EFPF: European Connected Factory Platform for Agile Manufacturing

European Factory Platform

WP11: Dissemination, Collaboration and Standardisation

D11.7: Regulatory Alignment, Compliance and Standardisation Strategies-I
Vs: 1.0

Deliverable Lead: Karl Grün, Andreas Feigl, Erwin Haubert and Martin Lorenz (ASI)

Contributing Partners: ICE, FIT, SRFG, A-D, CERTH, FOR, NXW, C2K, CNET, ASC, SRDC, IAI

Date: 2020-06-30

Dissemination: Public

Status: <~~Draft~~ ¦ ~~Consortium Approved~~ ¦ EU Approved>

Abstract

This EFPF deliverable provides a strategy for standardisation activities in the EFPF project and an overview on relevant regulations. This document describes the degree of participation of EFPF project partners in the standardization process and which regulations need to be considered in the project activities

Grant Agreement: 825075

Document Status

Deliverable Lead	Karl Grün, Andreas Feigl, Erwin Haubert and Martin Lorenz (ASI)
Internal Reviewer 1	Nisrine Bnouhanna, FOR
Internal Reviewer 2	Violeta Damjanovic-Behrendt, SRFG
Type	Deliverable
Work Package	WP11: Dissemination, Collaboration and Standardisation
ID	D11.7: Regulatory Alignment, Compliance and Standardisation Strategies-I
Due Date	2020-06-30
Delivery Date	2020-06-30
Status	<~~Draft~~ ¦ ~~Consortium Approved~~ ¦ EU Approved>

History

See Annex A.

Status

This deliverable is subject to final acceptance by the European Commission.

Further Information

www.efpf.org

Disclaimer

Project Partners:

Executive Summary

This report is part of the WP11 “Dissemination, Collaboration and Standardisation” and targets standardization, which is an important pillar in EFPF looking at how the results of the EFPF project can be brought to bear in the European economic. The work for this deliverable is performed in task T11.3, which focuses on regulatory alignment, compliance and standardisation strategies

This document serves as a guide for the EFPF partners on the most relevant standards (published and under development) and regulations with an impact on the successful operation of the tasks and technical deliverables of the project. This document additionally serves as a guide emphasizing standardization activities (standards under development) that are strategically important to EFPF, to ensure an alignment between the standards and the project outcomes.

Section 0 is an introduction to the EFPF project and provides information about the context, purpose and structure of this deliverable. Section 1 provides the detailed overview of active participation of the EFPF partners in standardisation activities and is based on an extensive survey. Section 2 summarises the responses received from EFPF partners on regulations that affect or may affect EFPF in the future. Section 3 contains the standardization strategy, which is divided in three parts, i.e. strategic areas of involvement in standardization committees elaborating standards, participation in strategic standardization groups and the concept of a CEN Workshop Agreement that supports EFPF as a digital platform. Section 4 highlights our strategy on regulations. Finally, Section 5 concludes the deliverable.

By presenting the EFPF Regulatory Alignment, Compliance and Standardisation Strategy, we highlight the importance of standardisation in the project and in ongoing digital manufacturing initiatives and define a coherent approach towards further standardisation and regulation activities.

Table of Contents

0 Introduction

0.1 EFPF Project Overview

EFPF – European Connected Factory Platform for Agile Manufacturing – is a project funded by the H2020 Framework Programme of the European Commission under Grant Agreement 825075 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 16M€. Further information can be found at efpf.org.

In order to foster the growth of a pan-European platform ecosystem that enables the transition from "analogue-first" mass production, to "digital twins" and lot-size-one manufacturing, the EFPF project will design, build and operate a federated digital manufacturing platform. The Platform will be bootstrapped by interlinking the four base platforms from FoF-11-2016 cluster funded by the European Commission, early on. This will set the foundation for the development of EFPF Data Spine and the associated toolsets to fully connect the existing platforms, toolsets and user communities of the 4 base platforms. The federated EFPF platform will also be offered to new users through a unified Portal with value-added features such as single sign-on (SSO), user access management functionalities to hide the complexity of dealing with different platform and solution providers.

0.2 Deliverable Purpose

This report is part of the WP11 "Dissemination, Collaboration and Standardisation" and targets standardization, which is an important pillar in EFPF looking at how the results of the EFPF project can be brought to bear in the European economic.

The strategic orientation towards an active participation in the standardisation process is essential for the EFPF project.

Based on the standardisation plan (D11.11), this document defines a first standardisation and regulation strategy in the areas of interest for the EFPF project.

This deliverable also contains an overview of regional, national, European, or International regulations which affect the operation and foreseen results of the project. These regulations need to be respected by all project partners.

0.3 Target Audience

This document is intended to refer the EFPF partners at the process of integration of the results of the project into standards and at the regulations with which the project results should be compliant.

0.4 Deliverable Context

This document is one of the cornerstones for achieving the project results. Its relationship to other documents is as follows:

- **Consortium Agreement (CA):** Deals with legal aspects between partners

- **Description of Action (DOA):** Provide the foundation for the actual research and technological content of EFPF. Importantly, the Description of Action includes a description of the overall project work plan.

0.5 Document Structure

This deliverable is broken down into the following sections:

- **Section 1: Overview of active Participation of EFPF Partners in Standardisation Activities** describes how the relevant areas of standardization in EFPF are identified
- **Section 2: Overview of Regulations affecting the EFPF Project Partners** describes relevant regulations in EFPF
- **Section 3: Standardisation Strategy** describes the standardisation strategy of the EFPF project
- **Section 4: Strategy on Regulations** describes the regulations affecting the EFPF project
- **Section 5: Summary**

Annexes:
- **Annex A**: Document History
- **Annex B**: References

0.6 Document Status

This document is listed in the Description of Action as “public” since it provides general information for the EFPF project that can also be of interest to other/similar initiatives.

0.7 Document Dependencies

This document is the second part of three deliverables within this task (T11.3) and will serve as the basis for the final regulatory alignment, compliance and standardisation strategy.

0.8 Glossary and Abbreviations

A definition of common terms related to EFPF, as well as a list of abbreviations, is available at: https://www.efpf.org/glossary

0.9 Supporting Documents

Supporting Documents:
- Survey on standardisation activities
- Survey on regulations

0.10 Reading Notes

- None

1 Overview of active Participation of EFPF Partners in Standardisation Activities

The standardisation activities in EFPF are designed with the focus on standardisation and utilisation of relevant standards.

ASI, as lead of T11.3, has prepared a survey of the relevant and active standardisation initiatives that EFPF partners can leverage, participate, and contribute towards. The survey was sent out from August 12th, 2019 to October 28th, 2019 for feedback from the partners. A consolidated outlook of the partner feedback is provided in Section 1.1.

Furthermore, a webinar was held on February 7th, 2020 to prepare the project partners for an active collaboration on standardization and to highlight available opportunities. The following topics were presented by ASI during the webinar include:

- The standardization process of CEN, CENELEC, ISO, and IEC in a nutshell
- How to influence/contribute to standards currently under development?
- How to initiate the elaboration of a new standard or the revision of an existing standard?
- Intellectual property issues in standardization (IPR policy of standardization bodies)
- Are there technical barriers in existing standards to the technical issues of current EFPF project activities? Relation to the current standardisation plan (D11.11).
- Survey on Standardisation Activities.
- Position of EFPF in the Digital Manufacturing Cluster (with ZDMP and QU4LITY projects).

As a follow up action, more webinars will be organised to gather partner feedback, highlight areas of interest and ong-going developments in the standardisation field and to assist partners in their standardisation activities.

1.1 Results of the Survey on Standardisation Activities

Based on the identification of relevant standardisation activities, the EFPF standardisation related contributions of project partners are expected in the following areas:

EFPF Focus Area	Industrial Processes
Relevant Technical Committee	CEN Workshop of MONSOON H2020 Project (MOdel based coNtrol framework for Site-wide OptimizatiON of data-intensive processes)
Relevant Standards	• CWA 17492, Predictive control and maintenance of data intensive industrial processes
EFPF Actions	• C2K has studied and implemented this standard for the realisation of data intensive industrial processes.

EFPF Focus Area	Industrial Automation Systems, Product Catalogues
Relevant Technical Committee	ISO/TC 184/SC 4 – Industrial data
Relevant Standards	• ISO 10303-236:2006, Industrial automation systems and integration - Product data representation and exchange - Part 236: Application protocol: Furniture catalogue and interior design - and Application modules • ISO 20534:2018, Industrial automation systems and integration -- Formal semantic models for the configuration of global production networks • ISO/AWI 23247, Digital Twin manufacturing framework • IEC 61131 Programmable controllers • IEC 62714 Automation Mark-up Language • IEC 62264 Enterprise-control system integration
EFPF Actions	• C2K will adopt and harmonise the above standards in relation to the Factory Connector Architecture (T4.1) to support the building blocks of the EFPF platform. C2K will do this by considering the format of data at all levels of the automation model and how this will support interoperability for the platform tools and services. • FOR will track the progress on ISO 20534 to analyse its adoption or application for inter-enterprise data exchange in the EFPF platform (e.g. as in T3.5) • CNet will study the activities on Digital Twin standardisations and Product Data representations which are both relevant to CNet's commercial activities related to the equipment manufacturing. • FOR is studying the ISO 20534 standard as a candidate to support the collaborative manufacturing network model, specifically the aspect of monitoring collaborative manufacturing process. This is still undergoing work; the first outcomes show that no further activities seem to have happened since the standard has been published. Also, the ISO 20534 standard focus on the business process of the collaborative network rather than the manufacturing process.

