IoT4CPS – Trustworthy IoT for CPS

FFG - ICT of the Future
Project No. 863129

Deliverable D1.1
Initial Data Management Plan

The IoT4CPS Consortium:
AIT – Austrian Institute of Technology GmbH
AVL – AVL List GmbH
DUK – Donau-Universität Krems
IFAT – Infineon Technologies Austria AG
JKU – JK Universität Linz / Institute for Pervasive Computing
JR – Joanneum Research Forschungsgesellschaft mbH
NOKIA – Nokia Solutions and Networks Österreich GmbH
NXP – NXP Semiconductors Austria GmbH
SBA – SBA Research GmbH
SRFG – Salzburg Research Forschungsgesellschaft
SCCH – Software Competence Center Hagenberg GmbH
SAGÖ – Siemens AG Österreich
TTTech – TTTech Computertechnik AG
IAIK – TU Graz / Institute for Applied Information Processing and Communications
ITI – TU Graz / Institute for Technical Informatics
TUW – TU Wien / Institute of Computer Engineering
XNET – X-Net Services GmbH

For more information on this document or the IoT4CPS project, please contact:
Mario Drobics, AIT Austrian Institute of Technology, mario.drobics@ait.ac.at

Document Control

Title: Initial Data Management Plan
Type: Public
Editor(s): Mario Drobics
E-mail: mario.drobics@ait.ac.at
Author(s): Mario Drobics, A. Treytl, V. Damjanovic-Behrendt
Doc ID: D1.1

Amendment History

Version	Date	Author(s)	Description/Comments
v1	06.06.2018	M. Drobics	Initial version prepared
v2	26.06.2018	M. Drobics	Update on deliverables and project contacts
V3	18.07.2018	M. Drobics, A. Treytl	Update based on review from A. Treytl
V4	20.07.2018	M. Drobics, V. Damjanovic-Behrendt	Update based on review from V. Damjanovic-Behrendt

The IoT4CPS project is partially funded by the "ICT of the Future" Program of the FFG and the BMVIT.

1. Inhalt

(This page is left blank intentionally.)

2. Introduction

This Initial Data Management Plan (DMP) is designed to identify data to be generated in the project and to describe the following aspects of data management:

- which data is collected, developed or generated in the project,
- how this data is handled in the project,
- which methods and standards are used,
- how the data is secured and maintained over the long term, and
- whether it is planned to make data records available to third parties and to enable them to re-use the data (so-called "open access to research data")

Currently, the IoT4CPS project does not plan to make data available to third parties. It will be only the evaluation results to be published anonymously through the project reports, publications and presentations.
This first deliverable on Data Management provides the plans for the collection, storage and usage of open access research data. Apart from a selection of platforms that will host and provide access to the various data, it is also important to identify how all the various data will link to each other. Moreover, the proper description of open access research data will eventually facilitate their future discovery by external researchers.

3. Legal regulations for the use of personal data

Every person has the right to protection and confidentiality of personal data. At the same time, it is often necessary for business and administration to work with this data. For the use of data certain conditions must be met and data protection measures taken. Violation of the Data Protection Act may result in administrative and judicial consequences. To protect the interests of both sides, individuals and businesses, there is the Data Protection Act in place, which has been replaced in May 2018 by the General Data Protection Regulation (GDPR) in the EU.

Changes due to the EU General Data Protection Regulation

The EU GDPR harmonizes the rules for processing of personal data, the rights of those affected and the obligations of those responsible across the EU. Although it has been directly applicable as an EU regulation in each EU Member State, it contains numerous opening clauses and leaves the national legislature certain leeway. In order to implement these opening clauses and margins, the Data Protection Amendment Act 2018, an amendment to the DSG 2000 (in future: DSG), was passed in Austria.

Data Protection Officer (DPO)

The EU GDPR requires companies to appoint a Data Protection Officer (DPO) if the core activity of the company is to regularly collect or monitor personal information (e.g. banks or insurance companies) or if the core activity is the processing of sensitive data (e.g. hospitals) or if they are public institutions.
At the time being, IoT4CPS does not plan to process personal information of this type. This, however, might change over the duration of the project. To identify any potential data protection issues, the project coordinator will frequently consult the DPO of AIT, DI Michael Löffler (michael.loeffler@ait.ac.at, +43 50550 2003).

4. Overview on Data

In the initial phase of the IoT4CPS project, the following data sets have been created or utilized, as summarized in the following table. A more thorough description of the data sets and how they are managed in the project, is given afterwards. Additionally, dissemination material will be provided by the project which is discussed in section 5.

No.	Dataset	Primary responsible partner	Personal Data
1	Project Documents	AIT	No
2	Project Asset Database	AIT	No
3	Project Contacts	SBA	Yes

1 – Project Documents	
Responsible partner	AIT
Type of data	Documents (e.g. reports, deliverables, etc.)
Contains personal data	Yes
Type of personal data	Name of editor(s)
Data collection (methods, standards used)	Manuel entry by project partners
Documentation available	Online
Storage	SharePoint Server hosted by AIT in its own data center
Backup	Daily backups
Access and security	• Online access for project members based on a personal invitation • Access to data center granted only to authorized personnel
Ethical issues	None
IPRs (data ownership, licensing, etc.)	The documents containing IPR relevant information to be marked in the respective documents (e.g. deliverables)
Planned use (documentation, validation, analytics, etc.)	Documentation; reporting
Data sharing (public, partners only, selected personal, etc.)	Specific documents (e.g. deliverables) will be shared with external partners on an individual level.
Preservation (delete-after-project, archive, etc.)	Archive

