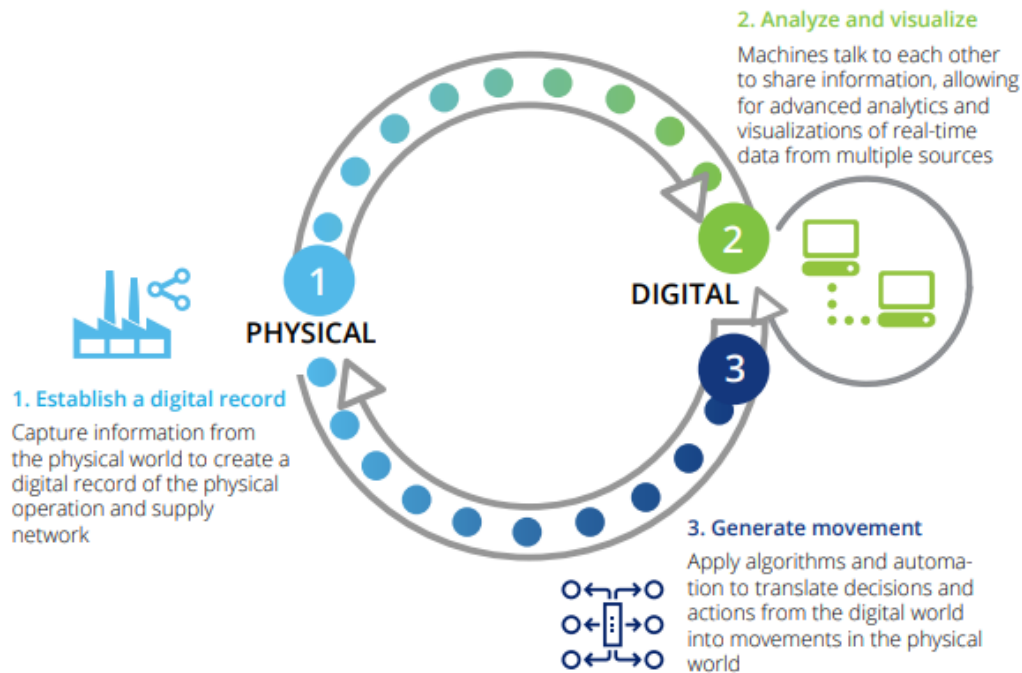


Figure 1: Physical-to-digital-to-physical loop [DEL 2016]

1.2 Types of Data in Smart Manufacturing

Data processed in a smart manufacturing environment is generated by diverse sources and in different forms. A first classification of the data could be made based on the origin of the data [TQL+18]:

- **Resource management data** collected from information systems (ie ERP). This is data related to product planning, material management, maintenance, inventory management, financial management, etc
- **Equipment data** collected from IoT devices. This is data related to operation conditions, real-time performance, or maintenance history of the equipment
- **User data** collected from internet sources such as operator log-ons, e-commerce platforms or social media platforms usually related to users' profile or users' behaviour
- **Worker Data** generated by the worker when interacting with the machines, through wearables, reports, etc
- **Product Data** collected from smart products and product services systems through IoT technologies. This is data related to product performance, environmental data (ie temperature, air quality), context of use (ie time, location)
- **Public data** collected through open databases. This is data related to civic infrastructures, Intellectual Property, scientific development, environment, etc, that

can be used by manufacturers to ensure that the manufacturing processes are compliant with the different regulations and industry standards

Other possible classification of the data processed in a smart manufacturing environment could be based on the stage in which the data is generated [KS18], for example:

- Machine data, raw data, and unprocessed data which are data sets collected from the relevant smart objects
- Processed data resulting from analysis of the raw data by any actor
- Input data entered by end users that interact with the relevant smart objects

Organisations in the manufacturing sector must be aware of the main data types to be shared in their inter-organisational relationships resulting from Industry 4.0 and implement adequate measures to protect each type.

Recommendations for ZDMP and ZDL	
Recommendation	Description
Types of data	<ul style="list-style-type: none"> • ZDL as well as the entities operating in ZDMP ecosystem, must be aware of the main data types to be shared in their inter-organisational relationships and implement adequate measures to protect each type (putting special attention on machine data and input data). Following this concept, it is recommended that contractual terms regulating the exchange of data cover at least raw data, process data, and input data

Figure 2: Recommendations Section 1.2

1.3 Techniques for Data Management

Today, organisations desire to predict, for example: Business trends through analytics, use machine learning and artificial intelligence in key knowledge-based processes, stream data from and to machines using the IoT. These are leading to new data management techniques, such as open-source projects, cloud-based architectures, and new storage hardware environments. Explanations of a few of them related to this deliverable in particular are as follows [DV18].

- **Data lakes / repositories:** Programs for distributed file services and which allow large-scale data storage at a relatively low cost. Their correct functioning depends on the management approaches defined by the organisation that must assure data is adequately catalogued and remains easy but secure to access. These are often (but not exclusively) based on open source. ZDMP implements data lake storage techniques for the persistence and processing of the data, with which the ZDMP services can consume and which, where applicable, can be used by zApps
- **Machine learning and artificial intelligence:** Companies are increasingly using machine learning to allow probabilistic matching of data. By using this approach, data that is similar, but different, to other data, can be matched and combined with little human intervention. It is recognised as a fast and effective method of data integration [DV18]. AI and Analytics are key aspects in ZDMP, and consequently machine learning processing techniques are implemented

1.4 Overview of the Legal Issues Affecting the Use of Data

The following table provides an overview of the main legal issues related to data management in a smart manufacturing environment. It should be considered and analysed

to apply the measures to avoid risks. This document develops the content of the table in greater detail and recommendations are provided to mitigate the related risks.

Legal issues related to data management	
Privacy / Data protection	<p>The processing of personal data should be compliant with the data protection regulations (GDPR).</p> <p>In a smart manufacturing environment (and particularly where the manufacturing companies are operating through a platform) there may be several situations in which the data used in different processes could be considered as personal data such as:</p> <ul style="list-style-type: none"> • Data generated by workers during the manufacturing process • Data generated by the end users • Personal data generated by suppliers or business partners • Personal data collected to be registered in the platform and to operate in the Marketplace (use of the zApps)
Data confidentiality (NDA / Trade Secrecy)	<p>Legal issues related to data shared with other companies operating in the smart ecosystem, eg through a manufacturing platform, when this data is sensitive or considered confidential. This include where data is related to the performance of the manufacturer or the supplier, their production processes, etc.</p>
Data Ownership	<p>Conflicts may arise when determining who is the legal owner of the data generated during the manufacturing process especially if shared with other partners in a design or supply chain.</p>
Intellectual Property	<p>Protection of databases and datasets.</p>

Figure 3: Legal issues related to data management

Recommendations for ZDMP and ZDL	
Recommendation	Description
Control of data sets and identification of possible legal issues	<ul style="list-style-type: none"> • All data sets processed should be under control, and the possible legal issues that may arise be identified. Data management components of ZDMP should focus on possible issues regarding privacy, data confidentiality, data ownership, and intellectual property

Figure 4: Recommendations Section 1.4

1.5 ZDMP Liaising with other Data Oriented Projects

It is expected that ZDMP liaise with experts such as International Data Spaces and data orientated projects, especially manufacturing ones, such as project Boost 4.0.

1.5.1 Boost 4.0

Boost 4.0 is the biggest European initiative in Big Data for Industry 4.0. The project aims to lead the construction of a European Industrial Data Space to improve the competitiveness of Industry 4.0. It introduces the use of Big Data in European manufacturing industry and provides the sector with the tools to obtain the maximum benefits from it [BOO19].

The initiative seeks to contribute to the international standardization of the European Industrial Data Space data models and open interfaces. This includes a certification program of equipment, infrastructures, platforms, and Big Data services. It will also

contribute to the adaptation and extension of cloud and edge digital infrastructures to ensure an optimal performance of the European Industrial Data Space [BOO19].

The Boost 4.0 initiative supports the International Data Spaces Association, whose main purpose is to guarantee the secure exchange and easy linking of data in business ecosystems. ZDMP will engage with Boost through this initiative. In this respect, data owners will be able to keep control over their shared data (eg they can set their own standards of data security), and ensure it is being exchanged with certified, trustworthy, and verifiable partners [IDS19].

1.5.2 International Data Spaces

The International Data Spaces Association set the basic conditions and governance for the creation of an international standard in the matter, providing a comprehensive and generally accepted way of handling data [IDS19].

In short, what IDS propose is a reference architecture and model to facilitate secure and standardized data exchange and data linkage in a trusted business ecosystem and provide a basis for creating smart services for companies to use for exchanging data. In this respect, each company will be required to register in the broker service provider, and then go to the service provider and select which service(s) they want to use. It should be noted that the underlying model is paid service/membership.

The secure data exchange implies that the information content or meaning assigned to the data being sent or received remains unaltered during the transition [OEC13]. The data linkage, which is a part of the process of data integration, will prevent duplicates and / or mismatches of the information shared with partners [EU19].

IDS will thus affect the way services are consumed and managed through the entire value chain whose current trend is pointing toward an end-to-end ecosystem. In the same way that Industry 4.0 has addressed the increasing complexity of supply chains and production processes; IDS aims to facilitate the exchange of data (eg users' preferences) amongst market participants without the risk of losing sovereignty over it through the dissemination and adoption of smart services concepts [IDS19]. To better understand IDS activities, several use cases can be found within its website¹.

In this respect, it has been identified by UNINOVA, who participates in the Boost 4.0 project (which forms part of IDS association), that ZDMP can contribute by providing one or two services, which should be decided in the following months, based on ZDMP components.

The next steps for month eighteen are:

- Discuss with IDS the possible contribution to define the services that can be provided by ZDMP
- Decide which partners should be involved in the development of these services
- Discuss internally the proposal that should be approved by the BOP

1.6 Blockchain in Smart Manufacturing

A blockchain is a digital record of transactions, in which individual records called blocks are linked together in a chain. A blockchain is a type of distributed ledger in which each transaction added is validated by multiple computers on the internet, forming a peer to

¹ <https://www.internationaldataspaces.org/success-stories/#usecases>

peer network. Consequently, invalid blocks cannot be added to the chain [TEC18]. Blockchain technology can be used for multiple purposes in smart manufacturing; for example [VID18] [MAT18]:

- Recognition and authentication of IoT devices remotely connected through blockchain
- Confirmation of dates and times of records to avoid editing or manipulation
- Automation of machines able to, autonomously and securely, initiate an order by using a blockchain between the ERP and parts supplier, as well as the cyber-physical system
- In smart contracts, it can be used as a secure and more legally binding way to draw up agreements between partners in a complex supply chain
- Cross-checking of manufacturers and suppliers' devices, ensuring confidentiality of sensitive information
- Blockchain may benefit manufacturing by offering an alternative for the partners operating in the smart manufacturing ecosystem to retain access to the most up-to-date records, technical documents, intellectual property, and trade secrets

After an assessment of the different scenarios developed in the context of the ZDMP project use cases, a need for implementing blockchain technology has not been identified, possibly because of the SME bias. In the following months, different possible blockchain applications for the project will be further analysed. The conclusion of this analysis will be included in the following iteration of this deliverable.

2 Data Protection

2.1 Personal Data Processing in Smart Manufacturing

Data generated by humans, objects, and systems is used together with other data sets from different devices and other companies in the manufacturing value chain. This data and the connected IIoT ecosystem are of relevance for privacy matters [KS18].

The stakeholders involved are various, from device and sensors manufacturers to software and applications companies, analytics companies, etc. They participate in a wide range of activities beyond the manufacturing process, including the process of collecting, transferring, storing, and analysing data.

In smart manufacturing, a large quantity of data is generated, transmitted, and processed. Amongst all this data it may be possible to find information related to an identified or identifiable person (eg workers of the manufacturing company, customers, etc). It is essential to identify which personal data is collected and processed to apply the necessary measures to comply with the General Data Protection Regulations (GDPR). This is a particularly delicate issue in a platform ecosystem in which a large amount of data is generated by, and shared among, different entities (manufacturers, suppliers, cloud services suppliers, app vendors, etc).

In accordance with the GDPR principles (Article 5 and others), organisations are duty-bound to achieve high levels of personal data transparency throughout the entire data lifecycle, which can be broken down into three major steps [LL19]:

- **Onboarding:** Activities related to bringing data objects into an organisation’s architecture and contains data collection steps from the sourcing of data to their deployment in data management systems
- **Data usage:** Activities related to the usage of data within the organisation and includes steps such as the management of data quality, the update of data objects, and their utilisation through the organisation processes
- **End-of-life:** Activities concerning the phasing out of data objects such as archiving and deletion

The table below shows the impact of data protection rights and requirements throughout the data lifecycle:

Requirement	Impacted data lifecycle		
	Onboarding	Usage	End-Life
Information duties	✓	✓	
Rights of access		✓	
Right of deletion			✓
Right of rectification		✓	
Right of consent	✓	✓	
Documentation requirements		✓	✓
Authorization requirements		✓	

Figure 5: Main data protection requirements throughout the data lifecycle [LL19]

In many cases, identifying personal data can be a complex task. Further subsections analyse different scenarios in which personal data may be collected and processed in

smart manufacturing, including the exchange and processing of data through manufacturing platforms.

2.1.1 Personal Data Concept

The concept of personal data should be explained before analysing the different possible scenarios.

Personal data is defined in the GDPR (Article 4.1) as “any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one 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, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person”.

According to the definition, the notion of personal data is very wide, and any information related to an identified or identifiable person is considered personal data. One person can be considered identified when, within a group of people, they can be distinguished from the others. On the other hand, one person is identifiable if they have not been directly identified yet but can be identified (ie by gathering different pieces of information) [AWP07].

Any statement about a person could be considered personal data, this means that the personal data concept could include information related to private life but also information regarding whatever types of activities undertaken by a person (working relations, economic, and social behaviour, etc) [AWP07].

According to Article 9 of the GDPR, the following information is considered sensitive data:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Processing of genetic data, biometric data to uniquely identify a natural person
- Data concerning health
- Data concerning a natural person’s sex life or sexual orientation

These special categories of sensitive data require enhanced protection and can only be processed under certain circumstances (eg explicit consent of the data subject) listed in Article 9 of the GDPR.

To be compliant with data protection regulations it is essential to identify the operations in which personal data are processed in the first place: In a smart manufacturing environment in which a vast amounts of data processing operations takes place, may be complex to detect those that involve the processing of personal data.

The following subsections provide different possible scenarios in which personal data is collected and processed in a smart manufacturing environment. This can help identify those operations in which personal data is processed and that requires the implementation of the organisational and technical measures necessary to comply with GDPR.

Recommendations for ZDMP and ZDL	
Recommendation	Description
Identify the processing of personal data	<ul style="list-style-type: none"> • ZDL, as well as the companies operating in ZDMPs ecosystem, must be aware of the data processing operations carried out and of the type of data processed • ZDL, as well as the entities operating in ZDMPs ecosystem, should make an assessment on all of their data processing operations to identify if the processing of personal data could be performed
Pay special attention to detecting the processing of sensitive data	<ul style="list-style-type: none"> • It is not expected that sensitive data is processed by ZDL or project partners in the ZDMP environment at this point in time. However, this should be thoroughly checked and monitored because of the particular nature of sensitive data • Furthermore, in smart manufacturing environments there are situations in which sensitive data may be collected and processed (eg the requirement of biometric identification for using a machine, operators using wearables that provide health related data). Consequently, all potential scenarios should be considered and analysed

Figure 6: Recommendations Section 2.1.1

2.1.2 Manufacturing Companies' Employees Personal Data Processing

There are several situations in which personal data from employees may be collected and processed in a smart manufacturing environment. Below are some examples in which processing of personal data may occur:

- The interaction between a machine and an operator may generate data related to the operator such as information about their performance or information related to time and attendance [BB15]
- To optimise the quality and efficiency of a smart factory, an assessment of staff productivity can be conducted. RFID chips and machine-fitted sensors offer information that enables the control of the whole production lifecycle, including information related to the behaviour of the operators involved [VDM16]
- The use of wearable devices in manufacturing is increasing; for example, production line staff using wearable devices to stay focused on what they are doing. These can be used to obtain additional information or deliver remote orders or commands [DRA18]). The use of wearables may generate data related to the performance of the operator, their location, and even related to their health
- The image of a person is considered as personal data. To assess and improve the production processes, images or videos may be recorded in the shop floor capturing the image of the operators
- Operators may generate reports (eg production process related reports, quality reports, etc) that are stored in the cloud; these reports may contain personal data
- The location of a person is considered personal data. The transport of materials or products is monitored on many occasions. When the location data of the vehicle that is transporting these products or materials is collected also the location data of the driver of the vehicle may be collected
- Operators may use applications provided through a platform (such is the case of ZDMP) to receive reports, warning messages, or different communications related to

the production processes. To use these applications, the operators will probably use a registration process where personal data must be provided

As indicated before, the examples provided above show scenarios in which it is possible that operators' personal data be collected and processed. However, this will depend on if such information is related to an identified or identifiable person (the operator). Each particular scenario should be examined and assessed.

2.1.3 Business partners and suppliers

A smart supply chain scenario is one where data is generated by ecosystems of suppliers, providers, distributors, retailers, and analytics is needed for value chain integration. Data generated (including personal data) in the course of the activities of the different entities integrating this ecosystem may be exchanged among the chain and consequently one entity can process the data generated in the course of the activities of other entities (eg a supplier, a business partner) [BDV18]. In essence all of the items mentioned in 2.1.2 apply here.

The ZDMP Marketplace allows a high level of connectivity between the parties (manufacturers, customers, and suppliers) in the supply chain. There it is possible to find different zApps that allow easy quality data sharing between manufacturers and suppliers but such zApps need to be GDPR compliant.

2.1.4 Customer Personal Data Processing

Within smart manufacturing, there are several situations in which the personal data of the manufacturers' customers are collected and processed. Follow are some example scenarios:

- Manufacturers are increasingly making products “to order” for individual customers. As these products are delivered directly to the customer some information such as the address or other personal data of the customer may be required [ARC18]
- Regarding product lifecycle management, the end product (a smart product) may communicate with the manufacturer and consequently transmit data from which facts about individuals (eg the owners of the product) can be inferred [VDM16]
- Personal data of customers may be processed in other situations (eg when the customer uses the manufacturing company website or customer databases are to be resold) [VDM16]

One possible scenario for ZDMP, not contemplated in the use cases, is regarding the developments of zApps that enable the monitoring of smart products after the production phase to detect possible defects. This kind of monitoring could reveal personal data of the owner of the smart product that is generating data when it is being used.

2.1.5 Platforms' Marketplace and Personal Data Processing

ZDMP and many other digital platforms use a Business Cloud / Marketplace providing an App store. The Marketplace allows a high-level of connectivity between the parties (manufacturers, customers, and suppliers) in the supply chain. Before starting to navigate such a (eg) Marketplace, users (the company and the related staff) need to be registered in the platform. During the registration process, personal data is provided. Moreover, personal data may be collected and processed when the clients are navigating through the marketplace website and interacting with it (cookies may be used, clients may provide comments and feedback about the apps, etc).

Recommendations for ZDMP and ZDL	
Recommendation	Description
General login for the platform	<ul style="list-style-type: none"> Many of the applications offered in the Marketplace will require the login of the people using them. One solution that should be assessed is the possibility of just using a general login (provided when registering in the platform) that could be used in the different applications

Figure 7: Recommendations Section 2.1.5

2.2 GDPR Compliance

As identified in the previous section, with the use of industry 4.0 technologies production data is increasingly generated and processed by the products and the production machines or through external platforms such as ZDMP [VDM16]. As shown in Section 2.1, there are many possible scenarios in which part of the data processed may be considered personal data because of its identification potential.

The General Data Protection Regulation (GDPR) relating to the protection of natural persons with regard to the processing of personal data and on the free movement of such data was published on May 4, 2016, and came into force on May 25, 2018, repealing the previous 95/46 directive. The GDPR is directly applicable to all the EU member states.

The new GDPR reinforces the principles, obligations, and rights set in the directive while also including additional mechanisms that allow individuals to better control their personal data [ENI17]. Recently GDPR has increased the penalties for non-compliance and consequently, organisations that fail to comply with the Regulation may face penalties up to €20 million or 4% of annual turnover of the previous year.

2.2.1 Scope

The material scope of GDPR (Article 2) is the processing of personal data wholly or partly by automated means or by other means.

GDPR applies to organisations when the processing of personal data is performed in the context of the activities of an establishment in the European Union (Article 3). However, GDPR also applies to the processing of personal data by organisations not established in the European Union when where the processing activities of these companies are related to:

- Offering of goods or services to persons in the European Union
- Monitoring of persons' behaviour when the behaviour takes place in the European Union

Regarding the UK situation after the Brexit, the UK Government has always maintained that the GDPR will be absorbed by the UK law following Brexit which would mean no material changes in data protection rules. However, it is likely that data protection regulators take the approach of treating UK as a “third country” in the event of a no-deal Brexit [DOS19].

2.2.2 Data Controller and Data Processor

There are two key roles in the GDPR that imply data protection obligations: The data controller, and the data processor.

According to the GDPR (Article 4.7), the “controller” is “the natural or legal person, public authority, agency, or another body which, alone or jointly with others, determines the purposes and means of the processing of personal data” [GDPR16]. The data controller is the main responsible for compliance with GDPR. Consequently, it should ensure a lawful, fair, and transparent processing of the personal data as well as the exercise of data subjects’ rights regarding their personal data. There will be joint data controllers where two or more controllers jointly determine the purposes and means of processing.

On the other hand, according to the GDPR (Article. 4.8), the data processor is “a natural or legal person, public authority, agency, or other body which processes personal data on behalf of the controller”. The role of the data processor usually appears when the controller delegates all or part of the data processing activities to an external organisation that processes the data on its behalf [AWP10].

In a manufacturing platform ecosystem such as ZDMP, in which many organisations (manufacturers, suppliers, developers, apps providers, cloud provider, platform provider, etc) are involved in the different data processing activities, it is important to analyse every case. It needs to be detected if any personal data is going to be processed and identify the data controllers and processors in each of these operations. For example, app providers usually fall under the definition of data controller, but manufacturers may also decide on the purposes and means of the processing of personal data. This is essential for determining the responsibilities of the different organisations involved in the processing of personal data.

Recommendations for ZDMP and ZDL	
Recommendation	Description
Identify the data controller and data processor roles in each operation in which personal data is processed	<ul style="list-style-type: none"> • ZDL and partners involved in data processing operations carried out within ZDMP framework should analyse the different processes that involve personal data processing, and identify who is / are the controller(s) and processor(s) in each of them • To make this assessment, it is necessary to identify who determines the purposes and means of the processing of personal data (data controllers), and who is processing data on behalf of the company that determines the purposes and means of the processing (data processor). It is possible that two or more data controllers exist (joint controllers) • In a smart manufacturing platforms such as ZDMP, in which many organisations (manufacturers, suppliers, developers, apps providers, cloud provider, platform provider, etc) are involved in different data processing activities, every process and the role of each of the organisations involved, should be carefully analysed by these organizations to determine who is the controller/s and processors in each of them
If there are joint controllers’, the obligations of each of them should be decided	<ul style="list-style-type: none"> • In those situations in which more than one controller is identified (eg if it is concluded that both, the manufacturer user and the app provider, determine the purposes and means of the personal data processing), the joint controllers should decide who will carry out which controller obligation, considering that each controller remains responsible for the compliance with the GDPR [ICO19]

Figure 8: Recommendations Section 2.2.2

2.2.2.1 Responsibilities of the Data Controller

The Data controller is responsible for implementing appropriate technical and organisational measures to ensure that the processing of personal data is compliant to the GDPR. This should take in account the scope, context, purpose, and nature of the processing as well as the risks for the rights and freedom of the natural persons whose data are processed (Article 24). The controller should be able to demonstrate that the processing of personal data complies with the regulation.

The GDPR (Article 25) requires a proactive attitude from the data controller who should apply the “privacy by design” approach to all the activities that involve the processing of personal data. Therefore, data protection should be considered from the beginning when a service, product, application, etc are designed. The main principles of the “privacy by design” approach is as follows [CAV10]:

- Proactive, rather than reactive measures, anticipating privacy invasive events before they happen
- “Privacy by design” should be embedded into the design of IT architecture and business practices
- Full functionality accommodating all legitimate interests
- End to end security. “Privacy by design” should have been embedded into the system before the first element of information is collected and extend securely through the whole data lifecycle
- Visibility and transparency for ensuring accountability and trust
- Respect for user privacy. Consider for any design, the data subject interests and needs whilst empowering them to play an active role in the management of their personal data

The controller should also apply a “privacy by default” approach where the required measures are applied to ensure that only the personal data that is necessary for the purposes of the processing activity are processed (Article 25).

The data controller, where applicable, should keep records of the processing activities containing the information required as per Article 30 of the GDPR. This includes contact details of the controller, purpose of the processing, description of the categories of data subjects / personal data.

Another main responsibility of the data controller is to inform the supervisory authority in case of a data breach without undue delay, and not later after 72 hours having become aware of it. The data controller should also communicate the data breach to the data subject, without undue delay if it is likely to result in a high-risk to their rights and freedoms.

Finally, the controller in certain circumstances should carry out an assessment of the impact of the envisaged processing operations on the protection of personal data prior to the processing. For example, when a type of processing (in particular the ones using new technologies) is likely to result in a high risk to the rights and freedoms of natural persons whose personal data are processed (Article 35). This Privacy Impact Assessment (PIA) should contain at least the following points:

- A description of the envisaged processing operations and the purpose(s) of the processing
- An assessment of the necessity and proportionality of the processing operations in relation to the purposes(s)
- An assessment of the risks to the rights and freedoms of data subject

- 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 the GDPR

Recommendations for ZDMP and ZDL	
Recommendation	Description
Privacy by design	<ul style="list-style-type: none"> A “privacy by design” approach should be applied to all the activities involving the processing of personal data. In this respect, data protection should be considered from the very beginning (the design of the product, service, zApp, etc) ZDL and all the partners involved in ZDMP should ensure the application of this principle to all data processing activities in which they are the controllers. For example, privacy by design may be applied when the zApps offered in ZDMP are designed by setting safeguard functionalities (eg encryption), setting limits to the app’s personal data collection, etc
Privacy by default	<ul style="list-style-type: none"> A “privacy by default” approach, should be applied to all activities involving the processing of personal data. This means that ZDL and all the partners involved in ZDMP should implement relevant measures to ensure that only personal data that is necessary is processed ZDL and all partners involved in the ZDMP project should ensure the application of this principle to all data processing activities in which they are the controller. They should analyse each of the processes that involve personal data processing and assess if the personal data processed is really necessary or if they could reach the same results by reducing the processing of personal data
Accountability	<ul style="list-style-type: none"> ZDL and all partners involved in the ZDMP project, should be able to demonstrate the application of the measures necessary to comply with GDPR requirements to all data processing activities in which they are the controller Compliance must be verifiable; especially by external stakeholders and data protection authorities It is also recommended to keep a record of the processing activities containing the information required as per Article 30 of the GDPR, such as contact details of the controller, purpose of the processing, and description of the categories of data subjects and personal data, amongst others. Even when it is not always mandatory to keep this record according to the GDPR (see Article 30), it is recommended to ensure a better control of the processing activities
Assessment	<ul style="list-style-type: none"> ZDL and all partners involved in the ZDMP project, should analyse, for the different operations that involve the processing of personal data, if a Privacy Impact Assessment (PIA) should be performed according to Article 35 of the GDPR However, even in those cases in which it is not mandatory, according to the Regulation, it is recommended to conduct a PIA for all the personal data processing operations carried out. This is a good method to detect potential risks and take actions to mitigate them

Privacy Policies	<ul style="list-style-type: none"> • ZDL, as well as all partners operating in ZDMP, should draft and implement transparent data protection policies [MET17]: <ul style="list-style-type: none"> • Policies (including web policies and cookies policies) must be drafted in conjunction with the organisation’s DPO or, at least, following the assessment of an expert in case a DPO is not required • Policies must be approved and endorsed by the highest-level management of each organisation • Policies should be accessible to the data subjects (eg ZDL should include its privacy policy in its website)
Raise employee awareness on data protection	<ul style="list-style-type: none"> • ZDL employees and ZDMP partners’ employees must be informed and trained on how to implement the privacy policies, especially those who are involved in the processing of special categories of personal data (eg an employee who keep records of other employee’s wearables) [MET17])
Fulfilment of the GDPR principles	<ul style="list-style-type: none"> • Controllers should ensure the fulfilment of the GDPR principles for personal data processing by implementing the necessary organisational and technical measures
Set a protocol to manage data breaches	<ul style="list-style-type: none"> • ZDL and all the partners operating in ZDMP should implement protocols, including the steps to be followed when a data breach occurs, such as: <ul style="list-style-type: none"> • Stop the data breach • Assess the damage(s) • Notify the breach to the supervisory authority and to those affected, if necessary, according to GDPR protections • Document the data breach including the facts, the effects, and the corrective actions taken • Control the notifications to the data subjects affected and keep all the evidence to prove that the notification was carried out

Figure 9: Recommendations Section 2.2.2.1

2.2.2.2 Responsibilities of the Data Processor

The processors conducting personal data processing on behalf of the data controller should provide sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of GDPR (Article 28).