EFPF Focus Area	Enterprise Systems, Interoperability, Integration
Relevant Technical Committee	ISO/TC 184/SC 5 – Interoperability, integration, and architectures for enterprise systems and automation applications
Relevant Standards	• ISO/CD 22549-1, Assessment on convergence of informatisation and industrialisation for industrial enterprises -- Part 1: Principles and framework

EFPF Actions	• NXW will monitor and adapt the activities of the above TC, due to its implications on automation platforms such as Symphony (the commercial platform by NXW)

EFPF Focus Area	**IoT, Device Integration**
Relevant Technical Committee	IEC/TC 65/SC 65E - Devices and integration in enterprise systems
Relevant Standards	• IEC 62264-1:2013, Enterprise-control system integration -- Part 1: Models and terminology • IEC 62264-2:2015, Enterprise-control system integration -- Part 2: Objects and attributes for enterprise-control system integration • IEC 62264-3:2016, Enterprise-control system integration -- Part 3: Activity models of manufacturing operations management • IEC 62264-4:2016, Enterprise-control system integration -- Part 4: Objects and attributes for manufacturing operations management integration • IEC 62264-5:2016, Enterprise-control system integration -- Part 5: Business to manufacturing transactions • IEC 61499-1:2012, Function blocks - Part 1: Architecture • IEC 61499-2:2012, Function blocks - Part 2: Software tool requirements • IEC 61499-4:2013, Function blocks - Part 4: Rules for compliance profiles • IEC PAS 63088:2017, Smart manufacturing - Reference architecture model industry 4.0 (RAMI4.0)
EFPF Actions	• NXW will monitor the outcomes of this SC and adopt those above-mentioned standards that have implications on automation platforms • ASI will promote IEC PAS 63088 that provides a reference model for EFPF as RAMI 4.0 is at the foundation of Industry 4.0 standardisation efforts. • CNet will monitor the above standardisation activities on the device integration with IoT platforms. The analysis carried out will be used to inform the design of Data Spine (T3.2) and align the development of Data Spine with latest standards on IoT integration.

EFPF Focus Area	Industrial-process measurement, control and automation
Relevant Technical Committee	IEC/TC 65 - Industrial-process measurement, control and automation
Relevant Standards	• IEC 62443-2-1 Ed. 1.0:2010, Industrial communication networks - Network and system security - Part 2-1: Establishing an industrial automation and control system security program • IEC 62443-2-4 Amd.1 Ed. 1.0:2017, Amendment 1 - Security for industrial automation and control systems - Part 2-4: Security program requirements for IACS service providers • IEC 62443-2-4 Ed. 1.1:2017, Security for industrial automation and control systems - Part 2-4: Security program requirements for IACS service providers • IEC 62443-2-4 Ed. 1.0:2015, Security for industrial automation and control systems - Part 2-4: Security program requirements for IACS service providers • IEC 62443-2-4 Ed. 1.0 Cor.1:2015, Corrigendum 1 - Security for industrial automation and control systems - Part 2-4: Security program requirements for IACS service providers • IEC 62443-3-3 Ed. 1.0:2013, Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels • IEC 62443-3-3 Ed. 1.0 Cor.1:2014, Corrigendum 1 - Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels • IEC 62443-4-2 Ed. 1.0:2019, Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components • IEC/TR 62443-2-3 Ed. 1.0:2015, Security for industrial automation and control systems - Part 2-3: Patch management in the IACS environment • IEC/TR 62443-3-1 Ed. 1.0:2009, Industrial communication networks - Network and system security - Part 3-1: Security technologies for industrial automation and control systems • IEC/TS 62443-1-1 Ed. 1.0:2009, Industrial communication networks - Network and system security - Part 1-1: Terminology, concepts and models

EFPF Actions	• NXW will further study IEC/TC 65 and adopt those standards that have implications on automation platforms such as NXW's Symphony platform • CNet will monitor the above standardisation activities on the device integration with IoT platforms. The analysis carried out will be used to inform the design of Data Spine (T3.2) and align the development of Data Spine with latest standards on IoT integration.

EFPF Focus Area	**IT Service Management**
Relevant Technical Committee	ISO/IEC/JTC 1/SC 40 - IT Service Management and IT
Relevant Standards	• ISO/IEC 38500, Information technology -- Governance of IT for the organization • ISO/IEC 38505-1, Information technology -- Governance of IT -- Governance of data -- Part 1: Application of ISO/IEC 38500 to the governance of data • ISO/IEC TR 38505-2:2018, Information technology — Governance of IT — Governance of data — Part 2: Implications of ISO/IEC 38505-1 for data management • ISO/IEC 38506, Information technology -- Governance of IT -- Application of ISO/IEC 38500 to the governance of IT enabled investments
EFPF Actions	• SRFG implements the ISO/IEC 38500 and assures that the data accountability map and associated matrix of considerations from ISO/IEC 38505-1 are fully adopted in EFPF. The data governing principles in EFPF are implemented according to the IT governance methods presented in these standards.

EFPF Focus Area	IoT
Relevant Technical Committee	ISO/IEC/JTC 1/SC 41 - Internet of Things and related technologies
Relevant Standards	• ISO/IEC 21823-1:2019 - Internet of things (IoT) -- Interoperability for internet of things systems -- Part 1: Framework • ISO/IEC 30141:2018 - Internet of Things (IoT) -- Reference Architecture • ISO/IEC NP 30144 - Information technology -- Sensor network system architecture for power substations • ISO/IEC NP 30147 - Information technology -- Internet of things -- Methodology for trustworthiness of IoT system/service • ISO/IEC NP 30149 - Internet of things (IoT) -- Trustworthiness framework • ISO/IEC NP 30160 - Internet of Things (IoT) -- Application framework for industrial facility demand response energy management • ISO/IEC NP 30161 - Internet of Things (IoT) -- Requirements of IoT data exchange platform for various IoT services • ISO/IEC NP 30162 - Internet of Things (IoT) -- Compatibility requirements and model for devices within industrial IoT systems • ISO/IEC NP 30163 - Internet of Things (IoT) -- System requirements of IoT/SN technology-based integrated platform for chattel asset monitoring supporting financial services • ISO/IEC NP TR 30164 - Internet of things (IoT) -- Edge Computing • ISO/IEC NP 30165 - Internet of Things (IoT) -- Real-time IoT framework
EFPF Actions	• NXW will monitor the above standards (e.g. the activities of ISO/IEC JTC 1/SC 41 on real-time IoT framework) based on their implications on automation platforms and relevance to the factory connectivity and IoT relevant task (T4.1) in the EFPF project • SRFG monitors the ongoing development of the Trustworthiness framework in the ISO/IEC NP 30149 - Internet of things (IoT). A possible cooperation with the ISO/IEC JTC 1/SC 41 will be investigated in the context of the EFPF task related to trust (T5.3) • CNet has monitored the above standardisation activities in the realm of IoT and this has informed the design and development of integration and interoperability mechanisms for IoT sensors and devices in the EFPF platform (T3.2, T4.4)

EFPF Focus Area	Data Interoperability, OPC & Industry 4.0
Relevant Technical Committee	• IEC/TC 65/SC 65E - Devices and integration in enterprise systems • ZVEI SG 'Models and Standards' and Platform Industry 4.0 working group WG1
Relevant Standards	• IEC/TR 62541-1:2016, OPC Unified Architecture - Part 1: Overview and concepts • IEC/TR 62541-2:2016, OPC Unified Architecture - Part 2: Security Model • IEC 62541-3:2015, OPC Unified Architecture - Part 3: Address Space Model • IEC 62541-4:2015, OPC Unified Architecture - Part 4: Services • IEC 62541-5:2015, OPC Unified Architecture - Part 5: Information Model • IEC 62541-6:2015, OPC Unified Architecture - Part 6: Mappings • IEC 62541-7:2015, OPC Unified Architecture - Part 7: Profiles • IEC 62541-8:2015, OPC Unified Architecture - Part 8: Data Access • IEC 62541-9:2015, OPC Unified Architecture - Part 9: Alarms and conditions • IEC 62541-10:2015, OPC Unified Architecture - Part 10: Programs • Industry 4.0: Specification Details of the Asset Administration Shell

EFPF Actions	• NXW is interested in the adoption of OPC UA standard for machine level communication, particularly in the context of their Symphony platform that will be linked with the EFPF platform. • ICE has started to investigate OPC UA, in particular on how it will be used by the new Administration Shell standard. ICE workflow platform WASP (T4.6) is being tuned to support OPC UA based communication in workflows/processes that are designed to link multiple shop-floor assets • FOR is an OPC Foundation member and has actively participated in the German Mechanical Engineering Industry Association (VDMA) efforts for OPC UA information model standardisation within the VDMA Robotics and Integrated Assembly Solutions Sector Groups. FOR will support EFPF partners in the adoption/uptake/alignment of OPC UA through sever development tasks (e.g. T3.2, T3.5, T4.1). OPC UA is the core Industry 4.0 communication protocol for machine connectivity with supervisory systems and other machines. Relevant domain specific standard extensions are developed in committees associated with the OPC Foundation before being submitted for formal standardisation. The VDMA strongly promotes the use of OPC UA among all its member companies and committees. • CNET is an OPC Foundation member and has started to promote the adoption of this standard in EFPF tasks (T3.5)
Activity from EFPF Partner	• NXW investigates models and ontologies from OPC UA, in particular IEC 62541-5:2015 OPC Unified Architecture – Part 5: Information Model at the border between building and factory concepts. • FOR is closely monitoring the progress of OPC foundation. In T4.1, the Dynamic Factory Connector (developed by FOR) supports an OPC UA interface both with the local data sources as well as with the EFPF platform through OPC UA PubSub over AMQPs and MQTTs. The goal is to support other EFPF Connectors and Gateways developers to provide an OPC UA interface. • ICE has studied the support OPC UA in its WASP tool for enabling direct reading from factory PLCs and sensors. The intention is to use sensor data in conditional gateways for dynamic process execution flows.

