EFPF: European Connected Factory Platform for Agile Manufacturing

European Factory Platform

WP11: Dissemination, Collaboration and Standardisation

D11.10: Data Management Plan - Vs: 1.0

Deliverable Lead and Editor: Florian Lipok, BRM

Contributing Partners: All

Date: 2019-06

Dissemination: Public

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

Short Abstract

The deliverable provides the plan for the management of data in the EFPF project. It describes the methods applied to making data findable, openly accessible, interoperable, re-useable and secure. Furthermore, the legal framework as well as risks and related measures associated to ethical aspects and the mechanisms for data protection as well as governance and trust are addressed.

Grant Agreement: 825075

Document Status

Deliverable Lead	Florian Lipok, BRM
Internal Reviewer 1	Usman Wajid, ICE
Internal Reviewer 2	Amparo Roca de Togores, AID
Type	Deliverable
Work Package	WP11: Dissemination, Collaboration and Standardisation
ID	D11.10: Data Management Plan
Due Date	2019-06
Delivery Date	2019-06
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 deliverable provides the plan for the management of data in the EFPF project. It describes the methods applied to making data findable, openly accessible, interoperable, re-useable and secure. Furthermore, the legal framework, risks and measures associated to ethical aspects, mechanisms for data protection as well as governance and trust are addressed.

In order to realise the **FAIR principle** along the EFPF project, this deliverable describes the following main mechanisms:

Document management: The project team set-up common procedures and practices that are used for handling documents within EFPF: the common WebDAV repository "OwnCloud", the usage of the Microsoft OneDrive cloud storage, internal templates with its document metadata that support them as well as the EFPF glossary.

Data management: The EFPF Marketplace framework provides the ground for interlinking multiple marketplaces from different platforms. Within this context, primarily the exchange of user data for single-sign-on, (meta-) data related to third-party offerings and accountancy services (for tracking the user journeys) are implemented. To access the different marketplaces, the EFPF Marketplace framework accesses each external marketplace through a central component called Data Spine.

Data accessibility: The Data Spine provides an open, platform-independent and secure communication and interoperability infrastructure with interfaces for the loosely coupled platforms, tools and services (e.g. third-party marketplaces). According to the current design, the security framework associated with Data Spine stores user data, i.e. username, password (and most probably the email address and/or phone number for password recovery).

Data interoperability: Considering overall interoperability, the Data Spine is the gluing mechanism in the context of connecting multiple tools, services and platforms to realise a federated platform and ecosystem. Based on the identification of common standards and abstractions, the APIs, connectors and interfaces that need to be implemented for the tools, systems and platforms federated through the Data Spine are defined and realised within the project. Besides the EFPF Data Spine being in the centre of the interoperability towards platforms, external interoperability is also fostered by means of open experiments of smart factory tools and solutions as well as the related data within the federated EFPF ecosystem. When it comes to **Data Security and Privacy**, the EFPF project carefully analyses the implications of, and compliance with, the relevant regulations on data management and consumption. This includes ensuring compliance with GDPR (General Data Protection Regulation) and NIS Direction (Directive on Security of Network and Information Systems). Besides the fact that the EFPF Consortium Agreement explicitly states that the project partners are GDPR compliant based on the requirements of the regulation, the following security controls are addressed within EFPF in the context of data integrity and quality:

- Data input validation
- Data and metadata protection
- Data protection at rest
- Data protection in shared resources
- Notification of data integrity violations
- Informed consent by design

In addition, the EFPF project defines and implements **Data Governance and Trust mechanisms**, covering information governance, a policy-based control of information to meet all legal, regulatory, risk and business demands as well as data governance, involving processes and controls to ensure that information at the data level is true, accurate, and unique (not redundant). It involves data cleansing to strip out corrupted, inaccurate, or extraneous data and de-duplication, to eliminate redundant occurrences of data.

Considering **Ethical Aspects**, EFPF does not introduce any critical issues or problems. However, several considerations typical to ICT and on-site industrial trials, where employees are also involved in the demonstration and evaluation stages, are considered. Here, the consortium is fully aware of these and has the necessary experience to address them seamlessly by being compliant with the relevant international and national law, regulations as well as directives, e.g.

- The Universal Declaration of Human Rights and the Convention 108 for the Protection of Individuals with Regard to Automatic Processing of Personal Data
- Directive 95/46/EC & Directive 2002/58/EC of the European parliament regarding issues with privacy and protection of personal data and the free movement of such data

Despite the far-reaching provisions implemented, **Potential Risks and Related Mitigation Activities** in the context of data management are continuously analysed by the EFPF team, including the following domains: Data security, storage and process of personal as well as confidentiality, privacy control, and transparency.

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 four base platforms from FoF-11-2016 cluster funded by the European Commission, early on. This will inform the design of the EFPF Data Spine and the associated toolsets to fully connect the existing 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 and Scope

The purpose of this deliverable "D11.10 Data Management Plan" is to document the framework for the management of all generated data in the project with a special focus on the FAIR data approach. Data management refers to all aspects of creating, housing, delivering, maintaining, archiving and preserving data; It is one of the essential areas of responsible conduct of research.

0.3 Target Audience

The deliverable at hand is of public nature, providing the EFPF project team the fundament for handling data generated and managed in the EFPF project.

0.4 Deliverable Context

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

- **Description of Action (DOA):** Provides 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
- **Project Handbook (D1.1)**: Provides the foundation for the practical work in the project throughout its duration and helps to ensure that the project partners follow the same well-defined procedures and practices also in terms of information sharing

0.5 Document Structure

This deliverable is broken down into the following sections:

- **Section 0 Introduction:** An introduction to this deliverable including a general overview of the project, an outline of the purpose, scope, context, status, and target audience of the deliverable at hand.
- **Section 1 Data Summary:** Provides an overview on data used and generated in the EFPF project as well as related parameters.
- **Section 2 FAIR Data:** Describes the ways applied to make data findable, openly accessible, interoperable and re-useable.
- **Section 3 Allocation of Resources:** Outlines the efforts towards the realisation of the FAIR data approach.
- **Section 4 Data Security:** Presents details about relevant regulations, data integrity and quality, data storage, data privacy, federated identity management and a blockchain approach.
- **Section 5 Ethical Aspects:** Provides information on relevant legal frameworks as well as potential data management risks and related mitigation measures.
- **Section 6 Other Issues:** Outlines project activities related to data protection, governance and trust.
- **Annexes:**
  - **Annex A**: Document History

0.6 Document Status

This document is listed in the Description of Action as “public”.

0.7 Document Dependencies

This document has no preceding documents or further iterations.

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 External Annexes and Supporting Documents

Annexes and Supporting Documents:

- None

0.10 Reading Notes

- None

1 Data Summary

The following table summarises the data generated and/or managed within the EFPF project as well as its fundamental parameters.

EFPF Context	Internal Documents
Description	Documents set-up and updated during the preparation and execution of the EFPF project. They include the Consortium Agreement (CA), Description of Action (DoA), document templates meeting minutes, working documents and the EFPF deliverables. The handling of EFPF related documents is done based on OwnCloud, a solution for document management and storage.
Purpose	Provision of all information to successfully perform the EFPF project tasks
Formats	.docx, .pptx, .xlsx, .pdf, .txt
Origins	EFPF partners
Size	Typically <20MB
Utility	Depending on the dissemination level the interested public, EFPF partners and/or the EC

EFPF Context	Marketplace
Description	The EFPF Marketplace framework provides the ground for interlinking of multiple marketplaces from different platforms. Within this context primarily the exchange of user data for single-sign-on, (meta) data related to third-party offerings (such as applications and services) and accountancy services (for tracking the user journeys) are implemented.
Purpose	Exchange and administration of all data to provide the user of the EFPF Marketplace a state-of-the-art service interaction and to enable user tracking and affiliate revenue models in the EFPF ecosystem
Formats	Database entries
Origins	EFPF partners
Size	Depending on registered users
Utility	EFPF partners including the EFF and third-party organisation, market-places and platforms that aim to make use of developed applications and services

EFPF Context	Data Spine
Description	The Data Spine provides an open, platform-independent and secure communication infrastructure with interfaces for the loosely coupled platforms, tools and services (e.g. third-party marketplaces). According to the current design, the security framework associated with the Data Spine may store user data for authorisation and authentication purposes. It is not envisioned to store any other data.
Purpose	Management of user data (username, password, email address and/or phone number for password recovery) to offer the authorisation, authentication and user-management services such as those associated with the user single-sign-on functionality
Formats	Database entries and Data Spine source code (open-source) and related specification documents
Origins	EFPF partners, user communities of marketplaces, platforms and generally the users in the EFPF ecosystem
Size	Depending on registered users
Utility	EFPF partners including the EFF, third-party marketplaces and platforms along with their user-communities

EFPF Context	Dissemination and Promotion
Description	Dissemination material generated and provided by the EFPF 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.
Purpose	Gain maximum awareness towards the EFPF project and its results as well as the EFPF ecosystem, including the EFPF Foundation
Formats	.docx, .pptx, .xlsx, .csv, .pdf Source code (open-source) and related specification documents
Origins	EFPF partners
Size	Typically <100MB
Utility	Interested public, EFPF partners, and/or the EC

2 FAIR Data

2.1 Making Data Findable, Including Provisions for Metadata

2.1.1 Document Management

This section introduces common procedures and practices that are used for handling various kinds of documents within EFPF common WebDAV repository “ownCloud”, the usage of the Microsoft OneDrive cloud storage, internal templates with its document metadata that supports them as well as the EFPF glossary.