The processing carried out by the data processor should be governed by a contract or other legal act under European Union or Member State law. Thus, binding the processor to the controller and which sets out 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. The processor should not engage another processor without the written authorisation of the controller.

The data processor, where applicable, should keep records of processing activities containing the information required in Art 30.2 of the GDPR. This includes contact details of the processor, categories of processing conducted, and data types.

Recommendations for ZDMP and ZDL	
Recommendation	Description
Sign a contract with the data processor	<ul style="list-style-type: none"> The processing of personal data by a processor shall be governed by a contract or other legal act under European Union or Member State law. It is binding on the processor with regard to the controller and which sets out the main obligations of the processor regarding the processing of personal data In the cases, in which ZDL or ZDMP partners delegate the processing of personal data to a processor (eg a cloud storage provider), a contract including the precise instructions to the processor and its obligations is necessary

Figure 10: Recommendations Section 2.2.2.2

2.2.3 Data Protection Officer

The Data Protection Officer (DPO) is a key figure in an organisation trying to comply with GDPR. The GDPR (Article 7) identifies that the data controller and the data processor should designate a DPO where:

- The processing is conducted by a public authority or body
- The core activities of the controller or the processor consist of processing operations which require regular and systematic monitoring of data subjects at a large scale
- The core activities of the controller or the processor consist of processing at a large scale of special categories of data (sensitive data) or personal data relating to criminal convictions

The DPO enables the controller and processor to be compliant to the GDPR by:

- Informing and advising the controller and processor regarding their obligations required by the GDPR
- Monitoring compliance with the GDPR
- Assisting the controller when performing a PIA
- Cooperating with the supervisory authority as a contact point

The DPO should act in an independent manner, which means that it/they should not receive instructions from the controller or the processor and should not be penalised for the performance of its tasks.

Recommendations for ZDMP and ZDL	
Recommendation	Description
Designate a DPO	<ul style="list-style-type: none"> It is highly recommended that ZDL designate a DPO. For all the partners involved in the ZDMP project, the designation of the DPO should be decided depending on their own circumstances However, even in those cases in which is not required by the GDPR, the designation of a DPO is always recommended, as it is a key figure that facilitates the compliance to the GDPR Moreover, a DPO can provide a good support, particularly in a complex environment for data management such as that of a manufacturing platform

Figure 11: Recommendations Section 2.2.3

2.2.4 Principles Relating to the Processing of Personal Data

The GDPR provides in Article 5 and others a series of principles that should govern the processing of personal data. These principles are explained in the following subsections.

2.2.4.1 Lawfulness, Fairness, and Transparency

According to this principle, personal data should be processed lawfully, fairly, and in a transparent manner in relation to the data subject.

For the processing of personal data to be lawful, it should be based on the valid consent of the data subject or on one of the other legitimate grounds provided in Article 6 of the GDPR (such as the existence of a legitimate interest of the controller). The consent should be freely given, specific, informed, and unambiguous and the data controller should be able to demonstrate that the consent has been given. The data subject should be able to withdraw the consent at any time and in a straightforward way. Finally, the processing of special categories of personal data (sensitive data) requires the explicit consent of the data subject.

This principle also requires that the data subjects are informed about the processing of their personal data. The data controller should inform the data subject, in a concise, transparent, intelligible, and accessible form about the purpose of the processing, the rights that they can exercise, and the time for which the data will be stored, amongst other information required in Article 13 of the GDPR. Different methods to provide the information (information sheet, web form, video, etc) can be used appropriate to the actual situation (eg if the data are collected through a website a web form could be appropriate but also a video) [AWP17].

Recommendations for ZDMP and ZDL	
Recommendation	Description
Analyse the possible legal basis for the personal data processing	<ul style="list-style-type: none"> The legitimate grounds for processing provided in Article 6 f of the GDPR should be assessed by the controller (ZDL or ZDMP partners depending on the circumstances). However, most of the time, the consent for processing will be based on the informed consent provided by the data subject If it is intended to base the personal data processing on the legitimate interest of the controller, special attention should be given to analysing and balancing this legitimate interest of the controller against the rights and interests of the data subject
Inform to the data subjects in a concise, transparent, intelligible, and accessible form	<ul style="list-style-type: none"> Data controllers should inform the data subjects about the purpose of processing, the rights they can exercise, and the time for which the data will be stored, as well as other information required in Article 13 of the GDPR Depending on the situation, controllers can choose the best way to inform the data subject, but always in an understandable way adapted to them. For example, if someone is navigating in the ZDMP marketplace, the website needs to submit personal data for registration, before collecting their consent. Then the electronic privacy policy contained in the website (in which the required information is provided) must be forwarded to them

Privacy Policies of the companies operating in ZDMP	<ul style="list-style-type: none"> It is recommended that ZDL demands all the companies operating in the ZDMP platform to have their own Privacy Policies accessible to data subjects
The controller should be able to demonstrate the consent	<ul style="list-style-type: none"> When ZDL or ZDMP partners base the personal data processing on the data subject's consent, they should be able to demonstrate the consent by keeping appropriate means of proof. For example, the signed consent forms, the log of activities in the website if the consent was submitted through the web, security copy of the email in which consent was provided, etc
Ensure the consent revocation rights	<ul style="list-style-type: none"> Free and simple means should be provided to enable the data subjects to revoke their consent. For example, ZDL (or ZDMP partners) can provide an email address to which the data subject can request the revocation of their consent

Figure 12: Recommendations Section 2.2.4.1

2.2.4.2 Collected for Specified, Explicit, and Legitimate purposes

According to this principle, personal data should be collected for specified, explicit, and legitimate purposes and no further processing incompatible with those purposes should be conducted. Consequently, the purposes of the processing, which should not be too vague or general, should be defined before starting the processing of the personal data [AWP13]. Additionally, these purposes should be explained to the data subjects in an understandable way.

In smart manufacturing environments, it is important to put in place adequate controls to comply with this principle when personal data is re-used or re-purposed which is something common in the processing activities carried out in these environments [ARK17].

Finally, as explained before, the personal data processing should be based on one of the legitimate grounds provided in Article 6 of the GDPR.

Recommendations for ZDMP and ZDL	
Recommendation	Description
Define the purposes of the processes	<ul style="list-style-type: none"> The purposes of the data processing operations that involve personal data should be defined and addressed before the collection of personal data by the controller (ZDL or ZDMP partners depending on the circumstances) Data processes and data sets should be monitored to identify if personal data is being re-used or re-purposed, which is something common in the processing activities carried out Data subjects need to be informed of any further processing of their information if it takes place with a purpose which is different from the purpose for which the personal data was collected in the first place. This should also include their consent (or the processing should be based on one of the legal grounds provided in the Article 6 of the GDPR)

Figure 13: Recommendations Section 2.2.4.2

2.2.4.3 Minimisation

According to this principle, personal data collected and processed should be adequate, relevant, and limited to what is necessary for the purposes of processing.

To comply with this principle, the data controller should collect and process the data needed for the purposes of the processing. This means that personal data can be processed only if the purposes established cannot be fulfilled in an alternative way by not processing, or processing fewer personal data. Consequently, the data controller should assess what personal data they are collecting, and why they need (or not) to collect this data. This can be a complicated task in smart manufacturing environments in which a large amount of data from diverse sources is continuously processed.

The application of this principle also affects to the quantity of the personal data processed, the extension of the processing, and the length of time that the personal data is stored, that should be minimised as much as possible.

One technique that should be implemented (as required by the GDPR) to make the processing of personal data less invasive is the pseudonymisation. Pseudonymisation is a process that transforms personal data in such a way that the resulting data cannot be attributed to a specific data subject without the use of additional information.

Another possibility is the use of anonymisation techniques, which consists of removing from the information processed all the elements that identify a person or makes a person identifiable.

GDPR does not apply to the processing of anonymous information. However, anonymisation techniques are not always completely effective since in many cases, the re-identification of the data subject is possible [AWP14]. Anonymisation is, therefore, a particularly good technique to reduce the risks associated with personal data processing but should be applied along with organisational and technical measures as required in the GDPR.

Recommendations for ZDMP and ZDL	
Recommendation	Description
Minimise the processing of personal data	<ul style="list-style-type: none"> Personal data should be processed when strictly necessary for the purposes of the processing. If the processing of personal data proves to be necessary, then it should be as minimum as possible. ZDL and ZDMP partners should assess to which extent the processing of personal data is necessary for those processing operations in which they are the data controllers
Make the processing of personal data the least invasive as possible and ensure privacy	<ul style="list-style-type: none"> Technical measures must be implemented to ensure appropriate levels of security and to mitigate identified risks [NCS17]: <ul style="list-style-type: none"> Implement safeguards such as encryption or pseudonymisation where anonymisation remains impossible or impractical for the purpose of the processing Implementation of strong authentication techniques

Figure 14: Recommendations Section 2.2.4.3

2.2.4.4 Accuracy

According to this principle, personal data collected should be accurate and kept up to date, where necessary. For this purpose, the data controller should set protocols to review the personal data that it is holding. In case any inaccuracy is detected, the data should be rectified or erased without delay.

2.2.4.5 Storage limitation

According to this principle, personal data should be kept in a form which permits identification of data subjects for no longer than what is necessary for the purposes for which personal data is processed. Data controllers should ensure that the data collected is stored strictly for the minimum time and must establish time limits for the erasure of the personal data. To do this, the controller may use automated tools that erase the data once the time limit expires or through periodic reviews of the data stored.

Recommendations for ZDMP and ZDL	
Recommendation	Description
Control of the data storage period	<ul style="list-style-type: none"> The implementation of procedures and protocols to control the storage period of personal data (eg to eliminate data when the set storage period has ended or when it is no longer necessary), is recommended

Figure 15: Recommendations Section 2.2.4.5

2.2.4.6 Security

According to this principle, personal data should be processed in a way that ensures appropriate security of this personal data, including protection against accidental loss, destruction, or damage using appropriate technical or organisational measures. See Section 6 for extended information related to security.

2.2.5 Data-Subjects Rights

The GDPR provides rights for the data subject that allows the individual to better control their personal data. The controller should implement adequate procedures and protocols to ensure that the data subject can exercise these rights. The data subjects' rights provided in chapter 3 of the GDPR are described in the following subsections with recommendations at the end.

2.2.5.1 Transparent Information

The controller shall take measures to provide any information and any communication relating to processing to the data subject in a concise, transparent, intelligible, and easily accessible form, using clear and plain language. The controller shall provide information on actions taken on a request related to the exercise of their rights to the data subject without undue delay and in any event within one month of receipt of the request (this period may be extended by two further months when necessary).

2.2.5.2 Access right

The data subject has the right to obtain the confirmation from the data controller on whether or not personal data concerning them is being processed, as well as the information related to the processing (eg purposes, categories of personal data, recipients, and other information established in Article 15 of the GDPR).

The GDPR encourages controllers to provide data subjects remote access to secure systems containing their personal data. In this regard, it would be a good practice to make available to the data subjects, information related to their personal data by providing them online access using secure log-ins.

2.2.5.3 Right to Rectification

The data subject has the right to obtain the correction to their personal data, when inaccurate, without undue delay.

2.2.5.4 Erasure of Personal Data

The data subject has the right to obtain from the data controller the deletion of their personal data without undue delay whenever one of the grounds provided in Article 17 of the GDPR applies.

The right to be forgotten, also included in Article 17 of the GDPR, is the right to obtain the removal of their personal data applied to internet search engines. When the controller has made the personal data public, and the data subject exercises the right to obtain the erasure of their personal data, the controller must take reasonable measures to inform all data controllers that such personal data must be erased.

2.2.5.5 Right to Restriction of Processing

Data subjects have the right to obtain from the controller the restriction of the processing when any of the situations provided in Article 18 of the GDPR applies.

2.2.5.6 Right to portability

Data subjects have the right to receive from the data controller the personal data concerning them, in a structured, commonly used, and machine-readable format. Additionally, the data subject has the right to have the personal data transmitted directly from one controller to another, where technically feasible.

2.2.5.7 Right to object

The data subject has the right to object to the processing of their personal data in those cases indicated in Article 21 of the GDPR. In the context of the use of information technology, the data subject should be able to object to the processing of their personal data by automated means, using technical specifications.

2.2.5.8 Data Subject Recommendations

The recommendations that relate to the previous subsections are:

Recommendations for ZDMP and ZDL	
Recommendation	Description
Application of protocols to ensure the exercise of data subjects rights	<ul style="list-style-type: none"> ZDL and all the partners operating in ZDMP should implement protocols to ensure the exercise of the data subjects' rights mentioned in the previous subsections (ie access right, right to rectification etc), the fulfilment of related requests, and to demonstrate the fulfilment of the obligations related. This includes: <ul style="list-style-type: none"> Provide a contact address of the company to which data subjects can send requests related to the exercise of their rights Set time limits to answer data subjects when requests are received and monitor the fulfilment of these times Keep evidence of the interactions with the data subjects

	<ul style="list-style-type: none"> • Keep control of the data sets that contain personal data to locate them when necessary (an adequate management of the metadata is necessary) • Implement the necessary technical measures to ensure the data portability right • Enable the exercise of data subject's rights by remote means (eg through internet), providing through secure log ins
--	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Figure 16: Recommendations Section 2.2.5

2.2.6 Automated Individual Decisions Making, Including Profiling

According to Article 22 of the GDPR, data subjects have the right not to be subject to a decision based solely on automated processing of their personal data, including profiling, which produces legal effects or that significantly affects them. There are some exceptions provided in the Article 22.

The automated decisions referred in Article 22:

- Are automated decisions solely based on automated processing without human intervention
- Produces legal effects (eg an employee is dismissed) concerning the data subject or similar significant effects (eg e-recruiting practices)

When an automated decision referred in Article 22 is made, the data subject has the right to:

- Be informed by the data controller about the automated decision making, including information about the logic involved and the expected consequences of the processing
- To obtain human intervention on the part of the controller, to express their point of view and to contest the decision

At this point, it is not expected that automated decisions with legal or significant similar effects will take place in ZDMP. However, this GDPR provisions should be considered when new automated processes are designed that involves personal data processing.

2.2.7 International Transfer of Personal Data

When smart factory models are designed, the exchange and processing of data across borders and legislative regimes is an inherent consideration [BB15]. The transfer of personal data outside the EU is an international transfer of personal data, according to the GDPR, and requires the compliance with certain rules. This is because the level of protection of the personal data provided by the legislations of these third countries may be lower than in the EU.

Prior to the international transfer of personal data to a third country, parties should check if there is an adequacy decision of the European Commission that certifies that country, a territory, or one or more specified sectors within that third country, with an adequate level of protection of the personal data. If this is not the case, the international transfer of data can be made when the controller or processor has provided appropriate safeguards established in Article 46 of the GDPR (ie Binding Corporate Rules, standard protection clauses adopted by the Commission) or under one of the conditions established in Article 49.1 of the GDPR, such as obtaining the explicit consent of the data subject after being informed of the risks of the transfer.

Recommendations for ZDMP and ZDL	
Recommendation	Description
Detect international transfers of data and the legal bases to carry out the transfer	<ul style="list-style-type: none"> • ZDMP partners and ZDL should monitor and register possible transfers of personal data to a third country • The countries for which there exists an adequacy decision from the Commission should be known • Analyse the possibility of providing appropriate safeguards • Analyse the possibility of making the transfer under one of the conditions of Article 49.1 of the GDPR

Figure 17: Recommendations Section 2.2.6

2.2.8 Cloud Storage and Data Protection

In smart manufacturing, there are two main options for data storage:

- OnPremise which refers to local hardware, meaning that the data is stored in local servers, computers, or devices [ANP17]. Even when this option can be costly for a company, OnPremise puts more control in the hands of the organisation, including the security of their data [HAL18]
- InCloud data storage which involves the storage of data on remote servers or hardware provided by a third party [ANP17]

The GDPR has led to a debate between those who think that OnPremise storage better meets the requirements of the GDPR, and those who think that the GDPR compliance may be achieved independently to the storage model [CAMP18].

Elasticity allows ZDMP users to adapt and scale to changing internal and partner scenarios through InCloud and OnPremise scalability.

ZDMP will typically not run its own cloud. Instead, it will use public cloud resources and/or make use of existing software frameworks to set up a private cloud, eg OpenStack. It is true that cloud storage of personal data entails some particularities regarding GDPR and thus compliance that should be carefully considered. The following list explains some of these:

- It may be complicated to fulfil the obligations of a data controller related to the data subjects' data portability and access to personal data rights, as finding the data stored in a multi-tenant cloud can be complex [CAMP18]
- Any type of information can be hosted in the cloud, including sensitive data. Cloud providers should ensure a secure service and take measures against data leakage
- It may not be clear where data is stored, and consequently, it can be difficult to determine the applicable law [TOL19]
- The data controller, which is using the services of a cloud provider, is externalising privacy. The controller should ensure, by signing (through a contract), that the cloud provider adopts the organisational and technical measures to comply with GDPR requirements
- The contract signed between the data controller and the cloud provider must also define a breach event and describe a procedure for the provider to notify the controller about any breaches and without undue delay [TOL19]
- It is important that the controller understands the technology of the cloud provider and the implication of these technologies on the security safeguards and protection of personal data [TOL19]

Recommendations for ZDMP and ZDL	
Recommendation	Description
Awareness on how the personal data is processed by the cloud storage provider	<ul style="list-style-type: none"> When contracting cloud storage services, ZDMP partners and ZDL should assess the different cloud services providers available in the market focusing on the organizational and technical measures that they implement to protect personal data
Sign a contract with the cloud provider	<ul style="list-style-type: none"> A contract should be signed with the cloud provider in which at least the following points should be considered [EDPS18] <ul style="list-style-type: none"> Applicable law Clauses related to the availability and quality of the service provided Transparency (eg communication about changes on infrastructure, proceedings, or results of security audits) Location of the company providing the cloud service Obligations of the cloud service provider to comply with data protection regulations Security measures applied by the cloud service provider The protocol to be followed by the cloud service provider in case of data breach Measures to ensure portability Cooperation of the cloud service with the data controller in the fulfilment of its obligations

Figure 18: Recommendations Section 2.2.7

3 Legal Issues Related to the Sharing of Data

3.1 Data Ownership and IP Protection of Data

The Internet of Things (IoT) stands as one of the most important and useful technologies present in Industry 4.0 and smart manufacturing. Through the utilisation of the IoT, factories can generate near real-time data insights regarding the condition of physical components and throughout the supply chain [DOR19].

To achieve successful outcomes, smart manufacturers need to consider the full array of supply chain partners and customers from the start [BML+17] since many are the stakeholders that can be using generated data in a single process.

As previously mentioned, there are many technologies involved in industry 4.0, from autonomous robots, augmented reality, simulation, and additive manufacturing, to Big Data analytics, distributed computing, artificial intelligence, and machine learning. The last four pose particularly serious concerns regarding IP protection of data and data ownership, especially where digital manufacturing platforms are involved.

For example, to collect data, IoT ecosystems rely on the use of sensors, which perform three major tasks: Sense and acquiring of data, communication of data following the appropriate protocols to relay relevant data to internet cloud services for further aggregation, and the analysis of trends. This data collected by the IoT sensors and systems can, however, pass through different stakeholders making it difficult to determine who owns it, as is the case of machine-generated data [AMR18].

Generally, Machine-Generated Data (MGD) is owned by the organisation that holds title to the apparatus connected to the IoT that records the data. This perfect scheme, however, is the less common of all, as data is often owned by one party and controlled by another, making it necessary to distinguish possession from ownership [KNI18].

The possibility of performing analytics on data from integrated smart objects has increased the value of data sets for organisations. It facilitates the generation of new knowledge whilst serving as a source to gain competitive advantage [KS18]. Following this logic, the efforts to ensure adequate protection of data have increased as well, and they go beyond intellectual property law as explained below.

As a first instance, data can be protected under trade secrets and copyright law, however, as both fall short in scope, organisations have had to resort on contractual agreements as part of their strategies to protect their intangible assets and even relying on property law [KS18].

Property law concerns the regulation of tangible assets scarcity. However, data is not only an intangible asset but rarely scarce. In this respect, it should be added that data can be easily copied and replicated, making it difficult and sometimes impossible, to exclude third parties from using it without authorisation, which is one of the pillars of property law [KS18].

Regarding copyright, the probability that collected data may lack the creative elements required to be protected under copyright law, also exacerbates the issues around data ownership. Protection is already considered weak when compared with other rights such as the ones under a contractual agreement. Fortunately, copyright protection is not the only possibility for protecting datasets. For database copyright, it is mandatory that

originality exists in the selection or arrangement of contents and a reduced level of protection can be given through sui generis right [KS18].

In general, databases in the European Union are protected under Directive 96/9/EC (Directive 96/9/EC, European Parliament and of the Council (March 11, 1996)). The Directive protects databases by copyright as long as they are original, while non-original databases can also be protected if the investment in obtaining, verifying, and presenting the data is considered substantial. The last is what is known as “sui generis” right [EC18].

The term of protection provided by the sui generis rights is 15 years following the database’s completion. If a new substantial investment is made to the existing database, its owner will have a new right of 15 years to the altered database or its substantial part [IPR17]. Notwithstanding the above, although copyright provides protection to data sets that meet the threshold for originality or based on the investment made by its owner through the sui generis right, it falls short in scope compared to the protection of the database in its most simple form [SCA18].

The scenario for sensors and machine-generated data in relation to the sui generis protection is quite contentious. For a database to obtain protection under sui generis right, substantial investment in the obtaining, verifying, and presenting the data must be demonstrated. However, in most Big Data situations this condition of substantial investment may not be fulfilled as investments into the “creation” of data are irrelevant for substantiality concerns, in accordance with the Directive [LEI18].

Depending on the type of databases created during the ZDMP project, parties can opt for one protection or another. Although, databases composed solely of sensors and machine-generated data usually fall under the scope of sui generis protection, the treatment such data receives after their collection, may allow for its protection under copyright law, based on the arrangement given to its content. Databases created by ZDL can also be protected under the same conditions.

Moreover, special attention must be given to the use of third parties databases (eg for training an algorithm necessary for the correct functioning of a ZDMP platform zApp). Private databases may require x authorisation from the creator or rights holder to avoid infringing intellectual property rights. However, this issue can be easily avoided by using public databases only.

In light of the above, contractual law appears as an alternative to guarantee the basic levels of legal protection of datasets and raw data. These are recognised as a valuable asset and are subject of important and numerous transactions worldwide. Moreover, as the property attribute of data and the rules of data ownership remain imprecise, contracts stand as a suitable solution to address the complex data value chain present in smart manufacturing ranging from data input, collection, maintenance, classification, verification, processing, exchange, reprocessing, analysis, and mining [QU17].

In this respect, contractual agreements impose obligations and are enforceable against other contracting parties, whilst the standard of proof for breach of contract is less stringent than for breach of intellectual property.

However, there are some disadvantages of contractual law relevant such as the private nature of contracts, which make agreements enforceable only against the other contracting party and not against other parties. It also includes the possibility that other rights in the legislation can override the contractual agreements (eg personal data rights) [KS18].

Data transaction contracts usually take the form of data sale contracts, data use contracts, and data service contract [QU17]. The following are examples of issues typically settled contractually [GLG+19]:

- Data ownership and use
- Treatment of original, derived, and usage data
- Receiving, collecting, or compiling of data from another party (ie a customer)
- Analysis and use of customer’s data to provide services
- Confidentiality of data
- Prohibition against using the data for purposes other than those envisaged in the contract except as necessary to provide its services or perform other contractual obligations

To conclude, the following table shows a series of recommendations regarding IP protection of data and data ownership in smart environments based on collaboration and characterised by an increasing connectivity, and a multiplicity of parties involved [KS18].

Recommendations for ZDMP and ZDL	
Recommendation	Description
Categorisation of data types	<ul style="list-style-type: none"> • Manufacturing companies should be at least aware of the main data types (raw data, machine data and unprocessed data; processed data; input data) to implement appropriate measures of protection • Once functioning, a full categorisation of the types of data that is being generated and stored in the ZDMP platform must be performed. This includes the source of the data (eg, the milling machine of a pre-determined party). The same is relevant to ZDL and zApp builders • Special attention must be given to zApp builders as they may require using third parties IP (eg databases) to train algorithms necessary for the correct functioning of ZDMP apps
Contracts to protect datasets	<ul style="list-style-type: none"> • Contractual law appears as an alternative to guarantee basic levels of legal protection of datasets and raw data. Data transaction contracts may be used to settle issues such as data ownership and use
Use of protected databases	<ul style="list-style-type: none"> • Companies operating in ZDMP must assure that contractual agreements surround ownership rights and licensing include, at least: <ul style="list-style-type: none"> • Data subject of the contract • Specific IP owned or licensed to which party • Identification of licensor and licensee • Territory and term (time) of the contract • Authorised use • Include references regarding EU regulations applied in the contract
Data ownership protection	<ul style="list-style-type: none"> • Companies operating in a smart manufacturing ecosystem should be aware of the different data ownership rights in relation to inter-organisational data exchange (who owns which data and to what extent, third parties involved, licenses granted, and under which conditions, etc) • Expectations, responsibilities, and liabilities regarding data security and privacy between parties may be established as both are vulnerable to breaches • ZDL should explicitly identify any third parties involved in inter-organisational exchanges of data, as it will function as ZDMPs main exploitation vehicle. A list of parties involved, licenses granted, and under which conditions, must be constantly reviewed and updated • ZDMP must assure that the utilisation of data from suppliers, partners, and customers is being performed without jeopardising data protection

	principles. Typically, anonymisations and pseudonymisation techniques may be required as well as avoiding any leakage of information that may constitute a trade secret or that hold a significant value for its owner
--	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Figure 19: Recommendations Section 3.1

3.2 Confidential Information and Trade secrets

There is constant exchange of confidential / sensitive information and data in smart manufacturing ecosystems (eg information related to a factories performance, information related to plant processes, etc). The utilisation of platforms such as ZDMP aggravates this phenomenon, as it facilitates the collaboration and interaction between companies and various stakeholders that constitute the supply chain.