EFPF Focus Area	Messaging, Message Exchange
Relevant Technical Committee	ISO/IEC JTC 1 – Information Technology
Relevant Standards	• ISO/IEC 19464:2014, Information technology -- Advanced Message Queuing Protocol (AMQP) • ISO/IEC 20922:2016, Information technology -- Message Queuing Telemetry Transport (MQTT) • ISO/IEC 21778:2017, Information technology - The JSON data interchange syntax • ISO/IEC 19845:2015, Information technology - Universal Business Language Version 2.1 (UBL v2.2) • ISO/IEC 30118-1:2018, Information technology - Open Connectivity Foundation (OCF) Specification - Part 1: Core specification
EFPF Actions	• AMQP, MQTT and JSON are essential standards for the application integration and the building blocks of the EFPF Data Spine and the platform. The uptake, interoperability and/or alignment of these standards will be carried out in the tasks dealing with message exchange in EFPF (T3.2 - Data Spine) • Considering the cross-platform data model, EFPF platform sees the UBL v2.2 (or v2.3) as a candidate. In the NIMBLE project, the UBL v2.1 version of the standard is used. In the scope of EFPF, the data model of NIMBLE will be upgraded to v2.2, or v2.3 that is expected in December 2019. In the scope of EFPF standardisation activities, SRDC will submit additional user requirements and/or user usage scenarios to the UBL community in order to contribute to UBL 2.3 • CNet will monitor the activities related to MQTT (ISO/IEC 20922:2016) due to its importance in the development of Data Spine (T3.2) and CNet's IoT applications. • ICE's WASP tool has been enabled to communicate with external process applications that use UBL. ICE will continue working towards a closed integration with UBL aiming at a closer interface with BPMN2.0 standard. • In the context of T4.1 and T3.2, FOR is working with MQTT and addressing interoperability issues towards other protocols, e.g., OPC-UA, CoAP. FOR is monitoring activities concerning MQTT (ISO/IEC 20922:2016) and its industrial counterpart, MQTT Sparkplug, in regards to the Dynamic Factory Connector and IIoT applications (T4.1).

EFPF Focus Area	Information Management
Relevant Technical Committee	• ISO/IEC JTC 1/SC 7 – Software and systems engineering Object Management Group – Business Process Management Initiative
Relevant Standards	• ISO/IEC TS 33052:2016 Information technology - Process reference model (PRM) for information security management • BPMN 2.0 – Ratified by ISO 19510 – Business process modelling • JSR 268 - Java Portlet specification v2.0
EFPF Actions	• ICE has adopted BPMN 2.0 as a modelling notation for workflows. ICE will continue monitoring the BPMN 2.0 standard. • ICE's WASP is using BPMN for designing processes and monitoring their execution. Future developments of WASP include functionalities that generate code to connect applications. WASP development team will study what would be a way to modify BPMN to accommodate this industrial application need. • ICE's WASP is implementing the standard Java portlet's as pluggable user interfaces. A portlet container runs the portlets with the run time environment.

EFPF Focus Area	Blockchain and distributed ledger technologies
Relevant Technical Committee	ISO/TC 307 Blockchain and distributed ledger technologies
Relevant Standards	• ISO/DIS 22739 Blockchain and distributed ledger technologies – Terminology • ISO/CD 23257.2 Blockchain and distributed ledger technologies — Reference architecture • ISO/DTR 23244 Blockchain and distributed ledger technologies — Privacy and personally identifiable information protection considerations • ISO/CD TR 23245 Blockchain and distributed ledger technologies — Security risks, threats and vulnerabilities
EFPF Actions	• CNET and CERTH will both monitor the above standardisation activities for application in the blockchain, distributed ledger and smart contracting efforts.

EFPF Focus Area	Information Security
Relevant Technical Committee	ISO/IEC JTC 1/SC 7 – Software and systems engineering
Relevant Standards	• ISO/IEC TS 33052:2016 Information technology - Process reference model (PRM) for information security management
EFPF Actions	• ICE will investigate this standard and promote its adoption for the development of security reference models (in T6.2)

EFPF Focus Area	Information Security
Relevant Technical Committee	ISO/IEC JTC 1/SC 27 – IT security techniques
Relevant Standards	• ISO/IEC 27000:2018, Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary • ISO/IEC 27001:2013, Information technology -- Security techniques -- Information security management systems -- Requirements • ISO/IEC 27002:2013, Information technology -- Security techniques -- Code of practice for information security controls • ISO/IEC 27005:2011, Information Technology -- Security Techniques -- Information Security Risk Management • ISO/IEC 27009:2016, Information technology -- Security techniques -- Sector-specific application of ISO/IEC 27001 – Requirements • ISO/IEC 27017:2015, Security Techniques -- Code of Practice for Information Security Controls Based on ISO/IEC 27002 for Cloud Services • ISO/IEC 15408:2009, Common Criteria – Information technology – Security techniques – Evaluation criteria for IT security • ISO/IEC WD 27032, IT Security Techniques -- Cybersecurity -- Guidelines for Internet Security" • ISO/IEC WD TS 27100, Information technology -- Cybersecurity -- Overview and concepts • ISO/IEC NP 24392, Information technology -- Security techniques --Security reference model for Industrial Internet Platform (IIP) • RFC 6749/ISSN: 2070-1721 - The OAuth 2.0 Authorization Framework • OpenID Connect

EFPF Actions	• SRFG considers the above set of Information Security standards for the design of security controls (T6.2) in EFPF. SRFG is also interested in contributing to cloud security standards, e.g. ISO/IEC 27017:2015. • Based on the plan in D11.11, WASP has already implemented OpenID Connect (built on top of OAuth 2.0 as a security standard to enable Single Sign-On functionality in EFPF federation. • SRFG will analyse ISO/IEC NP 24392 which is in an early stage of development.

EFPF Focus Area	**Data Management**
Relevant Technical Committee	ISO/IEC JTC 1/SC 32 – Data management and interchange
Relevant Standards	• ISO/IEC 6523-1:1998, Information technology -- Structure for the identification of organisations and organisation parts -- Part 1: Identification of organisation identification schemes • ISO/IEC 6523-2:1998, Information technology -- Structure for the identification of organisations and organisation parts -- Part 2: Registration of organisation identification schemes
EFPF Actions	• EFPF partners (SRFG, CERTH, VLC, C2K) have investigated the above standard that provides information on how to identify organisations and organisational parts in data interchange. EFPF tasks on matchmaking (T4.5) and marketplace framework (T3.3) are currently analysing the use of this standard at company registration phase or when exchanging business messages. Some implication on domain specific aspects are being investigated • VLC along with other partners is actively investigating the use of these standards for data sharing between platforms. The approach for Business and Networking Intelligence follows the matchmaking task which uses a combination of standard including the ones mentioned here and others such as eClass and UBL.

EFPF Focus Area	**IoT Architecture**
Relevant Technical Committee	IEEE – Institute of Electrical and Electronics Engineers
Relevant Standards	• IEEE P2413, Standard for an Architectural Framework for the Internet of Things (IoT)

EFPF Actions	• ICE is referencing this standardised in its platform development initiatives • CNet is promoting the uptake of this standard on IoT architecture in the development of Data Spine (T3.2). Monitoring this standard will also benefit CNet commercial activities in the area of IoT devices. • FOR is monitoring the IEEE P2413, the standard references for Smart Cities (P2413.1). FOR has interest in the future developments of this specific part, to ensure standardisation alignment.

EFPF Focus Area	**Cloud Computing**
Relevant Technical Committee	ISO/IEC JTC 1/SC 38 – Cloud Computing and Distributed Platforms
Relevant Standards	• ISO/IEC 17788:2014, Information technology -- Cloud computing -- Overview and vocabulary
EFPF Actions	• The above standard provides a comprehensive vocabulary that is relevant to all types of organisations. There is little potential to further enhance this standard and therefore the activities in EFPF project will focus on the use of this standard terminologies across project documents and dissemination channels.

EFPF Focus Area	**Risk Management**
Relevant Technical Committee	ISO/TC 262 – Risk Management
Relevant Standards	• ISO 31000, Risk management — Guidelines • ISO/TR 31004:2013, Risk management — Guidance for the implementation of ISO 31000
EFPF Actions	• Although a working group has been setup by the German Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, BSI) to focus on the Risk Management topic, there is no current activity in this area. This represents an opportunity for EFPF (particularly the partners involved in the development of Risk Management Tool in T4.4) to support and collaborate with BSI towards the development of standards in this area. One area of interest for EFPF will be to facilitate the exchange of knowledge between BSI and NIST's Risk Management Framework. ASI will facilitate the investigation and collaborations in this area. • FOR is actively involved in the development of the Gaia-X initiative to strengthen Europe's data infrastructure.

