Advanced Cyber-Threat Intelligence, Detection, and Mitigation Platform for a Trusted Internet of Things
Grant Agreement: 786698

D3.3 Legal and ethical recommendations

Work Package 3: Legal issues: data protection and privacy

Document Dissemination Level

P	Public	☐
CO	Confidential, only for members of the Consortium (including the Commission Services)	☒

Document Due Date: 31/12/2018
Document Submission Date: 31/12/2018

Co-funded by the Horizon 2020 Framework Programme of the European Union

Document Information

Deliverable number:	**D3.3**
Deliverable title:	Legal and ethical recommendations
Deliverable version:	1.4
Work Package number:	3
Work Package title:	Legal issues: data protection and privacy
Due Date of delivery:	31/12/2018
Actual date of delivery:	31/12/2018
Dissemination level:	CO
Editor(s):	Olga Gkotsopoulou (VUB) Paul Quinn (VUB)
Contributor(s):	Liza Charalambous (ADITESS) Gohar Sargsyan and Raymond Binnendijk (CGI) Stavros Shiaeles (CSCAN) Clement Pavue (Scorechain) Nicholas Kolokotronis, Spiros Skiadopoulos, Christos Tryfonopoulos, Costas Vassilakis (UoP)
Reviewer(s):	Gohar Sargsyan and Raymond Binnendijk (CGI) Stavros Shiaeles (CSCAN)
Project name:	Advanced Cyber-Threat Intelligence, Detection, and Mitigation Platform for a Trusted Internet of Things
Project Acronym	Cyber-Trust
Project starting date:	1/5/2018
Project duration:	36 months
Rights:	Cyber-Trust Consortium

Version History

Version	Date	Beneficiary	Description
0.1	12.11.2018	VUB	ToC and DDP
0.2	24.11.2018	ADITESS; CSCAN; Scorechain; UoP	Input via questionnaires
0.3	27.11.2018	VUB	Analysis of the input
0.4	15.12.2018	VUB	1st draft
0.5	19.12.2018	VUB	Incorporation of the DPIA questionnaires
0.6	20.12.2018	CGI	Feedback
0.7	22.12.2018	UoP; CSCAN	Feedback/Input
1.0	22.12.2018	VUB	Submission of the final draft to reviewers
1.1	26.12.2018	CGI	Review
1.2	28.12.2018	CSCAN	Review
1.3	30.12.2018	VUB	Internal review
1.4	31.12.2018	VUB	Submission of the final version to PC

Acronyms

ACRONYM	EXPLANATION
CTB	Cyber-Trust Blockchain
CY	Cyprus
DLT	Distributed Ledger Technologies
DDoS	Distributed denial-of-service
DPI	Deep Packet Inspection
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
ENISA	European Union Agency for Network and Information Security
eVDB	Enriched Vulnerability Database
GDPR	General Data Protection Regulation
GR	Greece
GrSM	Graphical Security Model
IDE	Intelligent Development Environment
IDS	Intrusion Detection System
iIRS	intelligent Intrusion Response System
IoT	Internet of Things
IPS	Intrusion Prevention System
ISP	Internet Service Provider
IT	Italy
LEA	Law Enforcement Agency
LU	Luxembourg
MISP	Open Source Threat Intelligence Platform & Open Standards For Threat Information Sharing
NL	The Netherlands
OS	Operation System
PET	Privacy Enhancement Technologies
RoQ	Reduction of Quality
SDN	Software-defined network
TMS	Trust management system
TOR	The Onion Router
TVA	Threat and Vulnerability Assessment
UC	Use Case
UI	User Interface
UK	United Kingdom
WP	Work Package

Table of Contents

Table of Tables

Executive Summary

The Deliverable 3.3, based on the findings of D3.1 and D3.2, as well as other deliverables discussed and drafted in parallel (specifically, D2.3, D2.4 and D4.1), provides a preliminary overview of the technical structure of the Cyber-Trust, in particular, the tools to-be-developed in Work Packages 5, 6 and 7 (WP5, 6 and 7). The technical partners elucidated the main characteristics of each component, including information about its role in relation to other solutions, also to be developed, in the project, the methods used for its development and its envisaged use and End-users. Based on this simplified technical overview, the present deliverable also provides a preliminary assessment of the primary data protection and privacy concerns, as well as other legal and ethical apprehensions identified by the technical partners, which will be, *inter alia*, useful for the overall architectural design of the platform which will take place in WP4.

Building upon the knowledge gained by the legal framework analysis, the D3.3 further offers a first assessment of mitigation tools to eliminate the recognised potential risks and a set of general and more specific recommendations. The general legal and ethical recommendations address the topics discussed in D3.1 and D3.2 and follow the three main pillars of data protection, privacy and electronic evidence, which will be taken into consideration during the design phase of the platform in WP4. The specific recommendations discourse the issues acknowledged in WP5, 6 and 7 and their respective tasks, as described by the technical partners.

The present deliverable also prepares the path towards two Data Protection Impact Assessments (DPIAs) to be carried out during the design and development phase of the Cyber-Trust platform and be presented in the deliverables D3.4 and D3.5. The methodology is tailor-made for the Cyber-Trust context and follows the requirements of Article 35 of the General Data Protection Regulation, enriched with elements of the sample templates as proposed by national supervisory authorities, the Article 29 Working Party and the European Data Protection Board, as well as expert groups. In order to visualize the suggested methodology, indicative questionnaires were drafted. The partners of the Cyber-Trust consortium, with the help of their Data Protection Officers, data processors (if applicable) and external experts will be invited to use them as guidance during the design phase of the project in WP4 and the actual development of the tools in WP5, 6 and 7, in order to verify that all the measures are in compliance with the data protection requirements as well as the additional privacy requirements.

1. Introduction

1.1 Project Overview

Cyber-Trust | Advanced Cyber-Threat Intelligence, Detection, and Mitigation Platform for a Trusted Internet of Things is a 36-month long research project in the Digital Security Focus Area, co-funded by the Horizon 2020 Framework Programme of the European Union, under the Grant Agreement no. 786698. Its principal goal is to revolutionise the way cyber-security systems are built and operate.

By establishing an innovative cyber-threat intelligence gathering, detection, and mitigation platform, as well as, by performing high quality interdisciplinary research in critical areas, the Cyber-Trust project aims to develop novel technologies and concepts to tackle the grand challenges towards securing the ecosystem of Internet of Things (IoT) devices. It is structured around three pillars: a. key proactive technologies, b. cyber-attack detection and mitigation, and c. distributed ledger technologies, as seen in the table below.

Key proactive technologies	**Attack detection and mitigation**	**Distributed Ledger Technologies**
▪ cyber-threat intelligence ▪ cyber-threat sharing ▪ reputation/trust management ▪ security games	▪ advanced targeted attacks ▪ network infrastructure attacks ▪ network visualisation ▪ mitigation and remediation ▪ forensics evidence collection	▪ registration ▪ update ▪ verification ▪ modelling ▪ consensus ▪ privacy

Table 1.1: The three pillars of Cyber-Trust

1.2 Purpose of the Document

The present document D3.3 is the first (out of three) outcome of Task 3.3 (T3.3) entitled “Recommendations and road ahead”, which will conclude on legal and ethical recommendations for the design of the Cyber-Trust platform and its tools to be developed in other technical work packages. The Leader of D3.3 is VUB and participants are all the partners. This deliverable, which is based on the research conducted in T3.1 (D3.1)[1] and T3.2 (D3.2)[2], will focus on the tools that will be used/developed for the creation of the Cyber-Trust prototype and will present legal and ethical recommendations on the basis of the input given by all the partners in the form of a questionnaire. The preliminary questionnaire template and the relevant instructions are included in Annex A. Moreover, the deliverable will provide a preliminary methodology for the data protection impact assessment to take place in the D3.4 and D3.5. The material produced will feed into tasks T4.1 and T4.2 and T8.1 and T8.4.

1.3 Scope and Intended Audience

The intended audience of the document are the project stakeholders and the Consortium members. According to the preliminary security scrutiny, this deliverable was classified as PU = Public. Nevertheless, after further consideration, the classification of the deliverable was changed to CO = Confidential.

[1] Cyber-Trust, D3.1 Regulatory Framework Analysis, August 2018.

[2] Cyber-Trust, D3.2 The legal analysis of the use of evidentiary material, November 2018.

1.4 Structure of the Document

Section 2 will provide the reader with a brief description of the tools that are going to be developed in the WP5, 6 and 7, their interdependencies with other components, their function in the whole system, the tools that will be used for their creation, as well as their envisaged end-users and use, based on the input of the technical partners who lead their creation process. Section 3 will give insight in the legal and ethical concerns as expressed from the partners, based on the T3.1 and T3.2, as well as relevant considerations in D2.3 concerning the use-cases. Section 4 will focus on the legal and ethical recommendations, setting out the mitigation measures identified by the partners and other relevant assessment. Section 5 will introduce a preliminary methodological approach to the Data Protection Impact Assessment that will take place in D3.4 and D3.5 during the architectural design and the actual development of each tool, formed by the latest findings.

2. Preliminary description of tools related to data processing per Work Package

Section 2 will give a selected insight into the tools that are going to be developed during the research phase in order to make the conception of a Cyber-Trust platform possible. A complete overview of the tools can be found in Annex B. By filling in the first part of the questionnaire, found in Annex A of the present document, concerning the general information about the technical structure of the component, the technical partners of the Work Packages 5, 6 and 7, involved in the process of the development of the core components of the platform, provided a preliminary description of the tools to-be-developed per Work Package and relevant task, related to data processing. The technical partners were also requested to elucidate the envisaged use after the research phase and determine the potential end-users, in other words, to demystify the relevant context of the possible application. For reasons of coherence, the relevant references to the pillars were also included in each tool, as well as the common asset-class actors, using the taxonomy defined in D2.3.[3]

This preparatory exercise was carried out at this stage because the assessment of the Cyber-Trust system can be conducted fruitfully only if every element of the envisaged processing operation is clear for all the parties. Therefore, in the forthcoming deliverables D3.4 and D3.5, information may also be requested by other technical partners involved in other tasks, who did not participate in this preliminary round, for the reason that as of now the component developed by them is not envisaged to include any personal data processing. As the technical structure becomes better-defined, other processing activities may also be added and described in the next deliverables.

2.1 Work Package 5: Key proactive technologies and cyber-threat intelligence

Here follow the tables concerning the tools to-be-developed as filled in by the technical partners of WP5.

2.1.1 Enriched Vulnerability Database (eVDB)

Partner **Work Package**	**UoP** **WP5**
Task	T5.1 Threat intelligence techniques
Task description	Cyber-threat intelligence discovery and sharing mechanism
Pillar	Key proactive technologies
Description of the tool/solution/method/mechanism to be developed	The tools and solutions to be developed in the context of the eVDB (including the cyber-threat discovery mechanism) aim at: 1. gathering public cyber-threat intelligence information from deepnet web fora or marketplaces and clearnet social platforms, 2. leveraging this information to identify emerging threats, zero-day vulnerabilities and new exploits to IoT devices, and 3. sharing the information with different Cyber-Trust modules and other stakeholders.
The role of the tool in relation to other tools/solutions (to be developed) in the project	• The cyber-threat discovery mechanism will be responsible for identifying cyber-treat intelligence from online sources. • The eVDB will be responsible for sharing cyber-threat related information to other components and modules in the Cyber-Trust platform.

[3] Cyber-Trust, D2.3 Use Case Scenarios, December 2018, p.16.

Tool(s)/method(s) used for the development of the specific tool/solution	• For the cyber-threat discovery mechanism, the following tools/technologies will be used: ACHE crawler, TOR, MongoDB, word2vec, nltk, Formasaurus/Opal, Selenium/Splash, Privoxy. • For the eVDB, the following tools/technologies will be used: MISP, ZeroMQ, lxml, PyMISP.
Common Asset-Class Actors	A07 eVDB Admin Module; A09 eVDB Sharing Service; A10 Crawling Service

Table 2.1 - Work Package 5, Task 5.1

2.1.2 Trust management system (TMS); Device attack detector

Partner **Work Package**	**UoP** **WP5 (with linkage to WP6)**
Task	T5.2 Trust establishment and risk assessment (in relation to T5.4. Cyber-Trust proactive technology tools) T6.2 Device attack detector
Task description	T5.2 refers to methods, algorithms and tools for realising the computation of a comprehensive trust score for devices and supporting devices in reasoning about mutual trust and regulating their communications, data exchanges and service provision and consumption. T6.2 refers to measuring device health and identifying vulnerabilities.
Pillar	Key proactive technologies; Attack detection and mitigation
Description of the tool/solution/method/mechanism to be developed	The tools and solutions to be developed in the context of the TMS aim at: 1. Synthesising a comprehensive profile for devices and computing a trust score for each one 2. Computing risk levels for devices 3. Triggering awareness and reaction events when appropriate conditions (e.g. demotions or elevations of trust/risk scores below/above certain thresholds) are met 4. Allowing TMSs to communicate according to the peer-to-peer paradigm towards synthesising a global view of device trust/risk levels, maintaining the autonomy of each TMS however. The tools and solutions to be developed in the context of the device attack detector are: • Host/device/network inventory tools • Remote health monitoring tools • Vulnerability scanner
The role of the tool in relation to other tools/solutions (to be developed) in the project	The TMS will be the central point for device trust and risk assessment. It will consume information from the device profile repository, the attack and anomaly detection modules as well as from other repositories (e.g. network architecture, assets etc.) and it will be able to: 1. Provide assessments of the trust and risk level of devices to (a) other devices and (b) tools that need this information, such as the intelligent UI. 2. Raise awareness events for the intelligent UI users.