In the new environment that surrounds smart manufacturing, trade secrets stand as an alternative for manufacturers to protect various proprietary aspects of the manufacturing process, including very specific matters such as requiring employees, suppliers, and any organisation having access to sensitive information or data, to enter into non-disclosure agreements because manufacturing processes are inextricably associated with a specific physical location [LAN19].

Contrary to other types of IP, trade secrets can protect a wider range of subject matters, including raw data, which is unlikely to receive protection as a database under copyright law or via a sui generis right as they both seek to protect expression and form rather than the substance of information [KEM14] (See Section 4.1 IP Protection of Data and Ownership), and that might represent a source of competitive advantage after undergoing a process of data analytics.

ZDMP is aiming at providing an extendable platform to help connected factories reach the goal of zero-defect production through a series of apps that will enhance a broad range of processes. Thus, it is to be expected that a large amount of data on the processes of the companies and their performance would be collected for the apps to work correctly. The following list shows operations performed inside organisations that may require trade secret protection to safeguard valuable data and information [KEM14]:

- **Data input operations:** Structured and unstructured data is collected from a variety of sources, such as instruments and sensors (eg distributed datasets generated from an IIoT device, data from mobile, and wearable)
- **Processing operations:** Comprise the processing of input data from internal and external platforms using, among others, business intelligence and analytics platforms, data visualisation, and machine learning
- **Data output operations:** Involves the utilisation of processed data for multiple purposes inside and outside an organisation (eg business analysis, risk management)

Trade Secrets would be equally useful for ZDL to regulate future relationships with users, customers, suppliers, and partners. To ensure the protection of trade secrets and confidential information, contractual measures are highly recommended to avoid data/information leakage and misappropriation of information. The following are common contractual measures used to protect trade secrets [VUK18]:

- **Non-disclosure agreements:** Are legally binding contracts that required employees (or party / parties involved in a negotiation) to keep valuable information secret. NDAs can be unilateral, bilateral, or multilateral depending of the amount of parties, and their conditions will depend on each specific case

- **Covenants not to compete:** Are promises that prohibit employees / parties to work for a competitor for a specific period of time. These promises aim to ensure that trade secrets are not revealed to competitors
- **Regulations:** Are explanations and security measures taken by a company to protect their trade secrets. In the case of ZDMP, this can ensure that all parties involved understand what is expected from them during and after the execution of the project

Furthermore, contractual measures should be complemented with technical measures that assure a minimal amount of people have access to confidential information to execute their functions and then only if necessary.

To conclude, the following table list a series of recommendations regarding the protection of data and information through trade secrets.

Recommendations for ZDMP and ZDL	
Recommendations	Description
Identification of possible trade secrets sources within the organisation	<ul style="list-style-type: none"> • Trade secrets stand as an alternative for manufacturers to protect proprietary aspects of the manufacturing process, from raw data to specific matters such as requiring employees, suppliers, and any organisation having access to sensitive information or data, to enter into non-disclosure agreements • The utilisation of non-disclosure agreements, which are the most common contractual measure associated with trade secrets, is recommended to ZDMP partners and ZDL • Organisations must identify all the various sources from which trade secrets and confidential information may be generated • ZDMP partners must identify possible sources of trade secrets by carefully reviewing all operations performed within their companies (eg a party or parties that, after performing analytics on certain inputs from a machine, discovers a method to enhance the functioning of a ZDMP app) • Once created, ZDL should identify commercially relevant information regarding the exploitation of the platform and evaluate the possibility of its protection through trade secrets
Implementation of technical, organisational, and contractual measures to protect trade secrets	<ul style="list-style-type: none"> • Organisations must ensure that all information subject to trade secret protection, enjoys additional measures (eg physical ones) that guarantee its secrecy, which is also a requirement of the Trade Secrets Directive • Technical measures must accompany contractual measures, especially those designed to limit the access to sensitive information or data, for example, concerning the performance of the machine of a specific partner. The criteria to address who can access which information, should be documented

Figure 20: Recommendation Section 3.2

4 Use Cases Analysis

The main objective of ZDMP is to develop a smart, SME friendly, open, zero-defect manufacturing reference platform, zApps, SDK, and marketplace for product and process quality in any factory. The D2.3: “Industry Scenario and Use Cases” provides an appropriate and representative collection of industrial scenarios to guide ZDMP’s development.

Different pilot scenarios, corresponding to the industrial sectors represented in the ZDMP consortium, have been provided in D2.3 for the use cases. For each pilot scenario the current state has been analysed, pointing out where the ZDMP platform and the applications that run on top of it can affect it the most. A detailed description in D2.3 of each ZDMP pilot is provided, describing the “AS-IS” scenario, the “TO-BE” scenario, and every application that will be developed in ZDMP for improving the “AS-IS” situation of the industrial pilot partners.

In this section, each of the use cases provided in the D2.3 is analysed to identify possible situations that should be considered from the legal point of view, or that may generate legal risks (eg processing of personal data, processing and sharing of sensitive or confidential data, data ownership). This analysis illustrates with examples, real situations in which potentially legal issues related to the data processing and data sharing may arise.

Each of the use cases analysed in this section includes the business model diagram “TO-BE” scenario, which represents the expected workflow of the process after the implementation of the ZDMP platform. It also includes a table of potential legal issues / risks, and a description of the situations that may generate them. The reading of x D2.3: “Industry Scenario and Use Cases”, is highly recommended for a more detailed explanation of the Use Cases and a better understanding of this deliverable. The table also contains a cross reference to the sections in this deliverable (D2.5) in which are developed the contents related to the possible legal issues identified.

Finally, note that this section only identifies, according to the information provided in Use Case deliverable D2.3, hypothetical situations in which it is possible that legal issues may arise (eg if there are operators involved in the production process, personal data may be collected and processed, but it is not necessarily the case).

The table below provides an index with all the use cases analysed:

Use cases analysis index	
Use cases	Partners involved
UC1.1: Engine Block Manufacturing: Defects Detection and Prediction in Aluminium Injection Operations	MRHS and FORD
UC1.2: Engine Block Manufacturing: Defects Detection and Prediction in Machining Operations	MRHS and FORD
UC1.3: Engine Block Manufacturing: Defects Reduction by Optimization of the Machining Process	ETXE and FORD
UC2.1: Moulds Manufacturing: Process alert System for Machine Tool Prevention	HSD, FIDIA, and FORM
UC2.2: Moulds manufacturing: Smart process parameter tuning	HSD, FIDIA, and FORM
UC2.3: Moulds Manufacturing: In-Line 3D Modelling	HSD, FIDIA, and FORM

UC3.1: Electronic Products Manufacturing: Component inspection	ALFA and CONT
UC3.2: Assembly line: AI-supported optical defects detection	CONT
UC3.3: Assembly line: Monitoring and Control System	MASS and CONT
UC4.1: Steel Tubes: Productor Monitor	PTM and FLEX
UC4.2: Stone Tiles: Equipment Wear Detection	CEI and ALONG
UC4.3: Supply Chain: Quality Control at Construction Site	FLEX, ALONG, and CONS
UC4.4: Supply Chain: Quality Traceability	FLEX, ALONG, and CONS

Figure 21: Use cases analysis index

4.1 UC1.1: Engine Block Manufacturing: Defects Detection and Prediction in Aluminium Injection Operations

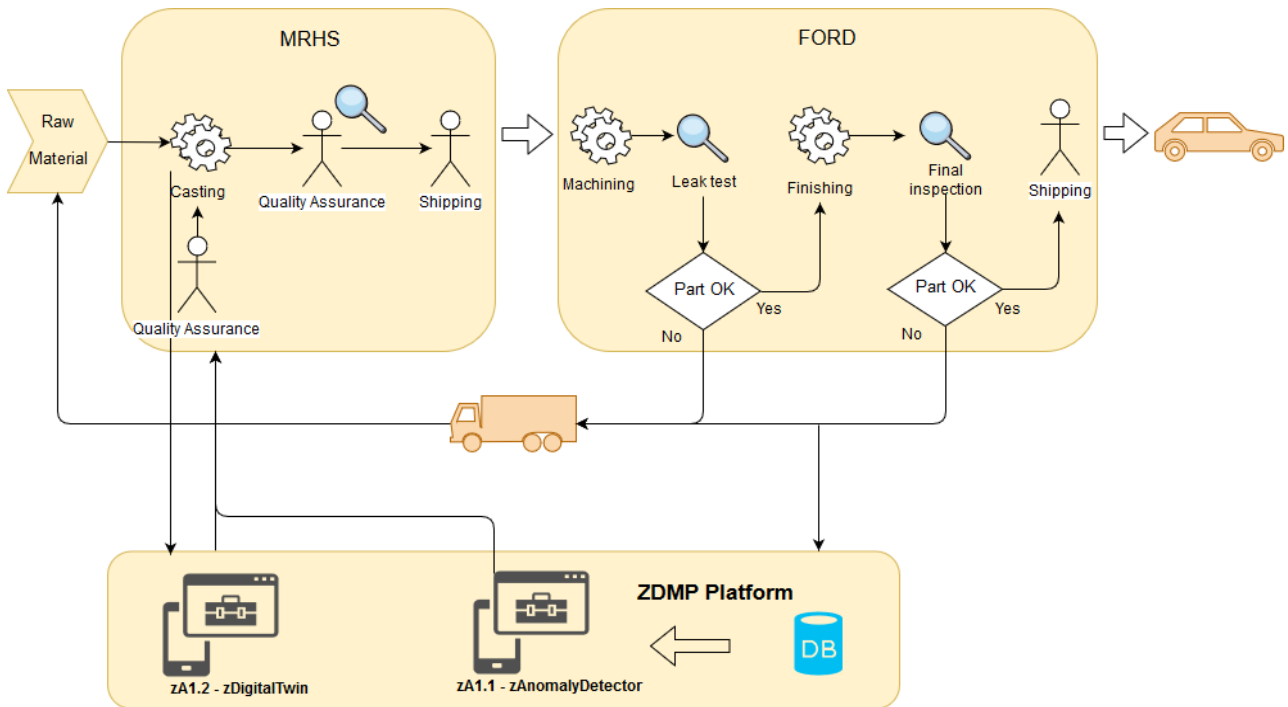


Figure 22: UC1.1: Business process model diagram “TO-BE”

UC1.1: Engine Block Manufacturing: Defects Detection and Prediction in Aluminium Injection Operations		
Situations identified	Potential related legal issues	Section
<ul style="list-style-type: none"> The zAnomalyDetector ingests real time data from multiple sources (MRHS machine sensors, process, and / or product results) and elaborates a multivariate analysis to detect system anomalies. It is possible that some personal data related to operators are collected and processed (eg data resulting from the machine / operator interaction such as information about operator’s performance or information related to time and attendance) 	<ul style="list-style-type: none"> Data Protection 	<ul style="list-style-type: none"> Section 2

<ul style="list-style-type: none"> • The ZDMP platform collects data from both MRHS and FORD processes • The location and security of the platform are highly relevant to this use-case, since the data to be managed is highly sensitive and confidential • Use of information stored in databases thus Copyright protection on databases should be considered to avoid possible infringements • Data sharing may cause data ownership related conflicts 	<ul style="list-style-type: none"> • Legal issues related to the sharing of data (IP protection of data, data ownership, confidentiality, trade secrets) 	<ul style="list-style-type: none"> • Section 3
-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------

Figure 23: UC1.1 related legal issues

4.2 UC1.2: Engine Block Manufacturing: Defects Detection and Prediction in Machining Operations

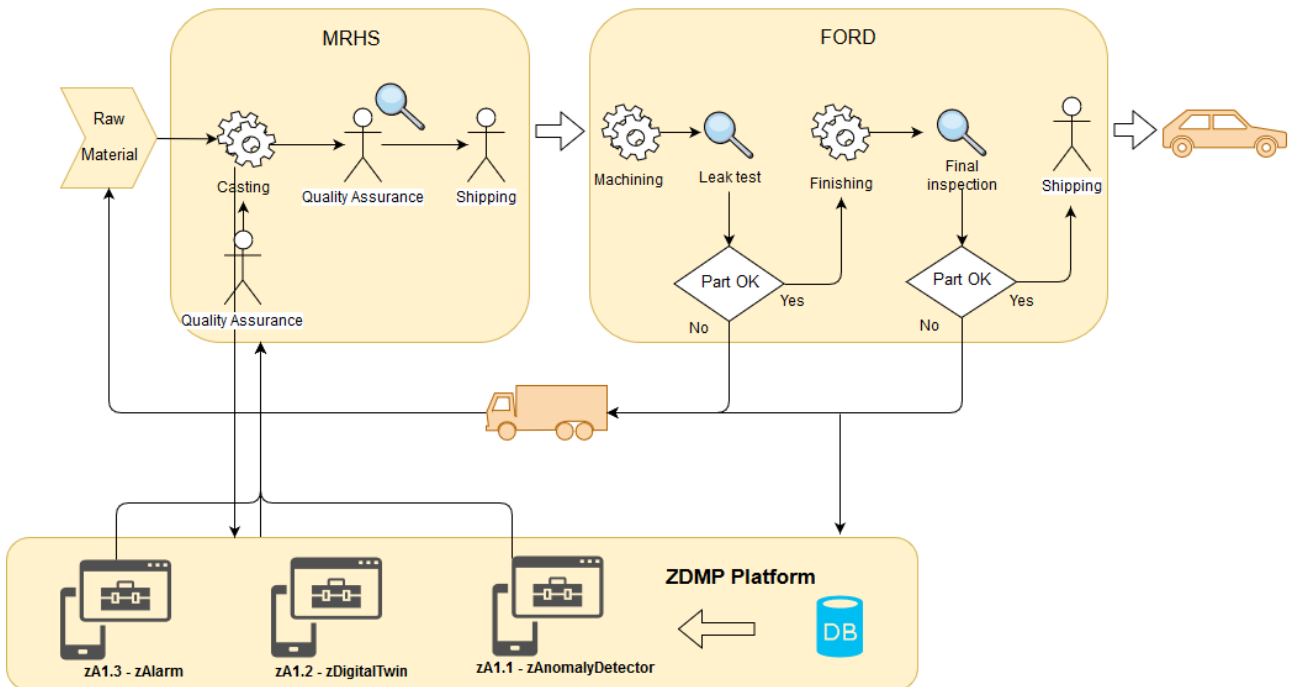


Figure 24: UC1.2: Business process model diagram “TO-BE”

UC1.2: Engine Block Manufacturing: Defects Detection and Prediction in Machining Operations		
Situations identified	Potential related legal issues	Section
<ul style="list-style-type: none"> • According to the data flow diagram of this use case, the Data Acquisition and Data Preparation steps require the ingestion of data from multiple sources; one of them is the operator input. Some personal data related to the operators may be collected and processed (eg operator’s performance related information) • The operators receive alerts when urgent actions need to be taken. Operators might be required to register on the platform (and provide personal data) 	<ul style="list-style-type: none"> • Data Protection 	<ul style="list-style-type: none"> • Section 2

<ul style="list-style-type: none"> It is possible that the interaction between the machine and the operator provides information related to the operator performance 		
<ul style="list-style-type: none"> The ZDMP platform collects data from both MRHS and FORD processes The location and security of the platform are highly relevant to this use case, since the data to be managed is highly sensitive and confidential Use of information stored in databases thus copyright protection on databases should be considered to avoid possible infringements Data sharing may cause data ownership related conflicts 	<ul style="list-style-type: none"> Legal issues related to the sharing of data (IP protection of data, data ownership, confidentiality, trade secrets) 	<ul style="list-style-type: none"> Section 3

Figure 25: UC1.2 related legal issues

4.3 UC1.3: Engine Block Manufacturing: Defects Reduction by Optimization of the Machining Process

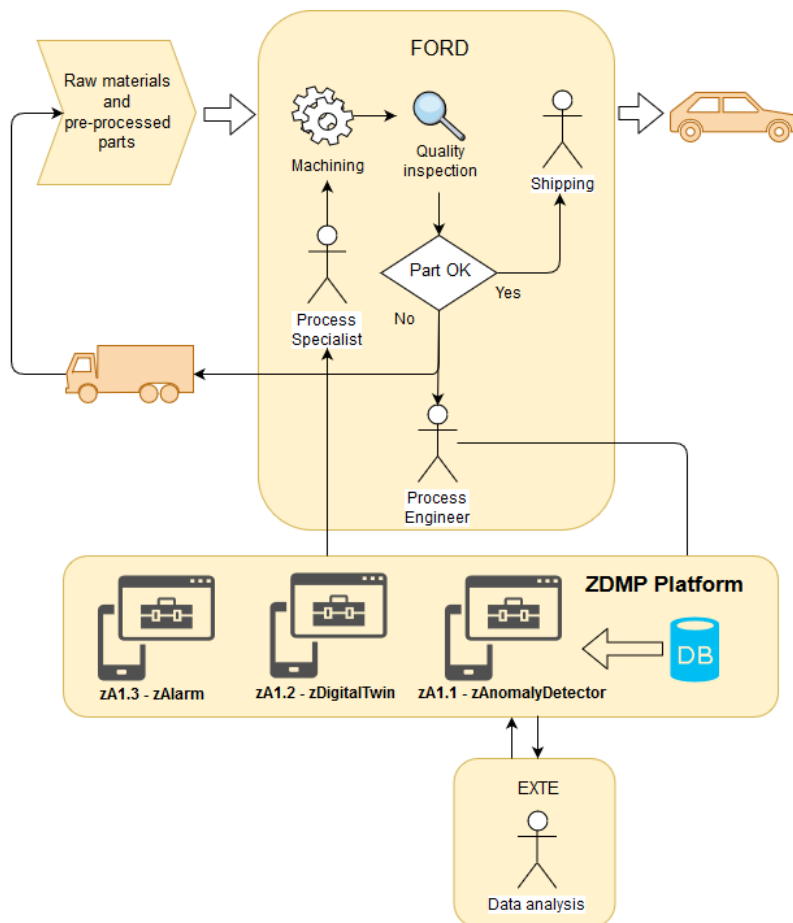


Figure 26: UC1.3: Business process model diagram “TO-BE”

UC1.3: Engine Block Manufacturing: Defects Reduction by Optimisation of the Machining Process		
Situations identified	Potential related legal issues	Section
<ul style="list-style-type: none"> • The operators receive alerts in the case of incidents or abnormal situations. Operators may be required to register on the platform (and provide personal data) • The recommended actions by ETXE-TAR are manually introduced into the platform. Probably the recommendations are introduced by an operator or analyst that should be registered in the platform as well (and thus provide personal data). Also, the recommendations report may contain such personal data • Service technicians can receive notifications with related information (machine, location, type of error, required tools, etc) on their smart wearable. In addition, technicians might be required to register on the platform (and provide personal data) • The technicians are using smart wearables. Depending on its functions, a wearable may provide personal data to the platform (eg the location of the technician) 	<ul style="list-style-type: none"> • Data Protection 	<ul style="list-style-type: none"> • Section 3
<ul style="list-style-type: none"> • ETXE-TAR receives the information captured by FORD for further analysis to decide concrete actions that should be taken to recover the “normal” condition of the whole system. Some of the information shared may be sensitive or confidential • FORD’s database, Cassandra, can transfer the data to the AI and Advance Data Analytics Module (zAnomalyDetector), included in the ZDMP platform. The Cassandra database may be protected by copyright • The information stored in the ZDMP databases could be accessed by ZDL. Some of this information could be considered confidential or sensitive information • Data sharing may cause data ownership related conflicts 	<ul style="list-style-type: none"> • Legal issues related to the sharing of data (IP protection of data, data ownership, confidentiality, trade secrets) 	<ul style="list-style-type: none"> • Section 3

Figure 27: UC1.3 related legal issues

4.4 UC2.1: Moulds Manufacturing: Process alert System for Machine Tool Prevention

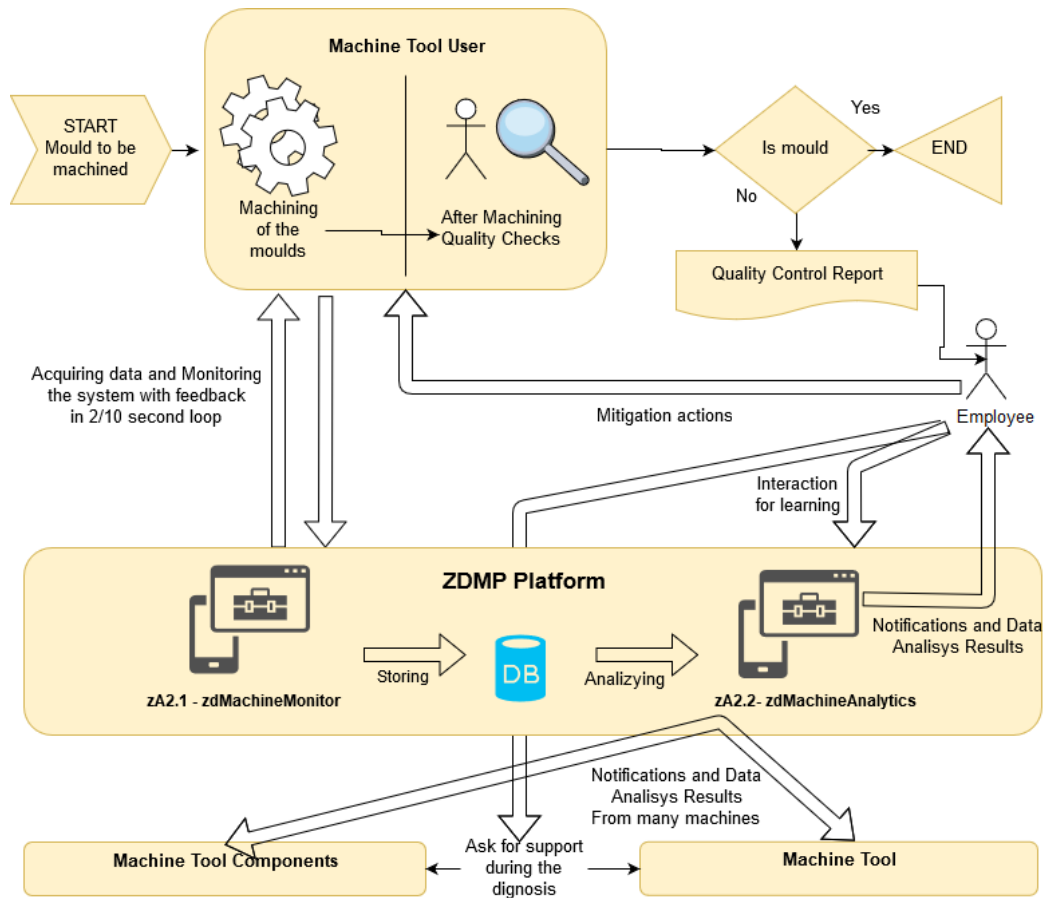


Figure 28: UC2.1: Business process model diagram “To-be”

UC2.1: Moulds manufacturing: Process alert system for machine tool failure prevention		
Situations identified	Potential related legal issues	Section
<ul style="list-style-type: none"> The operators receive alerts in case of sudden or abrupt changes that can lead to premature failure of a machine. Operators might be required to register on the platform (and provide personal data) 	<ul style="list-style-type: none"> Data Protection 	<ul style="list-style-type: none"> Section 2
<ul style="list-style-type: none"> The objective of zMachineMonitor is to automatically gather and store equipment and machining process data. Some of this data could disclose confidential or sensitive information related to machine processes. The central data storage should be able to gather data from several zMachineMonitor zApp's working on different machines for different customers. Consequently, data generated from different users is collected and accessed The machine tool user (FORM) receives information on the machine's health and process status. In case the machine tool user does not fully understand the reason why the 	<ul style="list-style-type: none"> Legal issues related to the sharing of data (IP protection of data, data ownership, confidentiality, trade secrets) 	<ul style="list-style-type: none"> Section 3

<p>machine status has changed, they can ask for help from the machine tool builder (FIDIA) or machine tool components manufacturer (HSD), who can provide support by accessing the same data remotely. In this case, data is clearly shared among different companies and, consequently, related legal issues associated to data sharing may arise (eg sharing of confidential data related to processes)</p> <ul style="list-style-type: none"> • The information stored in the ZDMP databases could be accessed by ZDL. Some of this information could be considered confidential or sensitive information • zMachineAnalytics will work on data already stored in a database by the zMachineMonitor zApp to identify degradation trends of the machine or its components. Possible copyright protection of the database should be considered • Data sharing may cause data ownership related conflicts 		
--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--	--

Figure 29: UC2.1 related legal issues

4.5 UC2.2: Moulds manufacturing: Smart process parameter tuning

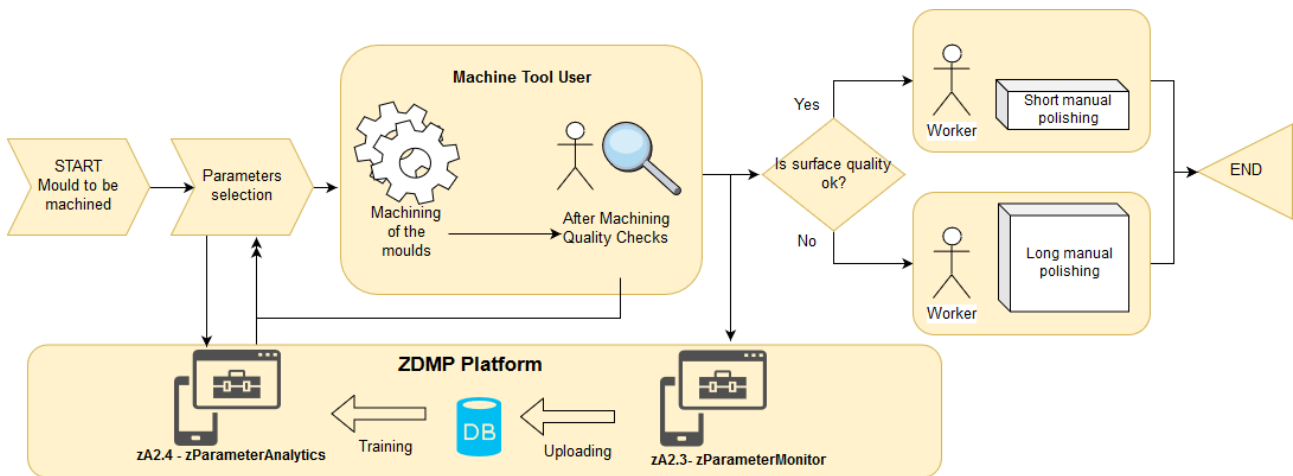


Figure 30: UC2.2: Business process model diagram TO-BE

UC2.2: Moulds Manufacturing: Smart Process Parameter Tuning		
Situations identified in the use case in which is possible that the related legal issues may arise	Potential related legal issues	Section

<ul style="list-style-type: none"> • After each machining operation and in-line quality assessment, the operator submits a report (automatically completed) containing all relevant parameter settings or environmental variables, and a quick assessment of the surface quality results (manually added). This information is stored in a ZDMP database. The operator probably needs to be registered in the platform (providing personal data). Also, the report may contain information related to the performance of the operator that could be considered personal data • The database could be enriched with (anonymised) data from a larger pool of customers, making the suggestions more accurate. This data could be considered personal data if it can be related in some way with an identified or identifiable person (eg an operator). Total anonymisation of data is difficult to achieve 	<ul style="list-style-type: none"> • Data Protection 	<ul style="list-style-type: none"> • Section 2
<ul style="list-style-type: none"> • The ZDMP database can be private or shared with suppliers, which means that the data contained in the database could be shared amongst different companies. Consequently, related legal issues associated to data sharing may arise (eg sharing of confidential data related to processes) • The information stored in the ZDMP databases could be accessed by ZDL. Some of this information could be considered confidential or sensitive information • Use of information stored in databases, thus the copyright protection on databases should be considered to avoid possible infringements • Data sharing may cause data ownership related conflicts 	<ul style="list-style-type: none"> • Legal issues related to the sharing of data (IP protection of data, data ownership, confidentiality, trade secrets) 	<ul style="list-style-type: none"> • Section 3