EFPF Focus Area	Application Development
Relevant Technical Committee	IPC-CFX (IPC 2-17 – Connected Factory Initiative Subcommittee)
Relevant Standards	• Software tools for Connected Factory Exchange SDK Version 1.0.5
EFPF Actions	• The identification of the above standard provides an impetus to EFPF (T5.5) to align the relevant application development activities (through the SDK in T5.5) with the IPC-CFX standard. The associated open source "Software tools for Connected Factory Exchange SDK" (Version 1.0.5) will be relevant in this regard. Relevant EFPF partners (e.g. CMS) will also investigate joining the IPC-CFX movement in order to contribute towards the further enhancement/ development of the standard e.g. for the manufacturing applications to be developed in the EFPF project.
Activity from EFPF Partner	• CMS is the leader of the Connected Factory SDK group (WG-DA-05) and is developing activities towards creating requirements and a common vision for a standard, innovative and reusable SDK to be adopted by the European projects, particularly in the manufacturing area. • CMS will continue working towards the standardisation of an SDK and towards the alignment of its current SDK to the new vision and suite of tools.

The overview of relevant standardisation activities and ongoing efforts in the EFPF project suggest that the project partners are following the initial plan presented in D11.11. In most cases progress has been reported by project partners either in terms of study of relevant standards or their adoption/implementation in the ongoing activities. This emphasis on standardisation is important to streamline the project activities with other/similar activities taking place in the digital manufacturing space. This is in addition to the joint CEN Workshop Agreement (CWA) activity being carried out in the Digital Manufacturing Platforms (DMP) Cluster – a collaborative initiative involving DT-ICT-07 projects, EFFRA and OPEN DEI and Connected Factories 2 CSA – more details of the DMP cluster are available in D11.1. In this respect, the T11.3 lead will continue to lead the standardisation activity in the EFPF project and support project partners in their pledge to contribute towards relevant standards.

2 Overview of Regulations affecting the EFPF Project Partners

The scope of this work package (WP11), the task T11.3 (Regulatory Alignment, Compliance and Standardisation Strategies) also includes the identification of regulations affecting the EFPF project.

Therefore, in the scope of T11.3, a preliminary survey has been carried out among the project partners to determine international, European, national, or regional regulations that affect the EFPF project partners and shall be considered to ensure legal compliance.

2.1 Results of the Survey on Regulations

The results collected from the regulations survey provide an outlook of relevant regulations that influence of the operations of project partners in the context of carrying out necessary activities in the project. The following feedback from individual partners will be taken into account while drafting the collaboration activities, technical developments and the governance mechanism in the EFPF project.

2.1.1 3DI

1	**Regulation:**	EN 9100
	How does this regulation affect EFPF:	General quality management requirements for aviation
2	**Regulation:**	Customer Regulation (e.g. Airbus)
	How does this regulation affect EFPF:	It describes the process and environmental requirements for the manufacturing of the components. It sets limit values.
3	**Regulation:**	Reach regulations
	How does this regulation affect EFPF:	They governs the use of rare and dangerous substances that may be used in the piloting activities

2.1.2 AAM

1	**Regulation:**	GDPR
	How does this regulation affect EFPF:	Privacy and data protection, privacy by design need to be applied including the right to be forgotten This regulation affects EFPF during the project time and in the post-project phase.
2	**Regulation:**	REACH
	How does this regulation affect EFPF:	It's a customer requirement and is important for EFPF to show its compliance to this regulation.
3	**Regulation:**	ISO 9001
	How does this regulation affect EFPF:	It's a customer requirement and is important for EFPF to show its compliance to this regulation.
4	**Regulation:**	Airbus T 81 (Handbook)
	How does this regulation affect EFPF:	It's a customer requirement to know which software and materials are used in the factory.

2.1.3 AID

1	**Regulation:**	Royal Decree 8/2020 [2]
	How does this regulation affect EFPF:	The right to adapt the work shifts or other features related to the work. With the current COVID-19 crisis in Spain, this regulation allows workers to have ample flexibility when structuring their daily routines. At the same time, some side effects cannot be avoided, e.g. delimiting physical meetings and unsupervised work that might yield to a reduction in the quality of work, especially in junior worker profiles.
2	**Regulation:**	Royal Decree 488/1997,of April 14th [3]
	How does this regulation affect EFPF:	It defines health and safety regulations related to the work with equipment that include visualization screens. This decree establishes a series of rules to guard the health and safety of workers that operates with such kind of devices. However, laptop screens are excluded from this regulation, providing that they are not used continuously to perform the daily work shift. With the current COVID-19 crisis in Spain, this comes into conflict with the previous Decree due to the fact that most

		of the employees are working from home using solely laptop screens, thus indirectly transgressing this Decree.
3	**Regulation:**	Royal Decree 486/1997 of April 14th [4]
	How does this regulation affect EFPF:	As the previous ones, this Decree establishes a series of rules to guard the health and safety of workers within the workplaces. It ensures that workers have all health and safety guarantees when working in offices, etc. With the current COVID-19 crisis in Spain, working from home does not necessarily fulfil all the safety requirements of the Decree. For instance, couches, home chairs, home tables or desks are no substitute for a fully equipped office.
4	**Regulation:**	GDPR
	How does this regulation affect EFPF:	Privacy and data protection (personal and industrial data) during the EFPF project time and in the post-project phase.

2.1.4 ALM

1	**Regulation:**	GDPR (EU)
	How does this regulation affect EFPF:	Privacy and data protection
2	**Regulation:**	Cybercriminality regulations in NL – Wet Beveiliging Netwerk – en Informatiesystemen (Wbni)
	How does this regulation affect EFPF:	Each of the EU countries has to follow Directive (EU) 2016/1148. In NL, this means that suppliers of a digital marketplace cloud service (if they have a certain size or relevance) need to ensure the security of their service against cyber-attacks and need to report incidents to the National Cyber Security Centre (NCSC) and the CSIRT-DSP from the ministry of economic affairs.
3	**Regulation:**	Benelux-verdrag inzake de intellectuele eigendom (NL)
	How does this regulation affect EFPF:	This Benelux-treatment deals with trademark law. It might not directly affect only EFPF but also products / services that are exposed via EFPF.

2.1.5 ASC

1	**Regulation:**	GDPR
	How does this regulation affect EFPF:	T5.2 Portal and T4.3 Secure Data Storage require to be adapted to the GDPR requirements.

2.1.6 ASI

1	**Regulation:**	GDPR
	How does this regulation affect EFPF:	Privacy and data protection, privacy by design need to be taken into account, incl. the right to be forgotten This regulation affects EFPF during the project time and in the post-project phase.
2	**Regulation:**	REGULATION (EU) 2019/424
	How does this regulation affect EFPF:	COMMISSION REGULATION (EU) 2019/424 of 15 March 2019 laying down ecodesign requirements for servers and data storage products pursuant to Directive 2009/125/EC of the European Parliament and of the Council and amending Commission Regulation (EU) No 617/2013 Since EFPF will provide a data intensive platform, energy efficiency and ecodesign aspects need to be taken into account.
3	**Regulation:**	Regulation (EU) 2019/1150
	How does this regulation affect EFPF:	Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services This regulation specifies kind of a code of conduct to be respected when operating an online platform such as EFPF.

2.1.7 BRM

1	**Regulation:**	BGBl. I Nr. 66/2002, Federal Law on the Granting of Privileges to Non-Governmental International Organisations (national Austrian law)
	How does this regulation affect EFPF:	This law is the basis for founding the EFF (European Factory Foundation).

2.1.8 CERTH

1	Regulation:	GDPR
	How does this regulation affect EFPF:	The data collected will be relevant and limited to the purposes of the use cases to be implemented in EFPF. The adopted security measures prevent unauthorised access to personal data and to the equipment used for processing of the data. In case that any personal data is collected it will be stored and processed only internally, encrypted or hashed.

2.1.9 ELD

1	Regulation:	GDPR
	How does this regulation affect EFPF:	All data provided by ELDIA through the EFPF portal will be used in a way that is GDPR compliant. The data will be processed only by the project members and exclusively for the purposes of the EFPF project.

2.1.10 ELN

1	Regulation:	GDPR
	How does this regulation affect EFPF:	We have to ensure that the data we receive from customers can't be accessed by anyone. We design and implement tools and services that provide security and privacy and are GDPR compliant.

2.1.11 FIT

1	Regulation:	GDPR
	How does this regulation affect EFPF:	Privacy and data protection, privacy by design need to be taken into account, incl. the right to be forgotten The Data Spine needs to take the integrity of the data flows into account. The Data Model Conversion tool and "HyCoDER" (Hybrid Configurable Data Extraction and Restructuring System) tool in WP4 need to take this into account regarding user access regulations and data integrity.

2.1.12 FOR

1	**Regulation:**	GDPR
	How does this regulation affect EFPF:	The data are collected from the use cases to which FOR participate. Specific security measures and security risk assessment shall be part of the work developed in the use cases. Aspects such as identifiers and equipment, e.g., MAC addresses, shall be obfuscated. FOR complies with GDPR requirements.