	3. Trigger execution of game-theoretic cyber-defence procedures. 4. Trigger mitigation actions, according to policy rules, especially through the iIRS. The Device attack detector will: • Arrange for obtaining device health metrics, in particular for firmware, operating systems and critical components • Identifying vulnerabilities present at devices Related to the device attack detector, tools for discovering assets and enumerating networks and services will be used.
Tool(s)/method(s) used for the development of the specific tool/solution	Currently, a number of tools are being investigated regarding their suitability to be used for developing the various functionalities. Short lists are given below: **Trust Management System** Linux SGX Trust Management Framework, Soutei, TrustAll, Trust Composer, kamban.org, Trust relationship management on blockchain for IoT, Trust Management System, Trust Management Library, Tennessee Risk Management Trust, Trust Guard, Django agent trust, Keynote TMS, Python extension module for the KeyNote trust management system, Declarative Trust Management System with Linked Credentials **Host/Device Inventory and Scanning** NMap, Angry IP scanner, Unicornscan, Masscan, Scanrand, Zmap, NetCrunch Tools, Scanmetender, Maltego, Netglub, Dnsdumpster.com, MyNet Toolset, LanTopoLog, Spiceworks Network Mapping, NetworkMiner **Vulnerability scanning** OpenVAS, Nessus, Nikto, Arachni, w3af, Vega **Attack mitigation** Tools for identifying appropriate mitigation actions (listed under https://www.cve-search.org/software/).
Common Asset-Class Actors	A05 Trust Management System; A08 TrustDB Admin Module

Table 2.2 - Work Package 5, Task 5.2

2.1.3 iIRS (intelligent Intrusion Response System)

Partner **Work Package**	**UoP** **WP5 (with linkage to WP6)**
Task	T5.3 Game-theoretic cyber-defence framework (in relation to T5.4. Cyber-Trust proactive technology tools) T6.3 Network attack detection and mitigation
Task description	The purpose of this task is to ensure awareness of the security condition and mitigation of any possible attack that may be applied. The associated defence tool that is envisaged, called iIRS (intelligent Intrusion Response System), aims at efficiently translating the system alerts (generated from IDS – Intrusion Detection System) into an accurate estimation of the current system security condition and respond with the appropriate mitigation action (either applied directly or by informing the corresponding security service) in real-time.

	iIRS has the ability to select the response actions in real-time to mitigate the progression of a cyber-attacker in the smart home network while minimizing the negative impact that reactions have to the availability of network resources to trusted devices (e.g. by refusing communication requests, shutting down running services, etc.). Balancing this tradeoff between ensuring system security against cyber-attacks and keeping network availability at the desired level (by taking into account the user's preferences as well) is one of the main goals of the iIRS.
Pillar	Key proactive technologies; Attack detection and mitigation
Description of the tool/solution/method/mechanism to be developed	The main components of iIRS are the following: 1. The module responsible for handling the Graphical Security Model (GrSM). 2. The communication module which is responsible for the interactions with the TMS, the IDS, Enriched Vulnerability Database (eVDB) and the cyber-defence service. 3. The security state belief computation module, which updates the belief of the system security condition in real-time. 4. The decision-making module which computes the optimal defence actions.
The role of the tool in relation to other tools/solutions (to be developed) in the project	The purpose of iIRS is the suggestion of the best available defence actions in order to enhance the system security. In doing so, there is a need to interact with other system components. More specifically, iIRS needs to retrieve information about the network configuration, attack likelihood probabilities and devices' profiles from the TMS, information about exploits and vulnerabilities from the eVDB, receives security alerts from the IDS and communicates with Cyber-Defence service.
Tool(s)/method(s) used for the development of the specific tool/solution	The module which is responsible for the GrSM generation and manipulation may possibly be based on a third-party tool (this is currently under consideration in D2.5). Examples of such tools include (but not limited to): TVA, NetSpa, Mulval, Advise, Naggen, CyberSage, and Cygraph. The rest of the iIRS components (see above) will be developed in-house.
Common Asset-Class Actors	A13 Smart Gateway iIRS app; A14 Smart Device iIRS app

Table 2.3 - Work Package 5, Task 5.3

2.2 Work Package 6: Advanced cyber-attack detection and mitigation

Here follow the tables concerning the tools to-be-developed as filled in by the technical partners of WP6.

2.2.1 Device Defender: for intrusion detection and malicious attacks

Partner **Work Package**	**ADITESS** **WP6**
Task	T6.2 Device tampering detection and remediation (with linkage to T6.1 Privacy-preserving IoT device profiling)
Task description	The implementation of modules for device level attacks and remediation
Pillar	Attack detection and mitigation

Description of the tool/solution/method/mechanism to be developed	The tool aids at preventing the transfer of malicious content or access on monitored IoT devices. This tool retains log information regarding the state of the devices OS, running processes as well as hashes and digital signatures for the immediate detection of malicious acts and rapid remediation.
The role of the tool in relation to other tools/solutions (to be developed) in the project	The tool will interact with a number of other platform components including the Cyber-Trust Device database, as well as the network attack detection and blockchain components.
Tool(s)/method(s) used for the development of the specific tool/solution	Different flavours of the agent are expected to be developed. These will aid use by mobile and web applications. Therefore, mobile development frameworks such as ionic, android development and Xamarin are candidates while for the rest implementations, technologies such as python, Django, Node.js and C will be used.
Common Asset-Class Actors	A03 Monitoring Service; A04 Cyber-defence Service; A12 Smart Device Agent; A17 Profiling Service

Table 2.4 - Work Package 6, Task 6.2

2.2.2 Machine Learning Intrusion Detection System; Machine Learning Deep Packet Inspection

Partner **Work Package**	**CSCAN** **WP6**
Task	T6.3 Network attack detection and mitigation (with linkage to T6.1 Privacy-preserving IoT device profiling)
Task description	This task aims at attacks targeting at (critical) network infrastructures, with a focus on botnet detection and mitigation. Botnets are used in many attacks, with DDoS and reduction of quality (RoQ) attacks being the most common ones. In principle, a posteriori DDoS detection is trivial, in the sense that it is noticed once the attack succeeds
Pillar	Attack detection and mitigation
Description of the tool/solution/method/mechanism to be developed	The purpose of the developed Intrusion Prevention System (IPS) is to block known and unknown attacks using Machine Learning, Software Define Networks (SDN) along with Deep Packet Inspection (DPI). The DPI will utilise the profiling information from devices as well as Cyber Threat intelligence to detect first the unknown threats and in a later state to produce the signatures required in order the malwares and the variations of them to be detected. This is a very challenging part as malware writers utilised techniques such as obfuscation in order to bypass detection.
The role of the tool in relation to other tools/solutions (to be developed) in the project	The tool will interact with various components of Cyber-Trust platform, in particular with WP5 and also other tasks of WP6.
Tool(s)/method(s) used for the development of the specific tool/solution	Snort-IDS, Bro-IDS, netsniff-ng, tcpdflow Custom tools also will be developed in order to identify attack patterns as well as creating new attack patterns from monitoring data.
Common Asset-Class Actors	A03 Monitoring Service; A04 Cyber-defence Service; A11 Smart Gateway Agent; A16 Network architecture and assets repository; A17 Profiling Service

Table 2.5 - Work Package 6, Task 6.3

2.3 Work Package 7: Distributed ledger technology for enhanced accountability

Here follow the tables concerning the tools to-be-developed as filled in by the technical partners of WP7.

2.3.1 Cyber-Trust Blockchain (CTB)

Partner **WP**	**Scorechain** **WP7**
Task	T7.2 Cyber-Trust's proposed DLT architecture T7.3 Blockchain security framework
Task description	Implementation of the blockchain, its architecture and management.
Pillar	Distributed Ledger Technologies
Description of the tool/solution/method/mechanism to be developed	The CTB will be used to store data collected by the Cyber-Trust platform such as forensic evidence meta-data or Trusted Logs
The role of the tool in relation to other tools/solutions (to be developed) in the project	The CTB will interact with the rest of the platform by formatting, validating then storing data provided by the other tools in the project
Tool(s)/method(s) used for the development of the specific tool/solution	• JavaScript IDE (Intelligent Development Environment) Atom /Sublim Text / etc. • HyperLedger as a blockchain solution • Node.js
Common Asset-Class Actors	A02 DLT Service ; A15 DLT Admin Module

Table 2.6 - Work Package 7, Task 7.3

2.3.2 Cyber-Trust forensics visualisation tool

Partner **WP**	**Scorechain** **WP7**
Task	T7.4 Blockchain forensic visualisation tool
Task description	This task is about the development of a tool (D7.5) for the easy-to-use blockchain, exploration and visualisation of the information that will be stored in the Cyber-Trust blockchain solution.
Pillar	Distributed Ledger Technologies
Description of the tool/solution/method/mechanism to be developed	The visualisation tool will provide a user-friendly way to explore the Cyber-Trust platform's blockchain
The role of the tool in relation to other tools/solutions (to be developed) in the project	The visualisation tool will interact with the blockchain to display the data previously stored on it.
Tool(s)/method(s) used for the development of the specific tool/solution	• JavaScript IDE (Intelligent Development Environment) Atom /Sublim Text / etc. • HyperLedger as a blockchain solution • Node.js
Common Asset-Class Actors	A01 Visualisation Portal ; A02 DLT Service

Table 2.7 - Work Package 7, Task 7.4

2.4 Envisaged end-users and use of the tools

The partners also described the envisaged use of the tools to-be-created. The Enriched Vulnerability Database (eVDB) will be used for cyber-threat intelligence discovery and sharing [T5.1]. The Trust management system (TMS) and the device attack detector will be used for the implementation of trust-based risk mitigation [T5.2; T6.2]. Specifically, the Device Defender for intrusion detection and malicious attacks will be used for the monitoring and detection of threats and attacks on the end-device and apply the accepted remediation policy, if necessary [T6.2]. The iIRS (intelligent Intrusion Response System) aims to estimate the overall security of a user's device or network and intelligently respond with the appropriate least intrusive mitigation actions in real-time [T5.3; T6.3], whereas the Intrusion Detection System and the Deep Packet Inspection, both relying on advanced machine learning techniques, will be used for the detection of misbehaving nodes in real-time and mitigate the verified malicious behaviour [T6.3]. Last but not least, the Cyber-Trust Blockchain (CTB) and visualisation tool will be used for the storage of material which may contain electronic evidence [T7.2; T7.3; T7.4].

The envisaged end-users are: stakeholders within the Cyber-Trust ecosystem [T5.1; T5.2; T5.3; T6.3], external entities for supervision of crawling and vulnerability assessment [T5.1], device owners [T5.3; T6.2; T6.3], smart home owners [T5.3; T6.3], Internet Service Providers [T5.3; T6.3], police authorities [T7.2; T7.3; T7.4]. In the table below, an overview is provided.

Partner **Work Package**	**UOP** **WP5**	**UOP** **WP5 (with linkage to WP6)**	**ADITESS** **WP6**	**UOP** **WP5 (with linkage to WP6)**	**CSCAN** **WP6**	**Scorechain** **WP7**	**Scorechain** **WP7**
Task	T5.1 Threat intelligence techniques	T5.2 Trust establishment and risk assessment T6.2 Device attack detector	T6.2 Device tampering detection and remediation	T5.3 Game-theoretic cyber-defence framework T6.3 Network attack detection and mitigation	T6.3 Network attack detection and mitigation	T7.2 Cyber-Trust's proposed DLT architecture T7.3 Blockchain security framework	T7.4 Blockchain forensic visualisation tool
Name of the Tool/solution/method/mechanism/system to be developed	Enriched Vulnerability Database (eVDB)	Trust management system (TMS); Device attack detector	Device Defender: for intrusion detection and malicious attacks	iIRS (intelligent Intrusion Response System)	Machine Learning Intrusion Detection System, Machine Learning Deep Packet Inspection	Cyber-Trust Blockchain (CTB)	Cyber-Trust visualisation tool
Envisaged end-user(s)	Stakeholders within the Cyber-Trust ecosystem; external entities for supervision of crawling and vulnerability assessment.	Stakeholders within the Cyber-Trust ecosystem.	Device owners	ISPs, smart home owners, device owners, and project's stakeholders.	ISPs, Device Owners, other organisations	Police authorities	

Envisaged use	For cyber-threat intelligence discovery and sharing.	For implementing trust-based risk mitigation.	For the monitoring and detection of threats and attacks on the end device. In case an attack is verified then the device agent will apply the accepted remediation policy	To estimate the overall security of a user's device or network and intelligently respond with the appropriate least intrusive mitigation actions in real-time.	To detect as first step the misbehaving nodes in real-time and as a second step will mitigate the malicious behaviour.	For the storage of material which may contain electronic evidence.

Table 2.8 - Use and End-users of the Cyber-Trust components

3. Legal and ethical concerns per Work Package

Section 3 focuses on the legal and ethical concerns expressed by the partners in the second and third part of the preliminary questionnaire, based on the regulatory framework analysis in D3.1 and D3.2. The second part of the questionnaire is relevant to the development of the tools during the research phase, whereas the third is related to the after-research use of the final prototype. Nevertheless, all the partners expressed the same or similar concerns in both stages. A few diversions may be justified by the fact that during the research phase only simulated data will be used in the processing operations, so no actual risk is imposed on data subjects. The recognition and evaluation of risks constitute a significant step in every risk-based approach. The more detailed the descriptions of the risks, the more sophisticated and efficient the mitigation strategies will be. This section opens the way for Section 4, where recommendations will be presented based upon these concerns, some more specific and some more generic.