Figure 31: UC2.2 related legal issues

4.6 UC2.3: Moulds Manufacturing: In-Line 3D Modelling

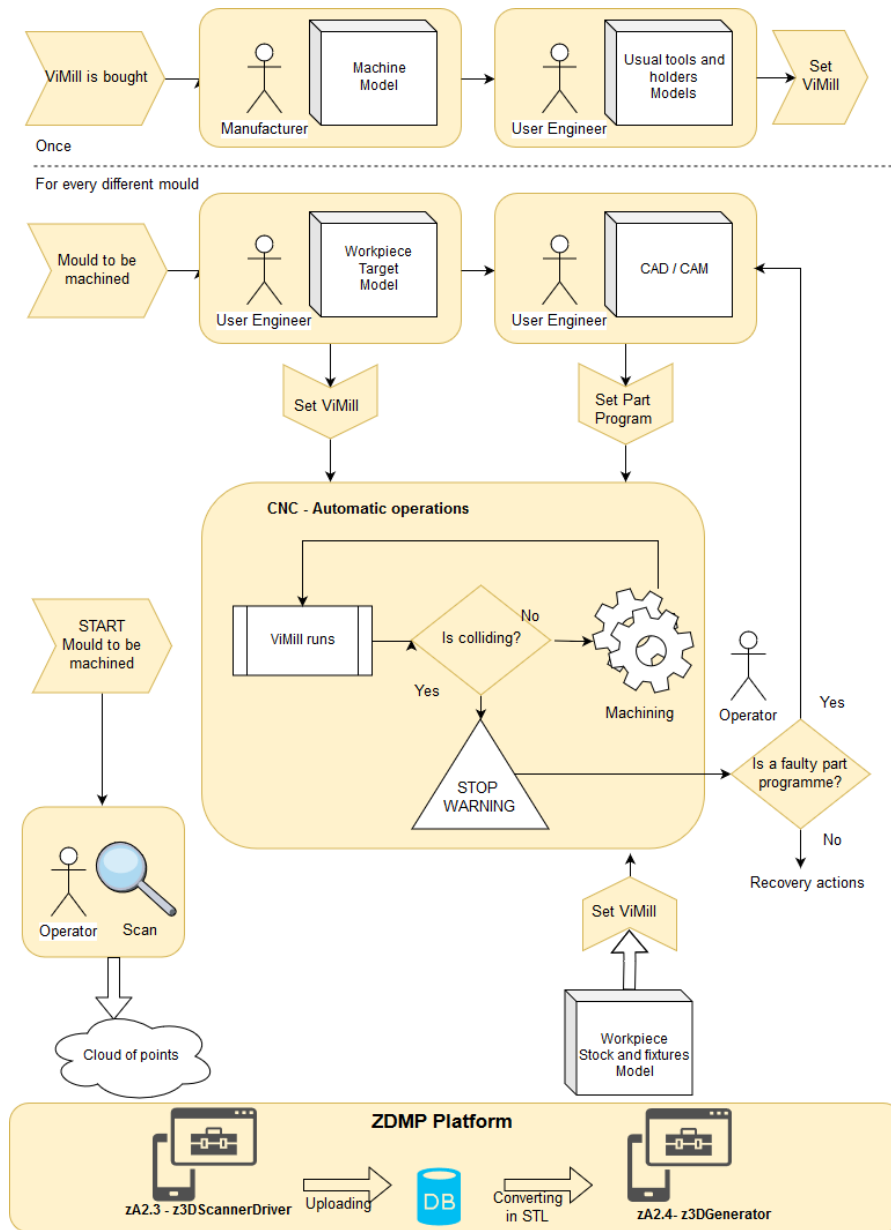


Figure 32: UC2.3: Business process model diagram TO-BE

UC2.3: Moulds Manufacturing: in-line 3D Modelling		
Situations identified in the use case in which is possible that the related legal issues may arise	Potential related legal issues	Sections
<ul style="list-style-type: none"> The objective of z3DScannerDriver is to make the upload of the cloud of points (from the working area scans) to the ZDMP platform more easily / automatically and then to trigger the conversion of the 3D format. This is an auxiliary application requiring the authorisation of the operator, which should substitute the manual upload. The operator 	<ul style="list-style-type: none"> Data Protection 	<ul style="list-style-type: none"> Section 2

<p>probably needs to be registered in the platform (providing personal data)</p> <ul style="list-style-type: none"> Although not clearly specified in the use case, it is possible that the image of an operator is captured during the scanning of the working area. The image of an identified or identifiable person is considered personal data 		
<ul style="list-style-type: none"> The target business process foresees the Machine Tool User (FORM) adopting the platform hosted outside the company. At this point, the operator scans the working area and the cloud of points is registered and sent to the dedicated zApp in the ZDMP where it is converted in the “stl” format ZDL could have access to the information stored in ZDMP database. This information could be considered confidential or sensitive Use of information stored in database, thus the copyright protection on databases should be considered to avoid possible infringements Data sharing may cause data ownership related conflicts 	<ul style="list-style-type: none"> Legal issues related to the sharing of data (IP protection of data, data ownership, confidentiality, trade secrets) 	<ul style="list-style-type: none"> Section 3

Figure 33: UC2.3 related legal issues

4.7 UC3.1: Electronic Products Manufacturing: Component inspection

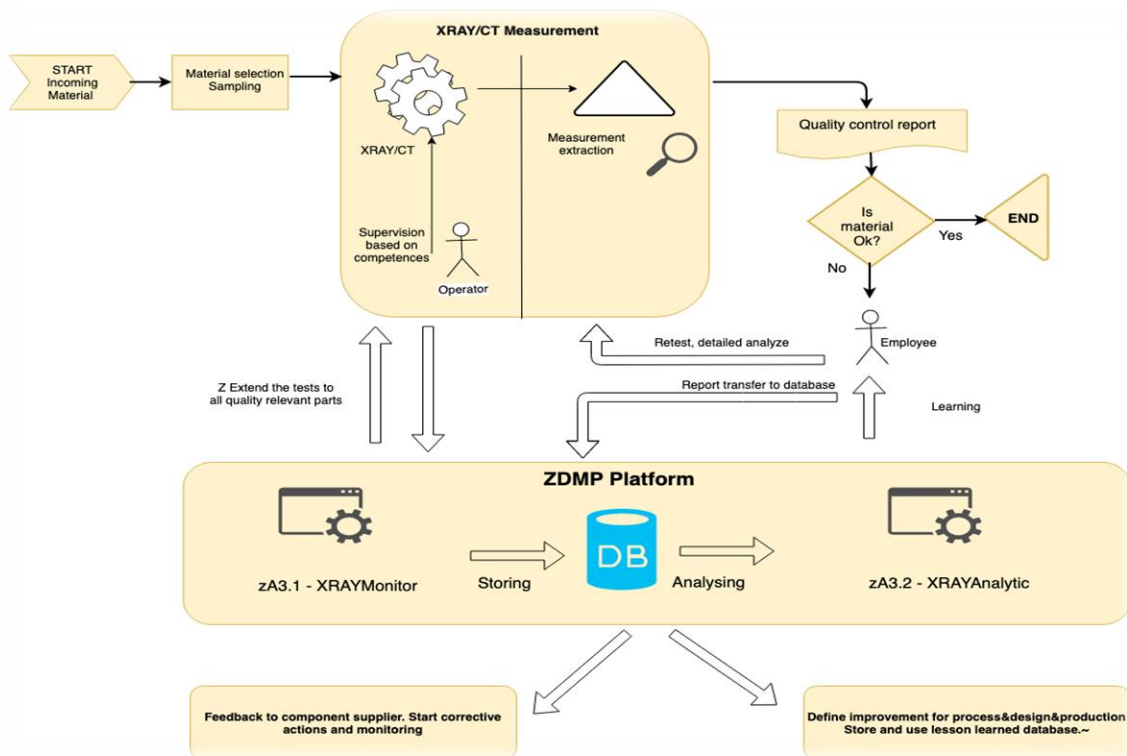


Figure 34:UC3.1: Business process model diagram “TO-BE”

UC3.1: Electronic Products Manufacturing: Component Inspection		
Situations identified	Potential related legal issues	Section
<ul style="list-style-type: none"> The zXRAYAnalytics application allows a fast-proactive approach in the case of component deviations, by sending alerts in a mail format to the involved parties. The operators receiving mails may be required to register on the platform (and provide personal data) 	<ul style="list-style-type: none"> Data Protection 	<ul style="list-style-type: none"> Section 2
<ul style="list-style-type: none"> Information related to product specific inspection is shared between the supplier of the product and the manufacturer. Related legal issues associated to data sharing may arise (eg sharing of confidential /sensitive data related to processes or products) The information stored in the ZDMP databases could be accessed by ZDL. Some of this information could be considered confidential information 	<ul style="list-style-type: none"> Legal issues related to the sharing of data (IP protection of data, data ownership, confidentiality, trade secrets) 	<ul style="list-style-type: none"> Section 3

Figure 35: UC3.1 related legal issues

4.8 UC3.2: Assembly line: AI-supported optical defects detection

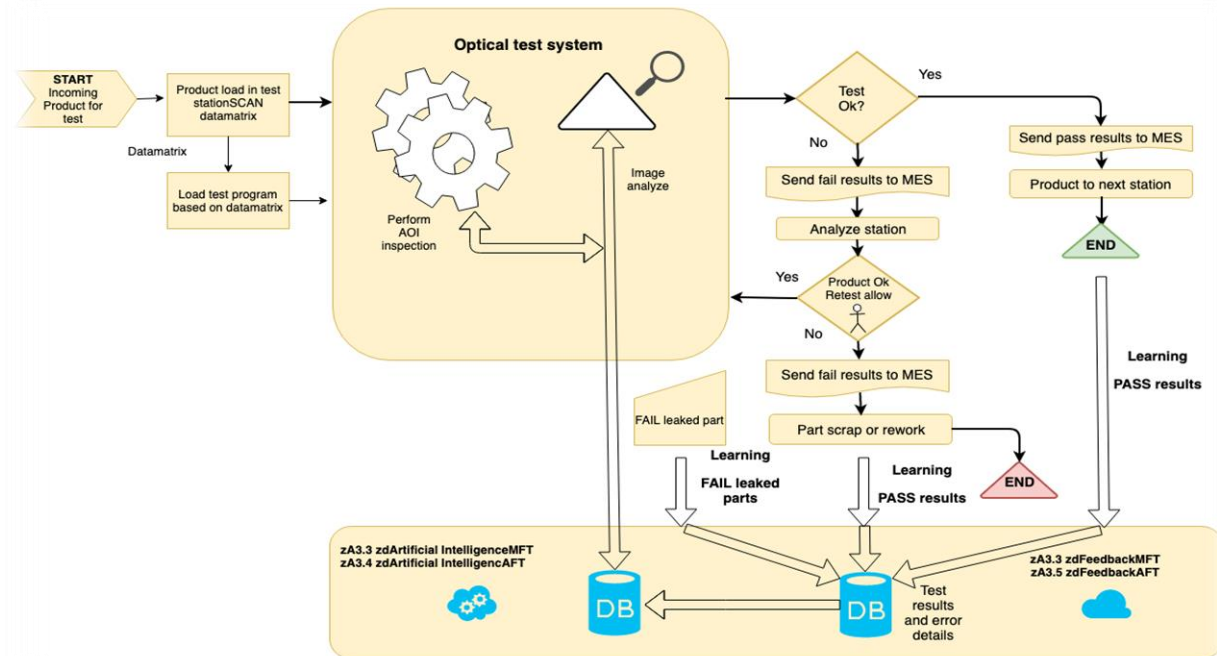


Figure 36: UC3.2: Business process model diagram “TO-BE”

UC3.2: Assembly Line: AI-Supported Optical Defects Detection		
Situations identified	Potential related legal issues	Section
<ul style="list-style-type: none"> The assembly line is mostly automated, but the operators still manually perform some steps. Personal data related to an identified or identifiable operator may be collected (eg operators' performance or attendance information) The Manual Final Test (MFT), requires the introduction of a camera to collect images during testing, and information about the operator's decisions, and reported failed parts. The information related to an identified or identifiable operator could be considered personal data Although not clearly specified in the use case, it is possible that the cameras capture the image of an operator. The image of an identified or identifiable person is considered personal data. After defect learning is completed, the application "zA3.4 zArtificialIntelligenceMFT" will run the tests and informs the operator on a test where quality risks have been identified. Operators receiving the mails might be required to register on the platform (and provide personal data) 	<ul style="list-style-type: none"> Data Protection 	<ul style="list-style-type: none"> Section 2
<ul style="list-style-type: none"> The information stored in the ZDMP databases could be accessed by ZDL. Some of this information could be considered confidential information Use of information stored in databases, thus the copyright protection on databases should be considered to avoid possible infringements Data sharing may arise data ownership related conflicts 	<ul style="list-style-type: none"> Legal issues related to the sharing of data (IP protection of data, data ownership, confidentiality, trade secrets) 	<ul style="list-style-type: none"> Section 3

Figure 37: UC3.2 related legal issues

4.9 UC3.3: Assembly line: Monitoring and Control System

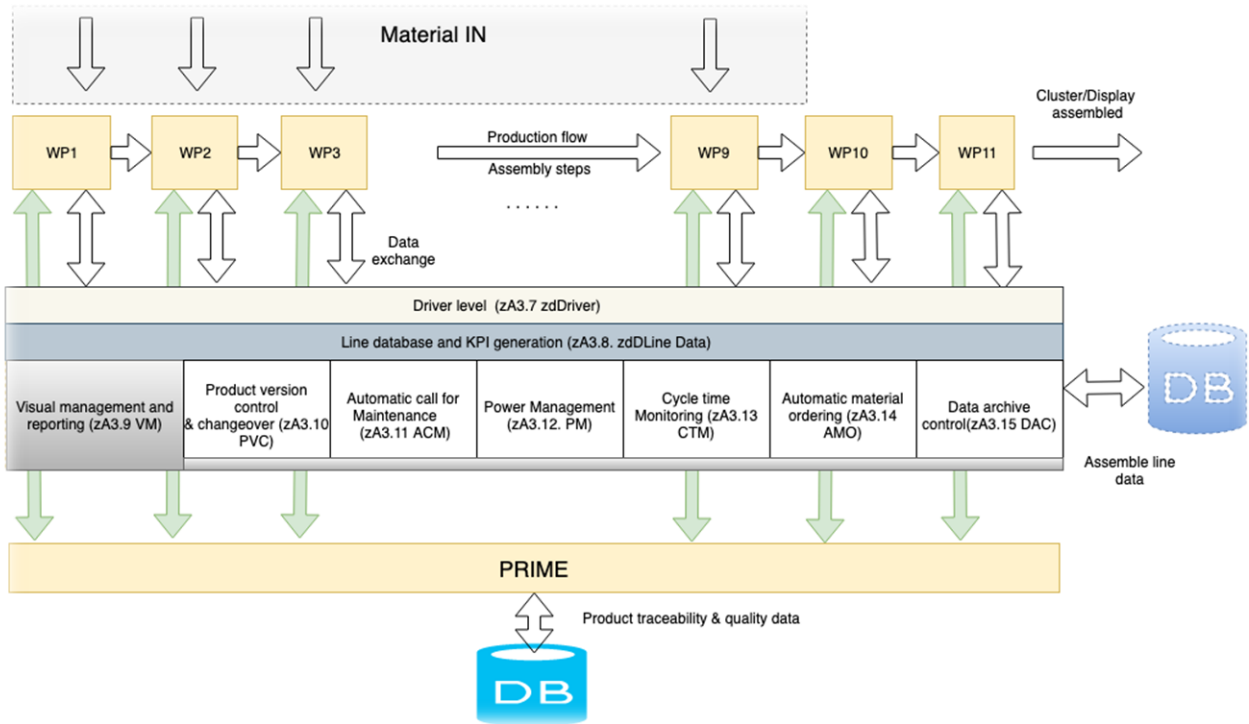


Figure 38: UC3.3 Business process model diagram “TO-BE”

UC3.3: Assembly Line: Monitoring and Control System		
Situations identified	Potential related legal issues	Section
<ul style="list-style-type: none"> There are assembly steps where an operator is mandatory. For example, for the handling processes (that cannot be automatized easily) or where the quality checks need the operator validation (aesthetic check). Data related to the performance of an identified or identifiable operator may be collected There is continuous monitoring of the machine cycle time and operator cycle time and thus this information could be considered personal data if related to an identified or identifiable operator This use case provides quality and production performance details to the assembly line personnel (just in time to the right person). It is likely that operators receiving the mails need to be registered in the platform (and provide personal data) 	<ul style="list-style-type: none"> Data Protection (data protection implications) 	<ul style="list-style-type: none"> Section 2
<ul style="list-style-type: none"> The information stored in the ZDMP databases could be accessed by ZDL. Some of this information could be considered confidential information Use of information stored in databases, thus the copyright protection on databases should be considered to avoid possible infringements 	<ul style="list-style-type: none"> Legal issues related to the sharing of data (IP protection of data, data ownership, confidentiality, trade secrets) 	<ul style="list-style-type: none"> Section 3

<ul style="list-style-type: none"> Data sharing may cause data ownership related conflicts 		
-----------------------------------------------------------------------------------------------------------	--	--

Figure 39: UC3.3: related legal issues

4.10 UC4.1: Steel Tubes: Productor Monitor

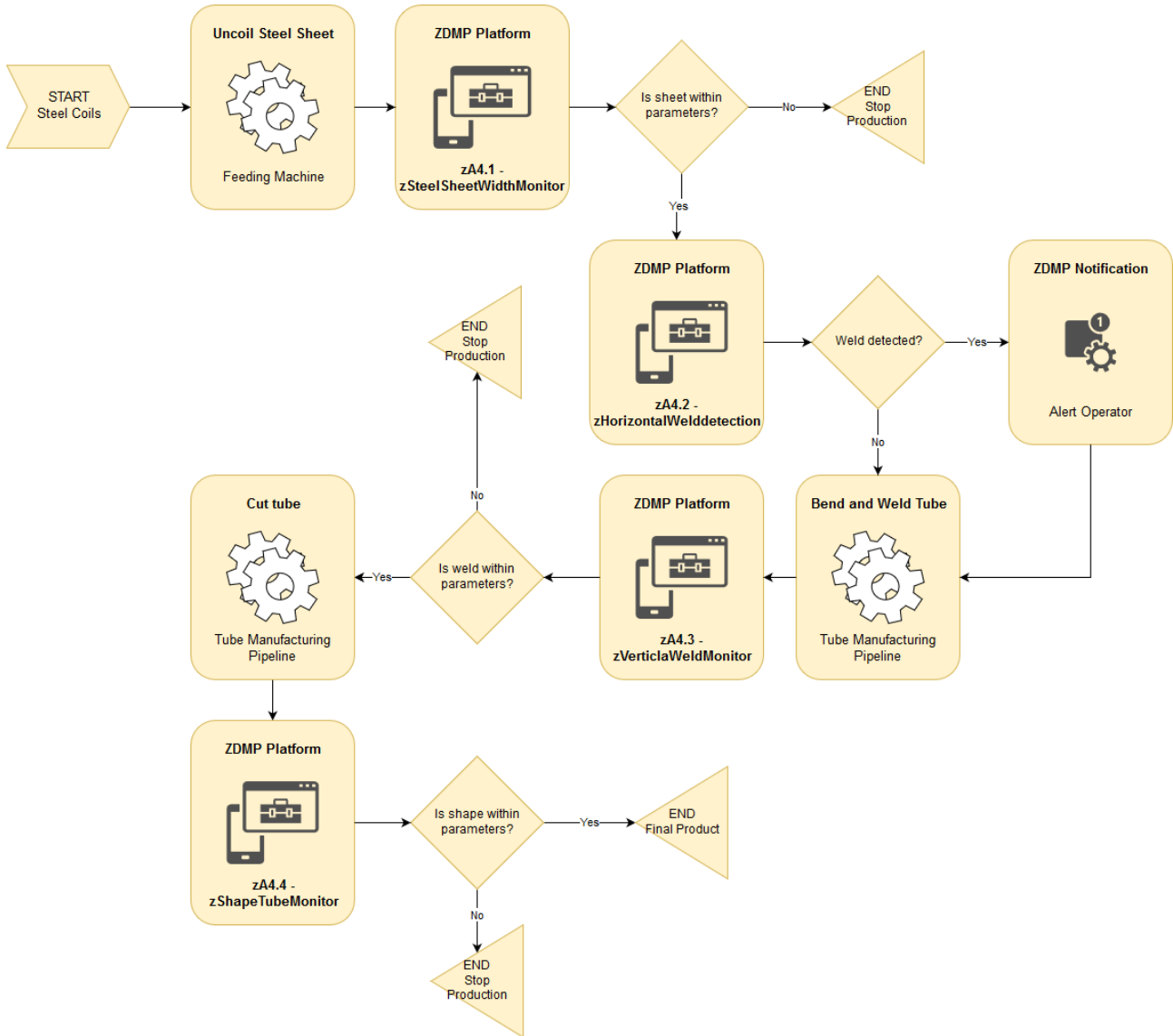


Figure 40: UC4.1 Business process model diagram “TO-BE”

UC4.1: Steel Tubes: Product Monitor		
Situations identified	Potential related legal issues	Section
<ul style="list-style-type: none"> The operator is constantly warned of abnormal situations in order to manage them efficiently. Operators receiving the mails may be required to register on the platform (and provide personal data) The production of tubes within FLEX is performed through the continuous feeding of steel strip sheets, welded together by weld operators, with specialised machinery. The machine-operator interaction could generate 	<ul style="list-style-type: none"> Data Protection 	<ul style="list-style-type: none"> Section 2

data related to the operator performance or working time, if the operator is identified or identifiable		
---------------------------------------------------------------------------------------------------------	--	--

Figure 41: UC4.1: related legal issues

4.11 UC4.2: Stone Tiles: Equipment Wear Detection

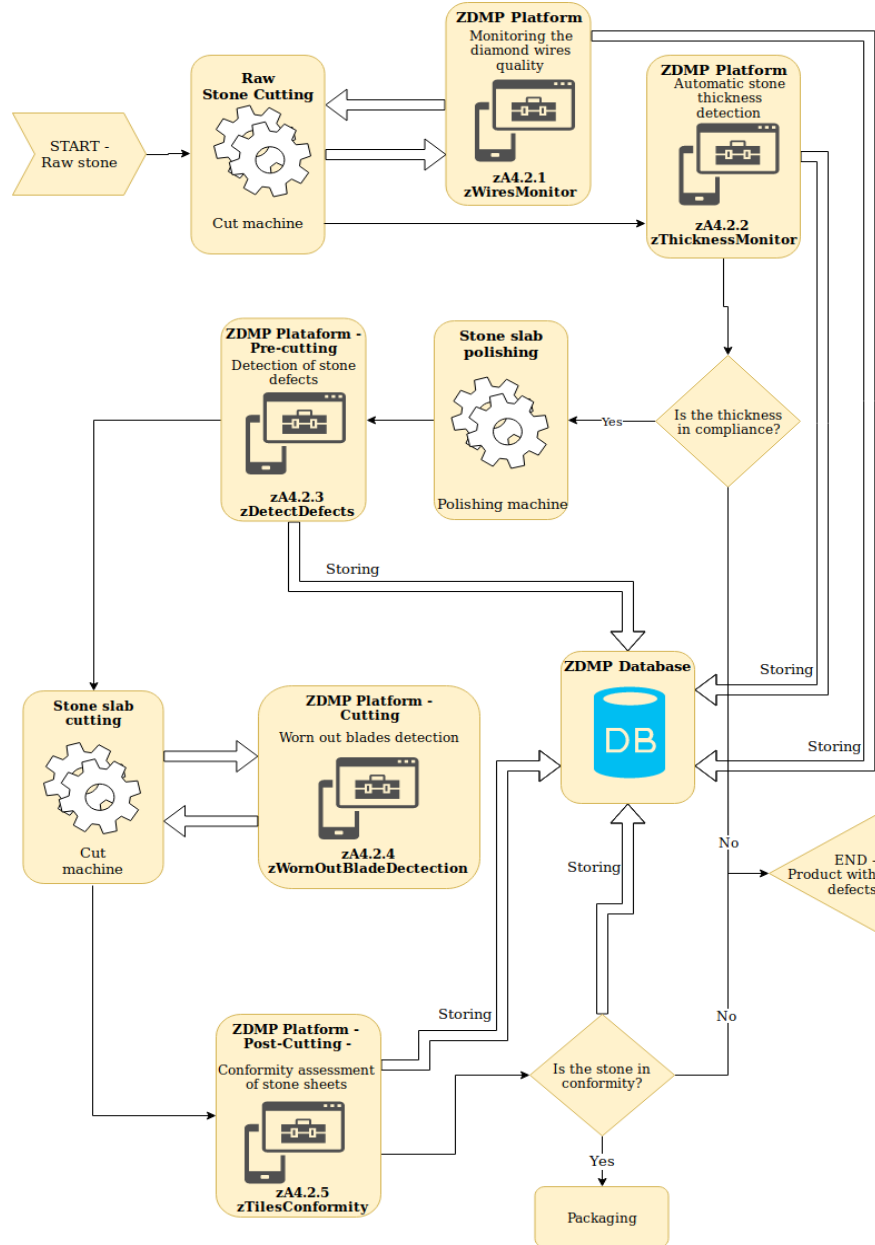


Figure 42: UC4.2 Business process model diagram “TO-BE”

UC4.2: Stone Tiles: Equipment Wear Detection		
Situations identified	Potential related legal issues	Section
<ul style="list-style-type: none"> The information stored in the ZDMP databases could be accessed by ZDL. Some of this information could be considered confidential information 	<ul style="list-style-type: none"> Legal issues related to the sharing of data (IP protection of data, data ownership, confidentiality, trade secrets) 	<ul style="list-style-type: none"> Section 3