2.1.13 HAW

1	**Regulation:**	GDPR
	How does this regulation affect EFPF:	HAW complies with GDPR requirements through continuous monitoring of the data collection and data usage procedures in the company, reviewing and updating Privacy Policy and website adjustments, and through trainings of employees to understand the importance of data protection and GDPR procedures, key concepts and GDPR articles.

2.1.14 IAI

1	**Regulation:**	EN 9100
	How does this regulation affect EFPF:	Assuring a certain level of quality/ reliability/ working standards contribute to EFPF. EN9100 certification can be seen as a requirement for products and services in EFPF.
2	**Regulation:**	Reach (Registration, Evaluation, Authorisation and Restriction of Chemicals) EU regulation No. 1907/2006
	How does this regulation affect EFPF:	This regulation has impact on whole supply chains as it is binding requirement for OEM and suppliers. EFPF should list only Reach conform products in catalogues etc.
3	**Regulation:**	Restriction of Hazardous Substances (RoHS) EU regulation No. 2011/65/EU
	How does this regulation affect EFPF:	This regulation has impact on the entire supply chain as a binding requirement for OEM and suppliers. EFPF should list RoHS conform products (e.g. no use of lead) in catalogues etc.
4	**Regulation:**	EASA Certification Specification and Acceptable Means of Compliance for Large

		Aeroplanes CS-25/EASA Part 21G, Section A, Subpart G “Production Organization Approval”/ EASA Part 21J, Section A, Subpart J “Design Organization Approval”/EASA Part 145 “Approved Maintenance Organization”
	How does this regulation affect EFPF:	EASA CS25 is a basic technical requirement for aerospace suppliers who develop, manufacture and maintain parts and equipment in the scope of mentioned chapter “Large Aeroplanes”. EASA 21G, 21J and Part 145 could be important for products and services offered from a company in EFPF catalogues etc. as the available certification might deemed mandatory from customers/OEM in the supply chain. This regulation might also be an important information for company profiles whether these certificates are available or not.
5	**Regulation:**	EU regulation 185/2010, laying down detailed measures for the implementation of the common basic standards on aviation security
	How does this regulation affect EFPF:	Since April 28 2013, companies who are wishing to have their cargo considered “secure” must be certified as “known consignors” by the respective national aviation security authority pursuant to chapter 6.4.1.1 of Commission Regulation (EU) 185/2010. The authority in Germany is the Luftfahrtbundesamt (LBA – Federal Aviation Office). Companies can only be certified if they have submitted an air cargo security program and have been audited by the relevant authority. As part of the air cargo security program, companies are required to describe their compliance with a wide range of security standards. These requirements also include that air cargo must be protected against interference by third parties. This can be achieved by ensuring that the facility itself is secure and that technical and staffing measures (security controls) are in place. For EFPF this might become relevant for tracking parcels/cargo using blockchain technology. Furthermore, in terms of the EFPF Risk Assessment Tool there might be an option to implement camera technology with applicable software which detects non-authorized personnel in secured areas.
6	**Regulation:**	EU regulation No. 428/2009, setting up a Community regime for the control of exports,

		transfer, brokering and transit of dual-use items
	How does this regulation affect EFPF:	Dual-use items are such items (also software and technology) that can be used both for civil and military purposes. As a worldwide operating company INNOVINT has to consider export control regulations in terms of listed dual-use items (e.g. https://www.zoll.de/EN/Businesses/Movement-of-goods/Export/Goods/Dual-use-items/dual-use-items_node.html). For EFPF this might become important as soon as order and delivery processes are available and performed via the platform, indicating that the applicable goods do not violate any regulation. This is also valid for any catalogue listed items.
7	**Regulation:**	GDPR
	How does this regulation affect EFPF:	Privacy and data protection, privacy by design need to be taken into account, incl. the right to be forgotten. [Already mentioned from other partners]
8	**Regulation:**	Conflict Minerals (On 1 January 2021 a new law will come into full force across the EU – the Conflict Minerals Regulation); In politically unstable areas, the minerals trade can be used to finance armed groups, fuel forced labour and other human rights abuses, and support corruption and money laundering. These so-called 'conflict minerals' such as tin, tungsten, tantalum and gold, also referred to as 3TG, can be used in everyday products such as mobile phones and cars or in jewellery. The regulation requires EU companies in the supply chain to ensure that these minerals and metals are imported from responsible and conflict-free sources only.
	How does this regulation affect EFPF:	For EFPF this might become important as soon as order and delivery processes are available and performed via the platform, as these should at least indicate that the applicable goods do not violate any regulation. This is also valid for any catalogue listed items. An option might be that any company that offers products through EFPF catalogues etc. must confirm during registering process that all the offered products are manufactured (in case mentioned minerals are part of them) with a supply chain that uses these minerals and metals from responsible and conflict-free sources only.

9	**Regulation:**	Regulations regarding social responsibility: • UN Global Compact • acc. to OECD • SA 8000 • UN Guiding Principles on Business and Human Rights • etc.
	How does this regulation affect EFPF:	All above documents are focussing on Human Rights, Working Conditions, Safety and Health, Environmental Protection, Business Ethics, Sustainable Supply Chain etc. For EFPF this will become important as soon as companies join the platform and become active users of platform's services. EFPF should ensure that no business is supported that violates any of the above-mentioned laws and rights.

2.1.15 ICE

1	**Regulation:**	GDPR
	How does this regulation affect EFPF:	Privacy and data protection, privacy by design need to be taken into account, incl. the right to be forgotten. This regulation affects ICE and EFPF during the project and in the post-project phase, since the project will be collecting data from the users of EFPF Portal and also the visitors of the EFPF website (maintained by ICE). This data will be used for analysis and contacting purposes.

2.1.16 LINKS

1	**Regulation:**	GDPR
	How does this regulation affect EFPF:	Privacy and data protection, privacy by design need to be taken into account, incl. the right to be forgotten The data analytics tools developed in T4.2 takes into account GDPR for the data management.

2.1.17 KLE

1	**Regulation:**	GDPR

	How does this regulation affect EFPF:	This regulation affects EFPF in terms of compliance with the legal framework for the protection of personal data. Data provided by KLE through the EFPF portal should be protected. The collected data will be processed exclusively for the purposes of the EFPF project.

2.1.18 NXW

1	**Regulation:**	GDPR
	How does this regulation affect EFPF:	Privacy and data protection issues affect most of the components provided to the Data Spine which store or otherwise handle any kind of private data. This regulation mostly concerns the post-project phase, when real world data is expected to be collected.

2.1.19 SIE

1	**Regulation:**	Machinery Directive
	How does this regulation affect EFPF:	The Machinery Directive covers the safety aspects of machinery, but also safety components, ropes and chains (e.g. robotics, self-configuring machines/ production lines and include cybersecurity aspects). The Machinery sector is an important part of the Engineering Industry. Machinery consists of an assembly of components, at least one of which moves, joined for a specific application. The drive system of machinery is powered by energy other than human or animal effort. This regulation affects EFPF in the post-project phase, when real data will be collected.
2	**Regulation:**	Radio Equipment Directive (RED)
	How does this regulation affect EFPF:	The RED establishes a regulatory framework for placing radio equipment on the market. It ensures a single market for radio equipment by setting essential requirements for safety and health, electromagnetic compatibility, and the efficient use of the radio spectrum. It also provides the basis for further regulation governing some additional aspects such

		as: technical features for the protection of privacy, personal data and against fraud, interoperability, access to emergency services, and compliance regarding the combination of radio equipment and software. This regulation has impact in the field of IoT (devices transmitting data between themselves) and affects EFPF in the post-project phase, when real data will be collected.

2.1.20 SRDC

1	**Regulation:**	GDPR
	How does this regulation affect EFPF:	Privacy and data protection, privacy by design need to be taken into account, incl. the right to be forgotten, right to be informed, right to restrict processing GDPR will affect EFPF in terms of the data collected by its various components, including the Accountancy Service, which is about tracking and tracing user behaviour and is developed within the scope of T3.3. At the moment, this service does not collect any personal data.

2.1.21 SRFG

1	**Regulation:**	The Directive on security of Network and Information Security (NIS Directive) [5]
	How does this regulation affect EFPF:	The goal of the NIS Directive is to enhance cybersecurity across the EU. From 09 May 2018, the NIS Directive incorporates national legislation through e.g. national capabilities "EU Member States must have certain national cybersecurity capabilities of the individual EU countries, e.g. they must have a national CSIRT, perform cyber exercises, etc." and a national supervision of critical sectors: "EU Member states have to supervise the cybersecurity of critical market operators in their country: Ex-ante supervision in critical sectors (energy, transport, water, health, digital infrastructure and finance sector), ex-post supervision for critical digital service providers (online market places, cloud and online search engines)".