3.1 Primary data protection and privacy concerns identified by the technical partners

Concerning the first question about concerns pertaining to data protection and privacy issues with regards to the creation of the tool based on other relevant deliverables, i.e. the D3.1, D3.2 and D2.3, the partners identified the interference with privacy, as the main concern [T5.3; T6.2; T6.3; T7.2; T7.3; T7.4]. An extensive analysis of privacy in its informational and broader sense in the Cyber-Trust context is provided in D3.1 – Part A. Two other primary concerns of the partners constitute the difficulty in assessing whether personal data will be processed [T5.1; T6.2; T6.3] and the likelihood of a personal data leakage [T5.2; T7.2; T7.3; T7.4]. Other concerns include the data filtering in order to achieve data minimisation [T6.2], the disclosure of information of sensitive character about the user´s device [T5.3; T6.3], the use of Deep Packet Inspection tools [T6.3], the access to material that may contain electronic evidence by third parties [T7.2; T7.3; T7.4] and last but not least the case-by-case assessment of proportionality [T6.2]. An overview of all those concerns can be found in the table below.

Q: Primary data protection and privacy concerns for the creation of your tool	**WP5** T5.1 Threat intelligence techniques	**WP5 (with linkage to WP6)** T5.2 Trust establishment and risk assessment T6.2 Device attack detector	**WP6** T6.2 Device tampering detection and remediation	**WP5 (with linkage to WP6)** T5.3 Game-theoretic cyber-defence framework T6.3 Network attack detection and mitigation	**WP6** T6.3 Network attack detection and mitigation	**WP7** T7.2 Cyber-Trust's proposed DLT architecture T7.3 Blockchain security framework T7.4 Blockchain forensic visualisation tool.
Possible leakage of personal data		×				×
Difficulty in assessing whether personal data will be processed	×		×		×	
Data filtering for minimisation			×			
Knowledge of possibly sensitive information about the user's devices				×		
DPI tools: view of data, if not encrypted					×	

Access to electronic evidence by external parties					✕
Interference with privacy		✕	✕	✕	✕
Assessment of proportionality		✕			

Table 3.1 - Primary concerns per Task

3.2 Major risks related to data subjects´ rights identified by the technical partners

As for all the WPs, it is to be noted that during the research phase, with the exception of T5.1, only simulated data will be used. Therefore, any risks identified by the technical partners during the research phase only relate to the development difficulties and complexities that must be overcome, as well as their preliminary assessment of each tool. The scale used for the assessment of likelihood and severity was: low, medium and high.

Concerning the Work Package 5, UoP identified risks relating to the crawling and storage of personal data [T5.1] of high likelihood but low severity; risks concerning the storage and processing of personal data and device vulnerabilities [T5.2 with linkage with T6.2] of high likelihood but low severity; and risks with regards to the intrusiveness of the mitigation actions suggested [T5.3 with linkage to T6.3] of low likelihood and low severity. UoP justified the low level of this latter risk category because the user's preferences and impact of actions on network availability are taken into account during the development phase of their tool and any mitigation actions will be applied under the minimum possible intrusiveness principle. UoP mentioned the same risks and levels of likelihood and severity both for the research stage and after the research phase.

As for the Work Package 6, ADITESS and CSCAN identified the same risks for both T6.2 and T6.3. During the research phase, the identified risks concern the confidentiality or loss of personal data. After the research and with regards to a potential deployment of the tool, the risks identified concern data minimisation, data confidentiality, data retention and privacy. The likelihood of those risks was considered as medium and the severity as high.

As for the Work Package 7, Scorechain also mentioned risks concerning the confidentiality and the loss of personal data stored in the Blockchain solution they are going to develop. Both the likelihood and severity of those risks were judged as high. An overview of the risks per task can be found below.

Partner Work Package	**UOP WP5**	**UOP WP5 (with linkage to WP6)**	**ADITESS WP6**	**UOP WP5 (with linkage to WP6)**	**CSCAN WP6**	**Scorechain WP7**
Task	T5.1 Threat intelligence techniques	T5.2 Trust establishment and risk assessment T6.2 Device attack detector	T6.2. Device tampering detection and remediation	T5.3 - Game-theoretic cyber-defence framework T6.3 - Network attack detection and mitigation	T6.3 Network attack detection and mitigation	T7.2 Cyber-Trust's proposed DLT architecture T7.3 Blockchain security framework T7.4 Blockchain forensic visualisation tool
Risks with regards to data subjects´ rights	Risks concerning the crawling and storage	Risks concerning the storage and processing	Risks concerning confidentiality or loss of personal data	A possible risk is related to the intrusiveness of the suggested action. The definition (UC-81) and	Risks concerning confidentiality or loss of personal data	Risks concerning confidentiality or loss of personal data.

	of personal data.	of personal data and device vulnerabilities.	Data minimisation, confidentiality, data retention	computation of the optimal mitigation actions (UC-78) will be chosen based on proportionality, on a case-by-case assessment and in accordance with best practices to ensure the minimum possible intrusiveness with regards to the user's privacy and personal preferences.	Data minimisation, privacy, data retention, confidentiality	
Likelihood of risks	**High**	**High**	**Medium**	**Low**	**Medium**	**High**
Severity of risks	**Low**	**Low**	**High**	**Low**	**High**	**High**

Table 3.2 - Likelihood and severity of risks

3.3 Other legal concerns identified by the partners

As for the question regarding other legal concerns, based on the legal framework analysis provided in D3.1 and D3.2, as well as some preliminary recommendations in D2.3 concerning use-cases, most of the partners identified challenges concerning the lawful collection [T6.2; T6.3] and storage of evidentiary material [T7.2; T7.3; T7.4], as well as the fragmented national framework [T5.3; T6.2; T6.3; T7.2; T7.3; T7.4]. Other concerns were expressed with regards to intellectual property [T5.1]; access rights of external entities to the vulnerabilities databases [T5.1], the collection and processing of subscribers´ data [T5.2], the proper handling of false positives [T5.2], and last but not least the implementation of appropriate safeguards for data stores pertaining to device level vulnerabilities [T5.2]. An overview can be found in the table below.

Q: Other legal concerns, based on the general legal framework explicitly described in D3.1 and D3.2, as well as recommendations included in other deliverables, e.g. D2.3.	**WP5** T5.1 Threat intelligence techniques	**WP5 (with linkage to WP6)** T5.2 Trust establishment and risk assessment T6.2 Device attack detector	**WP6** T6.2. Device tampering detection and remediation	**WP5 (with linkage to WP6)** T5.3 - Game-theoretic cyber-defence framework T6.3 - Network attack detection and mitigation	**WP6** T6.3 Network attack detection and mitigation	**WP7** T7.2 Cyber-Trust's proposed DLT architecture T7.3 Blockchain security framework T7.4 Blockchain forensic visualisation tool
Concerns about Intellectual Property	X					
Access rights of external entities to the eVDB (appropriate authorisation)	X					
Collection and processing of subscribers´ data		X				
Proper handling of false positives		X				
Lawful collection of electronic evidence			X		X	
Lawful storage of electronic evidence						X

Differences in the national law	✕	✕	✕
Appropriate safeguards for data stores with device level vulnerabilities	✕		

Table 3.3 - Other legal concerns per Task

3.4 Ethical concerns identified by the technical partners

The majority of the technical partners who filled in this preliminary questionnaire did not identify any ethical concerns with regards to their tool at this stage of the project. The only ethical concern that was identified was the likelihood of misuse [T6.3]. This possibility will be taken into consideration for the recommendations section of the present deliverable. Moreover, the Cyber-Trust consortium is benefited by the presence of an Ethics Committee, which is ready to assist the partners during the course of the project.

4. Legal and ethical recommendations per Work Package

Based on the legal and ethical concerns expressed by the technical partners, this section will focus on recommendations per Work Package and tool. Wherever preliminary risks were identified, the partners were requested additionally to provide provisional mitigation measures which they plan to consider and implement during the development phase of their tool. These propositions constitute subsection 4.1 of the present deliverable and comprise tentative guidance for the partners, as well as a ground to build upon the general and specific recommendations of subsections 4.2 and 4.3 respectively. Subsection 4.2 offers a summarised overview of the legal and ethical implications discussed in D3.1 and D3.2 in the form of more universal recommendations, whereas subsection 4.3 provides a list of recommendations per Work Package and tool. Both sets of recommendations aim to offer guidance for the overall architectural design of the Cyber-Trust platform as depicted in D4.1 and D4.2, and respectively to each component in the Work Packages 5, 6 and 7.

4.1 Mitigation measures identified by the technical partners

For all the risks identified, the technical partners were requested to determine preliminary mitigation measures. The partners referred to the following means:

- encryption serving confidentiality, integrity, availability and accountability purposes [T5.2; T6.2; T6,3; T7.2; T7.3; T7.4];
- additional measures for the preservation of data integrity [T6.2; T6.3];
- the development and implementation of security policies for the secure storage, retention and delivery of data [T6.2; T6.3];
- appropriate safeguards for the device health and vulnerability databases, including access protection measures [T5.1; T5.2; T6.2; T5.3; T6.3];
- use of anonymisation/pseudonymisation techniques [T5.1; T6.3].
- Other measures suggested by the partners are: appropriate design of cyber-threat intelligence extraction algorithms to avoid the identification of individuals and leveraging of user data [T5.1]; support predefined aggregate /low-granularity views over collected data [T5.1]; seeking the explicit consent of the user with well-designed opt-in and opt-out functions [T5.3; T6.3]; use of appropriate Privacy Enhancement Technologies [T5.3; T6.3]; putting particular emphasis on the design alternatives of the tool [T7.2; T7.3; T7.4].

Moreover, mentioned in another question, the partners highlighted that the optimal mitigation actions would be chosen based on proportionality, on a case-by-case assessment and in accordance with best practices to ensure the minimum possible intrusiveness with regards to the user's privacy and personal preferences [T5.3; T6.3]. The measures can be found also in the table below.

Q: Ways/measures to mitigate the risks previously identified	**WP5** T5.1 Threat intelligence techniques	**WP5 (with linkage to WP6)** T5.2 Trust establishment and risk assessment T6.2 Device attack detector	**WP6** T6.2. Device tampering detection and remediation	**WP5 (with linkage to WP6)** T5.3 - Game-theoretic cyber-defence framework T6.3 - Network attack detection and mitigation	**WP6** T6.3 Network attack detection and mitigation	**WP7** T7.2 CYBER-TRUST's proposed DLT architecture T7.3 Blockchain security framework T7.4 Blockchain forensic visualisation tool
Prevent leveraging/identification of individuals from the cyber-threat intelligence	✕					

extraction algorithms						
Use of anonymisation & pseudonymisation techniques	×				×	
Presentation of aggregated or low granularity data	×					
Appropriate safeguarding for device health and vulnerability databases, including access protection measures (access to trusted entities)	×	×		×		
Development of a number of security policies for the secure storage, retention and delivery of information			×		×	
Measures for the preservation of data integrity			×		×	
Seeking the explicit consent of the user with opt-in functions				×		
Use of appropriate PETs				×		
Cryptographic techniques that can ensure confidentiality, integrity, availability and accountability		×			×	×
Adoption of data protection and privacy by design techniques						×

Table 4.1 - Mitigation measures per task

4.2 General recommendations related to the Cyber-Trust project

The mitigation measures identified by the technical partners above could constitute a valid ground from where to generalise into more universal recommendations, which are also relevant for the overall architecture design, as rendered in WP4. Therefore, this Section offers a high-level overview of the recommendations provided in D3.1 and D3.2, by covering the three main pillars of interest, also in terms of a Data Protection Impact Assessment in the context of Cyber-Trust, in other words, data protection, privacy and electronic evidence, as categorised in Table 4.2, within the aim to facilitate the road ahead.

ID	Description
R01	Recommendations related to Data Protection
R02	Recommendations related to Privacy

R03	Recommendations related to Electronic Evidence

Table 4.2 - General recommendations

4.2.1 [R01] Recommendations related to Data Protection

In the Cyber-Trust project, processing activities may fall under the General Data Protection Regulation[4] or Directive 2016/680[5], depending on the end-users and the purposes of the processing. The Directive 2016/680 only applies in cases where the data controller is a "competent authority", and the processing takes place for "law enforcement purposes". Thus, it is essential to take into consideration both data protection frameworks, as well as national data retention regimes, as transposing Article 15 para 1 of the Directive 2002/58/EC (e-Privacy Directive)[6]:

1. All data processing activities of the Cyber-Trust project, including storage and processing of data in all the different databases that are going to be developed, must have a legal basis; the legal basis must be determined prior to the processing and must be documented.
2. It must be ensured that all types of processing of personal data adhere to certain processing principles, as described in D3.1, Section 5.4. The term "processing" in this context covers any operation on personal data, whether or not performed by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction:

a. The processing must be lawful (the partners have identified an appropriate lawful basis for the specific processing activity, as seen in D3.1, i.e. consent and legitimate interest, and they are not engaged in any unlawful processing); fair (the partners have taken into consideration the ways such processing may have an effect on the data subjects and can justify adverse impacts; the data subjects have a reasonable expectation about their data being processed in such way; the collection of the personal data does not take place with misleading or deceitful means); transparent (the partners comply with their obligations about the right of the data subjects to be informed);
b. The processing should have a specific, legitimate, and well-defined purpose. Further processing may take place only for additional purposes that are compatible with the initial purpose;
c. The project should ensure that the processed personal data is adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.
d. Measures must be taken to ensure that personal data is of satisfactory quality.
e. Personal data must be erased or anonymised once they are no longer needed for the purposes which they were collected for. This principle has to be taken carefully into consideration in the police sector, where national laws define different appropriate time periods for retention.
f. Appropriate technical and organisational measures should be taken so as to protect personal data against accidental, unauthorised or unlawful destruction, loss, alteration, disclosure, damage or

[4] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation) OJ L 119, 4 May 2016, pp. 1-88.

[5] Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

[6] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) OJ L 201, 31.7.2002, p. 37–47.

access. A regular review of the measures is also expected, while any personal data breaches must be notified to the national supervisory authority and in some situations, the affected data subject themselves.

g. The project should proactively demonstrate compliance with the rules of data protection law. To that end, the Cyber-Trust project shall maintain detailed documentation regarding the envisaged processing activities and carry out a DPIA prior to the deployment, and review the findings systematically.
h. The project should identify the most appropriate data protection by design and by default methods to ensure compliance.