OwnCloud

The EFPF document management approach aims at reducing the burden for project partners to synchronise, store, and locate documents. For this, the ownCloud solution for document management and storage is used, it is also referred to as synchronised file storage using the WebDAV protocol. It is similar in operation to the well-known Dropbox solution except that is self-hosted. This is convenient since it avoids issues associated with the geo-location of confidential material. OwnCloud is used within EFPF for the exchange and transfer of documents in progress and documents extensively used by all partners, e.g. the current version of the DOA or the EFPF templates.

The ownCloud software is installed on servers of the EFPF project partner ASC, who is located in Germany. **Access to ownCloud is personalised** via a dedicated username and password. If it is necessary to share the ownCloud folder with further colleagues, the ICE Project Office needs to be contacted.

A sample ownCloud **folder structure** is shown in the following figure. It **follows a hierarchical approach**, grouping horizontal documents like the Consortium Agreement, the Description of Action and templates as well as current and historical versions of work package related contents (subfolders such as “[Working]” and “[Final]” for the according documents).

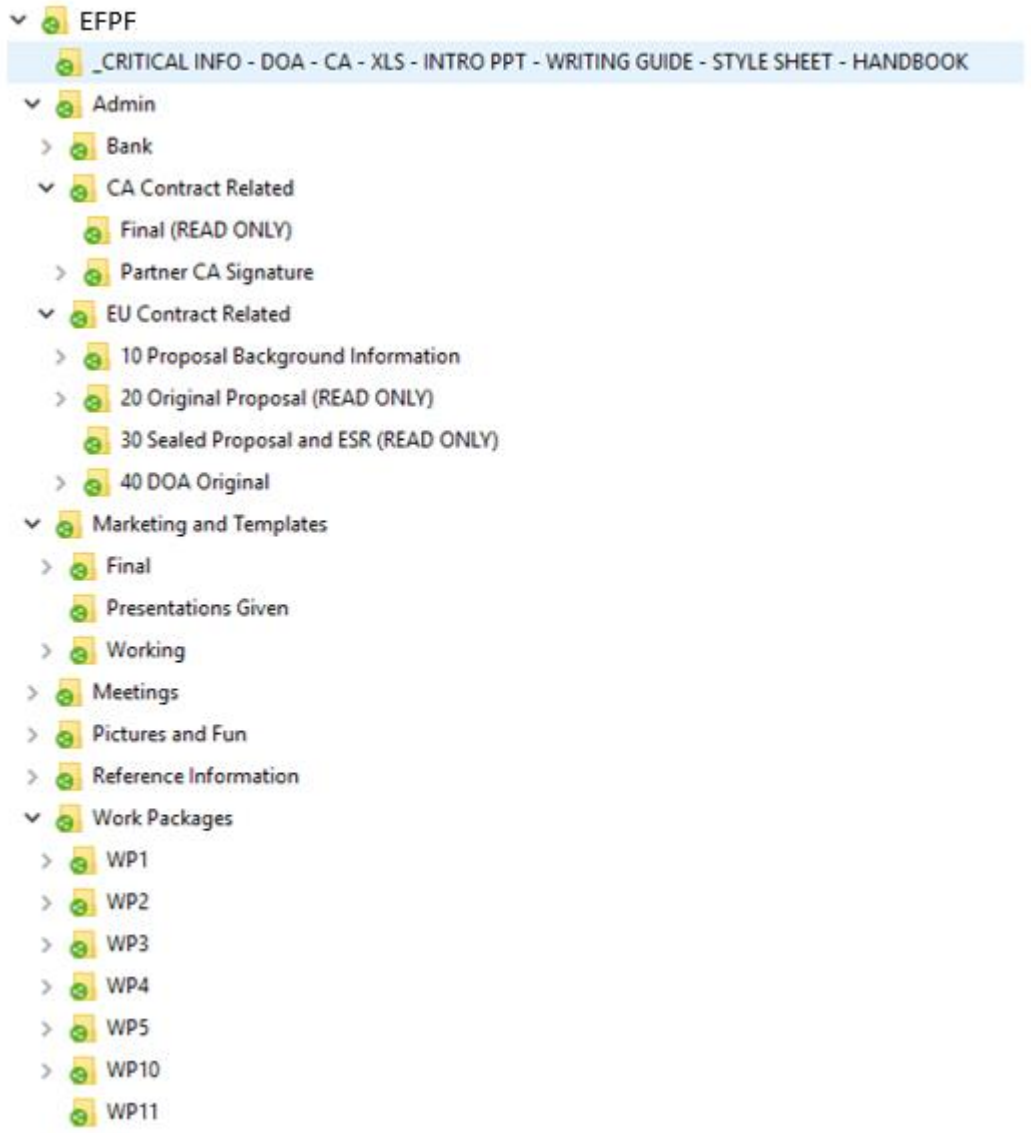


Figure 1: Sample ownCloud Folder Structure

The following list briefly describes the intended content of each key folder:

- CRITICAL: Critical documents for the project as mentioned above
- Admin: Source versions of previous and current EU Contract (including DOA) and CA
- Marketing and Templates: Logos, Graphics, Brochures, etc. and their sources
- Meetings: Resources and results primarily for physical meetings such as plenaries
- Reference Information: Important non-project document such as the Annotated Model Grant Agreement (AMGA)
- Pictures and Fun: Pictures from EFPF related events
- Work Packages: Contains subfolders for each work package and then within each subfolder, each task, and within each task there are subfolders for each deliverable.

In addition to the access management on a solution level mentioned above, ownCloud does not offer an access rights model for individual folders.

OneDrive

Although ownCloud provides distributed sharing and allows offline editing in common office tools in a latency-free way, it does not support multiparty editing and the dealing of conflicts.

Thus, a two-part solution is taken by EFPF, using Microsoft OneDrive cloud office solution based on Microsoft Excel spreadsheets for the recording of common financial or survey information. Each project partner is given a **coded link to this repository** and maintains the link securely such that only partners can access it.

Document Templates

In EFPF, Microsoft Word, Excel, and PowerPoint, as part of the Microsoft Office suite, are used for most documents. For Microsoft Word and PowerPoint, templates have been created and are available in ownCloud. To make sure that documents can be easily exchanged, all partners need to make use of at least Microsoft Office 2013.

For all formal deliverables, and informal ones that are submitted to the EC, the Microsoft Word template is applied (file: "**EFPF Document Template xxx**").

Within EFPF it is also mandatory to make use of the EFPF Microsoft PowerPoint template for external presentations regarding EFPF – i.e. at non EFPF events and reviews meetings. It is preferred to use this for internal meetings as well. If EFPF is only a minor part of a presentation, e.g. to show the different projects a partner is involved in, it is *not* mandatory to make use of the EFPF Microsoft PowerPoint template, but it should be considered (file: "**EFPF Presentation Template**").

2.1.2 Document Metadata

Deliverable Cover Page and Footer

The Word deliverable template cover page defines certain styles that are then referenced via field codes in other parts of the document – e.g. the status information on page 2 and in page footers of this deliverable. This allows information to be entered once and automatically referenced correctly throughout the document. This includes information for WP/Deliverable ID, name status, etc.