		The NIS Directive strongly promotes risk management and incidents reporting between the Operators of Essential Services (OES) and Digital Service Providers (DSP) in the EU. The scope of DSPs, in the context of NIS Directive, is limited to cloud computing services, online marketplace and online search engines, which regards EFPF as a DSP, e.g. as an online marketplace allowing business entities to share their product catalogues and business services with other consumers or businesses. Hence, EFPF must comply with the NIS Directive and provide risk management and incidence reporting. Article 16(4) of the NIS Directive lists the following parameters to be shared in order to determine any cross-border impact of an incidence: (1) the number of users affected by the incident, (2) the duration of the incident, (3) the geographical spread regarding the area affected by the incident, (4) the effect of the disruption, and (5) the extent of the impact on economic and societal activities. Article 16(11) defines that DSPs that are micro or small enterprises (employing fewer than 50 persons and having an annual turnover not exceeding €10 million) are excluded from the scope of the security requirements and incident notification, which shows a potential impact of the NIS Directive on EFPF after the expected growth of the EFPF platform ecosystem. The mandatory notification requirements of the NIS Directive are described in "Guideline on Notifications of DSP Incidents (formats and procedures)" from July 2018 [6].
2	**Regulation:**	National Cybersecurity Strategies (NCSS) by ENISA [7]
	How does this regulation affect EFPF:	NCSS are the main documents of national states to set strategic principles, guidelines, and objectives to mitigate cybersecurity risks. NCSS are directly required by the NIS Directive and supported by ENISA's good practice guidelines, implementation guides, cyber insurance, etc.

		ENISA's "Good Practices in Innovation on Cybersecurity under the NCSS" from November 2019 [8], analysis cybersecurity- related innovation, industrialisation and collaboration, and market and policy in the EU Member States. This publication analyses innovation dimensions related to market and market regulations across the EU, which is of a remarkable importance in EFPF. For example, it lists Austria's research in the area of cybersecurity through national and EU security research programmes (e.g. National Research Development Programme KIRAS Austria) and Austrian Cyber Security Platform launched by the Federal Chancellery in 2015.
3	**Regulation:**	Incident notification for DSPs in the context of the NIS Directive [9]
	How does this regulation affect EFPF:	It provides guidelines on how incident notification provisions for DSP could be effectively implemented across the EU, e.g. how to identify types of incidents, parameters and thresholds.
4	**Regulation:**	Technical Guidelines for the implementation of minimum security measures for Digital Service Providers (DSP) [10]
	How does this regulation affect EFPF:	It provides a common baseline security objectives and measures for DSPs across the EU. In addition, it maps the security objectives against well-known industry standards, national framework and certification schemes, which is necessary to be addressed in EFPF too. For example, this document describes how the DSP establishes and maintains asset management procedures and configuration controls for key network and information systems, and many other aspects of information security.
5	**Regulation:**	Ethical Trading Initiative (ETI)/ business ethics www.ethicaltrade.org
	How does this regulation affect EFPF:	This is a candidate regulation to be revised, adapted or re-introduced as an enabler and a safeguard in the context of digital business ethics; see ETI's guide to support companies uphold the right to freedom of associations within their supply chain [11]. It should be extended to

		include digital avatars (AI-driven, human-like robots) and other covert systems).
6	**Regulation:**	Ethics Guidelines for Trustworthy AI, by Independent High-Level Expert Group (HLEG) on AI set by the EC [12]
	How does this regulation affect EFPF:	This Guidelines set out a framework for achieving trustworthy AI. It offers an assessment list - "Trustworthy AI Assessment List (Pilot Version)" which includes (1) human agency and oversight, (2) technical robustness and safety, (3) privacy and data governance, (4) transparency, (5) diversity, non-discrimination and fairness, (6) societal and environmental well-being, and (7) accountability. This framework will be tried out in EFPF before operationalizing the EFPF platform for Open Calls and public usage.
7	**Regulation:**	Ethically Aligned Design (EAD) [13]
	How does this regulation affect EFPF:	EAD is an initiative created by the IEEE Standards Association. It covers many topics of interest to EFPF development, including e.g. general (ethical) principles; how to embed values into autonomous intelligent systems; methods to guide ethical design; safety and beneficence of artificial general intelligence and artificial superintelligence; personal data and individual access control; reframing autonomous weapons systems; economics and humanitarian issues; law; affective computing; classical ethics in AI; policy; mixed-reality, and well-being.
8	**Regulation:**	The General Data Protection Regulation (GDPR) [1]
	How does this regulation affect EFPF:	GDPR became enforceable in May 2018 in the EU. EFPF services are designed in a way that adopts the core principles for personal data collecting, storing and processing mechanisms.

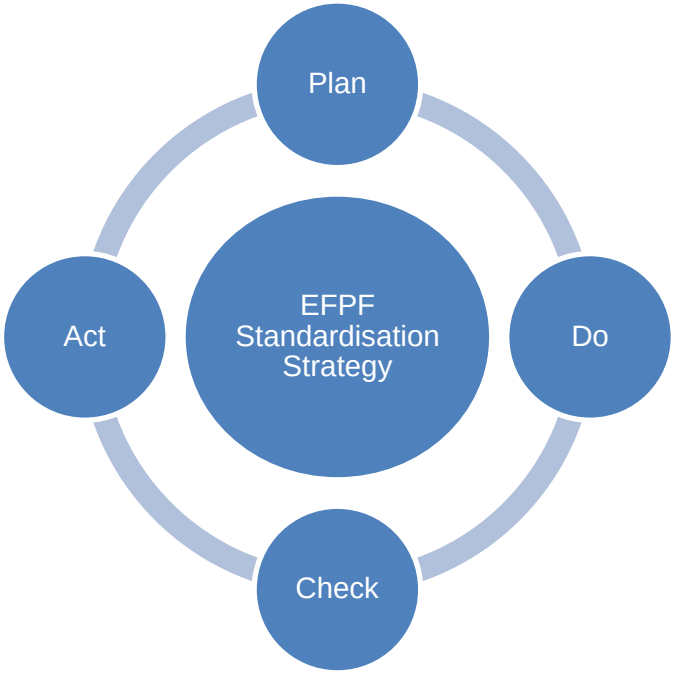
2.1.22 VLC

1	**Regulation:**	GDPR
	How does this regulation affect EFPF:	Privacy and data protection, privacy by design need to be taken into account, incl. the right to be forgotten This regulation affects EFPF during the project and in the post-project phase as

		the portal will need to collect and store information about users in order to facilitate access and further utilisation of the platform.

3 Standardisation Strategy

Based on the initial plan (D11.11) and the survey on standardisation (in Section 1), the standardisation strategy devised in the EFPF project is based on the P-D-C-A (Plan – Do – Check – Act) method. This involves pursuing the following activities:



- **Phase Plan:** Based on the surveys from Section 1 and Section 2, a decision on standards relevant for the project is carried out.
- **Phase Do:** The project partners ensure the compatibility and interoperability of their services and technical solutions with the relevant standards.

  Partners contribute towards the compliance, application, and development of standards in the areas of relevance to the EFPF as follows:

  - Common communications standards and reference architecture for connections between machines (M2M) and with sensors and actuators in a supply chain environment are seen as a priority in the project
  - Specific industrial needs, e.g. standards that support communications on broadband infrastructures and data formats to allow for the quick transfer of large volumes of data over networked industries
  - Improving interoperability and reducing overlap, redundancy, and fragmentation of the data
  - Project partners contribute to activities in Standards Development Organisations (SDOs) working on interoperability standards for security and for linking communication protocols in order to provide end-to-end security for complex manufacturing systems including the span of virtual actors (from devices and sensors to enterprise systems)
  - The project partners participate towards creating a hierarchical catalogue of technical and social measures for assuring privacy protection. That implies

processing of data which includes personal data within the definition of the GDPR.

- Partners participate towards the development of standards for ensuring long-term traceability of material to enable re-use and recycling.

- **Phase Check:** Partners shall periodically review and align their standardisation activities and provide a report for internal and external awareness.
- **Phase Act:** If the new subject areas and regulations relevant to the project are planned or identified by SDOs (e.g. CEN, CENELEC, ETSI, IEC, ISO, IEEE) the partners have to create a corresponding analysis of the target status and compare it with the current status. Furthermore, the questions of what can be optimized and where lay a further potential of standardization activities, must be clarified. If it is determined that the goal has not been reached, the cycle is run through again.

3.1 Strategic Areas of Participation

The analysis of the ongoing standardisation activities in the project and partners interests reveal the following key areas that require an active participation from a project's strategic point of view.

3.1.1 ISO/TC 184/SC 4 – Industrial data

- C2K will adopt and harmonise the standards in relation to the Factory Connector Architecture (T4.1) to support the building blocks of the EFPF platform
- FOR will monitor the progress on ISO 20534 to analyse its adoption or application for inter-enterprise data exchange in EFPF platform (e.g. as in T3.5)
- CNet will study the standardisation activities on Digital Twin standardisations and Product Data representations

3.1.2 ISO/TC 184/SC 5 – Interoperability, integration, and architectures for enterprise systems and automation applications

- NXW will monitor and adapt the activities of the ISO/TC, due to its implications on automation platforms such as NXW's Symphony platform

3.1.3 IEC/TC 65/SC 65E - Devices and integration in enterprise systems

- FOR has been studying the IEC 62264 and it various parts, to determine how the IEC 62264 can be used for the integration between control systems and the collaborative network layer. FOR's current understanding is that IEC 62264 standard is focused on intra-enterprise integration; therefore, to use it in the context of collaborative manufacturing network would require extending the standard to cover the inter-enterprise aspect
- FOR is no longer tracking the process of IEC 61499, which provides a generic model of concepts relevant in manufacturing operations management (MOM). FOR is addressing other standards that assist the interconnection of EFPF connectors and gateways as part of task T4.1. Specific efforts in this area concern the W3C "Web of Things" standards providing universal interconnection and covering legacy devices