3. The Cyber-Trust project shall clarify the status of data controllership (separate data controllers or joint data controllers, as well as data processors) of those entities in charge of the data processing operations;
4. It must also be ensured that data subjects´ rights are fully implemented, given the circumstances and the derogations at the national level. Sufficient information must be provided to the data subjects regarding the processing of any personal data by the Cyber-Trust system and notify data subjects about the deployment of the system;
5. Adequate protection must be provided when personal data, stored by the Cyber-Trust, is processed in third countries, in line with Articles 45, 46 and 49 GDPR;
6. The Cyber-Trust project should meet additional legal requirements when the processed personal data is used for law enforcement matters;
7. The Cyber-Trust project should meet additional legal requirements when the processed personal data is used in cross-border cooperation of police or judicial authorities.
8. The Cyber-Trust project should seek the views of data subjects as well as security and other experts in the field.

4.2.2 [R02] Recommendations related to Privacy

Apart from the informational privacy as understood with the terms of data protection, the notion of privacy in a broader sense is relevant for the Cyber-Trust platform. An assessment should be made in the particular context, in order to figure whether the conditions of proportionality and necessity are met and whether the usage of the tool is compliant with the specific national law in each case. The notion of proportionality and the respective proportionality test, as suggested in the case law of the European Court of Human Rights (ECtHR), provide a way of judging when such interferences with privacy may be acceptable or not. Internet research ethics, as well as computer ethics, could form a point of reference for areas which are still underdefined in law, during the research phase of the project.

4.2.2.1 Necessity

1. The Cyber-Trust components, in particular, those with regards to the detection and mitigation of cyberattacks should be capable of use in a range of various situations where the use of cybersecurity systems could be considered necessary.

4.2.2.2 Proportionality

1. The Cyber-Trust components should be as privacy friendly as possible, by implementing Privacy Enhancement Technologies.
2. The Cyber-Trust, where possible, in particular with regards to its attack detection and mitigation tools, should be able to adjust their level of privacy protection depending upon the circumstances in which it is to be deployed, taking into account the possibility that the collected data may indirectly or directly identify particular individuals.

3. The Cyber-Trust components should be capable of only capturing data where such information is related to the specific cyberattack in question.
4. Any incidental capturing of data that might constitute personal data or relate to the private or family life of the users, if not related to the purpose of the system components, should be deleted as soon as possible.
5. End-users should be able to configure the components of the Cyber-Trust platform in a relatively easy way to safeguard that their use would be proportional to a particular situation.

4.2.3 [R03] Recommendations related to electronic evidence

The material collected during the attack detection and mitigation phase may contain electronic evidence. This material will be stored off-chain and on-chain in the Cyber-Trust platform. Due to the novel character of the technical solution used and the fragmented legal framework, as seen in D3.2 as well as in Annex C of the present Deliverable, the following recommendations must be taken into account, in order for the material to have a better chance to be admissible in the legal proceedings:

1. The Cyber-Trust components for the collection of material that may contain electronic evidence should be only used where deployment has been approved as prescribed by the law.
2. The material collected by the Cyber-Trust platform must be collected and stored with the use of processes which are verifiable, repeatable and capable of explanation. All evidence and processes applied thereto should be capable of transparent disclosure to both defendants and the court.
3. In other words, the collection and preservation of the material should follow well-established principles in digital forensics. Since there is no comprehensive international or European framework, it is recommended to follow the principles introduced in the Council of Europe Electronic Evidence Guide[7] and the ENISA´s Handbooks concerning Digital Forensics[8] concerning the proper handling of electronic evidence, which comprise the fundamental common principles found in the vast majority of national legislations.
4. It should be possible to log and demonstrate any processes that have been applied to the collection and storage of the material that may contain electronic evidence, as well as to establish who has been in possession of the material in question from the very first moment of its collection until its presentation before the Court of Law.
5. The national evidence and electronic evidence law should be taken into consideration, including laws about data retention, cyber-threat intelligence gathering and sharing.
6. During the design of the CTB and the visualisation tool, the different cooperation channels of cross-border access to electronic evidence should be taken into account, in particular, with regards to the direct cooperation between law enforcement authorities and service providers, either on a voluntary or mandatory basis.

[7] See: Council of Europe, Electronic Evidence Guide, A basic guide for police officers, prosecutors and judges, Strasbourg, 15 December 2014.

[8] See: European Union Agency for Network and Information Security (ENISA), Identification and handling of electronic evidence –Handbook, document for teachers, September 2013; ENISA, Electronic evidence - a basic guide for First Responders Good practice material for CERT first responders, 2014; ENISA, Forensic analysis – Local Incident Response Handbook, Document for teachers, December 2016; ENISA, Network Forensics Handbook, Document for teachers, February 2015.

4.3 Recommendations per Work Package

The specific recommendations presented in this Section, particularise the general recommendations described in the subsection above. The specific recommendations are also developed with reference to legal and ethical dimensions discussed per use case in D2.3.

4.3.1 Recommendations related to Work Package 5

The T5.1 refers to the development of a cyber-threat discovery mechanism and of a vulnerabilities database (eVDB) for sharing cyber-threat related information to other components and modules in the Cyber-Trust platform. Further considerations on this component can be found in D3.1.

1. The data processed by the web crawler should be only manifestly public data. The partners should avoid crawling restricted areas of a website [R01; R02].
2. If no personal data is processed, the web crawler processing will not fall under the scope of GDPR. In the opposite occasion, the processing would fall under the scope of GDPR, and a legal ground for the processing should exist [R01].
3. The technical partners should consider the use of privacy-preserving crawling methods [R01; R02].
4. The web crawling should only occur with the right authorisation. The crawling of a specific source should be avoided, or proper license or permission should be asked from the lawful rightsholder, if the crawling in question [R01; R02]:
    a. is explicitly forbidden (for instance, expressly stated in the respective Terms and Conditions);
    b. concerns content which is protected under intellectual property rights; or
    c. is subject to unclear or dubious conditions.
5. The rules pertaining to the clear web are also, in principle, applicable to the deep and dark web [R01; R02].
6. If possible, the partners should follow identified good practice and codes of ethics in web-scraping, for instance, be transparent about your web-scraping operations and inform the website owners, when massive amounts of data are scraped [R01; R02].[9]
7. Only anonymised data should be stored in the eVDB, which must be kept up-to-date and accurate, in order to eliminate the possibility for false positives which may have adversarial effects on the rights of individuals [R01; R02].

The T5.2 refers to the computation of trust scores for devices, while the T6.2 refers to measuring device health, by determining potential or existing vulnerabilities. The T5.3 with linkage to T6.3 refers to a multitude of modules responsible for the interactions among different systems and the cyber-defence service, the real-time security state belief computation module and the computation of optimal cyber defence actions.

1. The optimal solutions selected must always be proportional and necessary for the purpose pursued. The purpose, in turn, must be legitimate. The least intrusive alternatives should always be preferred [R01; R02].
2. The need for human intervention before the implementation of a mitigation measure should always be assessed, in particular, when the function of a mission or life-critical device may be affected [R01].
3. The tools should be only activated when criminal activity is more likely to have occurred, also taking into account the different degrees of severity, potential impact and the likelihood of false positives [R01; R02].

[9] Eurostat and ESSnet Big Data, Netiquette - Deliverable 2.1 Legal aspects related to Web scraping of Enterprise Web Sites, December 2016, p. 20.

4. When third-party tools are used, it should be ensured that they are compliant with the applicable legal framework and carry adequate safeguards concerning the data subjects´ rights and freedoms [T5.3; T6.3] [R01; R02].

4.3.2 Recommendations related to Work Package 6

The aim of T6.2 is the creation of a tool for the prevention of a cyber-attack on Cyber-Trust monitored IoT devices, whereas the role of the component envisaged in T6.3 is to detect and mitigate attacks targeting at network infrastructures, with a focus on malicious botnets. Both tasks and their respective tools perform tracking, monitoring and collection of data, the amount of which depends on the user´s preferences, based on a number of available tracking as well as custom tools.

1. There should always be a legal basis for the collection and processing of personal data via the use of those tools [R01].
2. If the legal ground used is consent, then the data controllers must seek the express consent of the data subject during their registration to the platform, for each category of data and each processing activity. The consent form must be in an intelligible and easily accessible form, in clear and understandable language, without complex technical jargon [R01].
3. Under the same conditions as above, the individual users must be provided with information about how their data are going to be collected, used and processed, as well as their rights and relevant risks and implications [R01].
4. Where the user has consented to the processing of special categories of data, for instance, location data, the processing must be clearly indicated on the interface [R01].
5. Data protection and privacy must be guaranteed by design (every component must be built with data protection and privacy in mind) and by default (the strictest privacy settings must be the default option) [R01; R02].
6. The individual users must have full control over their data, by being able to specifically choose which devices and under what conditions will be monitored, by opting in. In other words, the users should be able to choose from different degrees of opt-in, depending on the different features they wish to activate. The minimum features must be accessible with the minimum degree of opt-in [R01; R02].
7. The users should also be able to access the privacy settings easily during and after their registration to the platform and be invited to review the default settings once starting using the platform [R01; R02].
8. The user must be asked to reconfirm her consent after a long period of use [R01].
9. If a legitimate interest is the chosen legal basis (either Cyber-Trust´s interest or a third party´s interest), then three elements must be taken into consideration (Legitimate Interest Assessment) and reviewed regularly [R01]:
    a. Purpose test: a legitimate interest must be identified;
    b. Necessity test: it should be proven that the processing is necessary to achieve the legitmate interest in question and there is no other reasonable way;
    c. Balancing test: the legitimate interest must be balanced against the individual's interests, rights and freedoms.
10. Monitoring should never be excessive, and thus, it should be ensured that only the most relevant data are collected and processed based on the principle of data minimisation and only the most appropriate and reasonable techniques are used, based on the principle of proportionality, serving a legitimate purpose [R01; R02].

11. It should be kept in mind that anonymised data fall out of the scope of the data protection legislation, but data subjects may still be entitled to protection, for example, under the confidentiality of their communications [R01; R02].
12. Given the possibility of misuse of such a system, security safeguards must be put in place and strict access mechanisms must be adopted [R01; R02; R03].
13. It should be ensured that only authorised entities have access to the monitoring and mitigation tools as well as the visualisation interfaces [R01; R02; R03].
14. Given that the terminal equipment of a user of electronic communications networks and any information stored on such equipment are part of the private sphere of the users, before the deployment of a device agent on the terminal equipment of any individual user, the user should be informed in detail about the characteristics of the agent, the data that will be collected, the time period of the data retention and consent must be requested [R01; R02].

4.3.3 Recommendations related to Work Package 7

The aim of T7.3 is to create a secure tool (CTB) based on the most appropriate DLT structure as analysed in T7.2, which will be used to store data collected by the Cyber-Trust platform in previous steps, such as metadata relating to material that may contain electronic evidence and Trusted Logs. The goal of T7.4 is to develop a Blockchain forensic visualisation tool for the exploration of the information stored in the CTB and it is dependent on the latter.

If data related to an identified or identifiable individual, such as IP addresses, are stored in the blocks, no matter whether these data are stored in plain text, in an encrypted form or as hashes, the CTB would be under the GDPR scope, because these data still qualify as personal, as explicitly discussed in D3.1 and D3.2.

1. Only authorised entities should have access to the metadata stored in the CTB, the visualisation tool and the off-chain database where the actual material is kept [R03; R01].
2. Given the current legal literature, it should be avoided to store any personal data on the CTB, because the tool would have fewer chances to be compliant with the current legal framework. Alternatively. the use of mere hashes, which point to actual data stored on an off-chain conventional database would be recommended. If a new database is going to be created, a legal basis for the off-chain database would have to be established [R01].
3. The data stored on the CTB and the off-chain database should be safeguarded against internal or external security threats, due to the potential sensitive character of the data they hold [R01].
4. The CTB and the off-chain solution accompanying it should follow the common principles with regards to the storage of electronic evidence, as described in D3.2 [R03].
5. A private and permissioned solution for the CTB seems favourable in this context [R03].
6. The status of the participants in the CTB must be clarified well in advance [R03].

5. The methodology of the Data Protection Impact Assessment

Having seen the preliminary assessment of the processing components, the potential risks and mitigation measures identified by the technical partners, as well as the recommendations drafted by the legal expert of the project, this section will shed light to the approach to be followed concerning the Data Protection Impact Assessment (DPIA) foreseen to be carried out in line with the requirements of Article 35 GDPR during the design and development phase of the project and its findings to be published in the D3.4 and D3.5. Subsection 5.1 will provide the general introduction to a DPIA and its main characteristics delineated after years of risk management in the field of privacy and data protection and on the basis of the Article 29 Working Party guidelines on the matter. The latter guidelines also set the minimum criteria such an assessment must take

into account, as explained in 5.2. In the next subsection, the attention turns upon Cyber-Trust, and a set of indicative questions is introduced in 5.4 to facilitate the partners to carry out an effective DPIA for every technical element they develop, with the guidance of the legal expert of the project.