Deliverable Status Information

The following states are used for deliverables:

- **Draft**: The working versions of a deliverable, i.e. work in progress which is not ready for review yet
- **For EU Approval** (implying Consortium Approved): A deliverable which has been accepted by the project-internal reviewers and is therefore sent to the EC (for approval)
- **EU Approved:** A deliverable accepted by the EC and therefore ready for publication at the EFPF Website

Naming Conventions and Versioning

In general, file names need to be meaningful and unique, and they should include the word 'EFPF' at the start to distinguish from other projects. For deliverables, this means that the file name indicates the deliverable number, its version, and any further specific information:

- Example: "EU-ID D104 – EFPF-ID D1.3.1a – Periodic Report (M6) – Draft - v0.9.0 - ICE"
- General Format: "EU-ID D[N] – EFPF-ID D[N].[N][a] – [AAA][(Mx)] – [BBB] - v[M].[M].[M] [- CCC]"
- The spaces (" ") and hyphens ("-") are critical parts of the structural format and must be used
- EU-ID D[N] →"EU-ID D104" The [N] represents the sequential number of the deliverable and which is used by the EU. This number can be found in the Budget XLS

on “ownCloud/_CRITICAL…” During the drafting process, the editor should already include this ID

- EFPF-ID D[N].[N][a] → “EFPF-D1.3.1a” is the first (“a”) formal release of deliverable D1.3.1. Note that the [a] indicator is only used if there are multiple versions of the same deliverable. Typically, these [a] versions are related to living or period deliverables
- [AAA][Mx] → “Periodic Report (M6)” i.e. the name of the document and for iterative deliverables the Month of the deliverable
- [BBB] →
  - “Draft” - Labelled draft until the document is ready for reviewer 1
  - “Reviewer1[a]”: The first (“a”) version ready for the internal Reviewer1 of the deliverable
  - “Reviewer 2[a]”*:* The first (“a”) version ready for the internal Reviewer2 of the deliverable
  - “For EU Approval”: The version of the document, which is submitted to the EC. For this (and subsequent versions) the version number is deleted
  - “Accepted”*:* The version of the deliverable that has been accepted by the EC. It is published at the project Website if the deliverable is marked as public

- v[M].[M].[M] → “v0.9.0” is the 9th major draft version 0.9.0 of the deliverable. It is better to number below “1.0” so that the final output of the consortium can be identified as “1.0”
- [- CCC] → “- ICE” indicates a branch of the deliverable typically signified by a partner (e.g. ICE) or an individual’s acronym (UW). Branches should only be temporal documents, e.g. to decrease the risk of version conflicts as different partners may work on various parts of a document in parallel

If generating a PDF (for example for the definitive version to the EC), e.g. from a Word document it should have the same filename as the original document except for the file extension (e.g. “pdf”).

Microsoft Office Metadata

Microsoft Office allows metadata properties for each document to be entered. In EFPF, the fields “Author” and “Title” are used. Usually, the author information is filled in automatically, provided the author (deliverable lead) stated the full name in the Word personalisation properties. The title needs to be filled in manually and should be the same as on the first page of a document.

Deliverable Confidentiality Information (Dissemination Levels)

There are two different dissemination levels for EFPF project deliverables: **Public (PU)** deliverables, which are potentially available to everybody and **Confidential (CO)** deliverables, which are available only for the members of the EFPF consortium. The dissemination levels of all EFPF deliverables have been defined within Table 3.2c of the EFPF DOA.

Information regarding the dissemination levels must be marked in each deliverable as defined in the EFPF template. Furthermore, a brief description of the dissemination level and the logic for it needs to be given in section 0.6 (Document Status) of each deliverable.

2.1.3 Data Management

EFPF Marketplace

The extensible EFPF Marketplace framework offers the interlinking of multiple marketplaces from different platforms (i.e. NIMBLE, COMPOSITION, DIGICOR and vf-OS). The framework will provide components, which can easily be integrated in each platform to enable the access to external marketplaces. Furthermore, in order to enable an integrated affiliate model for supporting sustainable EFPF business models, an Accountancy Service (AS) is intended to gather tracking data from user journeys; The figure below provides a representative example:

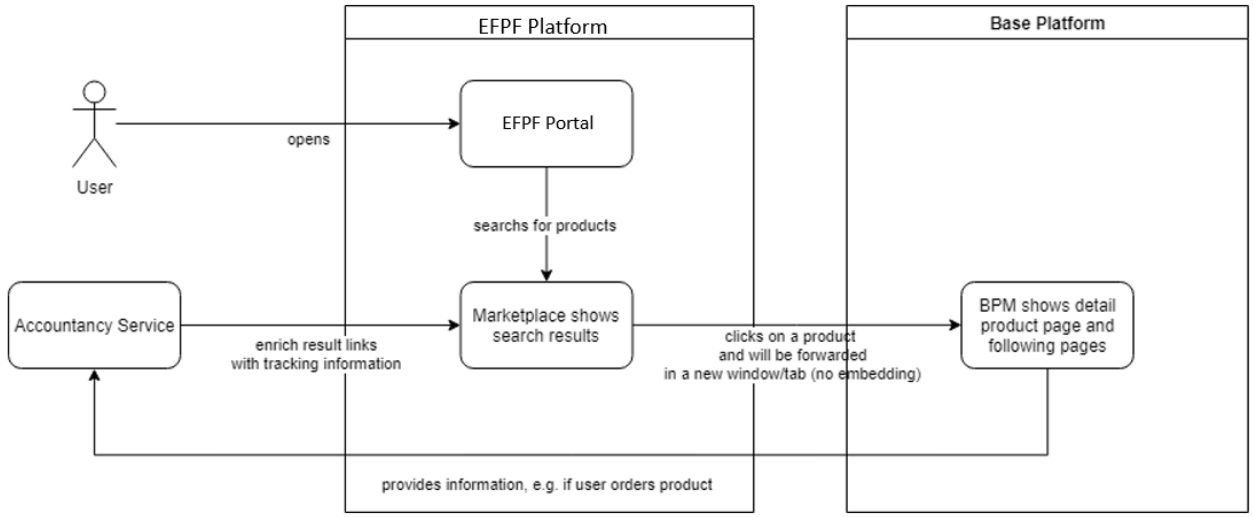


Figure 2: User journey example in the EFPF Marketplace

Rather than creating a centralised marketplace from scratch, the marketplace framework in EFPF interlinks existing marketplaces, enabling users to access offered tools and services through a unified interface, which will be embedded in the EFPF Portal and other platform's marketplaces.

Standards and open / reusable metadata

To access the different marketplaces, the EFPF Marketplace framework will access each external marketplace through the central component Data Spine. As each external marketplace provides different data structures, the Data Spine will provide a mechanism to implement the necessary metadata as well as the conversion logic between data models of different marketplaces. As a central aim in this context, the marketplace framework needs to handle minimum complexity in dealing with the offerings of multiple marketplaces as possible.

2.2 Making Data Openly Accessible

2.2.1 EFPF Data Spine

The realisation of the EFPF Data Spine is envisioned to be based on an **open-source technology**.

According to the current design, the security framework associated with the Data Spine will store user data, i.e. username, password (and most probably the email address for password recovery). It is not envisioned to store any other transactional data therefore the Data Spine does not provide any components for data storage and data management. Note: The EFPF Platform could provide components that allow data storage and management,

however, the utilisation of these components (e.g. for analysis or decision support) will be solely on the discretion of the EFPF users.

The Data Spine provides an open, platform-independent and secure communication and data exchange infrastructure with interfaces for the loosely coupled platforms, tools and services. This enables, for example, the analysis and fusion of real-time data to securely capture multi-tier supply chain intelligence. Clustering and propagation of business and supply chain intelligence will also be possible through the Data Spine. It will improve the competitiveness of the networked partner companies and increase the possibility for collaborations between organisations from different domains; allowing companies to share best practices and address dynamic market needs. The high-level architecture of the Data Spine, reflecting the approach described, is schematically shown in the following figure.