- ASI will promote IEC PAS 63088 that provides a reference model for EFPF due to the fact that RAMI 4.0 is in the core of Industry 4.0 standardisation efforts
- CNet will monitor the above standardisation activities on device integration with IoT platforms. The analysis carried out will be used to inform the design of Data Spine (T3.2) and align the development of Data Spine with latest standards on IoT integration

3.1.4 ISO/IEC/JTC 1/SC 41 - Internet of Things and related technologies

- NXW will monitor the activities of ISO/IEC JTC 1/SC 41 on real-time IoT framework based on their implications on automation platforms and relevance to the factory connectivity and IoT relevant task (T4.1) in the EFPF project
- SRFG will monitor the ongoing development of Trustworthiness framework in the ISO/IEC NP 30149 - Internet of things (IoT). Cooperation with the ISO/IEC JTC 1/SC 41 will be investigated for knowledge exchange between the technical committee and EFPF task related to trust mechanisms (T5.3)
- CNet will monitor the above standardisation activities in the realm of IoT and inform the design and development of integration and interoperability mechanisms for IoT sensors and devices in the EFPF platform (T3.2, T4.4)

3.1.5 IEC/TC 65/SC 65E - Devices and integration in enterprise systems

- NXW is interested in the adoption of OPC UA standard for machine level communication, in the context of their commercial platform Symphony that will be linked with EFPF
- ICE has started to study OPC UA and in particular on how it can be used by the new Administration Shell standard. ICE workflow tool development (T4.6) will support OPC UA based communication for linking multiple shop-floor assets
- FOR is an OPC Foundation member and has been actively participated in VDMA-led efforts for OPC UA information model standardisation within the VDMA Robotics and Integrated Assembly Solutions Sector Groups. FOR will monitor ongoing activities and will support EFPF partners in the adoption/uptake/alignment of OPC UA within relevant development tasks (e.g. T3.2, T3.5, T4.1). OPC UA is the core Industry 4.0 communication protocol for machine connectivity, both with supervisory systems and other machines. Relevant domain specific standard extensions are developed in committees associated with the OPC Foundation before being submitted for formal standardisation. In T4.1, the Dynamic Factory Connector (developed by FOR) supports an OPC UA interface both with the local data sources and with the EFPF platform through OPC UA PubSub over AMQPs and MQTTs. FOR's goal is to support other EFPF Connectors and Gateways developers to provide an OPC UA interface
- CNET is an OPC Foundation member
- NXW is investigating models and ontologies from OPC UA. In particular IEC 62541-5:2015 OPC Unified Architecture – Part 5: Information Model at the border between building and factory concepts
- ICE has studied the support OPC UA in its WASP tool for enabling direct reading from factory PLCs and sensors. The intention is to use sensor data in conditional gateways for dynamic process execution flows

3.1.6 ISO/IEC JTC 1 – Information Technology

- AMQP, MQTT and JSON are essential standards for application integration and core context to the building blocks of the EFPF data spine and platform. The uptake, interoperability and/or alignment of these standards will be carried out in the tasks dealing with message exchange in EFPF e.g. (T3.2 - Data Spine)
- Considering the cross-platform data model, EFPF platform sees UBL v2.2 or UB v2.3 as a candidate. In the NIMBLE project, the UBL v2.1 version of the standard has been used which will be upgraded to UBL v2.2 or v2.3, in EFPF. In the scope of EFPF standardisation activities, SRDC will submit additional user requirements and/or user scenarios to UBL community to contribute to UBL 2.3
- CNet will monitor the activities related to MQTT (ISO/IEC 20922:2016) due to its importance in the development of Data Spine (T3.2) and CNet's IoT applications.
- ICE's WASP tool has been enabled to communicated with external process applications that use UBL. ICE will continue working towards a closed integration with UBL aiming at a closer interface with BPMN2.0 standard
- In the context of T4.1 and T3.2, FOR is working with MQTT and addressing interoperability issues towards other protocols, e.g., OPC-UA, CoAP. FOR is monitoring activities concerning MQTT (ISO/IEC 20922:2016) and its industrial counterpart, MQTT Sparkplug, in regards to the Dynamic Factory Connector and IIoT applications (T4.1)

3.1.7 ISO/IEC JTC 1/SC 7 – Software and systems engineering Object Management Group – Business Process Management Initiative

- ICE has adopted BPMN 2.0 as the modelling notation for workflows. ICE will continue monitoring the BPMN 2.0 standard. ICE's WASP is using BPMN for designing processes and monitoring their execution. Future developments of WASP include functionalities that generate code to connect applications. The WASP development team will search for a practical way to modify BPMN to accommodate this industrial requirement

3.1.8 ISO/TC 307 – Blockchain and distributed ledger technologies

- CNET will monitor these standardisation activities for application in the blockchain, distributed ledger and smart contracting efforts

3.1.9 ISO/IEC JTC 1/SC 27 – IT security techniques

- SRFG will monitor Information Security standards for the further design of security controls (T6.2) in EFPF. SRFG would also look how to contribute to any of cloud security standards, e.g. ISO/IEC 27017:2015, ISO/IEC NP 24392
- WASP will implement OpenID Connect built on top of OAuth 2.0 as a security standard

3.1.10 ISO/IEC JTC 1/SC 32 – Data management and interchange

- EFPF tasks on matchmaking (T4.5) and marketplace framework (T3.3) will analyse the use of this standard for the company registration or when exchanging business messages
- VLC along with other partners is actively investigating the use of these standards for data sharing between platforms. The approach for Business and Networking Intelligence services follows the matchmaking task which uses a combination of standard including the ones mentioned here and others such as eClass and UBL

3.1.11 IEEE – Institute of Electrical and Electronics Engineers

- ICE is interested in future developments of this standard to ensure standardisation alignments in EFPF
- CNet will monitor and promote the uptake of this standard on IoT architecture in the development of Data Spine (T3.2). Monitoring this standard will also benefit CNet commercial activities in the area of IoT devices
- FOR is monitoring the IEEE P2413, in particular, the standard references for SmartCities (P2413.1). FOR has interest in the future developments of this specific part, to ensure standardisation alignment

3.1.12 ISO/IEC JTC 1/SC 38 – Cloud Computing and Distributed Platforms

- The above standard provides a comprehensive vocabulary that is relevant to all types of organisations. The activities in EFPF project will focus on the use of this standard terminologies across project documents and dissemination channels.

3.1.13 IPC-CFX (IPC 2-17 – Connected Factory Initiative Subcommittee)

- The identification of the above standard provides an impetus to EFPF (T5.5) to align the relevant application development activities (through the SDK in T5.5) with the IPC-CFX standard. The associated open source “Software tools for Connected Factory Exchange SDK” (Version 1.0.5) will be relevant in this regard. CMS will investigate how to contribute towards the further enhancement/development of the IPC-CFX
- CMS is the leader of the Connected Factory SDK group (WG-DA-05) and is developing activities towards creating requirements and a common vision for a standard, innovative and reusable SDK to be adopted by the European projects, in the manufacturing area
- CMS will continue working towards the standardisation of the SDK and towards the alignment of its current SDK to the new vision and suite of tools

Those partners participating in the standardisation areas above are committed to report latest and important developments to the project and feed findings from the project back to standardisation. Such two-way interaction between EFPF and standardization communities contributes to an optimal alignment of the project activities and outcomes with standards (published and under development).

Special attention needs to be given to those standardisation projects, which support regulations. Especially New Legal Framework (NLF) directives/regulations of the European Union foresee a strong link with standards. These standards are elaborated based on a standardisation request from the European Commission and gain the status of harmonized European Standards (hEN). Such NLF regulations are for instance the Machinery Directive and the Radio Equipment Directive.

3.2 Participation in Strategic Groups

The key EFPF participation in strategic groups resulted in the creation of the **CEN-CLC-ETSI Coordination Group on Smart Manufacturing**, in 2019. The objectives of this Coordination Group are the following:

- To advise the CEN and CENELEC Technical Boards (BTs) and ETSI Board on the standardization needs in the Smart Manufacturing sector and initiate appropriate actions
- To advise the CEN and CENELEC BTs and ETSI Board on political issues concerning smart manufacturing
- To establish a synchronisation model for the various standardization activities among CEN, CENELEC, ETSI and SDOs
- To advise the CEN and CENELEC BTs and ETSI Board on ways and means to improve their visibility and recognition in the process of industry digitalization

Stakeholders participating in the Coordination Group are:

- European Commission DGs and the EFTA Secretariat
- Representatives of interested Technical Bodies in CEN, CENELEC and ETSI
- IEC, ISO
- National members of CEN, CENELEC and ETSI
- SDOs, consortia and alliances (of industrial partners)
- European associations representing interested stakeholders
- National initiatives
- Major European research projects, large scale pilots, test beds
- Open source communities
- Industry, including SME
- National initiatives, including relevant National Research & Innovation Centres
- Societal stakeholders

ASI is committed to participate in the Coordination Group acting as liaison officer for EFPF. This has the strategic advantage of increasing EFPF's visibility among stakeholders represented in the Coordination Group and receiving the first-hand feedback from the Coordination Group for the project partners.

3.3 Initiation of a CEN Workshop Agreement

The strategic areas of involvement in standardization, described in Section 3.2, include cybersecurity, IoT, AI, Big Data, etc. Taking a holistic approach on standardisation in EFPF requires creating a report like this, to help platform's users to maximise connectivity, interoperability and efficiency of their services and participation across the supply chain in the EFPF platform ecosystem.