5.1 Introduction to Data Protection Impact Assessment (DPIA)

Risk management is a well-known notion in the field of data protection worldwide, as a tool that assists data controllers to ensure proper handling of personal data and effective protection of the fundamental rights of the data subjects.[10] Risk management has been a legal requirement in many jurisdictions with regards to data protection for many years.[11] Nevertheless, despite general agreement among some assessment criteria, such as harm caused by security breaches, financial harm and societal impacts, the elements of an impact assessment may vary considerably from field to field. The reasoning behind those variations is explained by the objectives the risk management aims to fulfil. As stated in Kuner et al. (2015), "the goal of risk management is not to eliminate risk, but to reduce the risk as fully as practical".[12] Apart from that, risk management must facilitate data controllers identify explicitly potential or existing risks as well as determine and implement appropriate mitigation measures and instances where the balancing of competing interests is necessary.[13]

After the entry into force of the General Data Protection Regulation in 2018, the carrying out of a Data Protection Impact Assessment (DPIA) is only mandatory for the controller pursuant to Article 35 (1) GDPR where processing is "likely to result in a high risk to the rights and freedoms of natural persons" and it is very important in particular when a new data processing technology is being introduced. Paragraph 3 of Article 35 GDPR provides a non-exhaustive list for what is likely to result in a high risk. Further guidance can be found in the Article 29 Working Party Guidelines on Data Protection Impact Assessment,[14] as endorsed by the European Data Protection Board.[15] In most cases, a data controller can consider whether a processing meeting one or two cumulative criteria would require a DPIA to be carried out. If in doubt about whether a DPIA is mandatory or not, it is advisable always to carry out a DPIA, if such an assessment can promote compliance with data protection obligations. However, it is to be noted that the more criteria are met, the more likely is that the processing or the technological product in question may present a high risk to the rights and freedoms of data subjects and therefore, require a DPIA, regardless the envisaged mitigation measures.[16] Since the criteria list is non-exhaustive, in accordance with Article 35 paragraph 4, national supervisory authorities have introduced lists with processing operations which require a DPIA and which do not.

A DPIA may concern a single data processing operation or multiple.[17] Nevertheless, in any case, the DPIA should be carried out "prior to the processing" (Articles 35(1) and 35(10), recitals 90 and 93). If the same DPIA is applicable to similar processing conducted by various data controllers, then a reference DPIA should be shared among them, and a justification for a common DPIA must be given.[18] Should joint controllers

[10] Kuner, C. et al (2015), Risk management in data protection, in: International Data Privacy Law, Vol. 5, No. 2, p.95.
[11] Idem.
[12] Ibid, p.97.
[13] Idem.
[14] Article 29 Working Party, Guidelines on Data Protection Impact Assessment and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 (WP 248 rev. 01).
[15] European Data Protection Board, Endorsement 1/2018.
[16] Article 29 Working Party, Guidelines on Data Protection Impact Assessment and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 (WP 248 rev. 01), p.11.
[17] Ibid, p.7.
[18] Ibid, p.8 and p.13.

undertake processing activities, they should determine their respective obligations precisely and designate which partner is responsible for what type of processing activity. The aim is to share useful information, without disclosing business secrets or vulnerabilities.[19] The controllers must also seek advice from the designated Data Protection Officers (DPOs), if necessary.

As read above, the data controllers should conduct a DPIA "prior to the processing", so as for the appropriate data protection by design and by default measures to be chosen and compliance solutions to be implemented (Article 25 and recital 78). Therefore, a DPIA methodology should be decided upon at an early stage, and the assessment process should start as early as possible in the design phase. Since carrying out a DPIA is a "continuous process and not a one-time exercise", the DPIA should be kept up-to-date throughout the project and take into consideration any alterations that occurred.[20] Although it is not obligatory for a data controller to publish a DPIA, it is considered a good practice to do so. However, a summary of the main findings of the assessment or even just a statement that a DPIA took place, may be sufficient to foster trust and demonstrate transparency and accountability.[21]

5.2 The minimum features of a Data Protection Impact Assessment

The methodology chosen by the data controller must be in line with the criteria identified in Annex 2 of the aforementioned guidelines.[22] The minimum features of a DPIA are set in Article 35 para 7 as well as recitals 84 and 90 and include:[23] "a description of the envisaged processing operations and the purposes of the processing"; "an assessment of the necessity and proportionality of the processing"; "an assessment of the risks to the rights and freedoms of data subjects"; and "the measures envisaged to address the risks and demonstrate compliance with this Regulation". Each of these blocks of requirements will be analysed separately in the next subsections.

5.2.1 Description of the envisaged processing operations and the purposes of the processing

According to Article 35(7)(a) GDPR, the partners should provide a systematic description of the processing activities concerning the nature, the scope, the context and its purposes. The description should also include information about the personal data, recipients and period for which the personal data are recorded, a description of the processing operation, the assets on which personal data rely (hardware, software, networks, persons, paper or transmission channels) are identified. Compliance with approved codes of conduct, if any, will also be taken into account (Article 35(8)).

5.2.2 Assessment of the necessity and proportionality of the processing

The necessity and proportionality of the processing are assessed taking into consideration the measures envisaged to comply with the GDPR (Article 35(7)(d) and recital 90). At the first stage, compliance with the data protection principles and the full enforcement of data subjects´ rights will be checked. The data controllers will be called to demonstrate that the processing takes place for specified, explicit and legitimate purpose(s) (Article 5(1)(b)); it is lawful (Article 6); the data processed are adequate, relevant and limited to what is necessary (Article 5(1)(c)) and are processed not further than the necessary time period (Article 5(1)(e)). At the second stage, the partners will have to explain the measures they have in place for the enforcement of data subjects rights: information provided to the data subject (Articles 12, 13 and 14); the

[19] Idem.
[20] Ibid, p.14.
[21] Ibid, p.18.
[22] Ibid.
[23] Ibid, p.16.

right of access and to data portability (Articles 15 and 20); the right to rectification and to erasure (Articles 16, 17 and 19); the right to object and to restriction of processing (Articles 18, 19 and 21). For the effective enforcement of data subjects´ rights, data controllers may have to clarify their relations with data processors (Article 28) or other joint controllers, safeguards surrounding international transfer(s) and wherever necessary, the reasons that they proceeded or not with a prior consultation (Article 36).

5.2.3 Assessment of the risks to the rights and freedoms of data subjects

In order to assess the risks with regards to the rights and freedoms of data subjects (Article 35(7)(c)), the data controllers would have to take into consideration the sources and nature of the risks as well as their likelihood and severity (recital 84 and 90), from a data subject´s perspective. In particular, potential threats and impacts to the rights and freedoms of data subjects should be identified and weighed, in particular in relation to illegitimate access, undesired modification and disappearance of data.

5.2.4 Envisaged and implemented measures

Given that risks were identified and assessed, the data controllers should determine measures envisaged to treat those risks (Article 35(7)(d) and recital 90). Wherever the advice of the DPO is or has been sought (Article 35(2)) as well as the views of data subjects or their representatives are or have been seeked (Article 35(9)), the relevant information should also be included in the DPIA. Moreover, the DPO, the data processors, the appointed Information Security Officers and other independent experts may assist with the drafting of the DPIA. However, in all the cases, it is the controller who remains accountable for the task to carry out a DPIA and ensure compliance.[24]

5.3 Data Protection Impact Assessment in the Cyber-Trust context

In the case of Cyber-Trust, a DPIA is intended to assess the data protection impact of a technological product, since this product is meant to be used by different data controllers who will conduct different processing operations.[25] The data controller who deploys later on the product will have to pursue its own DPIA, as new technologies may have been introduced by then, the societal context of the data processing may have evolved, or the processing purpose may have changed.[26] As a matter of good practice, “a DPIA should be continuously reviewed and regularly re-assessed”.[27] This is the reasoning and motivation behind the two DPIAs, which are planned in the context of Cyber-Trust; one right after the creation of the rapid prototype in WP4 and another one at the end of the development phase, in particular taking into account the rather fast evolving relevant legal framework.

Thus, a DPIA in the Cyber-Trust context includes a number of steps which have their roots in work conducted in all the deliverables of the WP3. First of all, it is important to assess which activities will require an impact assessment. In the case of Cyber-Trust, it is the launch of the Cyber-Trust platform with most of its components and operations that will fall under the need for an assessment, as discussed in D3.1. Second, it is imperative to outline the legal framework, the principles and the requirements in order to set the scope of the DPIA. The legal framework analysis took place in D3.1 and D3.2. After the first and the second step have been established, the third step - the actual assessment of the impact of the processing activities will take place, which will lead to the fourth step, the evaluation of the findings. The latter step will, in turn, assist with any relevant decision-making during the designing of the platform in WP4 (D3.4). The fifth and final step will be concluded with the monitoring and review of the processing activities will which occur in the D3.5, after the actual development of the individual components in WP5, 6 and 7.

[24] Ibid, p.15.
[25] Ibid, p.8 and p.13.
[26] Idem.
[27] Ibid, p.14.

In the present deliverable, the methodology for the DPIA of D3.4 and D3.5 will be provided, based on the preliminary contributions of the technical partners. Since the findings of the DPIA will not be available before June 2019 and in parallel the platform components will be developed, evolved and changed continuously as well as relevant aspects of the legal framework might be reformed during the course of the project, the questionnaires which will be actually used for the assessment may be revised and adjusted to fit the specific urgencies and new circumstances that may arise. Therefore, the questionnaires include an indicative list of questions, tailored for the components of the Cyber-Trust platform under assessment, based on the Article 29 Working Party Guidelines enriched with elements of the sample templates as proposed by national supervisory authorities,[28] expert groups[29] and legal scholars[30] The partners involved in the development of those components (WP5, 6 and 7) as well as the overall design of the project (WP4), using also as guidance the preliminary findings of this deliverable and the preparatory exercise, are expected to carry out, to the best of their ability and knowledge, the DPIA by providing as specific as possible replies to the questions. The ultimate goal is to ensure that they take into account the implementation of the legal and ethical recommendations found in the present deliverable, as well as in D3.1 and D3.2.

If the features of the component change in a way that may have an impact on the legal and ethical requirements identified, then the partner in charge should carry out the same process, irrespectively of whether the changes are minor or major. The legal expert of the Cyber-Trust project shall attempt to describe the reasoning behind the DPIA, including its methodology and final results, liabilities and possible consequences. The information provided will be collated in two consecutive evaluation reports (D3.4 and D3.5). The evaluation reports will also disseminate information with regards to the platform architecture and its overall evaluation, by highlighting the efforts that have been made in meeting the criteria in question up to that point, identifying good practices and calling for further action in consultation with the partners concerned, whenever necessary.

5.4 Indicative questionnaires for the DPIA

Except for the minimum requirements described in 5.1, for an impact assessment to be effective, strong cooperation, continuous communication and mutual understanding among the involved parties are essential elements, in particular when a high-complex, novel solution is being developed as is the case of the Cyber-Trust. Thus, the active participation of every partner and member of the wider consortium, wherever necessary, is of paramount importance, since it should not only be seen as a legal requirement but also as an opportunity to confirm that all the partners are on the same page. A full assessment cannot be carried out without the full picture of the processing operations and the involvement of each party and therefore, the partners are first asked to provide a technical description in an intelligible and plain language of the various Cyber-Trust components which relate to the processing of personal information, their functionality, necessity and interdependencies.

The next questionnaires focus more on the requirements pertaining to data protection and in specific, the scope, nature, purposes and context of the data processing activities, the clarification of the role,

[28] See: Information Commissioner´s Office, Sample DPIA Template, 9 February 2018, v0.3. See also: CNIL, Privacy Impact Assessment Templates, February 2018.

[29] Kloza, D. et al. (2017), Data protection impact assessments in the European Union: complementing the new legal framework towards more robust protection of individuals, d.pia.lab Policy Brief No. 1/2017, Brussels Laboratory for Data Protection & Privacy Impact Assessments (d.pia.lab). See also: Smart Grid Task Force 2012-14, Expert Group 2: Regulatory Recommendations for Privacy, Data Protection and Cyber-Security in the Smart Grid Environment, Data Protection Impact Assessment Template for Smart Grid and Smart Metering systems, 13 September 2018.

[30] See: ALLADIN project, D3.3 – Framework for Impact Assessment Against SoEL Requirements, May 2018. See also: FORENSOR project, Framework for impact assessment of Forensor against DAPPECL requirements, May 2016.

obligations and relations of data controllers and data processors, the data subjects and their rights, the identification of risks and respective mitigation measures as well as any relevant criminal law dimensions. The first column of the proposed template mentions who is expected to give input, whereas the second column includes the question and the respective reasoning, which serves a two-fold goal: first to justify the necessity and importance of the question and second to give some context to the parties filling in the questionnaire. Most of the fields to be-filled in are free text, and only very few are restricted or include scales. The parties should try to answer indicating where efforts have been made towards a specific direction or based on their expertise and know-how in the field. Moreover, it is to be noted that once the D4.1 concerning the system architecture is finalised and the development of each tool moves forward, these indicative questionnaires, which now cover the whole scope of the Cyber-Trust platform, will be further adjusted to each specific component, taking into account its position in the platform. Below follow the indicative DPIA templates.