2 – Project Asset Database	
Responsible partner	AIT
Type of data	Structured database containing: • Use-Case Descriptions • Requirements Specification • Threats Specification • Implementation Context Description • Data Sources Description • Building Blocks Description
Contains personal data	Yes
Type of personal data	Name of editor(s)

Data collection (methods, standards used)	Manuel entry by project partners
Documentation available	Online
Storage	SharePoint Server hosted by AIT in its own data center
Backup	Daily backups
Access and security	• Online access for project members based on a personal invitation • Access to data center granted only to authorized personnel
Ethical issues	None
IPRs (data ownership, licensing, etc.)	Data collected is partly IPR relevant
Planned use (documentation, validation, analytics, etc.)	Project internal usage only
Data sharing (public, partners only, selected personal, etc.)	Some data to be included in the project documents (e.g. deliverables) and be shared on an individual level
Preservation (delete-after-project, archive, etc.)	Archive

3 – Project Contacts	
Responsible partner	SBA Research
Type of data	Excel Sheet
Contains personal data	Yes (consent given)
Type of personal data	Contact information (user's name, e-mail address, company name)
Data collection (methods, standards used)	Registration via project's web-site Manual entry based on business cards received from interested persons
Documentation available	None
Storage	SharePoint Server hosted by AIT in its own data center
Backup	Daily backups
Access and security	Online access for project members based on an invitation Access to data center only for authorized personnel
Ethical issues	None
IPRs (data ownership, licensing, etc.)	None
Planned use (documentation, validation, analytics, etc.)	Addresses are used for sending newsletters and invitations for project related events

Data sharing (public, partners only, selected personal, etc.)	No.
Preservation (delete-after-project, archive, etc.)	Delete after project

5. Dissemination Material

IoT4CPS's dissemination material falls under the following main categories:

No.	Material	Primary responsible partner	Personal Data
1	Public deliverables	Author(s) of the deliverable	No
2	Scientific papers	Author(s) of the paper	No
3	Public presentations, posters, videos and flyers	AIT, SBA	No

This section provides a plan of where the aforementioned material will be stored and how it will be accessed. The particularities of each dissemination category, with respect to storage and access, are highlighted in the subsections below. Regarding the appropriate licensing schemes for certain material (e.g., presentations), the project will consider the *Creative Commons licence "Attribution", CC(by)* (creativecommons.org) where possible.

Public deliverables

The public deliverables of IoT4CPS document the progress of the work conducted by the consortium and provide all the necessary details to external parties to understand the IoT4CPS work in depth. Deliverables are expected to be accessed by interested researchers and stakeholders. The primary entry point for accessing the public deliverables is the IoT4CPS's web site (www.IoT4CPS.at).

1 – Public deliverables	
Responsible partner	Author(s) of the deliverable
Type of data	Document
Contains personal data	Yes
Type of personal data	Name and email of authors(s)
Storage	Web-server hosted by AIT in its own data center
Backup	Daily backups
Access and security	Public online access using web browser
Ethical issues	None
IPRs (data ownership, licensing, etc.)	None (Sections involving IPR related issues need to be removed before making the deliverable public)
Planned use (documentation, validation, analytics, etc.)	Information

Data sharing (public, partners only, selected personal, etc.)	Public
Preservation (delete-after-project, archive, etc.)	Keep available for at least 6 months after the end of the project

Scientific Papers

IoT4CPS is aiming at publishing a number of high quality scientific papers, targeting the cybersecurity and IoT research community as well as the respective industries. Access to the published articles aims to follow a combination of the 'gold' and 'green' open access models. The 'gold' and 'green' (after the embargo period, if any) open access will be realized by the IoT4CPS web site (www.IoT4CPS.at). Additionally, pre-publication text is also made available through Zenodo, or other research article repositories, like *ResearchGate* (www.researchgate.net) or *Acedemia* (www.academia.edu), from the authors personal accounts in those sites. This way, increased visibility of the papers will be achieved.

2 – Scientific papers	
Responsible partner	Author(s) of the paper
Type of data	Document
Contains personal data	Yes
Type of personal data	Name and email of authors(s)
Storage	Stored by publisher and in different archives
Backup	Depending on hosting institution
Access and security	Depending on hosting institution (see above)
Ethical issues	None
IPRs (data ownership, licensing, etc.)	None
Planned use (documentation, validation, analytics, etc.)	Information
Data sharing (public, partners only, selected personal, etc.)	Public (see above)
Preservation (delete-after-project, archive, etc.)	Keep available for after the end of the project

Public presentations, posters, videos and flyers

Apart from deliverables, scientific papers and technical blog entries, additional dissemination material is produced throughout the lifetime of the project for communication purposes. Such material includes public presentations in various events, posters, videos and flyers, all promoting the work done by IoT4CPS. Such material will be made available on the IoT4CPS web site (www.IoT4CPS.at).

3 – Public presentations	
Responsible partner	AIT, SBA
Type of data	Documents, images, videos
Contains personal data	Yes
Type of personal data	Name and email of presenter(s)
Storage	Web-server hosted by AIT in its own data center
Backup	Daily backups
Access and security	Public online access using web browser
Ethical issues	None
IPRs (data ownership, licensing, etc.)	None
Planned use (documentation, validation, analytics, etc.)	Information
Data sharing (public, partners only, selected personal, etc.)	Public
Preservation (delete-after-project, archive, etc.)	Keep available for at least 6 months after the end of the project

6. Conclusion and Next Steps

This deliverable provides the initial Data Management Plan of IoT4CPS. This document will be updated frequently to review the handling of those data sets listed and to integrate potential new data which is generated during the upcoming project activities.

7. References

8. Abbreviations

DMP	Data Management Plan
GDPR	General Data Protection Regulation
DPO	Data Protection Officer