Figure 43: UC4.2: related legal issues

4.12 UC4.3: Supply Chain: Quality Control at Construction Site

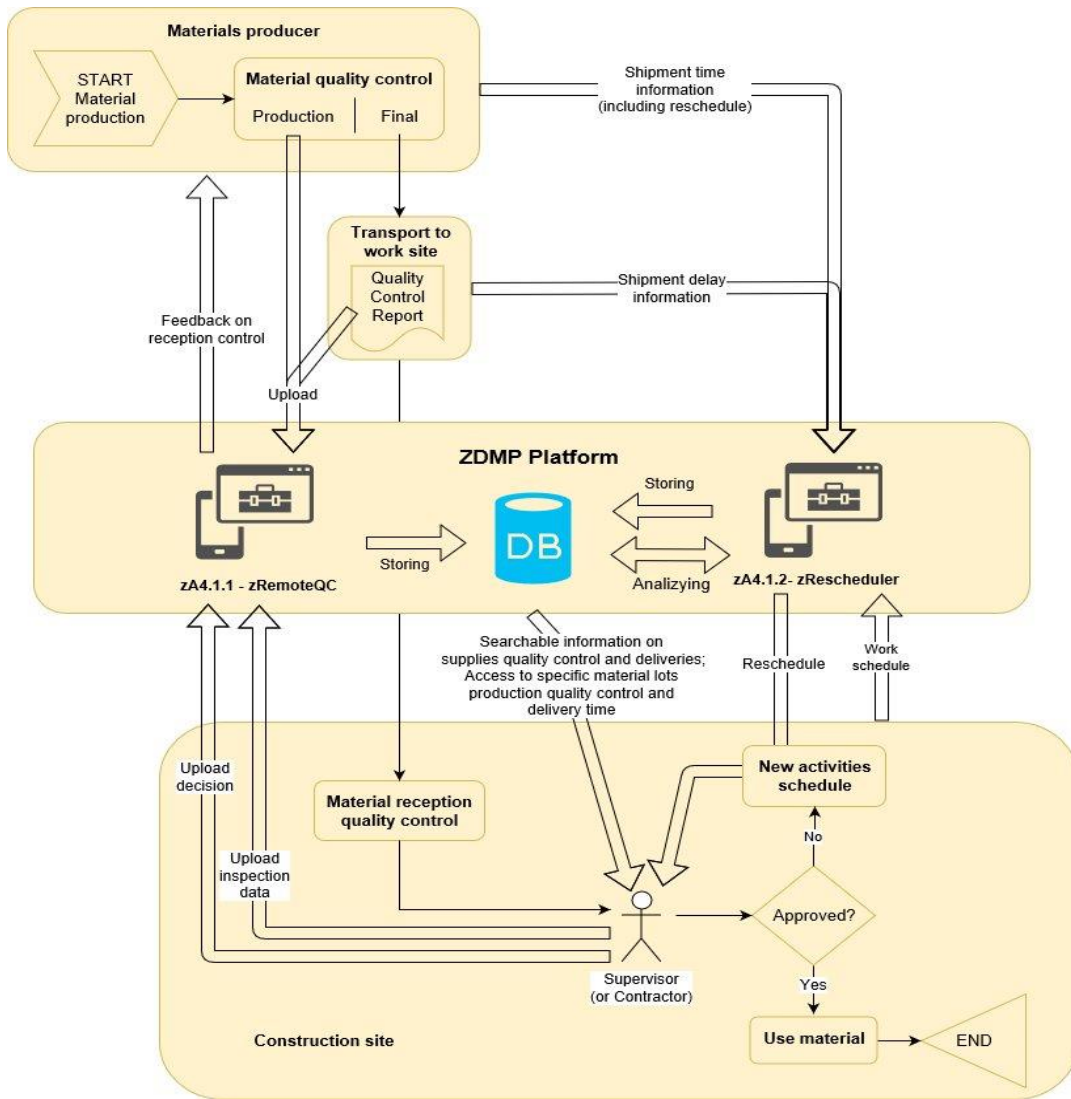


Figure 44: UC4.3 Business process model diagram “TO-BE”

UC4.3: Supply Chain: Quality Control at Construction Site		
Situations identified	Potential related legal	Section
<ul style="list-style-type: none"> • The target business process considers the use of zApps, accessible by the Supplier (FLEX and ALONG), by the Works Contractor and by the Supervisor (CONS.). The Works Contractor, the Supplier, and the Supervisor probably needs to be registered on the platform (and provide personal data) • There is a constant exchange of information between manufacturers and the Work Contractor. Information can be made available through an email that can be generated by the app itself, a mobile version of the app, or an alert system. Thus, a question is if any natural person (a worker) identified or identifiable in this process? • Trucks drivers can report their situation through a mobile app if any delays. Location data of a person of an identified or identifiable is considered personal data • The zApp must be set up with specific login data for each party (Supplier, Works Contractor, Supervisor), and through email and password. Each party will have access to different areas of the zApp 	<ul style="list-style-type: none"> • Data Protection 	<ul style="list-style-type: none"> • Section 2
<ul style="list-style-type: none"> • The first, zRemoteQC allows parties at the work site access to document evidence of compliance with specifications of the materials to be shipped and, should they choose to, to document production quality control information relating to the lots of material being supplied This information could be considered confidential or sensitive • The information stored in the ZDMP databases could be accessed by ZDL. Some of this information could be considered confidential information • Use of information stored in databases, thus the copyright protection on databases should be considered to avoid possible infringements • Data sharing may cause data ownership related conflicts 	<ul style="list-style-type: none"> • Legal issues related to the sharing of data (IP protection of data, data ownership, confidentiality, trade secrets) 	<ul style="list-style-type: none"> • Section 3

Figure 45: UC4.3: related legal issues

4.13 UC4.4: Supply Chain: Quality Traceability

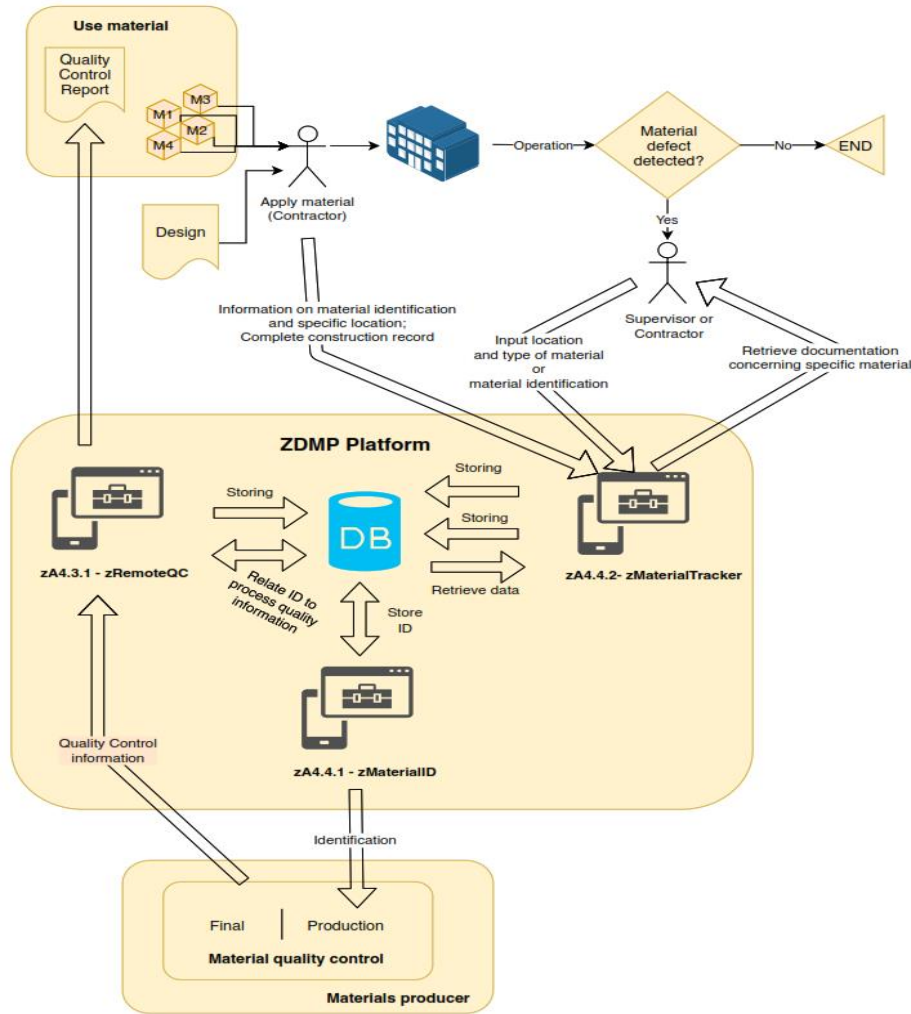


Figure 46: UC4.4 Business process model diagram “TO-BE”

UC4.4: Supply Chain: Quality Traceability		
Situations identified	Potential related legal issues	Section
<ul style="list-style-type: none"> Setting up login information must be required through an email and password or through similar in any other system in use. The Works Contractor, the Supplier, and the Supervisor probably need to be registered in the platform (and provide personal data) zApp4.13 (zMaterialTracker) allows the actors to associate a specific material to a specific location. This implies that all the supporting quality control documentary evidence associated to that specific material to be related to a location. The operator probably needs to be registered in the platform (and provide personal data) 	<ul style="list-style-type: none"> Data Protection 	<ul style="list-style-type: none"> Section 2
<ul style="list-style-type: none"> The target business process predicts the use of several zApps, one accessible by the Supplier (FLEX and ALONG), the other 	<ul style="list-style-type: none"> Legal issues related to the sharing of data (IP protection) 	<ul style="list-style-type: none"> Section 3

<p>accessible by the Works Contractor and the Supervisor (CONS), and others with access only to certain features by the supplier (FLEX and ALONG). Consequently, information related to the production process, that may be considered confidential or sensitive, may be shared among different companies</p> <ul style="list-style-type: none"> • The information stored in the ZDMP databases could be accessed by ZDL. Some of this information could be considered confidential information • Use of information stored in databases, thus the copyright protection on databases should be considered to avoid possible infringements • Data sharing may cause data ownership related conflicts 	<p>of data, data ownership, confidentiality, trade secrets)</p>	
--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------	--

Figure 47: UC4.4: related legal issues

4.14 Use Cases Summary Table

The following table includes a summary of the main potential situations identified in the use cases above, the legal issues related to these situations, as well as the section in the deliverable where an extended description of these legal issues and related recommendations are provided.

Use Cases: Summary Table		
Situations identified	Potential related legal issues	Section
<ul style="list-style-type: none"> • To use the different ZDMP functionalities (eg receiving alerts) manufacturers' employees may need to register on the platform (and provide personal data during the registration process) • Some operators involved in the production process are constantly interacting with machines. The machine-operator interaction could generate data related to the operator's performance or working time, if the operator is identified or identifiable • In some cases, reports are submitted by operators through the platform. These reports may contain personal data (eg identification data of the operator submitting additional content to the report or information related to the operator performance) • Some of the use cases involve the use of cameras. There is a possibility that these cameras capture images of the operators. The image of an identified or identifiable person is considered personal data • Truck drivers can report their situation through a mobile app (eg if any delays). Location data of an identified or identifiable is considered personal data 	<ul style="list-style-type: none"> • Data Protection 	<ul style="list-style-type: none"> • Section 2

<ul style="list-style-type: none"> Technicians are using smart wearables. Depending on its functions, a wearable may provide personal data to the platform (eg the location of the technician) 		
<ul style="list-style-type: none"> Sharing of information among different companies (eg manufacturers and suppliers). The information shared may be considered sensitive or confidential Sharing of information of the platform users with ZDL (the platform provider). The information shared may be considered sensitive or confidential Use of information stored in databases, thus the copyright protection on databases should be considered to avoid possible infringements Data sharing may bring data ownership related conflicts 	<ul style="list-style-type: none"> Legal issues related to the sharing of data (IP protection of data, data ownership, confidentiality, trade secrets) 	<ul style="list-style-type: none"> Section 3

Figure 48: Use Cases: Summary table

5 Other Legal Issues Related to Smart Manufacturing

Smart Manufacturing raises concerns around a variety of legal issues but particularly cybersecurity, privacy, data ownership, and intellectual property which have already been discussed in previous sections. However, legal issues surrounding smart manufacturing may involve other matters relating to Liability and Labour Laws, as explained in the following subsections.

5.1 Liability

In the first place, organisations must be aware of what are they liable to their customers and regulators, as well as to which liability needs to be borne by their vendors. Other subjects that require addressing include determining the different jurisdictions (and their implications) of all the countries in which the organisations are operating [GIL19].

In addition, the deployment of artificial intelligence in the manufacturing sector raises concerns over causation. In this respect, a series of questions must be answered to determine the legal remedies in case of an accident or malfunction of a machine in different scenarios; from deciding who is liable for faulty products to who is responsible of an injury caused to an employee [ZIM17].

The following table shows a series of liability-related issues that may affect ZDMP and ZDL as well as possible solutions to them [CDT18]:

Recommendations for ZDMP and ZDL	
Recommendation	Description
Damages caused by external causes (eg ransomware or other malwares)	<ul style="list-style-type: none"> The functioning of software and platforms can be affected by various forms of malware, compromising user's data, and information ZDMP must develop a secure infrastructure to ensure all data and information stored in the platform is safe to the extent possible. Moreover, action plans in case of security breaches or cyber-attacks that may compromise valuable data and information of partners and users must be carefully designed and implemented ZDL contracts with users should include detailed clauses addressing situations for which the company is liable and situations for which is not; always taking into consideration that no security measure is infallible
Damages caused by internal causes (eg failures of an zApp)	<ul style="list-style-type: none"> Users of the platform and zApps may suffer damages in their factories caused by malfunctions In the scenario that an erroneous functioning of the ZDMP platform / zApps causes damage on a user's machine or system, ZDL can opt for three different legal paths: Strict liability, negligence, and defective or inadequate warnings. If ZDL opts for a strict liability approach, for example, liability cannot be transferred to the user through a contract, meaning that ZDL would be liable for any malfunction. Contrarily, negligence will allow ZDL to argue that the cause of the failure is a breach of a duty of care by the user ZDL and ZDMP partners should review the conditions on which these liability legal paths operate in order to correctly apply them in case of any failure in the services offered by the platform or the Apps
Liability insurance	<ul style="list-style-type: none"> The possibility of a liability insurance should be assessed by ZDL and ZDMP partners

Change of public policies	<ul style="list-style-type: none"> • Sometimes government interventions in certain markets affects participants • Both ZDMP partners and ZDL must contemplate that changes in European regulations may affect them. For example, by creating additional requirements for providing platform services across the EU or to request protection under a specific type of IP. Both situations will require to re-evaluate their exploitations plans, and partners to reevaluate the options they have for protecting their results • A revision on European regulations and policies is recommended periodically during the project life cycle, as these changes may even affect the contractual provisions under which ZDMP platform services are provided
---------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Figure 49: Recommendations Section 5.1

5.2 Labour Laws

Furthermore, the implementation of new technologies in the digital transformation process of an organisation, may require legal assessment not only for the implementation of new business models but to avoid potential conflicts with existing labour laws and employees' representative groups. The last issue is critical as the implementation of certain technologies might make existing workers obsolete [ZIM17].

6 Cybersecurity

6.1 Cybersecurity in Smart Manufacturing Systems

The integration of complex smart manufacturing technologies has massively increased the scope for attack from those aiming at industrial espionage and sabotage [TH18]. Even when cybersecurity attacks may cause serious damages, ranging from economic damage and lost production through to injury and loss of life, in the rush towards manufacturing flexibility, quality, and productivity, security is often seen as being of secondary concern [TH18].

6.1.1 Cybersecurity challenges

The adoption of Industry 4.0 technologies that makes manufacturing smart, brings many security challenges, such as the ones described below. These are (are based on) recommendation from the European Union Agency for Cybersecurity (ENISA) related to smart manufacturing cybersecurity [ENI18]:

- **Vulnerable components:** Internet of Things has emerged with millions of connected devices. Securing IoT in smart manufacturing entails providing protection to a massive number of connected devices that in many cases were not designed with cybersecurity in mind
- **Processes complexity:** A multitude of complex processes involved in smart manufacturing should each be managed with cybersecurity in mind
- **Increased connectivity:** Smart manufacturing processes requires interaction with objects and environments, as well as collaboration across multiple organisations
- **IT / OT convergence:** Managing IT / OT (Operational Technology) integration is a considerable challenge due to factors such as insecure network connections, use of technologies that introduce risks into the OT environments, and the insufficient understanding of requirements for Industrial Control Systems (ICS) environments. OT is hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes, and events in the enterprise
- **Supply chain complexity:** Manufacturers need to rely on third party components most of the time. Ensuring product security requires being able to track every component to its source which is often difficult or impossible
- **Legacy industrial control systems:** New systems are built on top of legacy systems that may result in outdated protection measures and contain unknown vulnerabilities
- **Insecure protocols:** In modern network environments, the protocols used by manufacturing companies and equipment to communicate often fail to ensure adequate protection against cyberthreats
- **Human factors:** With the adoption of new technologies, workers must work with new types of data for which they may not be aware of the associated risks
- **Unused functionalities:** In industrial environments, machines, or their selected components, have access to unused functionalities that become gateways for the attackers
- **Safety aspects:** Security for safety is one of the main objectives in smart manufacturing
- **Security updates:** User interfaces available in IoT do not allow traditional updates mechanisms, which makes the application of security updates challenging

- **Security for the whole product lifecycle:** Device security should be considered throughout the product’s entire lifecycle

6.1.2 Security Measures

ENISA provides a categorisation of security measures for IoT in smart manufacturing as guidelines to operators, manufacturers, and users to prevent and respond to potential cyberattacks [ENI18]:



Figure 50: Good practices overview [ENI18]

The following subsections provide an overview of the above-mentioned categories of security measures for IoT in smart manufacturing.

Recommendations for ZDMP and ZDL	
Recommendation	Description
ENISA security measures	<ul style="list-style-type: none"> • ZDMP partners should consider ENISA’s proposed security measures for smart manufacturing as a guideline to prevent and respond to potential cyberattacks. Organisations should adapt the implementation of these measures to their own circumstances and previous assessments performed by their cybersecurity experts

Figure 51: Recommendations Section 6.1.2

6.1.2.1 Policies

To ensure an appropriate level of cybersecurity, policies and procedures should be established in organisations within ZDMP and ZDL. Additionally, organisations should ensure that their solutions do not violate privacy regulations [ENI18]:

- **Security by design:** Security measures should be applied from the beginning of product development. IoT cybersecurity should be treated as a cycle, adopting a security by design approach at every step of a smart manufacturing system development lifecycle
- **Privacy by design:** Security measures related to the protection of personal data and privacy should be applied from the beginning of product development
- **Asset management:** Security measures related to asset discovery, monitoring, and maintenance
- **Risk and threat management:** The adoption of an approach to the process of risk and threat management adapted to Industry 4.0 environment

6.1.2.2 Organisational Practices

The following security measures explain how smart manufacturing industry should operate by implementing organisation and governance principles to effectively manage cybersecurity incidents, manage vulnerabilities, and ensure the security of IIoT solutions throughout their lifecycle [ENI18], this applies to ZDMP and ZDL:

- **Endpoint lifecycle:** Measures related to security at various stages of the product lifecycle including the procurement process, supply chain, handover phase, exploitation, and end-of-life
- **Security Architecture:** Adopt a holistic architectural-based approach and develop a risk-aligned security architecture
- **Incidents handling:** Implementation of measures and processes for the detection and response to incidents that may occur
- **Vulnerabilities management:** Establish vulnerability disclosure and vulnerability management processes as well as to eliminate existing vulnerabilities
- **Training and awareness:** Adopt a comprehensive approach to security training and awareness of employees working with IIoT devices and systems
- **Third party management:** Security measures to control third party access and management of third parties' relations regarding security (ie to include security aspects in the agreements with third parties)

6.1.2.3 Technical Practices

This subsection provides an overview of the categories of technical measures that should be implemented to enable smart manufacturing companies to improve their security [ENI18]:

- **Trust and integrity management:** Security measures to ensure the integrity and trustfulness of data devices (ie verification of the integrity of software to ensure it comes from a reliable source)
- **Cloud security:** Measures aimed at ensuring various security aspects of cloud computing business and privacy impact assessment taking also into consideration laws and regulations applicable
- **Business continuity and recovery:** Ensure resilience and continuity of the operations in the event of security incidents by developing, testing, and reviewing a business continuity and recovery plan
- **Machine to machine security:** Security measures related to input validation and protection in machine-to-machine communications, key storage, and encryption
- **Data protection:** Security measures aimed at protecting personal data at various levels of an organisation and management of access to data

- **Software / Firmware updates:** Security measures related to verification, testing, and execution of patches
- **Access control:** Measures to ensure security related to control of remote access, authentication, privileges, accounts, and physical access
- **Networks, protocols, and encryption:** Ensure security of communications through adequate protocol implementation, encryption, and network segmentation
- **Monitoring and auditing:** Security measures related to the monitoring of network traffic and availability, logs collection, and reviews
- **Configuration management:** Security measures involving the management of changes in configuration, including device hardening and backup verification

6.2 General Guidelines to Implement a Robust ZDMP Platform

The ZDPM platform, as with any other digital platform, must be protected and preserved following the principles of confidentiality, integrity, and availability. In IT environments, the most important security property is the confidentiality. However, in industrial environments, availability is the most important factor based on the premise that an industrial process must (often or sometimes) not be stopped. For example, in the automotive sector, the simple stopping of any production lines involves losses of millions of euros.

Moreover, due to the heterogeneity of the ZDMP platform (ie Apps, SDK, Business Cloud) new threats arise from the interactions of such elements. For instance, software developers could develop and publish vulnerable software that could have a direct impact in a factory.

The specifics of ZDMP makes it a significant challenge in terms of security, and many threats must be considered since some services are publicly exposed:

- **Information Gathering:** An attacker might be able to gather sensitive information about the ZDMP platform
- **Configuration Management:** Attackers typically look for systems with default settings that are vulnerable
- **Secure Transmission:** Any information might be intercepted, and therefore it must be always sent in a secure way
- **Authentication / Authorisation:** Only authenticated users must have access to the platform
- **Session Management:** Attackers may be able to compromise passwords, session tokens, or keys to gain access to users' accounts and assume their identities
- **Cryptography:** Secure cryptography schemes are required to keep the platform secure from unauthorised information accesses
- **Data Validation:** Data may be manipulated and therefore this must be validated once received
- **Service availability:** Attackers might launch DoS (Denial-Of-Service) attacks to interrupt ZDMP services
- **Error Handling:** Errors must not be disclosed to attackers since they might contain sensitive information

Internal components (ie sensors, actuators, Programmable Logic Controllers) which are typically protected by internal firewalls and security zoning, are also exposed to attacks by means of web interfaces, and therefore also need to be protected. On the other hand, the security of zApps also need to be considered, since they play a critical role in ZDMP. Security must be considered from the zApp development to the app publication and

storage, ensuring an appropriate development and considering the whole software life cycle.

In general terms, in order to guarantee security and privacy, the platform must be designed following two standards: ISA/IEC-62443 and GDPR (General Data Protection Regulation).

6.2.1 International Electrotechnical Commission (IEC-62443)

Considering the above ZDMP elements (ie public services, internal services, and zApps), and the critical consequences that may follow a cyberattack to the platform, it is very important to make sure that ZDMP follows IEC-62443 (see next figure) which is a worldwide cybersecurity standard for industrial environments.

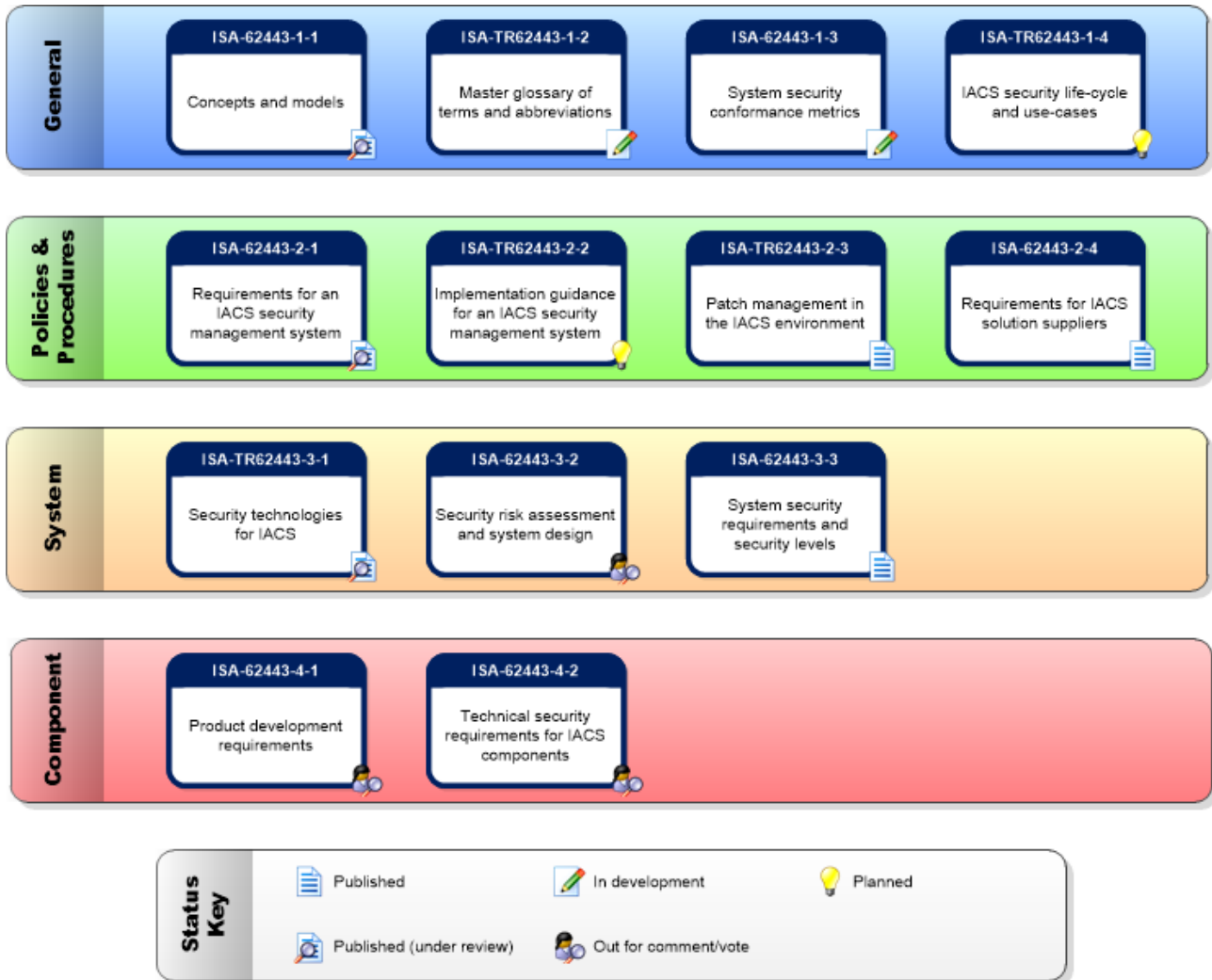


Figure 52: IEC 62443 Standard [ISA19]

Fulfilling IEC-62443 means that any industrial manufacturer must follow a particular flow. The first step is the precise specification of the services made available and their required protection levels which ranges from one to three. Based on this, the flow starts by designing the product according to the required protection level jointly with the Functional Security Assessment (FSA) and the Communication Robustness Tests (CRT). FSA is primarily focused on the security mechanisms of the operating system to cover the requirements of the specific protection level. CRT is the set of specific configurations and add-ons to protect the communication stack according to the protection level specified.

When the system has been developed according to all previous requirements, and the protection level is achieved, then, the second phase starts. This phase consists of selecting the location for the platform installation. This decision is based on the level of threat considering the levels classification of the standard:

- **Level 0:** Industrial field. This level groups physical actuators and sensors
- **Level 1:** Control. This level contains all control systems for level 0
- **Level 2:** Operation. This level groups the operation consoles, SCADA supervisors, etc
- **Level 3:** Enterprise. This level is where standard IT equipment is located for business purposes

All these levels are conveniently separated by using Next Generation Firewalls (NGFW) that provide capabilities to identify, not only ports or addresses, but they are able to recognize internal protocols at the level of operation. The main drawback is the high latency and for this reason additional, and high performance, firewalls are used in level 1. On the other hand, and based on the requirements, the majority of installations are beginning to use Intrusion Detection Systems (IDS). Jointly with IDS systems, a separate intelligence system for gathering all sources of information is used, and it is commonly named as “Security Information and Event Management” (SIEM), this system can recognize unusual patterns of traffic or flows. Based on this standard, any industrial environment can be divided into several zones (layers) and a set of conduits to connect them, such as physical zone, control zone, operation zone, and enterprise zone [ISA19]

Recommendations for ZDMP and ZDL	
Recommendation	Description
Adopt the IEC-6243 standard	<ul style="list-style-type: none"> • It is important to make sure that ZDMP follows IEC-62443, which is a worldwide cybersecurity standard for industrial environments
Demand the adoption of standards	<ul style="list-style-type: none"> • Demand the adoption of cybersecurity standards (ie ISO 27000 standards) to the companies that wish to operate in ZDMP

Figure 53: Recommendations Section 6.2.1

7 Trust and Trustworthiness in Complex Systems

7.1 Trust, Trustworthiness, and Risks

7.1.1 Definitions

This section describes trust related terminology and provides definitions for trust, trustworthiness, and risk. Trust can be described as a response to risk. A decision to trust someone (or something) is a decision to accept the risk that they will not perform as expected. To manage risk in a socio-technical system such as complex manufacturing, first it needs to be understood what trust decisions are being made, the consequences of trust decisions, and acquire information on the trustworthiness of other parties.