5.4.1 Technical description of the Cyber-Trust components

Relevant to Partner(s)	Required input
All technical partners	**Question 1: Please provide the name and a brief overview of the component of the Cyber-Trust platform you are developing (including a reference to the relevant Task and the Common Asset-Class Actors).** *Reason: Such a description would help persons with non-technical knowledge to better grasp and understand the Cyber-Trust system, its functionalities and its interdependencies. The more elaborated the description is, the more effectively and sufficiently the tool and the platform in their entirety can be assessed.*
	Input:
All technical partners	**Question 2: What is the functionality of this component?** *Reason: The description of the aims a component attempts to fulfil would contribute to the understanding of its role in the Cyber-Trust system.*
	Input:
All technical Partners, CGI	**Question 3: Why and how is this component necessary in the Cyber-Trust platform? Would it be possible to replace it with another component?** *Reason: The assessment of the necessity of a component can clarify its role and implementation in the overall system.*
	Input:
All technical Partners, CGI	**Question 4: Which are the interdependencies (input and output) of this component with regards to other components? How does the component contribute to the entire system?** *Reason: For the assessment of the system, it is important to understand the position of each component in the system and its connection to other components.*
	Input:

All technical partners, CGI	**Question 5: What are the costs of the deployment of the element? Is a cheaper solution with the same effectiveness available at present?** *Reason: The cost effectiveness should be taken into consideration at an early stage.*
	Input:
All technical partners	**Question 6: Please mention the tool(s)/method(s) you are using/you have used for the development of the specific component.** *Reason: Disclosing, where possible, the tools and methods used contributes to transparency and may assist with understanding the logic involved in the creation of each component. Moreover, it is important to acknowledge third-party services*
	Input:
All technical partners	**Question 7: Based on the Deliverable 2.3, please mention here the use-cases (number and title) which correspond to the specific component you are developing.** *Reason: The indication of the relevant use-cases, where a component plays an indispensable role, will improve the understanding concerning the envisaged use of the component. Categorise the use-cases as follows: use-cases of indirect relevance (the use-cases cannot exist without the component) and use-cases of direct relevance (the component cannot exist without the use-cases).*
	Input:
All technical partners	**Question 8: Please add here additional comments, if any. Here you can also add relevant diagrams or graphs, if you consider them necessary.** *Reason: Tailor-made assessments should include a space for additional comments. This way the partners can add any further information which they consider important for the full understanding of the component.*
	Input:

5.4.2 Requirements related to Data Protection

5.4.2.1 Scope of processing

Relevant to Partner(s)	Required input
All partners	**Question 1: What is the nature of the data that will be collected? Are the partners able to identify a natural person based on the collected data (as such or combined with other data)?** *Reason: Data which relate to an identified or identifiable natural person are personal data. In that case, data protection law becomes applicable.*
	Input:
All partners	**Question 2: Will any personal data be collected during the use-cases? If so, please describe the type of data for each use case (not only the data actor as described in D2.3 but in detail the data that will be collected, for instance: subscriber name, IP addresses, etc.).** *Reason: Same as in Q1.*

	Input:
All partners	**Question 3: If the processing operation includes the processing of personal data, will you process special categories of personal data ("sensitive data")?** *Reason: Special categories of data, such as health data, fall under the scope of stricter rules as their processing may result in a higher risk to the rights and freedoms of the data subjects. For instance, it may lead to discrimination against them.*
	Input:
All partners	**Question 4: If the processing of personal data occurs, would you be able to estimate the amount of processed data, the number of data subjects involved and the geographical area covered?** *Reason: A larger number of processed personal data and data subjects would mean higher severity of impact in case of a data breach. The same if a bigger geographical area is affected.*
	Input:
All partners	**Question 5: If the processing of personal data occurs, how frequently will the data be collected?** *Reason: More frequent collection entails a larger number of data and higher severity of impact in case of a data breach.*
	Input:
All partners	**Question 6: If the processing of personal data occurs, how long will you store the data? What will happen with the personal data afterwards [art.5 GDPR]?** *Reason: The data should be kept no longer than the period necessary for the purposes pursued.*
	Input:

5.4.2.2 Data controller(s) and data processor(s)

Relevant to Partner(s)	Required input
All partners and the Project Coordinator	**Question 7: Who is in charge of the processed personal data and who decides how the data will be used [art.24 GDPR]? Who determines the purposes and the means of the processing operation(s)? Please indicate the full contact details of the data controller(s) or joint controllers [art.27 GDPR].** *Reason: The controller is held accountable for the processing operation. The determination of the data controller is also of paramount importance for the effective enforcement of the data subjects´ rights. Thus, the roles and responsibilities of the controller(s) and processor(s) should be clarified.*
	Input:

All partners	**Question 8: If the processing of personal data occurs, will you hire a data processor? If yes, please provide a justification of this decision and include full contact details, information about the implemented technology, and if applicable, the data processing contract [art.28-29 GDPR].** *Reason: The data processor processes data on behalf of the data controller. The role of data processors should be explicitly discussed in terms of a contract, which ensures that processing will be carried out in line with the controller´s instructions and the applicable data protection law.*
	Input:
The project coordinator (KEMEA)	**Question 9: Would an organisational change (either in the consortium or internally, in a partner´s organisation) affect the processing of personal data in any sort of way?** *Reason: Appropriate safeguards must be put in place to ensure that internal changes will not have an effect on data processing.*
	Input:
End-users	**Question 10: Will any personal data be transferred to third countries? If yes, does the third country provide adequate protection? What is the legal ground of the transfer and how will you safeguard such transfers [art.44-49 GDPR]?** *Reason: Given the cross-border character of cyberattacks, the Cyber-Trust system might collect data which will be necessary for any form of international cooperation (for instance police or judicial cooperation, through voluntary assistance).*
	Input:
All partners, End-users, experts	**Question 11: How do you demonstrate compliance with data protection law, including the measures that you take in order to ensure that the data processors also comply? Do you or/and the data processor(s) have appointed a DPO [art.37 GDPR] or/and did you conduct a DPIA [art.35 GDPR]? Do you adhere to any approved Code of Conduct [art.40 GDPR] or a certification scheme [art.42 GDPR]?** *Reason: The principle of accountability is a cornerstone in GDPR. The data controller must proactively demonstrate compliance with data protection law.*
	Input:
All partners, End-users	**Question 12: What security measures do you implement in order to ensure data security and integrity [art. 32 GDPR]?** *Reason: Appropriate technical and organisational measures should be put in place to guarantee a suitable level of security.*
	Input:
All partners	**Question 13: What Privacy Enhancing Technologies (PETs) are used? What Data Protection by Design and by Default techniques are implemented [art.25 GDPR]?** *Reason: The data controllers must have in place a system of ICT measures which eliminate or minimise personal data, thereby preventing unnecessary or unauthorised processing, for instance, encryption or anonymisation.*
	Input:

All partners, End-users	**Question 14: If processing of personal data occurs, is the access to the personal data restricted? What are the rules of access (with special attention to its conditions, mode, and limits) [art.5 GDPR]?** *Reason: The details of processing operations should be clarified and documented (via, e.g. logs, permissions).*
	Input:

5.4.2.3 Nature, purposes and context of data processing

Relevant to Partner(s)	Required input
All partners	**Question 15: Please describe the data processing, with special attention to the method and the tools to be used. Be specific about the source of the data and the ways you will collect, use, store and delete them, in relation to the Cyber-Trust components as described in the section above concerning the technical description of the project [art.35 GDPR].** *Reason: The systematic description of the envisaged data processing operation is a minimum requirement for a DPIA and a crucial element for any further analysis.*
	Input:
All partners, VUB, DPOs End-users	**Question 16: What is your lawful basis for processing [art.6 GDPR]?** *Reason: Every personal data processing activity under the GDPR must have a legal basis.*
	Input:
All partners, VUB, End-users	**Question 17: Where the processing is based on consent, will it be possible to demonstrate that the data subject has consented to the processing of his or her personal data [art.7 GDPR]?** *Reason: This condition is of utmost importance for the accountability of the data controller as well as the assessment of whether consent was given under the necessary conditions (freely given, specific, informed).*
	Input:
All partners, DPOs and End-users	**Question 18: If processing personal data, what is the purpose of that? What are the expected benefits of the processing for you, as a data controller, and more broadly? [art.5 GDPR]** *Reason: The processing of personal data shall be conducted for fulfilling specified purposes.*
	Input:
	Question 19: Does the processing actually achieve your purpose? Is there another way to achieve the same outcome?

All partners, End-users	*Reason: The question is about necessity and proportionality. The processing must be necessary and proportional for the intended purpose.*
	Input:
All partners	**Question 20: What types of processing identified as likely high risk are involved?** *Reason: Since the GDPR requires the data controller to perform a DPIA for this type of processing activities.*
	Input:
All partners, End-users	**Question 21: What is the nature of your relationship with the individuals whose personal data will be collected? Would they have a reasonable expectation that their data are used this way?** *Reason: In order for some legal grounds to be applicable and the data subjects to be able to enforce their rights and freedoms fully, it is important that the data subjects have a reasonable expectation that their data are processed.*
	Input:
All partners, End-users, experts	**Question 22: Is the processing activity novel in any way? Are there prior concerns over this type of processing or any known security flaws?** *Reason: Compliance of a novel processing activity may be challenging. Therefore, assessing a technological application in its infancy may require the input of external experts.*
	Input:
All partners, End-users	**Question 23: How do you document your processing operations? Who has access to this documentation and up to what extent?** *Reason: Record-keeping and appropriate documentation may improve the process for the identification of risks both for the controller and the supervisory authority. However, unauthorised access to this documentation may pose security risks.*
	Input:

5.4.2.4 Data subjects

Relevant to Partner(s)	Required input
All partners, End-users	**Question 24: If processing personal data, how do you ensure that data subjects can exercise their rights? Please answer from the perspective of both research conducted during the Cyber-Trust project (i.e. stakeholders consultation and use-cases) and the use of the Cyber-Trust system in normal operating circumstances.** *Reason: Proper documentation should be kept and a platform of communication where data subjects can practice their rights should be established.*

	Input: **The data controller provided information to the data subject [art.13-14 GDPR]. Please describe methods to be used to provide information to the data subjects, including content and communication platform.**
	Is the right of access by the data subject guaranteed, and how? [art.15 GDPR]
	Is the right to rectification guaranteed, and how? [art.16 GDPR]
	Is the right to erasure guaranteed, and how? [art.17 GDPR]
	Is the right to restriction of processing guaranteed, and how? [art.18 GDPR]
	Is the right of data portability guaranteed, and how? [art.20 GDPR]
	Is the right to object to processing guaranteed, and how? [art.21 GDPR]
	If applicable, is the right to object to a decision based solely on automated processing, including profiling, guaranteed, and how? [art.22 GDPR]
All partners, End-users	**Question 25: Have you adopted or will you adopt procedures for dealing with data breaches and notification of breaches to the national supervisory authority or to the affected individuals, if applicable [art.33-34 GDPR]?** *Reason: The data controller is responsible, for reasons of transparency and accountability, to establish communication and notification procedures of a data breach, depending on its scale.*
	Input:
All partners, End-users	**Question 26: If processing personal data, how will the collected data meet the requirements of data quality (accuracy, integrity, up-to-date) and data minimisation (adequacy, relevance and storage limitation)? How do you ensure that data will remain accurate when disclosing it to third parties? [art.5 GDPR]** *Reason: The processed data should be relevant and accurate. The Cyber-Trust system should only collect those types of personal data which are necessary to reach the goal of the processing; furthermore, the processed data must be accurate and kept up to date.*
	Input:
All partners	**Question 27: If processing personal data, are data subjects involved in the development phase and if yes, to what extent?**

	Reason: The involvement of data subjects during the development phase could help with the identification of potential risks.
	Input:
All partners, End-users, experts	**Question 28: How do you plan to collect the views of stakeholders?** *Reason: Feedback can be collected in different ways, for instance, via an online platform, questionnaires, interviews, etc.*
	Input:

5.4.2.5 Identification of risks and mitigation measures

Relevant to Partner(s)	Required input
All partners	**Question 29: Describe the sources of potential risk and the nature of the potential impact on individuals.** *Reason: Proper documentation of potential risks can help better understand and assess the impact on individuals and integrate proactive mitigation measures into the project plan.*
	Source:
	The likelihood of harm: remote, possible or probable
	The severity of harm: minimal, significant or severe
	The overall risk: low, medium or high
All partners	**Question 30: Identify envisaged measures to reduce or eliminate the risks depicted as medium or high in the previous question.** *Reason: Proper documentation of the additional measures can help the data controller identify whether there is a need to seek the advice of the DPO or consult with the supervisory authority (accepted residual risk).*
	Risk (Illegitimate access to data; Unwanted change of data; Disappearance of data):
	Options to reduce or eliminate risk:
	Effect on risk: eliminated, reduced or accepted
	Residual risk: low, medium or high
	Measures: approved or not approved

5.4.2.6 Processing of personal data in the law enforcement context

Relevant to Partner(s)	Required input
End-users	**Question 31: If processing of personal data occurs, is the purpose of the processing the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties?** *Reason: Same reasoning as in the previous question.*
	Input:

End-users	**Question 32: If processing of personal data occurs, does the party in question constitute:** **a. a public authority competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, or** **b. any other body or entity entrusted by Member State law to exercise public authority and public powers?** *Reason: Personal data processed by an actor falling into one of the above categories for specific purposes (stated below) is subject to the Directive 2016/680.*
	Input:
All partners, End-users	**Question 33: If the processing of personal data occurs, will the personal data processed by the Cyber-Trust platform be used in cross-border cooperation with law enforcement authorities?** *Reason: In that case, additional legal requirements need to be met by the controller.*
	Input:
All partners, End-users	**Question 34: If the processing of personal data occurs, how do you plan to differentiate between personal data of different categories of data subjects?** *Reason: According to Directive 2016/680, where possible, distinctions should be made among different categories of data subjects such as suspects and victims.*
	Input:
All partners, End-users	**Question 35: How do you plan to keep a fair balance between the competing private and public interests (e.g. public safety and the right to access to personal data which is used as evidence)?** *Reason: As the processing of personal data by police or national security authorities constitutes an interference with fundamental rights, its proportionality and necessity should be taken into consideration.*
	Input:

5.5 Additional questionnaires with regards to privacy and electronic evidence

As stated above, the primary aim of the Cyber-Trust DPIA will be to assess potential impacts of the application of the Cyber-Trust system in terms of adherence to the legal and ethical principles outlined in the Deliverables 3.1 and 3.2, with respect to the use-cases and the whole architecture. As already explained earlier, the Cyber-Trust project will likely result in a risk to the right to the protection of personal data. However, it may also have an impact on privacy in the broader sense as well as the use and sharing of evidentiary material in related processes. Therefore, within the terms of a broader impact assessment, the partners should also assess the adherence to the privacy requirements, including both necessity and proportionality, and the use and exchange of evidentiary material.