Being part of the Digital Manufacturing Platforms for Connected Smart Factories and interacting with other projects in this cluster (including ZDMP and QU4LITY), resulted in the initiation of the **CEN Workshop for EFPF**, with the aim to create a standardization deliverable "**CEN Workshop Agreement (CWA)**[1]". The CWA will be a publicly available specification and a tool for the development of an interoperable EFPF platform and ecosystem. The CWA will cover the following issues:

- Data Spine
- Integration Flow Engine, incl. Protocol Connector
- Service Registry
- Message Bus
- API Security Gateway, incl. Gateway to EFPF platform, base platforms and external platforms, pilots and experiments
- EFPF Security Portal (EFS)
- Required metadata for EFPF platform
    - Metadata for management services, incl. requirements for the portal, for the marketplace and on governance and trust
    - Metadata for collaboration services, incl. requirements for matchmaking, on factory connectors and gateways, business and network intelligence, smart contracting, data analytics, workflow and business process, smart factory services as well as on secure data storage

The scope of the CWA needs to be further explored and approved by the EFPF partners. ASI as standardization partner in the project, will support other partners in the decision making.

[1] A CWA is a standardization deliverable, which may take various forms such as text file or computer code, developed and agreed by the participants in a temporary working group (CEN-CENELEC Workshop). It is designed to meet an immediate need and can be quickly developed and can be used as fast track to future standardization activities. The stakeholder involvement is limited itself to those directly interested in the subject. The development of a CWA is fast and flexible, on average between 10-12 months. For further information see https://boss.cen.eu/developingdeliverables/CWA/Pages/default.aspx

4 Strategy on Regulations

It is important for all project partners to know which regulations need to be followed both, during the design and development of the platform, as well as for its operation. The following regulations where identified by the partners[2]:

- The General Data Protection Regulation (GDPR)
- Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union
- COMMISSION REGULATION (EU) 2019/424 of 15 March 2019 laying down ecodesign requirements for servers and data storage products pursuant to Directive 2009/125/EC of the European Parliament and of the Council and amending Commission Regulation (EU) No 617/2013
- Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services
- DIRECTIVE 2006/42/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 May 2006 on machinery, and amending Directive 95/16/EC – Machinery directive
- DIRECTIVE 2014/53/EU - Radio Equipment Directive (RED)
- EU regulation 185/2010, laying down detailed measures for the implementation of the common basic standards on aviation security
- The Directive on security of Network and Information Security (NIS Directive) [5]
- National Cybersecurity Strategies (NCSS) by ENISA [7]
- Incident notification for DSPs in the context of the NIS Directive [9]
- Technical Guidelines for the implementation of minimum security measures for Digital Service Providers (DSP) [10]
- Ethical Trading Initiative (ETI)/ business ethics
- Ethics Guidelines for Trustworthy AI, by Independent High-Level Expert Group (HLEG) on AI set by the EC [12]
- Ethically Aligned Design (EAD) [13]
- EU regulation No. 428/2009, setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items
- EU regulation No. 1907/2006, Reach (Registration, Evaluation, Authorisation and Restriction of Chemicals)
- EU regulation No. 2011/65/EU, Restriction of Hazardous Substances (RoHS)
- Conflict Minerals (On 1 January 2021 a new law will come into full force across the EU – the Conflict Minerals Regulation)

[2] Survey responses related to standards, which are used for contractual purposes, were omitted.

- Royal Decree 8/2020 [2]
- Royal Decree 488/1997,of April 14th [3]
- Royal Decree 486/1997 of April 14th [4]
- Benelux-verdrag inzake de intellectuele eigendom (NL)
- BGBl. I Nr. 66/2002, Federal Law on the Granting of Privileges to Non-Governmental International Organisations (national Austrian law)
- EASA Certification Specifications and Acceptable Means of Compliance for Large Aeroplanes CS-25/EASA Part 21G, Section A, Subpart G “Production Organization Approval”/ EASA Part 21J, Section A, Subpart J “Design Organization Approval”/EASA Part 145 “Approved Maintenance Organization”
- Regulations regarding social responsibility, such as UN Global Compact, OECD-Guidelines, SA 8000, UN Guiding Principles on Business and Human Rights

Special attention needs to be given to those regulations with a link to standards. Especially New Legal Framework (NLF) directives/regulations of the European Union foresee a strong link with standards. These standards are elaborated based of a standardisation request from the European Commission and gain the status of harmonized European Standards (hEN). Such NLF regulations are for instance the Machinery Directive and the Radio Equipment Directives.

5 Summary

Standardisation is of a special importance in supporting the digital transformation of industrial domains. Standardisation is the powerful tool of the technological and economic infrastructure that greatly influences competitive abilities and the strategies of companies.

Therefore, it is important for all project partners to recognise the benefits of standardisation and to address findings that could improve the European and global framework of standards.

Digital transformation of industry is not happening in a regulation-free environment. Legal compliance is a must. This is valid not only in a physical world but for digitization of industry as well. Therefore, it is essential for all project partners to know which regulations need to be followed during the design and development of the platform as well as for its operation.

Based on the standardisation plan (D11.11) and extensive surveys, this deliverable of task T11.3 provides a detailed overview of the EFPF partners' participation in standardisation activities and on regulations that affect EFPF. The standardization strategy is divided in three parts:

- The involvement in standardization committees elaborating standards for strategic areas enables an optimum alignment between EFPF tools and related standards but needs to be regularly monitored and updated.
- The participation in strategic standardization groups enhances the visibility of EFPF among key stakeholders and facilitates the access to first-hand information being highly relevant for the project.
- The concept of a CEN Workshop Agreement as a standardization deliverable will support directly EFPF as a digital platform ecosystem, and will be further explored – together with related Digital Manufacturing Custer projects such as ZDMP and QU4LITY.

The subsequent work in T11.3 and the deliverable D11.9 (final report) will build on D11.11 and this deliverable, leading to a visible final impact of the EFPF project in the wider area of standardisation and to legal compliance with identified regulations.

Annex A: History

Document History	
Versions	V1.0: • Consortium approved and quality checked deliverable V0.4: • Feedback from internal review incorporated by ASI V0.3: • ASI final draft deliverable sent to partners for internal review V0.2: • Response from partners incorporated V0.1: • ASI draft deliverable circulated for partners input
Contributions	ASI: • Karl Grün • Andreas Feigl • Erwin Haubert • Martin Lorenz ICE: • Usman Wajid • Cesar Marin ASC: • Norman Wessel C2K • Simon Osborne FIT • Alexander Schneider NXW • Matteo Pardi SRFG • Violeta Damjanovic-Behrendt SRDC: • Yildiray Kabak FOR: • Georg Neugschwandtner, Nisrine Bnouhanna CNet: • Mathias Axling HAW: • Ingo Martens A-D: • Berend Koch IAI: • Lars Henschel CERTH: • Alexandros Nizamis

Annex B: References

[1] GDPR: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

[2] https://www.boe.es/diario_boe/txt.php?id=BOE-A-2020-3824

[3] https://www.boe.es/eli/es/rd/1997/04/14/488/con

[4] https://www.boe.es/eli/es/rd/1997/04/14/486/con

[5] The Directive on security of Network and Information Security (NIS Directive). Online: https://ec.europa.eu/digital-single-market/en/network-and-information-security-NIS-directive

[6] Guideline on Notifications of DSP Incidents (formats and procedures), 2018. Online: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=53675).

[7] ENISA, National Cybersecurity Strategies (NCSS) by ENISA; https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools

[8] ENISA, Good Practices in Innovation on Cybersecurity under the NCSS, 2019.

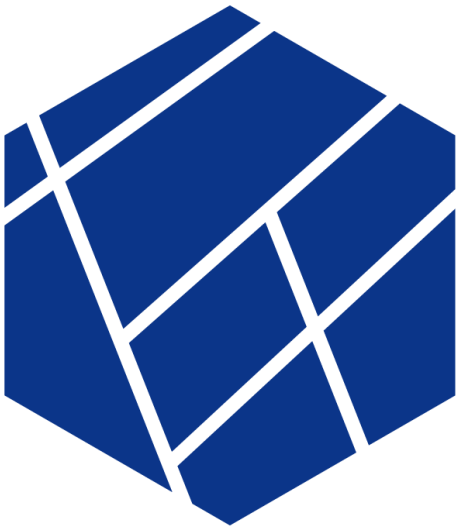
[9] ENISA, Incident notification for DSPs in the context of the NIS DirectivE, 2017. ONLINE: https://www.enisa.europa.eu/publications/incident-notification-for-dsps-in-the-context-of-the-nis-directive

[10] ENISA, Technical Guidelines for the implementation of minimum security measures for Digital Service Providers (DSP), 2017. Online: https://www.enisa.europa.eu/publications/minimum-security-measures-for-digital-service-providers

[11] New Guide Supports Companies in Upholding Freedom of Associations. Online: https://www.ethicaltrade.org/blog/new-guide-supports-companies-upholding-freedom-association (last accessed: 15-May-2020)

[12] Ethics Guidelines for Trustworthy AI, by Independent High-Level Expert Group (HLEG) on AI. Online: https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai

[13] Ethically Aligned Design (EAD). Online: https://ethicsinaction.ieee.org



European Factory Platform

www.efpf.org