The term “trust” appears in many research disciplines including psychology, sociology, economics, law, as well as in IT. Each discipline has its own understanding of “trust” that is specialised to address the needs of a given research community. The Oxford English Dictionary (OED) provides the following definition: “Trust: Firm belief in the reliability, truth, or ability of someone or something”.

The Internet Security Glossary v2 (RFC 4949) [SHI07], describes trust as: “...a feeling of certainty (sometimes based on inconclusive evidence) either (a) that the system will not fail or (b) that the system meets its specifications (ie the system does what it claims to do and does not perform unwanted functions)”. RFC 4949 focuses mainly on the role of trust related to security tokens such as X.509 certificates.

The notion of trust can also be described it as a possible response to security threats, ie events or situations that could cause danger, harm, or loss. In this case, a decision to trust means accepting the risk arising from one or more threats. This interpretation of trust provides a rigorous basis for understanding the role of trust in ZDMP.

Trustworthiness can be defined as follows: “Trustworthiness: The property of being reliable, truthful, and capable.” RFC 4949 describes a “trustworthy system” as “A system that not only is trusted, but also warrants that trust because the system's behaviour can be validated in some convincing way, such as through formal analysis or code review”.

Trust is related to the acceptance of risk, which can be defined as: “Risk: Exposure (of someone or something valued) to danger, harm or loss”.

In classical risk analysis, including information system risk management based on ISO 27001 [ISO13], a risk exists where there are potential threats, ie a threat is a source of risk. RFC 4949 defines threat as: “Threat: a potential for violation of security, which exists when there is an entity, circumstance, capability, action, or event that could cause harm”.

In risk analysis based on ISO 27005 [ISO11], or more generally on ISO 31010 [ISO09], the level of risk is determined from a combination of threat likelihood and impact. The correct treatment depends on the level of risk. In this care there are several alternatives to consider:

- Accepting the risk
- Avoid the risk (for example by disengaging with the untrusted entity)
- Transfer the risk (ie by insuring against the risk, transferring the responsibility to deal with the risk to a third party)

- Reduce the risk (by implementing control measures which reduce the likelihood of threat or to mitigate the consequences)

For a better understanding of trust relations in ZDMP a trust model will be constructed that captures the potential risks to ZDMP components, applications, and users. This model provides qualitative and quantitative measures of trust and trustworthiness.

Trustworthiness in the context of ZDMP can be expressed in terms of the probability that the trusted entity will fail to meet the trustor's expectations.

7.1.2 Trust Related Literature

This section provides several references covering trust related research papers that illustrate the approach taken for modelling trust in ZDMP. In ZDMP “trust” will be considered in the context of “acceptable level of security risk”. The following papers provide background information for this approach.

One of the first significant contributions to trust related research, was the thesis of Stephen Marsh who investigated trust in various contexts and made a direct link between trust and risk [MAR94].

The definition of trust as an “acceptable level of risk” was introduced by Bill Roscoe et al [CGR+06]. The paper suggested that this interpretation can be used for designing trustworthy systems. This goes beyond computational trust models in which the risk (and hence the consequences of a decision to trust) are implicit. This also means that trust relationships in secure systems cannot be expressed without also modelling risks.

Trust modelling is still far from being fully understood especially regarding modelling and quantifying trust. A composite trust concept attempts to bring together the results of trust related research in different disciplines such as social sciences, philosophy, and economics [CHO15].

The Operational Trustworthiness Enabling Technologies (OPTET) project used a multi-disciplinary and integrated approach to identify and address the drivers of trust and confidence. It also aimed for an improvement of trustworthiness of internet-based socio-technical systems, using a methodology in which trust is explicitly defined in relation to threats (ie sources of risk) [CCN+15], [MOH14], [MOH15]. The objective was to provide secure and trusted cloud and service-based ICT and enable users to make decisions about trustworthiness via evidence-based trust management. OPTET provided a complete implementation of a trust modelling approach in which trust is defined and automatically analysed in terms of threats and risks. The project developed a graphical tool called the Secure System Designer (SSD) and an associated ontology that allowed users to create graphical models of systems, browse the list of threats and specify security controls [CWC+15]. This will be taken advantage of in the System Security Modeller (SSM) component provided by UOS-ITI.

7.2 Trust Modelling

The main “message” of this section is that trust is one of the possible responses to risk. Risks in ZDMP arise from various threats and stakeholders have to decide whether to:

- Reduce the risk by implementing security measures
- Accept the risk (ie assume it will not happen or will not cause much harm)
- Transfer responsibility for managing the risk to other stakeholder, either explicitly (by agreement) or implicitly (because they seem trustworthy)

For illustration purposes, within the ZDMP Architecture Specification document “D4.3a: Global Architecture Specification” each component contains a table that summarises the potential risks. These risks can be related to security risks, but also to the interaction between different components. For example, risks related to the System Security Modeller (SSM) mentioned above are summarised in the table below:

Risk	Description	Contingency Plan
Knowledge transfer	The most critical part of the modelling process is the interaction and knowledge exchange between the security analyst and ZDMP module developers.	The discussions between the security analyst and ZDMP expert needs to be formalised and described. This is an iterative process and at each iteration the model needs to be validated and controls applied in order to minimise security risks.
Development of ZDMP specific domain model	The ZDMP domain model is an ontology that contains ZDMP assets, threats, controls, and patterns that describe various security scenarios.	The domain model approximates the reality. This model needs to be developed and validated in close collaboration with ZDMP experts to make sure that the model adequately represents the system

Figure 54: Risks related to SSM

The second item involves trust: The stakeholder either trusts that ZDMP will not misbehave or trusts another stakeholder to prevent the risk or mitigate any harm it causes them. The trust related requirements in the context of ZDMP can be summarised as:

- Helping ZDMP system / application designers and operators to avoid the abuse of the system
- Helping ZDMP system / application users to avoid errors of ‘Misuse’ or ‘Disuse’, by making potential risks and countermeasures more evident
- Providing a ZDMP platform for stakeholders to communicate their trustworthiness and improve their trust in each other, mediated by their technology

ZDMP is likely to support safety critical applications and generate substantial amounts of data. If trust is lacking, the resulting ‘disuse’ of the technology may lead to negative consequences that are also damaging for trust. The main steps of trust modelling can be described as follows:

- Identify primary threats within the ZDMP architecture; eg ways its components could be attacked or for other reasons fail
- Identify what effect each of these threats would have on each stakeholder by tracing how the immediate effects could cascade through the network
- For each stakeholder, compile a list of harmful effects they may experience, and for each effect, enumerate the possible primary causes
- For each harmful effect, identify which stakeholder(s) should manage the risk, using the security measures defined in the ZDMP security architecture
- For each stakeholder, compile a list of obligations and dependencies for managing risks to themselves and others

Trust modelling involves a development of a machine understandable trust model that can assist stakeholders in managing risk. This model allows a systematic treatment of trust and trustworthiness during system design. The model also includes a classification scheme for threats, and rules describing possible strategies for using security controls to mitigate the associated risks. One of the requirements is to use machine understandable

models and machine reasoning to help users systematically identify non-obvious risks and trust dependencies during system design.

Recommendations for ZDMP and ZDL	
Recommendation	Description
Implement a trust model which represents dependencies between the stakeholders, based on who could be affected by potential threats	<ul style="list-style-type: none">• Provide a framework for assigning responsibilities and allowing interactions between the entities to take place• The trust model should allow the analysis of the system or application, provides identification of threats, and support the selection of mitigation strategies that should be implemented by each stakeholder• Trust analysis should always accompany any multi-stakeholder architectural specification or standard. It should define the responsibilities of each stakeholder and clarify what assumptions they can make of other stakeholders

Figure 55: Recommendations Section 7.3

8 Recommendations

Based on, primarily, recommendations from the previous sections, the following primary recommendations are made for ZDMP and ZDMP Limited:

Recommendations for ZDMP and ZDL	
Data management related recommendation	Recommendation
Type of data	<ul style="list-style-type: none"> ZDMP Limited, as well as the entities operating in the ZDMP ecosystem, must be aware of the main data types to be shared in their inter-organisational relationships and implement adequate measures to protect each type. Following this concept, it is recommended that contractual terms regulating the exchange of data cover at least raw data, process data, and input data
Control of data sets and identification of possible legal issues	<ul style="list-style-type: none"> All data sets processed should be under control, and the possible legal issues that may arise must be identified
GDPR related recommendations	Recommendation
Identify the processing of personal data	<ul style="list-style-type: none"> ZDL, as well as the companies operating in the ZDMP ecosystem, must be aware of the data processing operations conducted and of the type of data processed ZDL, as well as the entities operating in the ZDMP ecosystem, should make an assessment on all of their data processing operations to identify if the processing of personal data could be performed
Pay special attention to detecting the processing of sensitive data	<ul style="list-style-type: none"> It is not expected that sensitive data is processed by ZDL or project partners in the ZDMP environment at his point. However, this should be thoroughly checked because of the particular nature and risks around sensitive data Furthermore, in smart manufacturing environments, there are situations in which sensitive data may be collected and processed (ie the requirement of biometric identification for using a machine, operators using wearables that provide health related data). Consequently, all potential scenarios should be considered and analysed
Identify the data controller and data processor roles in each operation in which personal data is processed	<ul style="list-style-type: none"> ZDL and partners involved in data processing operations conducted within the ZDMP framework, should analyse the different processes that involve personal data processing, and identify who is the controller(s) and processor(s) in each of them To make this assessment, it is necessary to identify who determines the purpose and means of the processing of personal data (data controllers), and who is processing data on behalf of the company that determines the purpose and means of the processing (data processor). It is possible that two or more data controllers exist (joint controllers) In a smart manufacturing platform such as ZDMP, in which many organisations (manufacturers, suppliers, developers, apps providers, cloud provider, platform provider, etc) are involved in different data processing activities, every process and the role of each of the organisations involved, should be carefully analysed to determine who is the controller(s) and processor(s) in each of them
If there are joint controllers', the obligations of each of them should be decided	<ul style="list-style-type: none"> In situations in which more than one controller is identified (eg if it is concluded that both the manufacturer user and the app provider, that determine the purposes and means of the personal data processing), the joint controllers should decide who will carry out which controller

	<p>obligation, considering that each controller remains responsible for the compliance with GDPR [ICO19]</p>
Privacy by design	<ul style="list-style-type: none"> • A “privacy by design” approach should be applied to all the activities involving the processing of personal data. In this respect, data protection should be considered from the very beginning (the design of the product, service, zApp, etc) • ZDL and all the partners involved in ZDMP should ensure the application of this principle to all data processing activities in which they are the controllers. For example, privacy by design may be applied when the zApps offered in ZDMP are designed by setting safeguard functionalities (eg encryption), setting limits to the app’s personal data collection, etc
Privacy by default	<ul style="list-style-type: none"> • A “privacy by default” approach, should be applied to all activities involving the processing of personal data, which means that ZDL and all the partners involved in ZDMP should implement definite measures to ensure that only personal data that is necessary for the previously defined are processed • ZDL and all partners involved in the ZDMP project should ensure the application of this principle to all data processing activities in which they are the controller. They should analyse each of the processes that involve personal data processing and assess if the personal data processed is really necessary or if they could reach the same results by reducing the processing of personal data
Accountability	<ul style="list-style-type: none"> • ZDL and all partners involved in the ZDMP project, should be able to demonstrate the application of the measures necessary to comply with GDPR requirements to all data processing activities in which they are the controller • Compliance must be verifiable, especially by external stakeholders and data protection authorities • It is also recommended to keep a record of the processing activities containing the information required in Article 30 of GDPR, such as the contact details of the controller, purpose of the processing, and description of the categories of data subjects and personal data. Even when it is not mandatory to keep this record according to the GDPR (see Article 30), it is recommended to do so for better control of the processing activities
Assessment	<ul style="list-style-type: none"> • ZDL and all partners involved in the ZDMP project, should analyse the different operations that involve the processing of personal data, if a Privacy Impact Assessment (PIA) should be performed according to Article 35 of the GDPR • However, even in the cases in which it is not mandatory, according to the regulation, it is recommended to conduct a PIA for all the personal data processing operations carried out. This is a good method to detect potential risks and take actions to mitigate them
Privacy Policies	<ul style="list-style-type: none"> • ZDL as well as all partners operating in ZDMP, should draft and implement transparent data protection policies [MET17]: <ul style="list-style-type: none"> • Policies (including web policies and cookies policies) must be drafted in conjunction with the organisation’s DPO or, at least, following the assessment of an expert in case a DPO is not required • Policies must be approved and endorsed by the highest-level management of each organisation • Policies should be accessible to the data subjects (eg ZDL should include its privacy policy in its website)
Raise employee’s awareness on data protection	<ul style="list-style-type: none"> • ZDL employees and ZDMP partners’ employees must be informed and trained on how to implement the privacy policies, especially those who are involved in the processing of special categories of personal data (eg

	an employee who keep records of other employee’s wearables) [MET17])
Fulfilment of GDPR principles	<ul style="list-style-type: none"> • Controllers should ensure the fulfilment of GDPR principles for personal data processing by implementing the necessary organisational and technical measures
Set a procedure to manage data breaches	<ul style="list-style-type: none"> • ZDL and all the partners operating in ZDMP, should implement procedures, including the steps to be follow when a data breach occurs; such as: <ul style="list-style-type: none"> • Stop the data breach • Asses the damages • Notify the breach to the supervisory authority and to those affected if necessary, according to GDPR • Document the data breach including the facts, the effects, and the corrective actions taken • Control the notifications to the data subjects affected and keep all the evidence to prove that the notification was carried out
Sign a contract with the data processor	<ul style="list-style-type: none"> • The processing of personal data by a processor is governed by a contract or other legal act under European Union or Member State law, that is binding on the processor with regard to the controller and that sets the main obligations of the processor regarding the processing of personal data • In the cases, in which ZDL or ZDMP partners delegate the processing of personal data to a processor (eg a cloud storage provider), a contract including the precise instructions to the processor and its obligations is necessary
Designate a DPO	<ul style="list-style-type: none"> • It is highly recommended for ZDL to designate a DPO. For all the partners involved in the ZDMP project, the designation of the DPO should be decided depending on their own circumstances • However, even in those cases in which it is not explicitly required by GDPR, the designation of a DPO is always recommended, as it is a key figure that facilitates the compliance to GDPR • Moreover, a DPO can provide a good support, particularly in a complex environment for data management such as that in a manufacturing platform
Analyse the possible legal basis for the personal data processing	<ul style="list-style-type: none"> • The legitimate grounds for the processing provided in Article 6f of GDPR, should be assessed by the controller (ZDL or ZDMP partners depending on the circumstances). However, most of the time, the consent for processing will be based on the informed consent provided by the data subject • If it is intended to base the personal data processing in the legitimate interest of the controller, special attention should be taken in analysing and balancing this legitimate interest of the controller against the rights and interests of the data subject
Inform data subjects in a concise, transparent, intelligible, and accessible form	<ul style="list-style-type: none"> • Data controllers should inform data subjects about the purpose of processing, the rights they can exercise, and the time for which the data will be stored as well as other information required in Art.13 of GDPR • Depending on the situation, controllers can choose the best way to inform the data subject providing it is in an understandable way and adapted to them. For example, if someone navigating the ZDMP marketplace website needs to submit personal data for registration, before collecting their consent, the electronic privacy policy contained in the website (in which the required information is provided) would be provided to them
Privacy Policies of the companies operating in ZDMP	<ul style="list-style-type: none"> • It is recommended that ZDL demands all the companies operating in the ZDMP platform to have their own Privacy Policies accessible to the data subjects

<p>Controllers should be able to demonstrate that the data subject has given consent for the processing of personal data</p>	<ul style="list-style-type: none"> • When ZDL or ZDMP partners base the personal data processing on the data subject's consent, they should be able to demonstrate that the data subject has given consent for the processing of personal data by keeping the appropriate means of proof. For example, the signed consent forms, the log of activities in the website if the consent was submitted through the web, security copy of the email in which consent was provided, etc
<p>Ensure the consent revocation rights</p>	<ul style="list-style-type: none"> • Free and simple means should be provided to enable data subjects to revoke their consent. For example, ZDL (or ZDMP partners) can provide an email address to which a data subject can request the revocation of their consent
<p>Define the purposes of the processes</p>	<ul style="list-style-type: none"> • The purposes of the data processing operations that involve personal data should be defined and addressed before the collection of personal data by the controller (ZDL or ZDMP partners depending on the circumstances) • Different data processes and data sets should be monitored to analyse if personal data is re-used or re-purposed, something common in the processing activities carried out • Data subjects need to be informed of any further processing of their information if it takes place with a different purpose
<p>Minimise the processing of personal data</p>	<ul style="list-style-type: none"> • Personal data should only be processed when strictly necessary for the purposes of processing. If the processing of personal data proves to be necessary, then it should be as minimal as possible. ZDL and ZDMP partners should assess to which extent the processing of personal data is necessary for those processing operations in which they are the data controllers
<p>Make the processing of personal data the least invasive as possible and ensure privacy</p>	<ul style="list-style-type: none"> • Technical measures must be implemented to ensure appropriate levels of security and to mitigate identified risks [NCS17]: <ul style="list-style-type: none"> • Implement safeguards such as encryption or pseudonymisation where anonymisation remains impossible or unpractical for the purpose of the processing • Implementation of strong authentication techniques
<p>Control of the data storage period</p>	<ul style="list-style-type: none"> • The implementation of procedures and protocols to control the storage period of personal data (eg to eliminate data when the set storage period has ended or when it is no longer necessary), is recommended
<p>Application of procedures to ensure the exercise of data subjects rights</p>	<ul style="list-style-type: none"> • ZDL and all the partners operating in ZDMP should implement procedures to ensure the exercise of the data subjects' rights, the fulfilment of related requests, and to demonstrate the fulfilment of the obligations related. This includes: <ul style="list-style-type: none"> • Provide a contact address of the company to which data subjects can send requests related to the exercise of their rights • Set time limits to answer data subjects when requests are received and monitor the fulfilment of these times • Keep evidence of the interactions with data subjects • Keep control of the data sets that contain personal data to locate them when necessary (an adequate management of the metadata is necessary) • Implement the necessary technical measures to ensure the data portability right • Description of the processing carried out and of the categories of personal data processed

Detect international transfers of data and the legal basis to carry out the transfer	<ul style="list-style-type: none"> • ZDMP partners and ZDL should monitor and register possible transfers of personal data to third country • The countries for which there exists an “adequacy” decision from the Commission should be known • Analyse the possibility of providing appropriate safeguards • Analyse the possibility of making the transfer under one of the conditions of Article 49.1 of the GDPR
Awareness on how the personal data is processed by the cloud storage provider	<ul style="list-style-type: none"> • When contracting cloud storage services, ZDMP partners and ZDL should assess the different cloud services providers available in the market focusing on the organizational and technical measures that they implement to protect personal data
Sign a contract with the cloud provider	<ul style="list-style-type: none"> • An agreement should be signed with the cloud provider which should consider at least the following points: <ul style="list-style-type: none"> • Applicable law • Clauses related to the availability and quality of the service provided • Transparency (eg, communication about changes on infrastructure, proceedings, or results from security audits) • Location of the company providing the cloud service • Obligations of the cloud service provider to comply with data protection regulations • Security measures applied by the cloud service provider • The protocol to be followed by the cloud service provider in case of data breach • Measures to ensure portability • Cooperation of the cloud service with the data controller in the fulfilment of its obligations
Sharing of data related recommendations	Recommendation
Categorisation of data types	<ul style="list-style-type: none"> • Manufacturing companies should be at least aware of the main data types (raw data, machine data and unprocessed data; processed data; input data) to implement appropriate measures of protection • Once functioning, a categorisation of the types of data that is being generated and stored in the ZDMP platform must be performed, including the source of the data (eg, the milling machine of a determined party). The same goes for ZDL and even zApp builders • Special attention must be given to zApp builders as they may require using third parties IP (eg databases) to train algorithms necessary for the correct functioning of ZDMP Apps
Contracts to protect datasets	<ul style="list-style-type: none"> • Contractual law appears as an alternative to guarantee basic levels of legal protection of datasets and raw data. Data transaction contracts may be used to settle issues such as data ownership and use amongst others
Use of protected data bases	<ul style="list-style-type: none"> • Companies operating in ZDMP must assure that contractual agreements surround ownership rights and licensing including at least: <ul style="list-style-type: none"> • Data subject of the contract • Specific IP owned or licensed to which party • Identification of licensor and licensee • Territory and term (time) of the contract • Authorised use • Include references to EU regulations applied in the contract
Data ownership protection	<ul style="list-style-type: none"> • Companies operating in a smart manufacturing ecosystem should be aware of the different data ownership rights in relation to inter-organisational data exchange (who owns which data and to what extent, third parties involved, licenses granted, and under which conditions, etc)

	<ul style="list-style-type: none"> • Expectations, responsibilities, and liabilities regarding data security and privacy between parties may be established, as both are vulnerable to breaches • Details regarding the gathering, anonymisation, and utilisation of suppliers, partners, and customer’s data • ZDL should explicitly identify any third parties involved in inter-organisational exchanges of data, as it will function as ZDMP’s main exploitation vehicle. A list of parties involved, licenses granted, and under which conditions, must be constantly reviewed and updated • ZDMP must assure that the utilisation of data from suppliers, partners, and customers is being performed without jeopardising data protection principles, for which anonymisations and pseudonymisation techniques may be required. It should avoid any leakage of information that may constitute a trade secret or that holds a significant value for its owner
Trade secrecy to protect confidential information	<ul style="list-style-type: none"> • Trade secrets stand as an alternative for manufacturers to protect proprietary aspects of the manufacturing process, from raw data to specific matters such as requiring employees, suppliers and any organisation having access to sensitive information or data, to enter into non-disclosure agreements • The utilisation of non-disclosure agreements, which are the most common contractual measures associated with trade secrets, is recommended to ZDMP partners and ZDL • Organisations must identify all the various sources from which trade secrets and confidential information may be generated • ZDMP partners must identify possible sources of trade secrets by carefully reviewing all operations performed within their companies (eg a party or parties that, after performing analytics on certain inputs from a machine, discovers a method to enhance the functioning of a ZDMP App) • Once created, ZDL should identify commercially relevant information regarding the exploitation of the platform and evaluate the possibility of its protection through trade secrets
Implementation of technical, organisational, and contractual measures to protect trade secrets	<ul style="list-style-type: none"> • Organisations must ensure that all information subject to trade secrets protection, enjoys additional measures that guarantee its secrecy, which is also a requirement of the Trade Secrets Directive • Technical measures must accompany contractual measures, especially those designed to limit the access to sensitive information or data, for example, concerning the performance of the machine of a specific partner. The criteria to address who can access which information, should be established in a document
Liability related recommendations	Recommendation
Damages caused by external causes (eg ransomware or other malware)	<ul style="list-style-type: none"> • The functioning of software and platforms can be affected by various forms of malware thus compromising user’s data and information • ZDMP must develop a secure infrastructure to ensure all data and information stored in the platform is safe to the extent possible. Moreover, action plans in case of security breaches or cyber-attacks that may compromise valuable data and information of partners and users must be carefully designed and implemented • ZDL contracts with users should include detailed clauses addressing situations for which the company is liable and situations for which it is not. It should always consider that no security measure is infallible
Damages caused by internal causes (eg failures of a zApp)	<ul style="list-style-type: none"> • Users of the platform and Apps may suffer damages in their factories caused by malfunctions • In the scenario that erroneous functioning of the ZDMP platform / zApps cause damage on a user’s machine or system, ZDL can opt for three different legal paths: Strict liability, negligence, and defective or inadequate warnings. If ZDL opts for a strict liability approach, for

	<p>example, liability cannot be transferred to the user through a contract, meaning that ZDL would be liable for any malfunction. Contrarily, negligence will allow ZDL to argue that the cause of the failure is a breach of a duty of care by the user</p> <ul style="list-style-type: none"> • ZDL should review the conditions on which these liability legal paths operate in order to correctly apply them in case of any failure in the services offered by the platform or the zApps
Liability Insurance	<ul style="list-style-type: none"> • The possibility of liability insurance should be assessed by ZDL
Change of public policies	<ul style="list-style-type: none"> • Sometimes government interventions in certain markets affects its participants • Both ZDMP partners and ZDL must contemplate that changes in European regulations may affect them. For example, by creating additional requirements for providing platform services across the EU or to request protection under a specific type of IP. Both situations will require to re-evaluate their exploitations plans, and partners to reevaluate the options they have for protecting their results • A revision on European regulations and policies is recommended periodically during the project life cycle, as these types of changes may even affect the contractual provisions under which ZDMP platform services are provided
Cybersecurity related recommendations	Recommendation
European Union Agency for Cybersecurity (ENISA) security measures	<ul style="list-style-type: none"> • It is recommended that ZDMP partners consider security measures for smart manufacturing proposed by ENISA as guidelines to prevent and respond to potential cyberattacks. Every organisation should adapt the implementation of these measures to their own circumstances and previous assessment performed by their cybersecurity experts
Adopt the IEC-6243 standard	<ul style="list-style-type: none"> • It is important to ensure that ZDMP follows IEC-62443, which is a worldwide cybersecurity standard for industrial environments
Demand the adoption of standards	<ul style="list-style-type: none"> • Demand the adoption of cybersecurity standards (ie ISO 27000 standards) to the companies that wish to operate within ZDMP
Implement a trust model	Recommendation
Implement a trust model which represents dependencies between the stakeholders, based on who could be affected by potential threats	<ul style="list-style-type: none"> • Provide a framework for assigning responsibilities and allowing interactions between the entities to take place • The trust model should allow the analysis of the system or application, to provides identification of threats, and supports the selection of mitigation strategies that should be implemented by each stakeholder • Trust analysis should always accompany any multi-stakeholder architectural specification or standard, to define the responsibilities of each stakeholder, and to clarify what assumptions they can make of other stakeholders

Figure 56: Recommendations for ZDMP and ZDL

9 Conclusions

This deliverable is the first one out of three, corresponding to Task 2.5 “Regulation and Trustworthy System”. It offers a first approach to the main legal issues related to data management in smart manufacturing by identifying them, whilst providing an outline on collateral aspects such as the ownership of machine-generated data and cyber security measures in the field of manufacturing industry. Furthermore, it provides an analysis of the regulations that should be applied, as well a series of recommendations to address the requirements that a data processing structure should observe in terms of governance to be compliant with GDPR, and other regulations while increasing proficiency, traceability, user-control over data, and maximising security.

This document offers an analysis on data management in smart manufacturing, including types of data processed, lifecycle of such data, applicable data management principles, and legal issues that could emerge. Due to the above, the first section is a useful aid to comprehend the data management framework in smart manufacturing, which is necessary for a better understanding of following contents of the deliverable.

This document also provides a preliminary overview and study of the identified legal issues concerning data management in smart manufacturing, (such as data protection, intellectual property, trade secrecy). To illustrate this with real examples of how legal issues related to data management may arise in smart manufacturing, the use cases provided in D2.3: “Industry Scenario and Use Cases” are analysed.

Furthermore, other related collateral aspects like as cybersecurity are analysed. In addition, it provides partners with a general view of the aspects to be taken into consideration when developing the ZDMP system, as well as guidelines on how to make the system compliant and trustworthy.