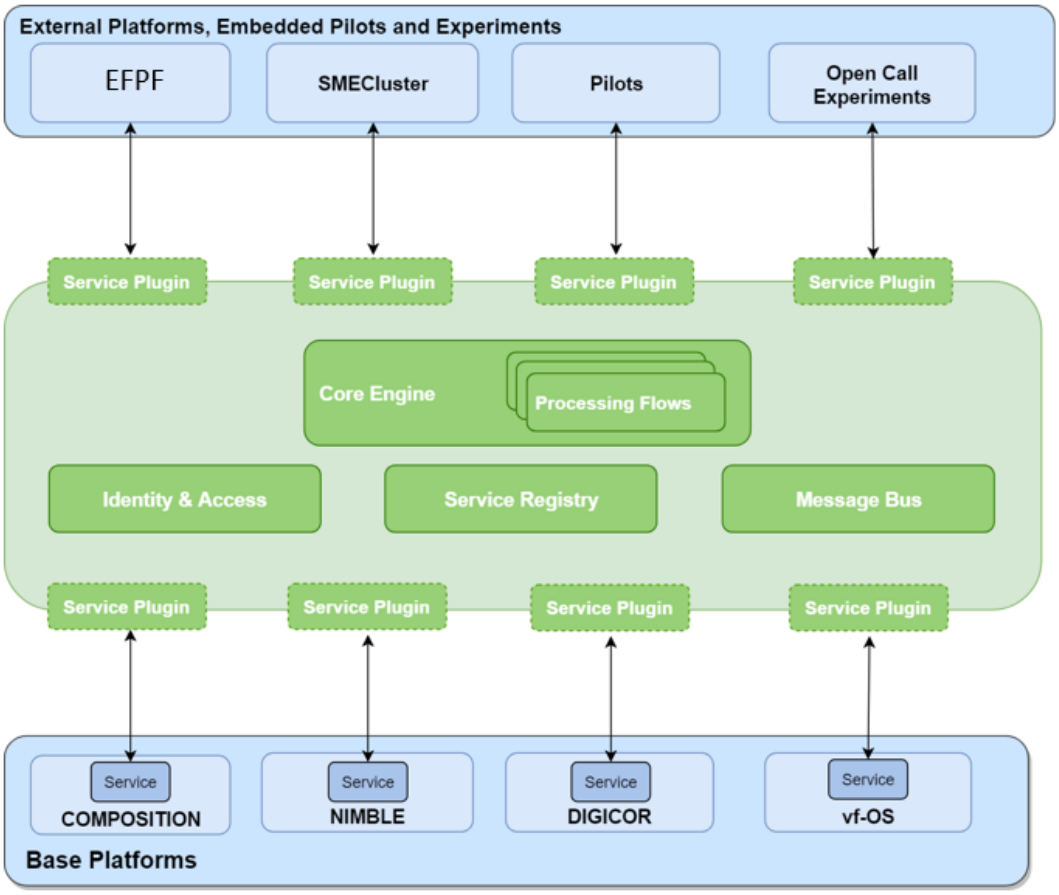


Figure 3: EFPF Data Spine Architecture

To give this ecosystem a maximum of flexibility, the tools and services interlinked within the EFPF platform are offered as far as possible as open-source resources under an Apache Licence (Version 2.0). This is already the IPR and licencing basis preferred in the four base platforms in EFPF. The Apache Licence only requires preservation of the copyright notice (attribution) but is otherwise permissive as it allows further use of the tools for any purpose, to distribute them, to modify them, and to distribute modified versions of the tools, under the terms of the license, without concern for royalties. The open-source nature of the EFPF tools also supports the strategic goal of co-creation of smart factory technologies. The adoption of permissive open-source licensing allows users to utilise the EFPF tools as standalone or combined/integrated functionalities. In addition, the EFPF platform provides open interfaces to the interoperable Data Spine, allowing the interconnectivity of EFPF platform with external

platforms, tools and services. Moreover, a platform level SDK is developed – building upon the SDK from (EU H2020) vf-OS to enable the development, customisation and integration of smart factory applications. The SDK (in Task 5.5 of EFPF work program) provides a Studio environment with intuitive interfaces, integrated libraries, execution environment and connectors to industrial systems and data sources to enable prototyping, application development and testing.

2.2.2 Software Versioning and Revision Control System

An EFPF instance of the open-source tool GitLab[1] 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. As GitLab provides many optional modules covering all DevOps activities, during the project runtime it will be decided if additional functionality will be added to the EFPF GitLab instance.

The source code of the open-source components (e.g. Data Spine) will be accessible in the project GitLab repository. Eventually, the open-source components to be developed during the EFPF project will be hosted in a publicly accessible software/code repository.

2.2.3 Dissemination of Results

What concerns the dissemination of project results, the EFPF partners are fully aware about the **open access policy** that applies to scientific publications as stated in the Article 29.2 of the H2020 Grant Agreement Open Access to Scientific Publications. In this sense, all peer review publications arising from EFPF, will be made freely and openly available via an online repository and the project website. The actions which will be taken by the project are:

- All presentations, contributions and publications even partially funded by the project will include the project logo, as well as the meta-data prescribed by the EC i.e. the acknowledgement of the grant agreement number, the term EU Horizon 2020, the name of the project, publication date and a persistent identifier
- The publications funded by the project will be uploaded to some social network such as ResearchGate as well as open-access repository such as OpenAire (https://openaire.eu) and Zenodo (https://zenodo.org), and no later than 6 months after its original date of publication
- Software not covered by IPR will be open source licensed and openly distributed (e.g. via Source Forge or GitHub) community
- The open access to research data article (GA Article 29.3) will also be of application to EFPF. This will allow the consortium to:
    - Deposit all the data generated in the project (specially data used in scientific publications) not affected by IPR or data privacy issues in an open repository such as FIWARE-LAB or the relevant open data initiatives of the partners involved in the proposal
    - Provide information available at the repository about tools and instruments at the disposal of the beneficiaries and necessary for validating the EFPF results

Moreover, appropriate presentation materials will be published at the project web site under a Creative Commons license.

[1] https://about.gitlab.com/

Some of the important industrial fairs in Europe are already being used (e.g. participation in AIX Expo, Paris Airshow and the IDSA Summit) to present the project results to a broad public. Partners will provide appropriate data and information to contribute towards project dissemination activities, which will be made visible through the project website and social media channels.

2.3 Making Data Interoperable

2.3.1 Overall Interoperability

The rapid growth of smart manufacturing enterprises and digital manufacturing platforms around Europe raises challenges of interoperability and questions regarding the suitability of existing platforms to support agile collaborations needed for lot-size-one production, particularly in cross-sectorial scenarios. What concerns industrial data acquisition and processing, advancements in CPS and IoT technologies have resulted in the proliferation of new communication mechanisms and protocols that add to the complexity of handling real time data exchange and analysis. The use of proprietary technology for data transfer and the lack of adherence to standard protocols can hinder the realisation and smooth operations of connected factories.

In its very centre, the **EFPF project realises a federated smart factory ecosystem** by initially interlinking four smart factory platforms, from the FoF-11-2016 cluster, through an open and interoperable Data Spine (see also Chapter 2.2.1). The federation of the four base platforms is complemented by industrial platforms, collaboration tools and smart factory systems, specifically selected to support connected factories in lot-size-one manufacturing.

The figure below schematically shows the information/data flow achieved by the interoperation of available and emerging smart factory tools and services. Starting at the bottom layers, there are groups of manufacturing firms registered with the four base platforms or – as would be expected from an open ecosystem – firms associated with another, similarly targeted platform. Each of the four base platforms offer communication with external entities via open APIs that are not homogenized yet. Furthermore, as the case of further external platforms illustrates, there will not be a standardised cross-platform interoperation layer for some time to come. This brings us to the first important technical innovation of EFPF, the Data Spine:

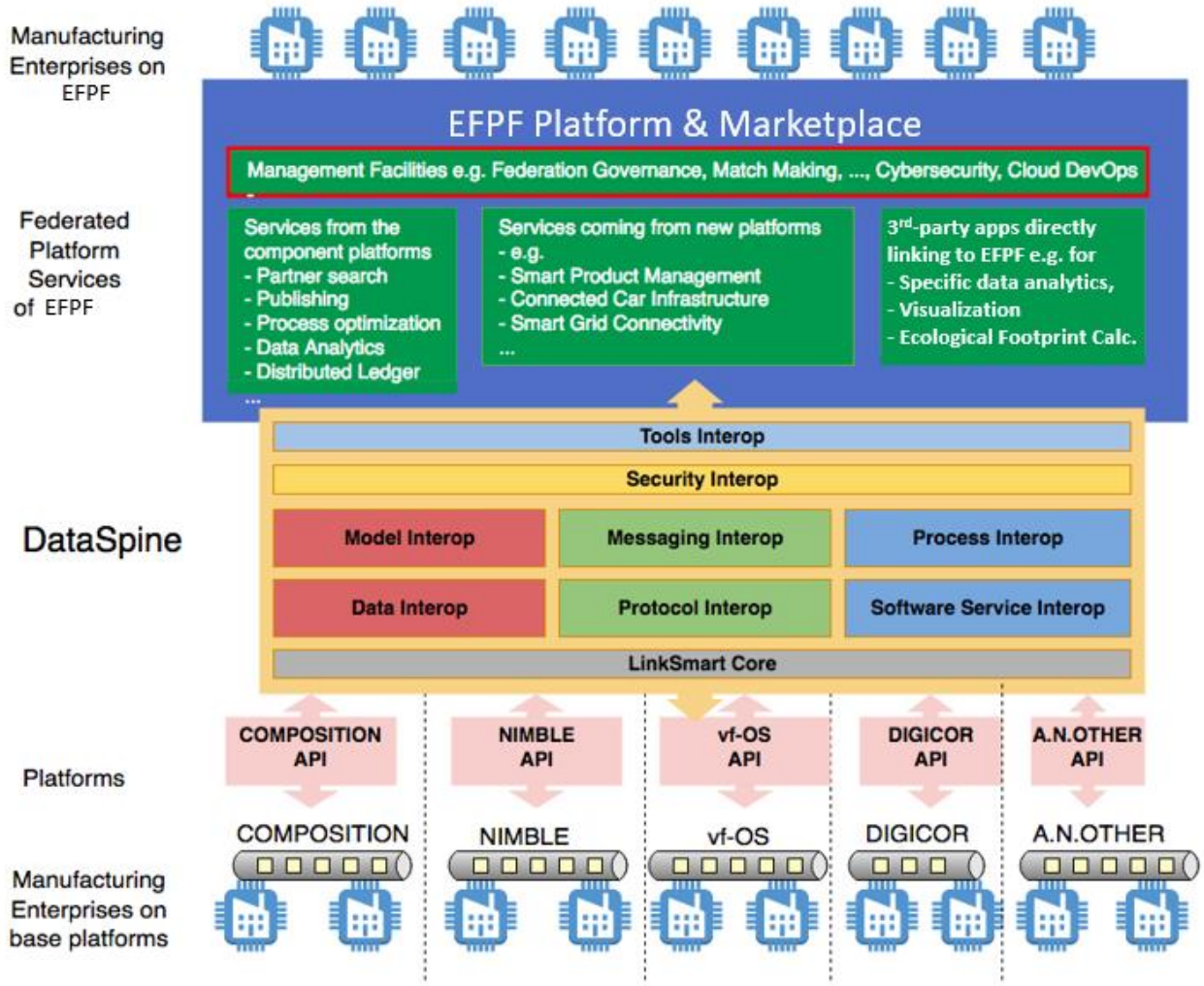


Figure 4: Technical Concept of EFPF

The Data Spine interlinks the APIs of the participating platforms so that each platform's functionality is visible and accessible at the level of EFPF. Overarching this, interoperable security features will give EFPF a layer of tools that can be used transparently at the platform and marketplace. The functionality of the EFPF Platform and Marketplace is thus composed of:

- Selected services offered by each of the original component platforms present in EFPF
- Services offered by any further platform that is willing to expose its API for alignment via the Data Spine
- Third party apps that are offered directly via EFPF either as free or paid services
- Dedicated management facilities to manage the governance, security and cloud deployment, etc.

For the ecosystem of EFPF, many engagement options arise from the federated nature of the system: Manufacturers may

- Connect directly to the EFPF platform
- Develop new tools and services using the EFPF SDK
- Use the marketplace to transparently use underlying services that may come from any of the participating platforms, with internal cross-billing managed by EFPF, in the case of commercial offerings

2.3.2 Platform Interoperability

The interoperable Data Spine is the gluing mechanism that connects multiple tools, services and platforms to realise an integrated platform. Based on the identification of common standards and abstractions, the APIs, connectors and interfaces that need to be implemented for the tools, systems and platforms federated through the Data Spine are defined and realised within the project. The implementation of the EFPF Data Spine through open-source technologies will interlink and establish interoperability between - initially the existing deployments of four base platforms (COMPOSITION, DIGICOR, NIMBLE and vf-OS) along with their respective tools and services as schematically shown in the following figure.

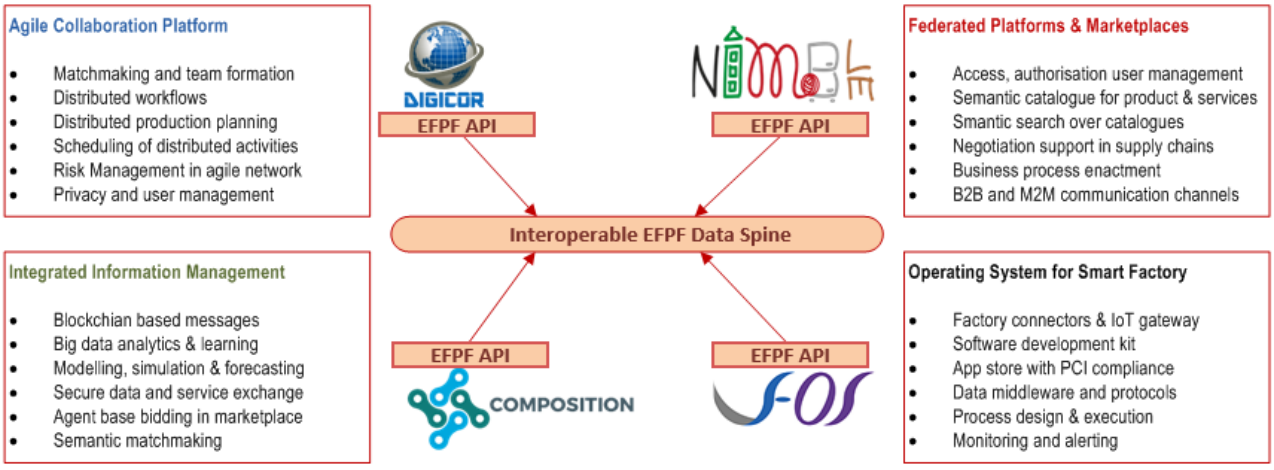


Figure 5: Federation of the 4 base platforms

The interconnectivity of the four base platforms will be followed by the integration of other platforms (such as ValueChain's iQluster, Siemens's Mind Works, Fortiss's Future Factory, C2K's Industreweb) and standalone tools brought forward by the EFPF partners. Here, the Data Spine will enable the integration of third-party platforms through a modular plugin system. Data model conversions between two or more platforms will have to be handled by so called "Processing Flows" that have to be implemented in order to make the data interoperable between the platforms. The related generic flow of data is schematically shown below:

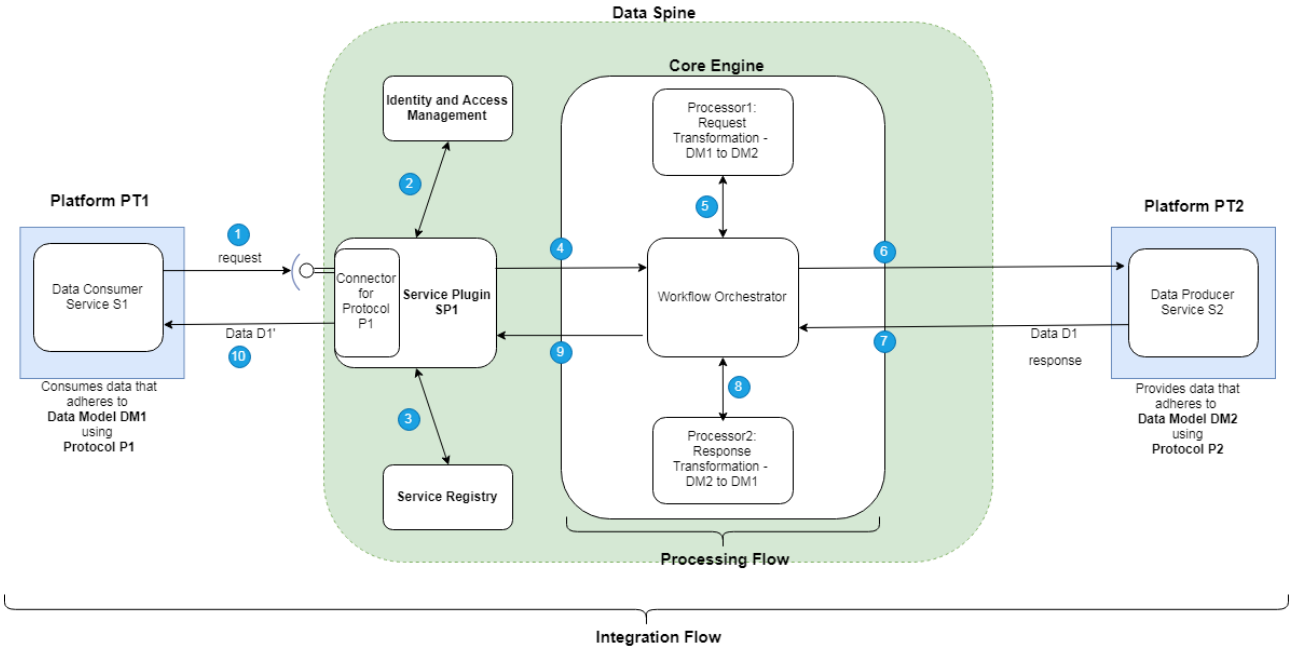


Figure 6: Generic data flow between EFPF-connected platforms

2.3.3 External Interoperability

The basic building blocks of the EFPF ecosystem are the individual tools, systems and platforms that are provided by different partners (and external entities) to the EFPF project. These tools, systems and platforms are interlinked through the Data Spine. In this respect, the tools, systems and platforms need to be able to communicate through the Data Spine technology, which means relevant interfaces and APIs to handle heterogeneous data will be defined during the EFPF project.