5.5.1 Privacy requirements

The Cyber-Trust project aims to develop a multifaceted technological platform, which by its very nature and its potential end-users, interferes with the privacy of individuals, even though during the experimental stage,

only simulated data will be used. The partners are, thus, invited first to answer questions with regards to necessity and then proportionality, as further discussed in D3.1.

5.5.1.1 Necessity

Relevant to Partner(s)	Required input
End-users, VUB	**Question 1: Does the use-case scenario represent a situation where the use of the Cyber-Trust component/service would be justified?** *Reason: For instance, a service provider, in conjunction with the provider of the network, is obliged to take, at its own costs, appropriate and immediate measures to remedy any new, unforeseen security risks and restore the normal security level of the service.*
	Input:
End-users, VUB	**Question 2: Are there situations outside the use-case scenarios where the use of a Cyber-Trust component would be necessary?** *Reason: The more situations that can be considered as "necessary", the wider potential usability for the platform/component will exist.*
	Input:
End-users	**Question 3: Are there procedures within your operating experience for determining the necessity (in legal terms) of cyberattack detection and mitigation practices and would a Cyber-Trust prototype fit within such contexts?** *Reason: It is important to be aware of the procedures that exist in varying jurisdictions for determining "necessity".*
	Input:

5.5.1.2 Proportionality

Relevant to Partner(s)	Required input
All partners, End-users	**Question 4: In the case of a service provider as end-user, will the Cyber-Trust component process traffic data? Will it process location data other than traffic data?** *Reason: If the Cyber-Trust component does not process traffic or/and location data, it is more likely to be proportional.*
	Input:
All partners, End-users	**Question 5: If processing traffic and location data, can individuals be identified? And if yes, under what conditions?** *Reason: If individuals cannot be identified or are identified only under strict conditions and safeguards, the component has more chances to be considered more proportional.*
	Input:
	Question 6: Who will have access to the data in question?

All partners, End-users	*Reason: The less restricted is the access, the less likely that the use of the component will be proportional in a particular circumstance.*
	Input:
All partners, End-users	**Question 7: How will the Cyber-Trust individual users be informed about the agents that will be deployed in their devices?** *Reason: As foreseen in the e-Privacy Directive, the terminal equipment of users of electronic communications networks and any information stored on such equipment are part of the private sphere of the users. Thus, the deployment of device agents should be allowed on condition that the users are provided with clear and precise information about the purposes of those device agents and should be able to refuse to have them stored. The methods for giving information or requesting consent should be made as user-friendly as possible.*
	Input:
All partners, End-users	**Question 8: How will the Cyber-Trust individual subscribers be informed about the data processing activities? How will they be enabled to provide or withdraw their consent?** *Reason: As foreseen in the e-Privacy Directive, the data relating to subscribers processed within electronic communications networks contain information on the private life of natural persons. Any further processing of such data may only be allowed if the subscriber has agreed to this on the basis of accurate and full information of the types of data processed and the purposes and duration of the processing.*
	Input:
All partners, End-users	**Question 9: Will incidentally collected data be deleted? Will they be deleted automatically and if so, how soon after their collection and how often?** *Reason: Traffic data used for the provision of value-added services should also be erased or made anonymous after the provision of the service. The more regularly any data is deleted, the more likely that a particular use will be deemed proportional.*
	Input:
Technical partners	**Question 10: Will the monitoring system continuously monitor and collect data or the data will be collected only when an activity which is very likely to be criminal has occurred or is currently happening?** *Reason: If the monitoring system is activated only when criminal activity has occurred, then the system has more chances to be considered proportional.*
	Input:
Technical partners	**Question 11: Can the algorithms for the activation of attack detection be altered in a relatively easy and cost-efficient manner (i.e. by the service providers which use the system)?** *Reason: The easier a system is customisable, the more "proportional" in a given circumstance it may be.*
	Input:

Technical partners	**Question 12: Can the algorithms for the activation of attack mitigation be altered in a relatively easy and cost-efficient manner (i.e. by the service providers which use the system)?** *Reason: The easier a system is customisable, the more "proportional" in a given circumstance it may be.*
	Input:
Technical partners	**Question 13: Which privacy-preserving methods will be used in the case of the web crawler?** *Reason: Due to the massive processing of information, privacy-preserving solutions must be adopted during the design of the web crawler.*
	Input:

5.5.2 Requirements concerning the use of electronic evidence

This section addresses questions to the Cyber-Trust consortium with regards to the third pillar of the project and the use of the CTB for the storage and transfer of material that may contain electronic evidence.

Relevant to Partner(s)	Required input
All partners, End-users, VUB, experts	**Question 1: What is the procedure in your jurisdiction for the transfer of electronic evidence from a private entity (service provider) to a law enforcement authority in the case of a cyberattack? If such procedures are not followed, can material that may contain electronic evidence still be used in criminal proceedings?** *Reason: The procedure usually depends upon national criminal procedural law and varies from Member State to Member State. The Cyber-Trust platform will have to comply with the requirements of each jurisdiction where it operates in order for the material to have better chances to be admissible in the respective Court of Law.*
	Input:
All partners, End-users, VUB, experts	**Question 2: What are the safeguards for the access to retained data by law enforcement authorities in your area of operation? Is the procedure different in cases of emergency?** *Reason: The procedure usually depends upon national criminal procedural law and varies from Member State to Member State. In many states, prior review by a court or an independent body is mandatory, but other conditions and substantive or procedural safeguards may be in place as well, such as the nature or the crime, the seriousness of the act, the assessment of necessity and proportionality or the urgent character of the request.*
	Input:
All partners, DPOs and End-users, VUB, experts	**Question 3: Is there ad-hoc legislation or case law in your country of operation with regards to Distributed Ledger Technologies for the storage of material that may contain electronic evidence?** *Reason: Since DLTs are a novel solution, ad-hoc legislation or case law is scarce.*
	Input:

Technical partners, End-users	**Question 4: Will the actual forensic data that may contain electronic evidence be stored in an existing database at the service provider´s auspices, where the latter stores all its retained data?** *Reason: Every data processing activity must have a legal basis. If the data are stored in the same database as they were stored until now, then most likely the same legal basis can cover their processing.*
	Input:
End-users, technical partners, VUB	**Question 5: If the answer to the previous question is no, will the actual data that may contain electronic evidence be stored in a separate (off-chain) database, which will function as a dedicated repository? If yes, what is the legal basis for that separate database? Is the database controlled by the service provider or the Cyber-Trust consortium?** *Reason: Every data processing activity must have a legal basis.*
	Input:
End-users, technical partners	**Question 6: How are you planning to ensure and demonstrate the integrity and validity of the storing processes (both on-chain and off-chain) and the quality of the evidentiary material, in particular, since you are using a novel solution in the field which might raise questions in the legal proceedings? What organisational and technical measures will be put in place to ensure security and prevention of unauthorised access?** *Reason: It will be crucial to demonstrate that no tampering took place, for instance, by providing timestamps, information about who has access to the information and what processes occurred to it from the first moment of its collection until its acquisition by the law enforcement authorities. Moreover, it has to be ensured that the retained data is stored in the European Union, since this is a mandatory condition in some jurisdictions, for instance, the Netherlands.*
	Input:
Technical partners, LEAs	**Question 7: Will it be possible to present defendants with copies of the evidentiary material? Will it be possible to explain and demonstrate to the defendants the processes that have been implemented?** *Reason: A defendant may wish to access evidence against her/him, both before and during court proceedings in order to prepare his or her defence.*
	Input:
All partners, End-users	**Question 8: How do you document your processing operations? Who has access to this documentation and up to what extent?** *Reason: Record-keeping and appropriate documentation may improve the process for the identification of risks both for the controller and the supervisory authority.*
	Input:
	Question 9: What will be the status of the service providers, the Cyber-Trust consortium and the law enforcement authorities in the CTB?

All partners, End-users	*Reason: It is important to define access rights and how these rights will be restricted to authorised personnel only.*
	Input:
Technical partners, End-users	**Question 10: What metadata will be stored on-chain? Who will have access to them?** *Reason: It is important to define what type of data will be stored, because of the difficulty to store personal data on-chain in full compliance with the data protection regime.*
	Input:
Technical partners, End-users	**Question 11: Unless the data have been accessed and preserved, what will happen to the on-chain metadata that remain unused?** *Reason: In most jurisdictions, these data must be deleted after the end of the retention period.*
	Input:
Technical partners, End-users	**Question 12: What is foreseen to happen with the on-chain metadata after the legal proceedings?** *Reason: In some jurisdictions, these data may need to be deleted.*
	Input:
All partners, End-users	**Question 13: Will the data subject concerned be notified of the request made to the service provider by the law enforcement authorities and if yes, under which circumstances?** *Reason: In some jurisdictions, the concerned data subjects may need to be notified about the proceedings.*
	Input:

6. Conclusions

Section 2 provided a brief description of the tools that are going to be developed in the WP5, 6 and 7, based on the input of the respective technical partners. Section 3 shed light in the legal and ethical concerns as expressed from the partners, whereas Section 4 put emphasis on the legal and ethical recommendations, both general and more specific concerning data protection, privacy and electronic evidence. Section 5 introduced a preliminary methodological approach to the Data Protection Impact Assessment that will take place in D3.4 and D3.5 and based on the previous findings, presented indicative questionnaires which will form the basis of the assessment. Annex C provides a legislative map, as a guiding tool for the technical partners involved in the designing of the data processing activities as well as the end-users with regards to the national legislation applicable in their jurisdictions.

7. References

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation) OJ L 119, 4 May 2016, pp. 1-88.

Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) OJ L 201, 31.7.2002, p. 37–47.

ALLADIN project, D3.3 – Framework for Impact Assessment Against SoEL Requirements, May 2018.

Article 29 Working Party, Guidelines on Data Protection Impact Assessment and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 (WP 248 rev. 01).

Cyber-Trust, D3.1 Regulatory Framework Analysis, August 2018.

Cyber-Trust, D3.2 The legal analysis of the use of evidentiary material, November 2018.

Cyber-Trust, D2.3 Use Case Scenarios, December 2018.

CNIL, Privacy Impact Assessment Templates, February 2018.

European Data Protection Board, Endorsement 1/2018.

Eurostat and ESSnet Big Data, Netiquette - Deliverable 2.1 Legal aspects related to Web scraping of Enterprise Web Sites, December 2016

FORENSOR project, Framework for impact assessment of Forensor against DAPPECL requirements, May 2016.

Information Commissioner´s Office, Sample DPIA Template, 9 February 2018, v0.3.

Kloza, D. et al. (2017), Data protection impact assessments in the European Union: complementing the new legal framework towards more robust protection of individuals, d.pia.lab Policy Brief No. 1/2017, Brussels Laboratory for Data Protection & Privacy Impact Assessments (d.pia.lab).

Kuner, C. et al (2015), Risk management in data protection, in: International Data Privacy Law, Vol. 5, No. 2.

Smart Grid Task Force 2012-14, Expert Group 2: Regulatory Recommendations for Privacy, Data Protection and Cyber-Security in the Smart Grid Environment, Data Protection Impact Assessment Template for Smart Grid and Smart Metering systems, 13 September 2018.

Annex A – Questionnaire used for receiving input from the partners

Suggestions on how to fill in the following template

1. Read through this template and highlight areas which need more information or attention, either from your side or our side. The final document should meet afore most your needs for an efficient road ahead, so feel free to add input, which you consider necessary, even though it is not explicitly asked.
2. Assess your tool in its entirety – ensure that you have full information and background. If not, provide us with as much information as possible in plain language. Technical language can be used, as long as it is accompanied with full descriptions and practical examples. Please keep in mind that this is only a preliminary assessment which will be followed by two explicit Data Protection Impact Assessments.
3. If you have not decided yet upon the design, please present the 2 or 3 alternatives that you are considering, so as for us to proceed with their legal and ethical assessment.
4. Check in with your Data Protection Officer, if necessary, in order to provide concrete answers, in compliance with your GDPR obligations, if personal data is being processed. Also, mention any relevant Codes of Conduct or certifications.
5. If you develop more tools for the same task, please list them separately. If tools are co-developed by two or more partners and the components are not clear, then please co-ordinate with your partner(s) in order to decide whether it is better to provide one or more forms.
6. If it is deemed necessary after the initial submission of this input, further input may be requested.
7. As guidance, you can use the findings of D2.3 concerning Use-cases.