In following versions of this deliverable both, the identified legal issues (especially those related to data protection), and those yet to be identified as well as the recommendations provided to be compliant with the applicable regulations and to overcome possible legal barriers, will be further developed in line with the partners’ needs that may arise as the project develops. Besides, additional aspects such as recommendations related to cybersecurity will be extended in the following versions of the deliverable.

All the above-mentioned contents will be adapted to the project’s needs and to the information provided in the upcoming deliverables from the different WPs. When necessary, experts such as the International Data Spaces and Data orientated projects, especially manufacturing ones, such as project Boost 4.0, will be liaised with.

This deliverable will be used as a basis for RTD WPs 4-8, as well as other applicable WPs to ensure that a system for Data Management and Governance is both holistic and mandatory (where applicable).

10 Implementation Actions

In this section are briefly described the actions already implemented and the ones that will be implemented during the upcoming months regarding data management, data protection and data sharing within the project activities.

10.1 Data Management Planning within ZDMP

This subsection summarises the actions to be conducted for the management of data in ZDMP. It briefly describes the methods applied to make data findable, openly accessible, interoperable, reusable, and secure. Most of these actions have already been described in past deliverables and will only be referenced along this section, to avoid duplicated content.

Although the project did not explicitly commit to this as a formal deliverable, in line with good practice, the submission of a Data Management Plan is forecast for month 18 as part of T2.5b. Below are some highlights which will be further explored in T2.5b.

10.1.1 Data Summary

The following tables briefly describe the datasets managed (or to be managed) in ZDMP, that have already been identified by the project partners.

ZDMP General		
Name of the dataset:	Internal Documents	Dissemination and Promotion
Work Package:	N/A	WP 13
Description:	Documents set-up and updated during the preparation and execution of the ZDMP project. They include the Consortium Agreement (CA), Description of Action (DoA), document templates meeting minutes, working documents and the ZDMP deliverables. The handling of ZDMP related documents is done based on OwnCloud, a solution for document management and storage.	Dissemination material generated and provided by the ZDMP consortium. Includes presentations, contributions and publications at domain-specific conferences and journals, software not covered by IPR as well as research data not affected by IPR or data privacy.

Figure 57: ZDMP General datasets

T5.2 Secure Authentication / Authorisation	
Name of the dataset	User's credentials
Work Package	WP5
Description	The system is used by various users who have different authentication / authorisation. This information should also be considered for constructing the system security model

Figure 58: T5.2 Secure Authentication / Authorisation datasets

T5.2 Secure Communication	
Name of the dataset	User's credentials
Work Package	WP5
Description	Information about the security setting of physical links of the network topology

Figure 59: T5.2 Secure communication

T5.3 Data Harmonisation		
Name of the dataset	CSV example file	JSON example file
Work Package	WP 5	WP 5
Description	A minimal working example of a CSV file	A minimal working example of CSV file

Figure 60: T5.3 Data Harmonisation datasets

T5.4 Monitoring and Alerting						
Name of the dataset	KPI	KPI Operators	KPI Rules	KPI Rules Log	KPI Notification	KPI Values History
Work Package	WP 5	WP 5	WP 5	WP 5	WP 5	WP 5
Description	A set of information used to extract KPI's values from documents	A set of Operators used to compare KPI values accordingly to its value type	A set of Rules used to trigger actions and notifications when the KPI value gets out of the desired range	A set of information about the execution of actions and notifications triggered by KPI Rules	A set of notifications triggered by KPI rules, that may receive additional information from the recipient of the notification	A set of KPI's values captured on every change, keeping a historic data

Figure 61: T5.4 Monitoring and Alerting datasets

T5.5 Autonomous Computing						
Name of the dataset	KPI Subscription	Autonomous Process Definition	Autonomous Process Log	Autonomous Processes Relation with Orchestration Processes	Autonomous Processes Relation to KPI's	Autonomous Processes History
Work Package	WP 5	WP 5	WP 5	WP 5	WP 5	WP 5
Description	A set of subscriptions that connects the user to the KPI	A set of information describing an	A set of information about the life cycle of the	A set of orchestration processes and parameter	A set of KPI's and values related to an Autonomous	A set of Autonomous Processes data captured on

	values changes	autonomous process	autonomous processes	values related to an Autonomous processes' definition	processes' definition	every change or event, keeping a historic data
--	----------------	--------------------	----------------------	-------------------------------------------------------	-----------------------	------------------------------------------------

Figure 62: T5.5 Autonomous Computing datasets

T5.5 Distributed Computing						
Name of the dataset	Resource Location	Sites Location	Area Location	Computational Task	Task Query	zApp's Physical Connections
Work Package	WP5	WP5	WP5	WP5	WP5	WP5
Description	A set of information indicating the physical location of a computational resource	A set of information indicating the physical location of sites and plants	A set of information indicating the physical location of buildings, areas and rooms	A set of information of a task to be computed using the distributed computing component	A set of queries parameters for the computation of tasks	A set of queries parameters for the computation of tasks

Figure 63:T5.5 Distributed Computing datasets

T6.1 SDK and Application Builder				
Name of the dataset	zApp Metadata	User Login Metadata	zApp bundled information	Logs
Work Package	WP 6	WP 6	WP 6	WP 6
Description	A set of information about the application that is able to define how to sell it, how to install it, which permissions it needs to work, etc. All information is set by the creator of the zApp. Will be a flat text file document in JSON format, and will be consumed by the Marketplace, the Platform, and possibly the Secure Install component. This data might need to be transferred to the platform.	For some of the function in the application builder, ZDMP services are called. To only call the services and being able to obtain data for which the user has permission, the user needs to be logged in into the platform. The app builder will not directly store any user information, but metadata connected to the user login (eg a session string)	All other information that is obtained during app building which might contain information about concrete interfaces or interfaces location, parameters and return values are completely bundled in the app, which is defined as the intellectual property of the user of the app builder, who creates the zApp.	The component needs to save logs mainly for the developer. Logs are only saved locally. By default, no sensitive information will be logged.

Figure 64: T6.1 SDK and Application Builder datasets

T6.2 Storage	
Name of the dataset	Security Controls Document
Work Package	WP6
Description	Contains storage-specific security information for the given component

Figure 65: T6.2 Storage dataset

T6.2 Marketplace (Table 1)			
Name of the dataset	zApp Metadata	User Login Metadata	zApp bundled information
Work Package	WP 6	WP 6	WP 6
Description	A set of information about the application to be able to define how to sell it, how to install it, which permissions it needs to work, etc	For the functions in the marketplace to work, a user login is required to only call the services and being able to obtain data for which the user has permission	All other information that is obtained during app building which might contain information about concrete interfaces or interfaces location. Parameters and return values are completely bundled in the app

Figure 66: T6.2 Marketplace datasets (Table 1)

T6.2 Marketplace (Table 2)			
Name of the dataset	zApp Customer data	zApp Publisher data	Auditing and Logs
Work Package	WP 6	WP 6	WP 6
Description	The marketplace links to user information from the user management system (eg email address, user settings, etc.), and stores data about all customers in the marketplace, to keep their purchases intact, be able to measure the consumed services and bill the costs to the users using the payment information provided by the users.	The marketplace links to user information from the user management system (eg email address, user settings, etc.), and stores data about all publishers of zApps in the marketplace, to manage the application manifest (listed as zApp metadata), their institution account and the related zApps, and sales preferences as well as data about sales and licenses.	The component needs to save logs and auditing trails to make purchase processes retraceable in case customers or publishers complain.

Figure 67: T6.2 Marketplace datasets (Table 2)

T6.3 Human Collaboration		
Name of the dataset	Security Controls Document	zApp's Physical Connections
Work Package	WP 6	WP 6

Description	The Security Controls Document contains information about the security control settings of a given component	Information about the physical deployment of zApp's components
-------------	--------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------

Figure 68: T6.3 Human Collaboration datasets

T6.4 Application Run-Time	
Name of the dataset	zApp's Logical Connections
Work Package	WP6
Description	Information about the Logical connections between the components which make up zApp.

Figure 69: T6.4 Application Run-Time datasets

T7.1/T7.2/T7.3/T7.4: Process Quality and Optimisation Designer (Table 1)			
Name of the dataset	Users profile records	Users session information	Project data
Work Package	WP 7	WP 7	WP 7
Description	A set of records containing basic user profile information to support user authentication	A set of records storing usage information to improve user experience	A JSON description of an optimisation / prediction development project

Figure 70: T7.1/T7.2/T7.3/T7.4: Process Quality and Optimisation Designer datasets (Table 1)

T7.1/T7.2/T7.3/T7.4: Process Quality and Optimisation Designer (Table 2)			
Name of the dataset	Problem taxonomy	Solution taxonomy	T7.1/T7.2/T7.3/T7.4: Process Quality and Optimisation Designer
Work Package	WP 7	WP 7	WP 7
Description	A taxonomy with optimisation/prediction problems and objectives in manufacturing processes	A taxonomy with optimisation / prediction techniques applicable to manufacturing process optimisation / prediction problems	A JSON description of a particular optimisation / prediction algorithm optionally including developer contact information

Figure 71:: T7.1/T7.2/T7.3/T7.4: Process Quality and Optimisation Designer datasets (Table2)

T8.2 / T8.4 Product Assurance Run-time			
Name of the dataset	Martinrea	Column distillation	Ford
Work Package	WP8	WP8	WP8
Description	Database in MySQL format with 23 tables with data about several production stages of the engine block casting process	Simulated dataset of a binary distillation column with 4 manipulated inputs, 3 disturbances, 41 internal	Cassandra database with several process parameters: vibrations, temperature, flowrate, etc.

		temperatures and 4 outputs (2 flows and 2 quality variables)	
--	--	--------------------------------------------------------------	--

Figure 72: T8.2 / T8.4 Product Assurance Run-time datasets

T8.3 Non-Destructive Inspection			
Name of the dataset	Electronic Instrument cluster / display images for AI analysis	Construction of stone slabs images for AI analysis	Construction of steel tubes images of the finished tube profiles for shape conformity control
Work Package	WP8	WP8	WP8
Description	A set of good and faulted instrument / cluster display images acquired on quality control machine in automotive plant	A set of images of stone cut slabs with a complete variety of interesting stone surface defects	A set of images of welded tube profiles in conformity and not to the expected shape

Figure 73: T8.3 Non-Destructive Inspection datasets

WP12: Open Calls					
Name of the dataset	Interested Parties Contact List	Open Call applications	Open Call evaluations	Open Call deliverables and reporting documentation	Experimental data sets
Work Package	WP12	WP12	WP12	WP12	WP12
Description	Register of interested parties' names / emails collected via zdmp.eu/register registration form and stored on ICE servers	Applications received in response to Open Calls and stored on the (still to be chosen) submissions platform	Evaluation (scoring) of Open Call applications according to evaluation processes and stored on the (still to be chosen) submissions platform	Open Call winner will report progress, provide end-of-project feedback and deliver final report describing outcomes	Data sets provided by ZDMP partners to support Open Call experimentation phase

Figure 74: Open Calls datasets

10.1.2 FAIR Data

ZDMP follows the FAIR Principles (Findable, Accessible, Interoperable, Reusable) for the management of digital assets within the project's activities.

10.1.2.1 Findable data

Several procedures and practices that are used for handling various kinds of documents within ZDMP are described in the D1.1: "Project Handbook". Section 3.1 of the D1.1, deals with the use of a common WebDAV repository, OwnCloud, whereas Section 3.2 deal with the usage of the Microsoft OneDrive cloud storage. Section 3.3 identifies the internal templates and Section 3.4 the document metadata that supports them.

Furthermore, the Marketplace framework is anticipated to provide several components that will enable the retrieval and gathering of tracking data from user journeys. The Marketplace component and all its subcomponents are described in Section 4.4 of the D4.3a: “Global Architecture Specification”.

Finally, the T6.2 Storage component acts as a potential central store (a data lake), if chosen, of all enterprise data including back-up copies, machine learning models, reports, and anything else that needs to be accessed centrally. The main benefit of a data lake is the centralisation of disparate content sources. Once gathered together, these sources can be combined and processed using big data, search and analytics techniques which would have otherwise been impossible (see Section 4.5 of the D4.3a: “Global Architecture Specification”).

10.1.2.2 Making Data Openly Accessible

The ZDMP infrastructure is based on an open architecture platform, open I/O protocols, open operating system, open source where appropriate, open feedback processes, and open engagement with its ecosystem. The adoption of “open source by default” for ZDMP, is based on Apache 2.0 License (see Section 3.2. of the D3.4a: “Societal / Economic Value and IPR Management”). This allows ZDMP to reuse existing projects’ code, and to make its own code available, allowing the research community to contribute and reuse it during and after the project closure.

A ZDMP instance of the open-source tool GitLab has been installed and is to be used for all development activities. GitLab covers the full software development lifecycle from source code management over integrated bug tracking mechanisms and continuous integration support.

To protect resources from unauthorised access the Secure Authentication/Authorisation component stores users and the corresponding authorisation policies, to control that only legitimate communications are allowed using well-known protocols, such as OpenID and OAuth 2.0. More information about this component can be found in Section 4.4 of D4.3a: “Global Architecture Specification”.

Finally, ZDMP will publish its findings through academic and international scientific and industrial journals, following the principle of open access. ZDMP aims to disseminate and achieve good results, so it intends to use the Open Access Research Infrastructure in Europe (OpenAIRE) as explained in Section 1.2.4 of the D13.1b: “Target-Driven Dissemination Strategy, Plan, and Reporting”.

10.1.2.3 Making Data Interoperable

“Interoperability” is critical in Industry 4.0 – interconnecting machines and partners allows maximum advantage of data and feedback to influence both Product and Process Quality. “Interoperability” allows the ZDMP Platform, which contains modules offering different technologies, such as data analytics, pattern recognition, or artificial vision, to be interconnectable to multiple real-world applications easily and cheaply through the provision of configurable gateways, connectors, and data-interoperability features.

Several ZDMP architecture components enable data interoperability. The main ones are:

- Data Harmonisation Designer / Runtime: This component has access to raw data and ensures that data can be integrated using unified and standardised formats or the formats needed by the data recipient (See Section 3.1 of the D4.3a: “Global Architecture Specification”)

- Service and Message Bus: The purpose of this component is to provide holistic communication for all services, end-user applications and components being used within ZDMP. It encapsulates and acts as the interface between zApps, Enterprise and Platform Tier components and external platforms (see Section 3.1 of the D4.3a: “Global Architecture Specification”)
- Inter-platform Interoperability: This component aims to integrate the ZDMP platform with other external platforms. It supports the ability to sell ZDMP services to other platforms and purchase other components from some them. It also includes a layer to link data sources from different platforms (see Section 4.9 of the D4.3a: “Global Architecture Specification”)
- AI-Analytics Designer: This component creates machine learning models from historical data and uploads them to the Marketplace. The AI-Analytics designer component deals with machine learning integration into ZDMP

10.1.2.4 Increase Data Reuse

In the ZDMP project, the possibility of sharing and reusing data for research and experimentation purposes will be determined by the data owner i.e. the entity that has the data under its jurisdiction. It is necessary to take into account that the data owner and data provider may not be the same entity. In line with EC’s interests, the ZDMP project supports the exchange, sharing and re-use of non-personalised data through the ZDMP solution, following the fair use policy (data is only used with consent of the owner). The data used for the validation of ZDMP tools will be made available for use in further experimentation (e.g. open-calls) through an open-access repository.

Furthermore, the project supports the development of collaborative solutions (within the project or through open calls) and provides an appropriate technology infrastructure to address the data sovereignty and data protection issues.

10.1.3 Allocation of resources

The management of data in the ZDMP project is conducted through the provisioning of relevant tools and systems (such as OwnCloud), which provide the required level of fairness towards data sharing, security and privacy. During the ZDMP project, data management systems are provided by the project partners as part of their commitment towards the project (see Section 3.1 of the D1.1: “Project Handbook”).

All partners should be involved in the management of the data in the ZDMP project. The project manager takes the lead role in establishing the procedures and monitoring the utilisation of available infrastructure. The underlying infrastructure is maintained by the respective owners (e.g. ASC). The owner of the OwnCloud document management system is responsible for ensuring the continuous provisioning and quality of service of OwnCloud system.

The management of data is the responsibility of data owners who decide which data to share, with whom, for what purpose and under what conditions. The provisioning of data for research purposes is ensured by putting in place the relevant procedures (based on H2020 guidelines) and by using open-access repositories.

10.1.4 Data Governance and Security

ZDMP will follow the IEC-62443, a worldwide cybersecurity standard for industrial environments (a comprehensive description of cybersecurity challenges and

recommendations can be found in Section 6 of this deliverable). The ZDMP will implement a trustworthy system that aims to provide a framework for assigning responsibilities and allowing interactions between the entities to take place and allows to analyse the system or application, provides identification of threats and supports the selection of mitigation strategies that should be implemented by each stakeholder (a comprehensive description of the trustworthy system can be found in Section 7 of this deliverable).

Furthermore, in the D4.3a: “Global Architecture Specification”, have been identified different security and data governance-related issues for each of the components of the ZDMP architecture. Measure to solve the issues identified have been proposed as well. Below you can see some examples extracted from the D4.3a corresponding to the “Data Harmonisation Designer” component:

Security Issue	Description	Need
Execution Context	As the IDP is run in parallel to the Platform and not within it, it is not held to the same policies that govern the rest of the Platform. However, the Data Maps and components produced will be run on the platform and will need to be under the security policy	The data maps need to be made secure for the platform. As with any other submitted component (zApp). This will need to be checked by the T6.2 Marketplace and T5.2 Security Run-time
Accessing to the platform	This component (outside the security protection of the platform) needs to access aspects of the platform such as an example data schema	The platform needs to provide an example of the meta-data

Figure 75: Example of the “Security Issues Table” extracted from D4.3a

Data Governance Issue	Description	Need
Need data examples.	IDP needs example data to generate data maps.	Data examples need to be appropriately anonymised and licensed in order to be used with the IDP

Figure 76: Example of the “Data Governance Issues Table” extracted from D4.3a

10.2 Ethics Forum

An Ethics Forum has been created during January’s ZDMP Plenary Meeting with the approval of the BOP. The ethics Forum will deal with legal and regulatory compliance as well as with the ethical rules and standards of the project (such as ethical practices in research, ethical development of AI etc.).

Ethical issues such as the treatment of genetic material information of human beings or human biological samples are not included as part of this project, neither the processing of information related to the search of human cloning for reproductive purposes nor the modification of their genetic heritage. Consequently, one of the main issues the Ethics Forum will deal with in the ZDMP project is data protection, as well as other data-related aspects, such as data management or data exchange,

The Ethics Forum is composed of:

- A legal coordinator, leading the Forum (Alvaro Moreton Poch from Rooter)
- Vice lead (Laura Melo from Ascora)

- Project Administration's DPO and ZDMP DPO (ICEs DPO: Oscar Garcia)
- Indirectly the members of the Executive Board of the Project

The Ethics Forum will meet (through call conferences or with personal attendance during the Plenary Meetings) once per quarter or as necessary, but extraordinary meetings may be organised if necessary.

The main functions of the Ethics Forum will be:

- Analyse possible ethical and legal issues related to the activities carried out within the project
- Provide recommendations to comply with GDPR and advise on good practices (eg ethical practices in the use of data, Machine Learning technologies, etc.) to the partners of the Consortium
- Provide recommendations regarding possible issues that may arise as a result of the data exchange within the project activities (eg data ownership, confidentiality, IP) to the partners of the Consortium
- Make a follow up of the implementation of the measures based on the recommendations of the Ethics Forum by the partners

These functions will be performed within the framework of WP2 and WP 5 activities and using the resources assigned to these WPs (person month). The required analysis, recommendations and results will be included in the corresponding deliverables.

The following actions to be carried out include:

- Preparing an action plan during February (will be included in D2.5b)
- Sharing the plan with the Forum members
- February meeting / Marc
- Preparing a living document to report on the activities of the Ethics Forum

10.3 Data Protection Implementation Plan

The project carefully analyses the implications of relevant regulations on data management, data protection and security like the GDPR (General Data Protection Regulation).

In the ZDMP project, each of the partners that decide on the means and purposes of personal data involved when carrying out the project activities will be considered data controllers (alone or jointly with others, depending on the specific case). This means that they will be responsible for implementing the organisational and technical measures necessary to comply with the GDPR.

Partners should be responsible for implementing the necessary measures to comply with the GDPR based on the recommendations provided by Ethics Forum, that should be assessed and adapted to each particular case (Privacy Impact Assessments when necessary, privacy by design etc).

10.3.1.1 Use Cases and I4FS Platform

D2.5a contains a preliminary analysis of the possible data protection issues arising in smart manufacturing, focusing specifically in the use cases developed within the ZDMP project and on the potential of personal data processing in smart manufacturing platforms (such as I4FS).

A set of comprehensive recommendations have been provided in x D2.5a (Section 2), which will be extended in the next (two) iterations of the deliverable at M18 and M30. Partners that are data controllers in the different operations that involve the processing of personal data are responsible for implementing the necessary organisational and technical measures, based on the recommendations provided to be compliant with the GDPR.

The actions that each of the consortium partners should conduct before starting the processing of personal data are as follow (progress made will be reported in month 18 D2.5b):

- Conduct a thorough analysis to identify personal data that may be processed
- Designate a DPO (if necessary) or a person within their organisations responsible for the processing of personal data
- Identify who are the controllers and processors in the different operations involving the processing of personal data
- Assess if a Privacy Impact Assessment (PIA) needs to be performed and conduct a PIA (see Section 2.2.2.1)
- Implement organisational and technical measures considering the recommendations provided in this deliverable
- Reporting to the Ethics Forum on the previous actions

As mentioned in the last bullet point, partners should report to the Ethics Forum on the measures implemented to be compliant with the GDPR. A template that should be filled by month 18 will be sent to every partner. The template questions may be updated if necessary, during the project.

Below you can see the first version of the template. Should be noted that some questions may be changed or appended if considered appropriate:

Data Protection Questionnaire (ONLY RELATED TO ZDMP ACTIVITIES)		
Question	Answer	References
<p>An assessment of all of the data processing operations within the project framework in which your company is involved should be made.</p> <p>Is any personal data is processed or is expected to be processed in any of these operations?</p>		<ul style="list-style-type: none"> • Section 2.1 • Section 4
<p>Is your organization acting as a data controller in any of these operations?</p> <p>If it's not your organization, who is the data controller?</p>		<ul style="list-style-type: none"> • Section 2.2.2
The following questions just need to be answered if your organisation is a data controller		
<p>Is your organization acting as a joint controller?</p> <p>If yes. Have you reached an agreement with the other joint data controller/s to determine the respective responsibilities for compliance with the obligations under GDPR?</p>		<ul style="list-style-type: none"> • Section 2.2.2

<p>Should your company designate a DPO according to the criteria provided in Art 37 of GDPR?</p> <p>Has your company designated a DPO?</p>		<ul style="list-style-type: none"> • Section 2.2.3
<p>Indicate which type personal data is expected to be collected and processed by your organization within the framework of the project activities</p> <p>Specify if any sensitive data (special categories of personal data, such as ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation) will be collected, and indicate which type of sensitive data</p>		<ul style="list-style-type: none"> • Section 2.1 • Section 4
<p>Will any personal data coming from a different source than the data subject be processed? If yes, from which source does this personal data originate?</p>		<ul style="list-style-type: none"> • Section 2.1 • Section 4
<p>Could you explain the purposes (the motivations, why is your organization processing personal data) of the processing for which the personal data are intended?</p>		<ul style="list-style-type: none"> • Section 2.2.4.2
<p>How will personal data be processed (what is your organisation doing with it, meaning the operations performed on the personal data, and with whom is this data shared)?</p>		<ul style="list-style-type: none"> • Section 2.2.4.2
<p>How is your organisation informing data subjects about the processing of their personal data (eg through an information sheet, electronic privacy policy etc)</p>		<ul style="list-style-type: none"> • Section 2.2.4.1
<p>Does your organisation have Privacy Policies accessible to the data subjects?</p>		<ul style="list-style-type: none"> • Section 2.2.4.1
<p>Please indicate the legal grounds (legal basis included in Article 6 of GDPR) for the processing of personal data that your organisation is carrying out. For example:</p> <ul style="list-style-type: none"> • The data subject has given consent to the processing • The processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the 		<ul style="list-style-type: none"> • Section 2.2.4.1

<p>data subject prior to entering into a contract</p> <ul style="list-style-type: none"> Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party 		
<p>For those cases in which personal data processing is based on informed consent. Have your organisation collected the data subject consent?</p>		<ul style="list-style-type: none"> Section 2.2.4.1
<p>How are your organisation collecting the consent from data subjects (eg through an electronic form)?</p>		<ul style="list-style-type: none"> Section 2.2.4.1
<p>Has your organisation implemented adequate means (free and simple) to enable data subjects to revoke their consent?</p>		<ul style="list-style-type: none"> Section 2.2.4.1
<p>Can your organisation demonstrate the collection of informed consent from the data subject?</p>		<ul style="list-style-type: none"> Section 2.2.4.1
<p>Is your organisation minimising the processing of personal data? (Only processing personal data if it is strictly necessary and, if necessary, processing as minimal as possible personal data)</p>		<ul style="list-style-type: none"> Section 2.2.4.3 Section 2.2.2.1
<p>Is your organisation implementing procedures and protocols to control the storage period of personal data?</p>		<ul style="list-style-type: none"> Section 2.2.4.5
<p>What measures is your organisation implementing (eg encryption, pseudonymisation etc) to reach adequate levels of security?</p>		<ul style="list-style-type: none"> Section 2.2.4.6 Section 6
<p>Should your organisation perform a Privacy Impact Assessment (PIA) according to criteria provided in Art 37 of GDPR?</p> <p>Has your organisation performed a PIA?</p>		<ul style="list-style-type: none"> Section 2.2.2.1
<p>Is the processing likely to create a high risk to the rights and freedoms of data subjects?</p> <p>If the answer is yes, which measures is your organisation implementing to mitigate those risks?</p>		<ul style="list-style-type: none"> Section 2.2.2.1
<p>Which procedure to be followed (including the steps) is your organisation implementing in case of a data breach?</p>		<ul style="list-style-type: none"> Section 2.2.4.6 Section 2.2.2.1
<p>Are transfers of personal data to third countries or international organisations expected during the project? To which country or international organisation?</p>		<ul style="list-style-type: none"> Section 2.2.7

<p>If the answer to the previous question is yes, please indicate under which of these bases the transfer is justified</p> <ul style="list-style-type: none"> • An “adequacy” decision from the Commission • Appropriate safeguards are provided according to the criteria established under article 46 of the GDPR • The transfer is made under one of the conditions of Article 49.1 of the GDPR 		<ul style="list-style-type: none"> • Section 2.2.7
<p>What measures your organisation is implementing to ensure the exercise of the data subjects’ rights?</p>		<ul style="list-style-type: none"> • Section 2.2.5
<p>Which actions is your organisation carrying out to demonstrate the application of the measures necessary to comply with GDPR requirements (eg document internal processes, carry out a registry of the different operations that involve personal data processing?)</p>		<ul style="list-style-type: none"> • Section 2.2.2.1
<p>Any data processor will participate in any of the operations involving personal data processing?</p> <p>If yes. Has your organisation signed a contract setting the main obligations of the processor regarding the processing of personal data?</p>		<ul style="list-style-type: none"> • Section 2.2.2

Figure 77: Data protection questionnaire

10.3.1.2 Project Administration and Dissemination

In addition to research activities and activities related to use cases, personal data will be processed within the project when other activities, such as project administration, subcall processing, or the communication and dissemination of results, are carried out.