What concerns the interoperability of smart factory tools and solutions are the open experiments performed (through funded call) with the focus on the enhancement of the EFPF platform e.g. through the integration of innovative solutions in the federation. The open experimentation in EFPF will include:

- Experiments that integrate a 3rd party application in the EFPF platform, providing a validation scenario to demonstrate the seamless access and utilisation of the 3rd party system/application by EFPF services and users
- Experiments that focus on the integration of 3rd party platforms with EFPF through agreements on security framework (e.g. single-sign-on, user authorisation, rights management etc) with the emphasis to provide EFPF users with wider access to Industry4.0 and digital manufacturing solutions

2.3.4 Message Interoperability

In the context of EFPF Data Spine, data model interoperability corresponds to the ability to share information among partner messages and processes, as well as to trigger appropriate actions based on the events received from existing EFPF platforms. Considering the interoperability guidelines designed and developed in Task 3.2, the data model interoperability task aligns the data models of the federated platforms to support meaningful message exchange and viable business processes that spread across two or more of the existing EFPF platforms. The task utilises the proven methods and open-source tools for

data-model alignment to establish synergies and resolve overlaps and conflicts between different data models.

2.3.5 Data Analytics

EFPF enhances the data handling, analytics and interoperability modules from the four base platforms to (a) use/integrate them within the EFPF platform in a way to make them accessible to wider use-base in cross-platform scenarios, and (b) exposes them as analytic services that can be used in the pilots/ experiments in on-demand basis. The TRL of the existing analytic toolset (such as COMPOSITION's Deep Learning toolkit and vf-OS's Data Analytic services) is enhanced with the aim of capturing in-factory implicit data knowledge and providing the analytics that can help optimise the manufacturing processes. By deploying the analytic services as untrained plug-and-play applications, the EFPF platform will provide the means to analyse heterogeneous datasets and propagate meaningful information to dashboards and HMIs. The handling of the data by the analytic services will be the responsibility of the service providers – as typical in a federated ecosystem. The EFPF project will provide secure data storage service, if needed by the analytic services, to temporarily store the raw or analysed data from processes, shop-floor and manufacturing systems – see Section 4.3. However, no handling or analytics of sensitive data (e.g. personal details or data of high business value) is envisioned in the project.

2.4 Increase Data Re-Use

In the EFPF project, the sharing and re-use of 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 EFPF project supports the exchange, sharing and re-use of non-personalised data through the Data Spine and other EFPF solution with the fair use policy that the data is used with consent of the owner. The data used for the validation of EFPF tools will be made available for use in further experimentation (e.g. open-calls) though an open-access repository.

It is important to note that the EFPF project does not include any purely technological solutions to prevent the mis-use of data during or after the project lifetime. However, it supports these important aspects by putting in place the necessary authentication and authorisation checks that govern the access and (to certain extent) the utilisation of data stored in the EFPF platform. 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.

3 Allocation of Resources

The management of data in the EFPF project is carried out through the provisioning of relevant tools and systems, as described in Section 2.1.1. These systems (such as OwnCloud) provide the required level of fairness towards data sharing, security and privacy. During the EFPF project, the data management systems (described in Section 2.1.1) are provided by the project partners as part of their commitment towards the project.

The management of the data in the EFPF project is a collective activity of all partners, where the project manager takes the lead role of establishing the procedures and monitoring the utilisation of available infrastructure. The underlying infrastructure is maintained by the respective owners e.g. ASC is the owner of the OwnCloud document management system and therefore responsible for ensuring the continuous provisioning and quality of service of OwnCloud system. Similarly, the ownership of the other infrastructure e.g. Data Spine, Marketplace etc. will be defined during the course of project.

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. This data will be limited to the purpose of the research and prototyping activities conducted within the scope of this project, in accordance with the data minimisation principle. If processing activities of the personal data is needed, an explicit confirmation will be put in place to make explicit that the beneficiary has lawful basis for the data processing and that the appropriate technical and organisational measures are in place to safeguard the rights of the data subjects.

4 Data Security

In Task 5.3, the EFPF team defines and implements data governance mechanisms, covering the following aspects (for more information see Section 6.2):

- Information governance, a policy-based control of information to meet all legal, regulatory, risk, and business demands
- Data governance, involving processes and controls to ensure that information at the data level is true, accurate, and unique (not redundant). It involves data cleansing to strip out corrupted, inaccurate, or extraneous data and de-duplication, to eliminate redundant occurrences of data

For the security analytics in Task 6.2, some of the following open datasets will be considered:

- https://github.com/defcom17/NSL_KDD
- http://www.shubhamsaini.com/datasets.html
- https://web.archive.org/web/20150205070216/http://nsl.cs.unb.ca/NSL-KDD/

4.1 Regulation

The project carefully analyses the implications of, and compliance with, the relevant regulations on data management and consumption. This includes ensuring compliance with GDPR (General Data Protection Regulation)[2] and NIS Direction (Directive on Security of Network and Information Systems)[3]. The tasks responsible for data storage (T4.3) and security framework (#T6.2) are the core activities concerned with the management of data and ensuring the compliance with relevant data security and privacy regulations. Furthermore, the EFPF Consortium Agreement explicitly states that the project partners are GDPR compliant.

4.2 Data Integrity and Quality

Based on GDPR requirements, the following security controls are addressed within EFPF in the context of data integrity and quality.

- **Data input validation**: Controls over various factors like predictable behaviour, manual override, timing, etc. corresponding to the Data Quality Principle and the GDPR requirement for verifying sensitive data for its accuracy, completeness and for being up-to-date
- **Data and metadata protection**: Protection against unauthorised access and manipulation, automated restricted access and cryptographic protection for supporting subject's requests to access personal data and deletion of personal data and/or personal data modification
- **Data protection at rest**: Cryptographic protection and off-line storage (GDPR requirement for deletion and/or modification of personal data by the data subject)
- **Data protection in shared resources**: Cryptographic protection (GDPR requirement for deletion of personal data and/or personal data modification by the data subject)
- **Notification of data integrity violations**: Monitoring services for detecting, reporting and investigating personal data breaches as well as for reviewing existing privacy notices and keeping them up-to-date

[2] https://www.eugdpr.org/
[3] https://www.itgovernance.eu/nis-directive

- **Informed consent by design**: User must have an informed consent on the data usage, which prevents the use of data in a way that is not according to the user wish (GDPR requirement for implementing privacy procedures for seeking, recording, and managing user's consent)

4.3 Data Storage

Data gathered from shop-floors (Task 4.1) and analysed data (Task 4.2) is stored in a secure data-store that will be made available as docker containers, allowing users to deploy the container on the cloud or deploy on premise. Access to the data storage is secured such that only authenticated (using the single-sign on credentials) and authorised persons within the federation are granted access. These data protection mechanisms ensure fine-grained access control based upon the User Managed Access (UMA) standard, where the data owners can themselves control who can use the data (even when this is stored in the cloud). Privacy enforcing mechanisms are utilised to ensure that stored personal data (if any) complies with privacy regulations (in particular, GDPR), e.g., access to any personal data in the store must follow informed consent. The data storage may also store and disclose personal data in pseudonymised data sets – the data store provides support to developers to convert data sets to a pseudonymised format (where personal data is involved). Moreover, tools are also created to evaluate the extent sensitive personal data is at risk of disclosure using the chosen form of pseudonymisation and it is ensured that cross federation security and privacy is achieved in a holistic end-to-end manner.

4.4 Data Privacy

The EFPF project pays specific emphasis on data privacy by putting in place procedures where parties attempting to access information must be authenticated (confirming their identity) and authorised (confirming they have permission from the data owner for access). During the project data confidentiality is maintained, whereby access to data is revealed only to authorised parties.

Within Task 4.3 (Secure Data Storage Solution), data owners can configure access to stored data using the User Managed Access (UMA) protocol standard, which works in conjunction with OAuth to authentication user identities. For this purpose, a holistic (platform level) framework for security, privacy and management of data, as well as users on the EFPF platform, is developed within the EFPF project Task 6.2. In terms of data and information security, the framework specifies and implements the protocols that ensure EFPF's (i.e. interlinked platform, systems and tools) compliance with relevant cybersecurity and privacy mechanisms. This includes mechanisms and standards related to data security (e.g. encryption, cryptography) and privacy (e.g. GDPR and NIS).

In terms of user management, the framework ensures that the EFPF users have seamless access to the integrated resources while satisfying the security and privacy concerns of users are satisfied. A preliminary study of the 4 base platforms identified a common set of security protocols and standards (e.g. OpenID Connect, OAuth2.0 and SAML 2.0) that are being used across them. The open-source solutions KeyCloak and WSO2 have been identified as extensible solutions that implement those open protocols and standards to provide delegated identity management and role-based access management. These technology implementations provide foundations for centralised access and security infrastructure for the EFPF platform. In addition, the standardised data encryption and cryptography techniques used in base platforms are tuned to work in conjunction to ensure

security and privacy of data exchanged through EFPF. Moreover, during the EFPF project continuous checks are done so that the interconnected platforms, systems and tools in the federation adhere to the holistic security and privacy concepts.