General information	
Name of partner(s)	*Eg. VUB*
Work package	*Eg. WP3*
Title of the task	*Eg. T3.3 Road ahead*
Task description	
Name of the Tool/solution/method/mechanism/system to be developed	
Description of the tool/solution/method/mechanism to be developed	*Please describe the components of the tool.*
What role will this tool play in relation to other tools/solutions (to be developed) in the project?	*Please describe its functionality (interdependencies with other tools or contribution to the whole system) and necessity.*
Other comments	
DURING the research phase – corresponding to Tasks 4.1 and 4.2	
Which tool(s)/method(s) will you use for the development of the specific tool/solution, in order to be in compliance with the regulatory framework, as described in D3.1 and D3.2?	*Name the tools or methods that you will use in order to develop the specific solution/tool. It can be a tool provided by a third party or the services of a data processor. Here you can also include sub-tools of lesser significance which you may develop, which cannot be assessed in a standalone way.*
What are your primary data protection and privacy concerns for the creation of the tool, based on the general legal framework explicitly described in D3.1 and D3.2, as well as recommendations included in other deliverables, e.g. D2.3? **If no personal data is being processed, please mention it explicitly.**	*Concerns during and after the research phase may be the same.* *e.g. the legal framework is fragmented; it is difficult to assess whether personal data will be processed.*

Have you identified any particular risks with regards to data subjects´ rights? If yes, please clarify.	*e.g. Risks concerning confidentiality or loss of personal data; data accuracy.*
Likelihood of risks	*Low, medium or high*
Severity of risks	*Low, medium or high*
If you have identified any risks, please mention ways/measures to mitigate them during the research phase.	*e.g. designing the tool in a specific way, using specific PETs.*
Other legal concerns, based on the general legal framework explicitly described in D3.1 and D3.2, as well as recommendations included in other deliverables, e.g. D2.3?	*e.g. lawful collection of electronic evidence in the EU Member States*
Ethical considerations to be taken into account during the research phase?	*e.g. dual use risks? Misuse risks?*
AFTER the research phase – corresponding to Tasks 8.1 and 8.4	
Envisaged end-user(s) after the research phase	*e.g. Police authorities. If dual or multiple uses, please mention and explain.*
Envisaged use after the research phase	*e.g. for the storage of material which may contain electronic evidence. If dual or multiple uses, please mention and explain.*
Potential legal ground for the use of the tool in a specific context?	*e.g. For law enforcement purposes – relevant legislation related to the police and judicial matters.*
What are your primary data protection and privacy concerns for the use of the tool, based on the general legal frameworks described in D3.1 and D3.2, as well as recommendations included in other deliverables, e.g. D2.3? If no personal data is being processed, please mention it explicitly.	*e.g. potential interference with individuals´ privacy; sharing of evidentiary material with third countries (in case of voluntary assistance)*
Have you identified any particular risks with regards to data subjects´ rights? If yes, please clarify.	*e.g. data minimisation*
Likelihood of risks	*Low, medium or high*
Severity of risks	*Low, medium or high*
If you have identified any risks related to data protection and/or privacy, please mention ways/measures to mitigate them.	
Other legal concerns, based on the general legal framework described in D3.1 and D3.2, as well as recommendations included in other deliverables, e.g. D2.3?	
Ethical considerations to be taken into account?	*e.g. dual use risks? Misuse risks?*
Additional comments	

Table 0.1 - Preliminary questionnaire

Annex B – List of all the tools

Partner **WP**	***UOP*** **WP5**	***UOP*** **WP5 (with linkage to WP6)**	***ADITESS*** **WP6**	***UOP*** **WP5 (with linkage to WP6)**	***CSCAN*** **WP6**	***Scorechain*** **WP7**	***Scorechain*** **WP7**
Task	T5.1 Threat intelligence techniques	T5.2 Trust establishment and risk assessment T6.2 Device attack detector	T6.2. Device tampering detection and remediation	T5.3 - Game-theoretic cyber-defence framework T6.3 - Network attack detection and mitigation	T6.3 Network attack detection and mitigation	T7.2 Cyber-Trust's proposed DLT architecture T7.3 Blockchain security framework	T7.4 Blockchain forensic visualisation tool
Task description	Cyber-threat intelligence discovery and sharing mechanism	T5.2 refers to methods, algorithms and tools for realizing the computation of a comprehensive trust score for devices and supporting devices in reasoning about mutual trust and regulating their communications, data exchanges and service provision and consumption. T6.2 refers to measuring device health and identifying vulnerabilities.	The implementation of modules for device level attacks and remediation	The purpose of this task is to ensure awareness of the security condition and mitigation of any possible attack that may be applied. The associated defence tool that is envisaged, called iIRS (intelligent Intrusion Response System), aims at efficiently translating the system alerts (generated from IDS – Intrusion Detection System) into an accurate estimation of the current system security condition and respond with the appropriate mitigation action (either applied directly or by informing the corresponding security service) in real-time. iIRS has the ability to select the response actions in real-time to mitigate the progression of a cyber-attacker in the smart home network while minimizing the negative impact that reactions have to the availability of network resources to trusted devices (e.g. by refusing communication requests, shutting down running services, etc.). Balancing this tradeoff between ensuring system security against cyber-attacks and keeping network availability at the desired level (by taking into account the user's	This task aims at attacks targeting at (critical) network infrastructures, with a focus on botnet detection and mitigation. Botnets are used in many attacks, with DDoS and reduction of quality (RoQ) attacks being the most common ones. In principle, a posteriori DDoS detection is trivial, in the sense that it is noticed once the attack succeeds	Implementation of the blockchain, its architecture and management.	This task is about the development of a tool (D7.5) for the easy-to-use exploration and visualisation of the information that will be stored in the Cyber-Trust blockchain solution.

				preferences as well) is one of the main goals of the iIRS.			
Name of the Tool/solution/method/mechanism/system to be developed	**Enriched Vulnerability Database (eVDB)**	**Trust management system (TMS); Device attack detector**	**Device Defender: for intrusion detection and malicious attacks**	**iIRS (intelligent Intrusion Response System)**	**Machine Learning Intrusion Detection System, Machine Learning Deep Packet Inspection**	**Cyber-Trust Blockchain (CTB)**	**Cyber-Trust visualisation tool**
Description of the tool/solution/method/mechanism to be developed	The tools and solutions to be developed in the context of the eVDB (including the cyber-threat discovery mechanism) aim at: 1. gathering public cyber-threat intelligence information from deepnet web forums or marketplaces and clearnet social platforms, 2. leveraging this information to identify emerging threats, zero-day vulnerabilities and new exploits to IoT devices, and 3. sharing the information with different Cyber-Trust modules and other stakeholders.	The tools and solutions to be developed in the context of the TMS aim at: 5. Synthesizing a comprehensive profile for devices and computing a trust score for each one 6. Computing risk levels for devices 7. Triggering awareness and reaction events when appropriate conditions (e.g. demotions or elevations of trust/risk scores below/above certain thresholds) are met 8. Allowing TMSs to communicate according to the peer-to-peer paradigm towards synthesizing a global view of device trust/risk levels, maintaining the autonomy of each TMS however. The tools and solutions to be developed in the context of the device attack detector are: • Host/device/network inventory tools • Remote health monitoring tools • Vulnerability scanner	The tool aids at preventing the transfer of malicious content or access on monitored IoT devices. This tool retains log information regarding the state of the devices OS, running processes as well as hashes and digital signatures for the immediate detection of malicious acts and rapid remediation.	The main components of iIRS are the following: 5. The module is responsible for handling the Graphical Security Model (GrSM). 6. The communication module which is responsible for the interactions with the TMS, the IDS, Enriched Vulnerability Database (eVDB) and the cyber-defence service. 7. The security state belief computation module, which updates the belief of the system security condition in real-time. 8. The decision-making module which computes the optimal defence actions.		The CTB will be used to store data collected by the Cyber-Trust platform such as forensic evidence meta-data or Trusted Logs	The visualisation tool will provide a user-friendly way to explore the blockchain.

The role of the tool in relation to other tools/solutions (to be developed) in the project	The cyber-threat discovery mechanism will be responsible for identifying cyber-treat intelligence from online sources. The eVDB will be responsible for sharing cyber-threat related information to other components and modules in the Cyber-Trust platform.	The TMS will be the central point for device trust and risk assessment. It will consume information from the device profile repository, the attack and anomaly detection modules as well as from other repositories (e.g. network architecture, assets etc.) and it will be able to: 5. Provide assessments of the trust and risk level of devices to (a) other interested devices and (b) tools that need this information, such as the intelligent UI. 6. Raise awareness events for the intelligent UI users. 7. Trigger execution of game-theoretic cyber-defence procedures. 8. Trigger mitigation actions, according to policy rules, especially through the iIRS. The Device attack detector will: • Arrange for obtaining device health metrics, in particular for firmware, operating systems and critical components • Identifying vulnerabilities present at devices Related to the device attack detector, tools for discovering assets and enumerating networks and services will be used.	The tool will interact with a number of other platform components including the Cyber-Trust Device database, as well as the network attack detection and blockchain components.	The purpose of iIRS is the suggestion of the best available defence actions in order to enhance the system security. In doing so, there is a need to interact with other system components. More specifically, iIRS needs to retrieve information about the network configuration, attack likelihood probabilities and devices' profiles from the TMS, information about exploits and vulnerabilities from the eVDB, receives security alerts from the IDS and communicates with Cyber-Defence service.	The tool will interact with various components of Cyber-Trust platform, in particular with WP5 and also other tasks of WP6.	The CTB will interact with the rest of the platform by formatting, validating then storing data provided by the other tools in the project	The visualisation tool will interact with the blockchain to display the data previously stored on it.

Tool(s)/method(s) used for the development of the specific tool/solution	For the cyber-threat discovery mechanism, the following tools/technologies will be used: ACHE crawler, TOR, MongoDB, word2vec, nltk, Formasaurus/Opal, Selenium/Splash, Privoxy. For the eVDB, the following tools/technologies will be used: MISP, ZeroMQ, lxml, PyMISP.	Currently, a number of tools are being investigated regarding their suitability to be used for developing the various functionalities. Short lists are given below: **Trust Management System** Linux SGX Trust Management Framework, Soutei, TrustAll, Trust Composer, kamban.org, Trust relationship management on blockchain for IoT, Trust Management System, Trust Management Library, Tennessee Risk Management Trust, Trust Guard, Django agent trust, Keynote TMS, Python extension module for the KeyNote trust management system, Declarative Trust Management System with Linked Credentials **Host/Device Inventory and Scanning** NMap, Angry IP scanner, Unicornscan, Masscan, Scanrand, Zmap, NetCrunch Tools, Scanmetender, Maltego, Netglub, Dnsdumpster.com, MyNet Toolset, LanTopoLog, Spiceworks Network Mapping, NetworkMiner **Vulnerability scanning** OpenVAS, Nessus, Nikto, Arachni, w3af, Vega **Attack mitigation** Tools for identifying appropriate mitigation actions (listed under https://www.cve-search.org/software/).	Different flavours of the agent are expected to be developed these will aid use by mobile and web applications. Therefore mobile development frameworks such as ionic, android development and Xamarin are candidates while for the rest implementations, technologies such as python, Django, Node.js and C will be used.	The module which is responsible for the GrSM generation and manipulation may be based on a third-party tool (this is currently under consideration in D2.5). Examples of such tools include (but not limited to): TVA, NetSpa, Mulval, Advise, Naggen, CyberSage, and Cygraph. The rest of the iIRS componetns (see above) will be developed in-house.	Suricada-IDS, Bro-IDS, netsniff-ng, tcpdflow Custom tools also will be developed in order to identify attack patterns as well as creating new attack patterns from monitoring data.	JavaScript IDE (Intelligent Development Environment) Atom /Sublim Text /etc. HyperLedger as a blockchain solution Node.js	JavaScript IDE (Intelligent Development Environment) Atom /Sublim Text /etc. HyperLedger as a blockchain solution Node.js

Table 0.1 - List of all the tools

Annex C – Legislative Map per Member State relevant to Cyber-Trust

State	The centerpiece of evidence law	Other relevant law	Data retention	Cybercrime	NIS Directive (Deadline: 09.05.2018)
CY	Law of Evidence, Chapter 9	The Cypriot Criminal Code, Chapter 154; Law for the organisation of the Courts n.14/60; Law for the Interpretation, Chapter 1; Law 112(I)/2004	Law 183(I)/2007 **Retention period: 6 months**	Law 22(III)/2004 (Budapest Convention); Law 147(I)/2015 (Directive 2013/40/EU)	Law 17(I)/2018 of 05.05.2018
GR	Greek Code of Criminal Procedure; Greek Constitution	The Greek Criminal Code; Law 2225/1994 (lawful interception); Law 2867/2000; PD 47/2005; PD 150/2001; PD 131/2003; Law 3431/2006; Law 3471/2006 (e-Privacy Directive); Law 3674/2008; Law 3783/2009; the forthcoming Law transposing GDPR and the Directive 2016/680 into domestic legislation	Law 3917/2011 **Retention period: 12 months**	Law 4411/2016 (Budapest Convention and Directive 2013/40/EU)	Draft submitted to the Greek Parliament on 12.11.2018
IT	Italian Code of Criminal Procedure	The Italian Criminal Code; Legislative Decree no. 231 of 08.06.2001; Legislative Decree no. 259 of 01.08.2003; Legislative Decree 82/2005; Ministerial Decree of 28.04.2008	Law No. 167/2017 **Retention period: up to 6 years, under specific conditions**	Law 48/2008 (Budapest Convention); 39 Amendments introduced in existing legislation in 2015 (Directive 2013/40/EU)	Law of 06.07.2016; Legislative Decree 65/2018
LU	Luxembourgish Code of Criminal Procedure	The Luxembourgish Criminal Code; The amended Law of 30 May 2005	Data retention Act No. 6763/2015	Law of 18.07.2014 (Directive 2013/40/EU); Ratification Act of 01.02.2015 (Budapest Convention)	In June 2018 the government announced the first steps towards its transposition into Luxembourgish Law
NL	Dutch Code of Criminal Procedure	The Dutch Criminal Code; Computer Crime Act III	Dutch Communications Act ~~Telecommunications Data (Retention Obligation) Act 2009~~ (invalidated in 2015) Law enforcement can request the data that the service providers store for business purposes **The retention period depends on the time the service providers store the data for business purposes**	Computer-crime Law II/2006 (Budapest Convention); Computer Crime Act III will enter into force in January 2019 and will be reviewed in 2 years; Law of 22.04.2015 and Decree of 05.06.2015 (Directive 2013/40/EU)	Law of 17.10.2018; Decree on Networks and Information systems of 2018; Decree of 30.10.2018
UK	Police and Criminal Evidence Act 1984	ACPO guidelines (not legally binding); the Terrorism Act 2000; Police and Justice Act 2006; the Telecommunications Regulations; the Data Protection Act 2018	~~Investigatory Powers Act 2016~~ In April 2018, the UK High Court ruled that the Investigatory Powers Act 2016 violated EU law and the Act must be re-drafted accordingly. **Retention period: 12 months**	Computer Misuse Act 1990; Ratification act of 01.09.2011 (Budapest convention); Serious Crime Act 2015 c. 9, Part 2 Computer Misuse (Directive 2013/40/EU)	The Network and Information Systems Regulations 2018

Table 0.1 - Legislative Map