Personal data of the project members related to administrative and general management issues in the framework of the project is used for the following purposes:

- Creation of a contact list: Excel file, contact application, or other storage containing name, surname, company, professional email, professional phone number, and optional private email / mobile / private phone / skype user, passport number and photograph
- Creation of a participation list: Excel file or other storage per events meetings organised by the Consortium / EC only for logistic organisation purposes. Containing name, surname, organisation, ID / Passport (optional) (eg for accessing to the EC facilities or wifi in some countries), dietary requirements, hotel and travel information, attendance information, social information, special needs. This document could be shared with the staff in charge of the control access, or logistics, of the venue chosen for the event or other parties which may need this information.
- Signature sheet: For assistance control and justification purposes. Containing name, surname, company and signature or attendance indicator.

- Tools: To be included in the needed project's tools for the proper development of the project. The tools will be managed by ICE or an assigned party specified in the CA/GA/or BOP decision (or equivalent) as Project Coordinator and/or Manager
- Email distribution list: Subscription of the project members to all the distribution lists relevant to their assigned tasks
- Document repository: Access of the project members to the project repository where all the relevant documentation will be stored, including those listed in the section Data Storage
- Contact or Similar Applications: Upload provided mandatory/optional information to valid contact applications to be used within the project

Regarding dissemination and communication activities, some personal data from the project participants may be collected too (eg images resulting from photo or video filming during the event).

The data controller of the above-mentioned personal data used for administration and dissemination, and communication purposes is the Project Coordinator ICE. To collect these personal data ICE sent a consent form to all project members (all persons from the different organisations which are partners of the Consortium) through the "Signable app" – See below (the complete document is included in Annex C)

Company: Information Catalyst for Enterprise, Ltd.
 Registered Address: BB/St Georges Court, Wilmington Avenue, Northwich, Cheshire (CW8 4EE), UK
 Phone: +44 1270 254520
 Email: info@informationcatalyst.com
 VAT No: GB203780724

ICE Information Catalyst
 Services Data Software

Data Protection Consent Form

Version: [] Last updated: []

1 Personal Information

M=Mandatory, O=Optional

Note if you have already provided any other personal information, such as passport number, during (for example) project kick-off phases or in attendance lists, it will also be implied this information is for sharing/projection under the terms of this agreement. If you wish to update this please see procedure at end of document.

Name (M)	[]
Work Email (M)	[]
Private Email (O)	[]
Work Phone (M)	[]
Mobile Phone (O)	[]
Private Phone (O)	[]
Skype (O)	[]
Organisation (M)	[]

I agree to the policies in the template and have provided all information with due care:

Signed: [] 08/07/2019

You will need to tick all boxes marked in RED and return this form via the electronic signature system. You will receive a copy of this form, as will ICE, and if you need to correct any information at a later date see procedures below.

Figure 78: Consent form front page

Regarding dissemination activities, events such as workshops or hackathons are expected to be organised by project partners. In case personal data from persons that are not ZDMP’s project members (eg, participants of the events) are collected during these events, their informed consent should be collected. Partners that will act as organisers of these events and as data controllers of the personal data collected, should previously inform the Ethics Forum of the measures that will be implemented (eg the collection of informed consent) to comply with the GDPR.

10.3.1.3 Sub-calls

ZDMP will provide Financial Support for small pilots conducted by third party SMEs (who may receive justified support by other entities albeit it in subservient roles), to use and validate ZDMP functionalities. The primary coordination work will be via UOS-ITI and UNINOVA. In this sense, UNINOVA will be the contracting party for ZDMP.

UNIN / UOSITI will be required to organise the subcall collection of personal data from the participants (name, email, ID etc.). Subcall coordinator (UNINOVA) will obtain informed consent from the participants for the collection and processing of their personal data.

UNINOVA will also implement the necessary measures, that should be reported to the Ethics Forum, to comply with the GDPR. The participants should sign up a contract that covers various aspects, such as data management, data exchange (including confidentiality clauses if needed) and personal data protection if needed.

It is very unlikely that during the subcalls datasets from the partners will be used beyond the individual subcall partner themselves. However, if the onward use of these datasets is necessary, they should not contain personal data or be completely anonymised.

10.4 Data Exchange Implementation Plan

D2.5a contains a preliminary analysis of possible legal issues that may arise as a consequence of data sharing among organisations that collaborate in a smart manufacturing ecosystem (such as intellectual property, data ownership, confidentiality of the shared information).

It is possible that ZDMP stakeholders, particularly large manufacturers, have concerns regarding the sharing of their data with a large group of actors operating in the platform, especially when this data provides them with a competitive advantage or are sensitive data that they don't want to be disclosed.

There are two aspects to this:

- How data will be shared and who with – if at all
- If it is shared what are the data sharing issues

Considering the 'how' question first. The statement above supposes that manufacturers MUST put their data at the disposal of ZDMP. This is a misunderstanding. Providers will provide zApps, potentially to specific manufactures (possibly including their supply chain), potentially as generic solutions. It will be up to the providers to decide the features and what is best for their business (sales etc) which may or may/not include the sharing of data with the ZDMP central platform (eg storage) or not. They may decide to share of local platforms for example, or simply use existing internal databases. The buyers of applications will seek to purchase on the basis of their needs – for example in the field of data sharing. Indeed, as identified in WP3 deliverables, larger manufacturers are more likely to host their own platforms because of the issues.

In terms of sharing then as the protection of data under copyright and trade secrets fall short in scope, to protect datasets and regulate data sharing between the different stakeholders operating in ZDMP a contractual approach has been considered as the best option to cover all the necessary aspects and avoid possible conflicts as a result of data sharing. Additionally, virtual data space models that support secure exchanges, such as International Data Space will be analysed. Moreover, cooperative actions will be fostered.

A set of comprehensive recommendations have been provided in this D2.5a (Section 3), which will be extended in the next (two) iterations of the deliverable, focusing mainly on the different aspects that should be covered in a data sharing agreement, as well as the good practices for a trustable data sharing between ZDMP stakeholders. Partners will perform the necessary actions based on the recommendations provided.

The actions that each of the consortium partners must carry out before they start sharing data are listed below. Progress will be reported in month 18 in the D2.5b:

- Identification and categorisation of the types of data that is being generated and stored within ZDMP activities
- Identify protected databases that will be used during the project

- Identify data owners
- Identify all the parties involved in data sharing activities
- Sign a data transaction/data sharing contract
- Identify sensitive or confidential information that will be shared
- Sign Non-Disclosure Agreement if needed
- Reporting to the Ethics Forum on the previous actions

As mentioned in the last bullet point, partners should report to the Ethics Forum on the measures implemented. A template that should be filled by month 18 will be sent to every partner. The template may be updated, if necessary, during the project.

Below is the first version of the template. It should be noted that some questions may be changed or added if considered appropriate:

Data Exchange Questionnaire		
Questions	Answers	References
Has your organization categorised the data types used?		<ul style="list-style-type: none"> • Section 3.1 • Section 4
Has your organisation identified the source or sources of the data? (e.g., the milling machine of a pre-determined party)?		<ul style="list-style-type: none"> • Section 3.1 • Section 4
Has your organisation signed any type of data transaction / data sharing contractual agreement?		<ul style="list-style-type: none"> • Section 3.1
Has your organisation signed any licensing agreement in relation to IP assets? If so, does it include at least the following: data subject of the contract, specific IP licensed, identification of the licensor and licensee, territory and term (time) of the contract?		<ul style="list-style-type: none"> • Section 3.1
Has your organisation signed any agreement related to data ownership rights? If so, does it include at least the following: who owns which data and to what extent, conditions, expectations, third parties involved, responsibilities, and liabilities regarding data security and privacy?		<ul style="list-style-type: none"> • Section 3.1
Has your organisation identified any possible trade secrets source?		<ul style="list-style-type: none"> • Section 3.2

<p>If any, is it protected under a non-disclosure agreement (or similar)?</p>		<ul style="list-style-type: none"> • Section 3.2
<p>Has your organization implemented any technical or organisation measure to protect trade secrets or any proprietary aspect of the manufacturing process?</p>		<ul style="list-style-type: none"> • Section 3.2

Figure 79:Data exchange questionnaire

Annex A: History

Document History	
Versions	<p>V0.1.0:</p> <ul style="list-style-type: none"> • First draft with document structure <p>V0.2.0:</p> <ul style="list-style-type: none"> • Partners' contributions integrated • Intermediary version as specified in DOA <p>V0.3.0:</p> <ul style="list-style-type: none"> • Partners' contributions revised <p>V0.4.0</p> <ul style="list-style-type: none"> • First draft for the coordinator's pre- review <p>V0.4.1</p> <ul style="list-style-type: none"> • Draft for the first review <p>V0.4.2</p> <ul style="list-style-type: none"> • Draft for the second review <p>V0.4.3</p> <ul style="list-style-type: none"> • Draft for the PMs review <p>V1.0.0</p> <ul style="list-style-type: none"> • PM Review and EU Submission <p>V1.0.1</p> <ul style="list-style-type: none"> • Resubmission following review 1
Contributions	<p>ROOT:</p> <ul style="list-style-type: none"> • Alvaro Moreton - Entire document • Conrado Castillo - Entire document • Laura Merlo - Entire document • Ariadna Jaramillo - Entire document <p>IKER</p> <ul style="list-style-type: none"> • Marc Barcelo - General Guidelines to Implement a Robust Cybersecurity System <p>UOS ITI</p> <ul style="list-style-type: none"> • Juri Papay -Trust and Trustworthiness in Complex Systems <p>TUT</p> <ul style="list-style-type: none"> • Ronal Bejarano - First reviewer <p>MRHS</p> <ul style="list-style-type: none"> • Eduardo Vila - Second reviewer <p>ICE</p> <ul style="list-style-type: none"> • Stuart Campbell-Continuous and Third reviewer

Annex B: References

- [ANP17] Advanced Network Professional. “On premises vs cloud data storage: Which is right for your organization?”. November 2017. Available: <https://www.getanp.com/blog/8/on-premises-vs-cloud-data-storage-which-is-right-for-your-organization.php>
- [AMR18] Amrit, S. “Who Owns Data Generated by IOT?” Retrieved August 2019. Available: <https://opterna.com/blog/2018/06/25/who-owns-data-generated-by-iot/>
- [ARC18] ARC Advisory Group. “Legal Issues in Smart Manufacturing Part 2”. June 2018. Available: <https://www.arcweb.com/blog/legal-issues-smart-manufacturing-part-2>
- [ARK17] Arkan, C. “Achieving GDPR compliance in manufacturing”. December 2017. Available: <https://cloudblogs.microsoft.com/industry-blog/manufacturing/2017/12/15/achieving-gdpr-compliance-in-manufacturing/>
- [AWP07] The Art 29 Working Party. “Opinion 4/2007 on the concept of personal data”. June 2007. Available: https://ec.europa.eu/justice/articleArticle-29/documentation/opinionrecommendation/files/2007/wp136_en.pdf
- [AWP07] The Art 29 Working Party. “Opinion 1/2010 on the concepts of controller and processor”. February 2010. Available: https://ec.europa.eu/justice/articleArticle-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf
- [AWP13] The Art 29 Working Party. “Opinion 03/2013 on purpose limitation”. April 2013. Available: https://ec.europa.eu/justice/articleArticle-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf
- [AWP14] The Art 29 Working Party. “Opinion 05/2014 on Anonymisation Techniques”. April 2014. Available: <https://www.pdpjournals.com/docs/88197.pdf>
- [AWP17] The Art 29 Working Party. “Guidelines on transparency under Regulation 2016/679”. November 2017. Available: https://ec.europa.eu/newsroom/articleArticle29/item-detail.cfm?item_id=622227
- [BB15] F. Baum, F., Bulthuis W. “Managing security, safety and privacy in Smart Factories”. 2015. Available: <https://www.tuev-sued.de/uploads/images/1461847200956222661681/it-security-in-smart-factories-white-paper.pdf>
- [BML+17] Burke, R., Mussomeli A., Laaper S., Hartigan M., Sniderman B. “The Smart Factory: Responsive, adaptive, connected manufacturing”. Retrieved August 2019. Available: <https://www2.deloitte.com/insights/us/en/focus/industry-4-0/smart-factory-connected-manufacturing.html>
- [BOO19] “Boost 4.0 Big Data for Factories”. Available: https://boost40.eu/wp-content/uploads/2018/02/boost_leaflet.pdf
- [CAMP18] Campbell, M. “Is On-Premise a Better Fit for SaaS Compliance with GDPR?”. July 2018. Available: <https://www.infoq.com/news/2018/07/saas-compliance-gdpr-on-premise>
- [CAV10] Cavoukian A.” Privacy by design. The 7 foundation principles. 2010. Available: https://iapp.org/media/pdf/resource_center/Privacy%20by%20Design%20-%207%20Foundational%20Principles.pdf

- [CCN+15] Chakravarthy, A., Chen, X., Nasser, B., SurrIDGE, M. “Trustworthy systems design using semantic risk modelling, Cham, 1–12”. February 2015. Available: <https://eprints.soton.ac.uk/383465/>
- [CDT18] Center for Democracy and Technology. “An Exploration of Strict Products Liability and the Internet of Things”. April 2018. Available: <https://cdt.org/files/2018/04/2018-04-16-IoT-Strict-Products-Liability-FNL.pdf>
- [CGR+06] Creese, S.J., Goldsmith, M.H., Roscoe, A.W., Zakiuddin, I. “Research directions for trust and security in human-centric computing, in Privacy, Security and Trust within the Context of Pervasive Computing, Netherlands, The Springer International Series In Engineering and Computer Science ”. 2006.
- [CHO15] Cho, J. “A Survey on Trust Modelling. ACM Comput. Surv. Surv. 48, 2, Article 28”. October 15. Available: <https://doi.org/10.1145/2815595>
- [CWC+15] A.Chakravarthy, S.Wiegand, X.Chen, B. Nasser, M. SurrIDGE, M. “Trustworthy Systems Design using Semantic Risk Modelling. Procs 1st International Conference on Cyber Security for Sustainable Society”. 2015.
- [DAV16] Davies, C. W. “Managing IP issues is a challenge for manufacturers in the age of 3D printing, says expert” June 2016. Available: <https://www.pinsentmasons.com/out-law/analysis/managing-ip-issues-is-a-challenge-for-manufacturers-in-the-age-of-3d-printing-says-expert>
- [DEL2016] Deloitte. “Technological evolution spurs the rise of Industry 4.0 and ushers in disruption”. 2016. Available: https://www2.deloitte.com/content/dam/insights/us/articles/3465_Digital-supply-network/DUP_Digital-supply-network.pdf
- [DOR19] Dorselaer D. “Industry 4.0: IoT is the Key to Smart Factory.” Retrieved August 2019. Available: <https://www.manufacturing.net/Article/2019/01/industry-40-iot-key-smart-factory>
- [DOS19] Dosen D. “GDPR and Brexit -- Is your cloud provider ready for the UK 'being treated like a third country’”. August 2019. Available: <https://betanews.com/2019/08/30/gdpr-and-brexite/>
- [DRA18] Draper S. “How wearable technology could revolutionize manufacturing industry”. November 2018. Available: <https://www.wearable-technologies.com/2018/11/how-wearable-technology-could-revolutionize-manufacturing-industry>
- [EC18] European Commission. “Protection of Databases”. Retrieved August 2019. Available: <https://ec.europa.eu/digital-single-market/en/protection-databases>
- [EDPS18] European Data Protection Supervisor. “Guidelines on the use of cloud computing services”. March 2018. Available: https://edps.europa.eu/sites/edp/files/publication/18-03-16_cloud_computing_guidelines_en.pdf
- [ENI17] ENISA. “Privacy and data protection in mobile applications” 2017. Available: <https://www.enisa.europa.eu/publications/privacy-and-data-protection-in-mobile-applications>
- [ENI18] ENISA. “Good practices for security of Internet of Things in the context of Smart manufacturing” November 18. Available: https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot/at_download/fullReport

[EP18] European Parliament. “3D printing: Sorting out the legal issues: News: European Parliament”. June 2018. Available:

<http://www.europarl.europa.eu/news/en/headlines/economy/20180615STO05928/3d-printing-sorting-out-the-legal-issues>

[EU19] European Commission. “Methodology: Data linkage”. Available:

https://ec.europa.eu/eurostat/cros/system/files/s-dwh-m_4.2_methodology_data_linkage_v2.pdf

[GIL19] Gill, B. “Legal Issues/Problems in Smart Manufacturing, Industry 4.0: ARC Advisory Group”. June 2019. Available: <https://www.arcweb.com/blog/legal-issues-smart-manufacturing>

[GLG+19], D., Lebowitz H., Greenberg J., Fried, Frank, Harris. “Data Licensing: Taking into account data ownership and use”. March 2019. Available:

<https://legal.thomsonreuters.com/en/insights/articleArticles/data-licensing-taking-into-account-data-ownership>

[GLU18] Glueck U. “Trade Secrets and Data Protection under Industry 4.0/ Made in China 2025- What does China do?” September 2018. Available: <http://www.apk2018.com/trade-secrets-and-data-protection-under-industry-4-0-made-in-china-2025-what-does-china-do/>

[HAL18] Hale, Z. “Cloud ERP vs On-Premise ERP”. October 2018. Available:

<https://www.softwareadvice.com/resources/cloud-erp-vs-on-premise/>

[ICO19] International Commissioner’s Office. “What does it mean if you are joint controllers?”. 2019. Available: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/controllers-and-processors/what-does-it-mean-if-you-are-joint-controllers/>

[IDS19] “International Data Spaces Association” Available:

<https://www.internationaldataspaces.org/>

[IPR17] European IP Helpdesk. “What are the conditions for the sui generis protection of a database?” Retrieved August 2019. Available: <http://www.iprhelpdesk.eu/node/2017>

[IPR17A] European IPR Helpdesk. “Trade secrets: An efficient tool for competitiveness”. June 2017. Available: <https://www.iprhelpdesk.eu/sites/default/files/newsdocuments/Fact-Sheet-Trade-Secrets-Efficient-Tool-Competitiveness-EN.pdf>

[IPR18] European IPR Helpdesk. “Non-Disclosure Agreement: A business tool “[. April 2018. Available: <http://www.iprhelpdesk.eu/Fact-Sheet-Non-Disclosure-Agreement>

[ISO09] ISO/IEC 31010:2009. “Risk management – Risk assessment techniques”.

ISO11] ISO/IEC 27005:2011. “Information technology -- Security techniques -- Information security risk management.

[ISO13] ISO/IEC 27001:2013. “Information Technology - Security Techniques - Information Security Management Systems – Requirements”.

[KNI18] Knight D.” Who Owns the Data Generated by Machines?” Retrieved August 2019. Available: <https://www.aem.org/news/who-owns-the-data-generated-by-machines/>

[KS18] Kauffman M., Soares M. “Industry 4.0 challenges to intellectual property in manufacturing”. July 2018. Available: https://easychair.org/publications/preprint_open/S61t

[LAN19] Lanza, J. D. “Right Tool, Right Job: Smart Manufacturing Requires Focus on Intellectual Property”. April 2019. Available:

<https://www.natlawreview.com/articleArticle/right-tool-right-job-smart-manufacturing-requires-focus-intellectual-property>

[LEI18] Leistner M. “Big Data and the EU Database Directive 99/9/EC: Current Law and Potential for Reform”. September 2018. Available: <https://ssrn.com/abstract=3245937>

[LL19] Legner, C., & Labadie, C. “Data Management for Data Protection (GDPR)”. June 2019. Available: <https://www.cc-cdq.ch/data-management-for-data-protection-gdpr>

[MAR94] Marsh, S. “Formalising Trust as a Computational Concept. Ph.D. Dissertation”. 1994.

[MAT18] Matthews, C. “6 ways blockchain will benefit manufacturing”. December 2018. Available: <https://www.smartindustry.com/blog/smart-industry-connect/6-ways-blockchain-will-benefit-manufacturing/>

[MET17] MetaCompliance. “GDPR Best Practices Implementation Guide. Transforming GDPR Requirements into Compliant Operational Behaviours”. Last updated: April 2017. Available: https://www.infosecurityeurope.com/_novadocuments/355669?v=636289786574700000

[MOH14] N.G. Mohammadi. “Maintaining Trustworthiness of Socio-Technical Systems at Run-Time In Trust, Privacy, and Security in Digital Business”. 2014.

[MOH15] N.G. Mohammadi. “Combining Risk-Management and Computational Approaches for Trustworthiness Evaluation of Socio-Technical Systems. In Proceedings of CAiSE 2015. 237–244”. 2015.

[MR17] Malaty, E., Rostama, G. “3D printing and IP law”. February 2017. Available: https://www.wipo.int/wipo_magazine/en/2017/01/articleArticle_0006.html

[NCS17] NCS London. “GDPR Recommendations”. November 2017. Available: <https://www.ncs-london.com/gdpr-recommendations/>

[NIR17] Nirwan, P. “Trade secrets: The hidden IP right”. December 2017. Available: https://www.wipo.int/wipo_magazine/en/2017/06/articleArticle_0006.html

[OEC13] Organisation for Economic Co-operation and Development. “Data Exchange”. Last updated: June 2013. Available: <https://stats.oecd.org/glossary/detail.asp?ID=1355>

[QU17] Qu, M. “Data Transaction Contracts and Related Legal Issues”. March 2017. Available: <https://www.lexology.com/library/detail.aspx?g=f22aa6e0-da59-4aa4-8980-a2d7929cb508>

[RS18] Remore, A. J., & Schaap, M. A. “Protecting Your Trade Secrets from Cyber Threats”. October 2018. Available: <https://www.csgcybersecuritylaw.com/2018/10/protecting-trade-secrets-cyber-threats/>

[SCA18] Scassa T. “Data Ownership”. Retrieved August 2019. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3251542

[SHI07] Shirey, R. “RFC 4949: Internet Security Glossary v2”. 2007. Available: <http://www.ietf.org/rfc/rfc4949.txt>

[SPS+19] Saqlain M., Piao M., Shim Y., Lee J. “Framework of an IoT-based Industrial Data Management for Smart Manufacturing”. April 2019. Available: <https://www.mdpi.com/2224-2708/8/2/25/pdf>

[TEC18] TechTerm. “Blockchain”. April 2018. Available:

<https://techterms.com/definition/blockchain>

[TEC19] Techopedia. “Data Management”. 2019. Available:

<https://www.techopedia.com/definition/5422/data-management>

[TH18] N. Tuptuk, S. Hailes. Security of Smart manufacturing systems. April 2018. Available:

<https://www.sciencedirect.com/science/article/pii/S0278612518300463>

[TOL19] Tolsma, A. “GDPR and impact on cloud computing”. Available.:

<https://www2.deloitte.com/nl/nl/pages/risk/articles/cyber-security-privacy-gdpr-update-the-impact-on-cloud-computing.html>

[TQL+18] Tao F., Quinglin Q., Ang L., Kusiak A. “Data driven Smart manufacturing. January 18. Available:

https://www.researchgate.net/publication/322566556_Data-driven_smart_manufacturing/link/5a61b1844585158bca4a1106/download

[WIK19] Wikipedia. Smart manufacturing. August 2019. Available:

https://en.wikipedia.org/wiki/Smart_manufacturing


[VDM16] VDMA Legal Services. “Data Protection and Industry 4.0”. 2016. Available:

https://industrie40.vdma.org/documents/4214230/26342484/Guideline_Data_Protection_Industrie_40_1529498365334.pdf/43b2b08b-34ca-ec88-ad17-ad823cdbe6

[VID18]: Vidrih, M. How will Blockchain work in Industry 4.0? May 2018. Available:

<https://medium.com/datadriveninvestor/how-will-blockchain-work-in-industry-4-0-efdb5446e40c>

Annex C: Consent Form

Company:	Information Catalyst for Enterprise, Ltd.	 Services Data Software
Registered Address:	BB/St Georges Court, Winnington Avenue, Northwich, Cheshire (CW8 4EE), UK	
Phone:	+44 1270 254000	
Email:	info@informationcatalyst.com	
VAT No:	GB203780724	

Data Protection Consent Form

Version		Last updated	
---------	--	--------------	--

1 Personal Information

M=Mandatory, O=Optional

Note if you have already provided any other personal information, such as passport number, during (for example) project kick-off phases or in attendance lists, it will also be implied this information is for sharing/projection under the terms of this agreement. If you wish to update this please see procedure at end of document.

Name (M)	
Work Email (M)	
Private Email (O)	
Work Phone (M)	
Mobile Phone (O)	
Private Phone (O)	
Skype (O)	
Organisation (M)	

I agree to the policies in the template and have provided all information with due care:

Signed	08/07/2019
--------	------------

You will need to tick all boxes marked in **RED** and return this form via the electronic signature system. You will receive a copy of this form, as will ICE, and if you need to correct any information at a later date see procedures below.

3.1 Data Storage

I AGREE on the storage of my professional data in the project repositories, during the project life + 5 years for auditing purposes as specified in the Grant Agreement or Consortium Agreement of the Project. I understand that these data will be available and accessible for all the project members for its use during the project lifetime. Specifically, the data will be stored by the following means.

3.1.1 Contact List

Excel File, Contact Application, or other storage containing name, surname, company, professional email, professional phone number, and optional private email/mobile/private phone/skype user, passport number and photograph.

3.1.2 Participant List

Excel file or other storage per events meetings organised by the Consortium/EC only for logistic organisation purposes. Containing name, surname, organisation, ID/Passport (optional) (eg for accessing to the EC facilities or Wifi in some countries), dietary requirements, hotel and travel information, attendance information, social information, special needs. This document could be shared with the staff in charge of the control access, or logistics, of the venue chosen for the event or other parties which may need this information.

3.1.3 Signature Sheet

For assistance control and justification purposes. Containing name, surname, company & signature or attendance indicator.

3.2 Tools

I AGREE to be included in the needed project's tools for the proper development of the project. The tools will be managed by ICE or an assigned party specified in the CA/GA/or BOP decision (or equivalent) as Project Coordinator and/or Manager. I will always have the right to be unsubscribed at any time I wish although this may invariably impact my engagement in the project. Specifically, the following tools will be implemented.

3.2.1 Email Distribution List

ICE, as Coordinator and/or Project Manager, will subscribe you to all the distribution lists relevant to your assigned tasks.

I AGREE

3.2.2 Document Repository

ICE, as Coordinator and/or Project Manager, will grant you access to the project repository where all the relevant documentation will be stored, including those listed in the section Data Storage.

I AGREE

3.2.3 Contact or Similar Applications

ICE, as Coordinator and/or Project Manager, will upload provided mandatory/optional information to valid contact applications to be used within the project

I AGREE

3.3 Access to Data

I understand that Consortium members and their third parties involved in the project can access my personal data stored in by the different means detailed in the previous sections, which include contact details (name, professional email address, professional telephone number).

3.4 Image (Photo/Video/Sound)

I grant to the project the right to use the imagen resulting from photo or video filming during the project activities, for dissemination purposes and without any commercial purpose. That include (but not limited to) the right to use then in the printed and online dissemination materials, social media, and press releases.

3.5 Rights over the Personal Data Stored by ICE

I understand that I have the right, at all time, to require to ICE, free of charge:

- The access to my personal data
- The rectification and correction of my personal data
- The erasure of my personal data (the "right to be forgotten") after the said period defined the Data Storage section
- The limitation of my data processing
- The opposition of my data processing.

To execute these rights, I have to send an email to dataprotection@informationcatalyst.com. Data will not be shared outside the project consortium without my permission. In every case, if a legal rule or legal obligation is in force which supersedes my rights, ICE reserves the right of denial of the data subject request (and/or to determine restrictions to said request, if and when applicable), duly communicating to the data subject the respective grounds of said decision.

ZERO DEFECTS
Manufacturing
Platform

ZDMP

www.zdmp.eu