4.5 Federated Identity Management

To access the administrative environment and for the separation of duties, EFPF uses the Federated Identity Management, which includes:

- Single Sign On (SSO): It replaces various passwords with a single set of enterprise credentials and provides a consistent authentication experience
- Access security: It centralises access control with a policy-driven security layer for all apps and APIs

When it comes to the integrating of diverse platforms the priority is given to standardised and modern technologies for identification, authorisation and authentication methods. Furthermore, the registration is clearly separated from the access to resources and backup authentication methods are put in place.

The following figure shows the outline of the Security, Privacy & User Management framework in EFPF:

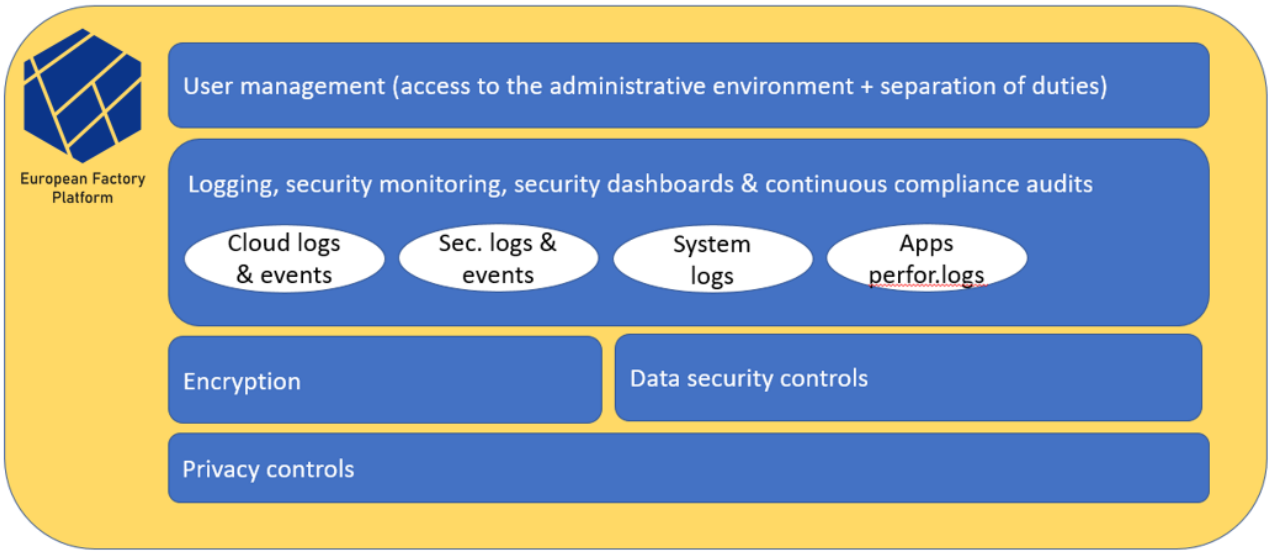


Figure 7: Security, Privacy & User Management Framework

4.6 Blockchain Approach for Secure Data Exchange

The blockchain approach is currently being tested in several application domains, including financial services, eHealth and supply chain management. For traceability in supply chains, blockchain can be used to provide an audit trail for products and their associated manufacturing and supply chain data. Blockchain and Distributed Ledger Technologies (DLTs) stand to offer an end-to-end accountancy mechanism that can facilitate product data integration, services interoperability, cost-effectiveness and increased trust in supply and value chain management. Towards this goal, companies such as IBM, Oracle, and SAP are building their blockchain platforms on Hyperledger, a blockchain technology more suitable to building business applications. Microsoft Azure, Amazon AWS and IBM have all started offering blockchain as a service to streamline the adoption of the technology and its applicability in several fields.

While the most prominent use of blockchain is in cryptocurrencies, such as Bitcoin, it can be used for in several applications such as fulfilment, agreements/contracts, tracking and, of course, payments. The value it offers is inherent to the technology, which is essentially a distributed ledger of transactions kept on cryptographically protected blocks. As such transactions across multiple parties, protected by security and privacy layer, are immutable offering transparency and trust in supply chain management.

EFPF leverages blockchain technology to ensure trust, security and automated exchange of supply chain data among all authorised actors. The goal is to ensure the origin, quality, compliance and appropriate handling of data/documents tracked throughout connected factories, while supporting interoperability and product traceability. The EFPF blockchain service realised in Task 5.4 is sectoral agnostic to serve cross-sectorial stakeholders (production, distribution, customers, etc.). As a federation level solution, no single entity owns the process of Blockchain but all stakeholders can access and use Blockchain as a Service Platform.

5 Ethical Aspects

EFPF does not introduce any critical ethical issues or problems. However, several considerations typical to ICT and on-site industrial trials, where employees are also involved in the demonstration and evaluation stages, shall be considered. The consortium is fully aware of these and has the necessary experience to address them seamlessly as summarised below.

5.1 Legal Framework

EFPF proposed solutions do not expose, use or analyse personal sensitive data for any purpose. In this respect, no ethical issues related to personal sensitive data are raised by the technologies to be employed in the industrial pilots planned in Greece, Germany, and Spain. Furthermore, the EFPF consortium considers during the project lifetime the ethical rules and standards of H2020, and those reflected in the Charter of Fundamental Rights of the European Union. Generally speaking, ethical, social and data protection considerations are crucial and are given all due attention. EFPF addresses any ethical and other privacy issues in Task 1.4 for the investigation, management and monitoring of ethical and privacy issues that could be relevant to its envisaged technological solution and will establish a close-cooperation with the Ethics Helpdesk of the European Commission.

Besides these general conditions, the consortium is aware that a number of privacy and data protection issues could be raised by the activities (i.e. in all pilots planned in WP9 activities) to be performed in the scope of the project. The project involves the carrying out of data collection in all industrial pilots and trials in order to assess the technology and effectiveness of the proposed smart factory and digital manufacturing solutions. For this reason, if any human participants are needed to be involved in certain aspects of the project, then it will be done in full compliance of any European and national legislation and directives relevant to the country where the data collections are taking place (International/European). The EFPF partners found the following regulations to be relevant and considered when dealing with personal data:

- The Universal Declaration of Human Rights[4] and the Convention 108[5] for the Protection of Individuals with Regard to Automatic Processing of Personal Data
- Directive 95/46/EC[6] & Directive 2002/58/EC[7] of the European parliament regarding issues with privacy and protection of personal data and the free movement of such data.

Specifically, when dealing with personal data the EFPF partners will observe the following guidelines:

- Unnecessary personal data collection is avoided (for example, unless it is absolutely required for security or it constitutes the nature of a research study, there is no collection of personal details, identities, bio-identification data at registration to EFPF software systems foreseen, i.e. nick names can used instead of real names whenever possible)
- The personal data needed for statistical analysis is collected anonymously, i.e. without association with the names of individuals;

[4] https://www.un.org/en/universal-declaration-human-rights/
[5] https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108
[6] https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML
[7] https://eur-lex.europa.eu/legal-content/FRF/TXT/?uri=celex:32002L0058

- Any personal data is collected only with the explicit permission of the individuals in question
- The personal data collected is treated confidentially and carefully (taking proper technical means of information protection, e.g. storing general and personal data separately, using encryption for personal data and identities, deleting personal data when it becomes unnecessary)
- Individuals are given the right to access their personal data and the analysis and user models made based on it

To further ensure that the fundamental human rights and privacy needs of participants are met whilst they take part in the project, in the evaluation plans a dedicated section will be delivered for providing ethical and privacy guidelines for the execution of the industrial trials. In order to protect the privacy rights of participants, a number of best practice principles are followed. They include:

- Data is not collected without the explicit informed consent of the individuals under observation. This involves being open with participants about what they are involving themselves in and ensuring that they have agreed fully to the procedures/research being undertaken by giving their explicit consent
- No data collected is sold or used for any purposes other than the current project
- A data minimisation policy is applied at all levels of the project and is supervised by each Industrial Pilot Demonstration responsible. This ensures that no data which is not strictly necessary to the completion of the current study is collected
- Any shadow (ancillary) personal data obtained during the course of the research is immediately deleted. However, the ultimate plan is to minimise this kind of ancillary data as much as possible. Special attention is also paid to comply with the Council of Europe Committee of Ministers Recommendation R(87)15 on regulating the use personal data in the police sector, Art.2
- The collection of data on individuals solely on the basis that they have a particular racial origin, particular religious convictions, sexual behaviour or political opinions or belong to particular movements or organisations which are not proscribed by law is prohibited and is not done within the project
- Compensation – if and when provided – will correspond to a simple reimbursement for working hours lost as a result of participating in the study. Special attention is paid to avoid any form of unfair inducement
- If employees of partner organisations are to be recruited, specific measures will be in place in order to protect them from a breach of privacy/confidentiality and any potential discrimination. In particular their names will not be made public and their participation will not be communicated to their managers

The pilot implementation activities (Task 9.1 –Task 9.4) are performed in three European countries under the leadership of the pilot coordinating partner. Below the relevant national legislation for the countries involved in the pilot is outlined:

Greek Pilot (Kleemann, ELDIA, MilOil):

- Law 2472/1997 (and its amendment by Law 3471/2006) of the Hellenic Parliament
- Regulatory authorities and ethical committees
- Hellenic Data Protection Authority http://www.dpa.gr/

German Pilot (Airbus, Innovint Aircraft Interior GmbH, Walter Otto Müller GmbH & Co.KG, AM Allied Maintenance GmbH):

- Federal Commissioner for Data Protection and Freedom of Information (https://www.bfdi.bund.de/DE/Home/home_node.html)

- Data protection authorities for its various states (https://www.ldi.nrw.de/mainmenu_Service/submenu_Links/Inhalt2/Aufsichtsbehoerden/Aufsichtsbehoerden.php)

Spain Pilot (AIDIMME, LAGRAMA):

- Organic Law 3/2018, of December 5th, of Personal Data Protection and guarantee of the digital rights (https://www.boe.es/eli/es/lo/2018/12/05/3)
- Law 34/2002, of July 11th, of services of the information society and electronic commerce (https://www.boe.es/eli/es/l/2002/07/11/34/con)
- Law 9/2014, of May 9th, General on Telecommunications. (https://www.boe.es/eli/es/l/2014/05/09/9/con)

In addition to the relevant national legislation, the main EU and international policy documents that are relevant to EFPF are listed below:

- Charter of Fundamental Rights of the European Union
- European Convention for the Protection of Human Rights and Fundamental Freedoms
- Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data
- Directive 2000/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)
- Directive 2002/58/EC on data protection

5.2 Risks and Related Measures

The table below summarises the ethical risks identified related to EFPF activities. Within WP1 (Task 1.4), such risks are further elaborated prior the execution of the industrial pilots and results will be included in the corresponding reports of WP9.

No.	Ethical Risk	Description of Risk	Foreseen Risk Management Measures
1	Data Security	Difficulty in ensuring the security of shared personal data in the trials.	Special attention will be given to ensure confidentiality and for incorporating privacy enhancing technologies (pseudo-anonymisation, etc.) to ensure protection from data breaches. EFPF partners have the capacity and the experience to cope with the delivery of security mechanisms, if needed.
2	Storage and process of personal data, Confidentiality	Measurements from various sensors will be transmitted wirelessly. Difficulty in ensuring the security of privacy-related data collected before and/or during the execution of the trials.	CERTH have the expertise and the know-how from similar past and ongoing research projects, towards providing the necessary ethical guidelines that should be adopted during the execution of the trials. Local ethical committee (and the National committee, if needed) will be informed towards getting an official permission for the execution of the selected trials.
3	Loss of Privacy Control	Storage and process of privacy-related data towards the validation of the EFPF integrated tools in the selected trials.	For activities related to the factory optimisation, existing data will be initially categorised and only those that are not exposing privacy or ethical issues will be utilised. In any case, if needed for conducting

			the research activities of the project, records or data dealing with privacy will anonymised and will be totally destroyed after the research study. Always, the data management policy will take care that such activities are not forbidden by law of the country in which the information was collected, stored and analysed.
4	Delegation of Control Privacy Incidental Findings	Need to notify proper trial authorities.	Within Task 1.4, a sub-activity has been included to address local and European legislation. In that context, all the pilots will be performed according to them and relevant data protection authorities will be informed on time.
5	Lack of Transparency	Work of professionals (Workers, Employees in selected trials, etc.).	An ethics manual will be delivered for each of the trials towards all activities performed to be in compliance with National and European legislation. Prior the execution of the pilots the local ethical committees will be informed for any data analysis or collection needed, as part of the EFPF Evaluation and the necessary documents will be created by the respective Industrial Pilot Responsible in order to get an ethical approval.

Summarising, privacy-related issues within the EFPF project are related to:

- Concerns arising from the project's activities and fields of implementation (use of existing data or newly collected information through the shop floor involving human activities or confidential information dealing with enterprise performance)
- Privacy protection and confidentiality of volunteers for the shop-floor data analysis and potential new collection during the industrial trials. Here, special guidelines will be delivered in the ethics manual of EFPF and informed consent will be created for the implied data utilisation by requesting all involved persons to read, be informed and sign the appropriate forms

6 Other Issues

6.1 Data Protection

In the course of the entire project, the fundamental rights of data protection and the right to privacy of the volunteer research participants will be strictly followed. Furthermore, the developments and tests performed within EFPF project life will observe the Charter of Fundamental Rights of the European Union 11 (2000/C 364/01). The following articles of this Charter apply directly to this project:

- Article 1: Human dignity is inviolable. It must be respected and protected
- Article 7: Everyone has the right to respect for his or her private and family life, home and communications
- Article 8.1: Everyone has the right to the protection of personal data concerning him or her
- Article 8.2: Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data, which has been collected concerning him or her, and the right to have it rectified
- Article 8.3: Compliance with these rules shall be subject to control by an independent authority – in this case this responsibility lies with the EFPF Project Manager (ICE)
- Article 23: Equality between men and women must be ensured in all areas, including employment, work and pay. The principle of equality shall not prevent the maintenance or adoption of measures providing for specific advantages in favour of the under-represented sex

6.2 Governance Rules and Trust Mechanisms

Task 5.3 of the EFPF project sets-up a formal model of distributed collaborative activities where each activity is defined by its contribution to the overall goal in a recursive approach. Formal contracts gather the way in which companies are given responsibility for activities, and ensure the results of the activity conform to the relevant regulations. The contracting framework also covers the process used by a company to implement its activity, ensuring compliance at process and at results level. Using this theoretical model, the requirements for relevant regulations, smart contracting mechanisms, secure message exchange, company sourcing, monitoring protocols and coordination mechanisms are developed, ensuring support for regulation compliance and trusted distributed and coordination of activities.

Based on these activities, the following governance rules and trust mechanisms are implemented.

Information level

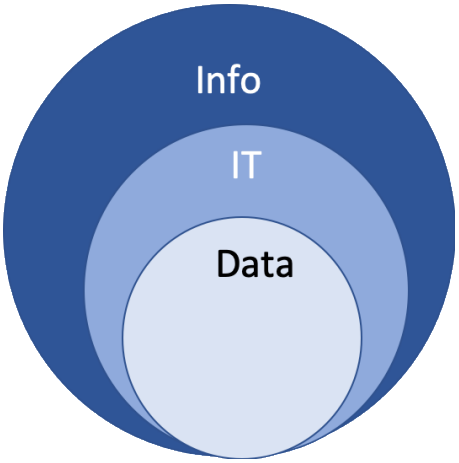
- Policy based control of information to meet legal, regulatory and business demands

IT level

- Aligning IT efforts with the business objectives of EFPF

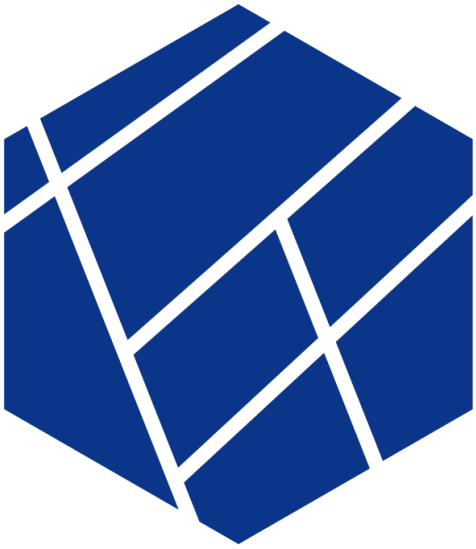
Data level

- Ensuring that data are accurate and true
- Eliminating corrupted and inaccurate data (data cleansing)
- Eliminating redundant data (de-duplication)
- Ensuring security controls for data integrity and quality



Annex A: History

Document History	
Versions	V0.1: • Document set-up and draft Table of Contents V0.2: • First draft version of Data Management Plan V0.3: • Document version sent to ASC, FIT, HAW, ICE and SRFG for partner inputs V0.4: • Document version including partner inputs V0.5: • Document version sent to HAW (WP11 lead) and ICE V0.9: • Document version sent to internal reviewers V1.0: • Deliverable approved by project-internal reviewers
Contributions	AID: • Amparo Roca de Togores ASC: • Brian Clark • Norman Wessel BRM: • Florian Lipok • Dieter Meinhard FIT: • Alexander Schneider HAW: • Ingo Martens ICE: • Usman Wajid SRFG • Violeta Damjanovic-Behrendt



European Factory Platform

www.efpf.org