ANASTACIA

Advanced Networked Agents for Security and Trust Assessment in CPS/IoT Architectures

D2.3

Privacy Risk Modelling and Contingency Initial Report

This deliverable presents the results of the first 16 months of research for ANASTACIA Task 2.3. It includes the general data protection requirements and privacy risks to be addressed, the generic mitigation and contingency actions to be considered, and the specific approaches to be implemented when addressing four selected use-cases.

Distribution level	[PU]
Contractual date	30.04.2018 [M16]
Delivery date	02.05.2018
WP / Task	WP2 / T2.3
WP Leader	UMU
Authors	Adrian Quesada Rodriguez (MAND) Cedric Crettaz (MAND) Euhah Kim (DG) Pasquale Annicchino (AS) Sébastien Ziegler (MAND) Antonio Skarmeta (UMU)
EC Project Officer	Carmen Ifrim carmen.ifrim@ec.europa.eu
Project Coordinator	Softeco Sismat Srl Stefano Bianchi Via De Marini 1, 16149 Genova – Italy +39 0106026368 stefano.bianchi@softeco.it
Project website	www.ANASTACIA-h2020.eu

ANASTACIA has received funding from the European Union's
Horizon 2020 research and innovation programme under Grant Agreement N° 731558
and from the Swiss State Secretariat for Education, Research and Innovation

TABLE OF CONTENTS

INDEX OF TABLES

TABLE OF FIGURES

PUBLIC SUMMARY

This deliverable presents the results of the first 16 months of research for ANASTACIA Task 2.3. It includes the general data protection requirements and privacy risks to be addressed, the generic mitigation and contingency actions to be considered, and the specific approaches to be implemented when addressing four of the use-cases selected by the ANASTACIA consortium for the initial demonstrator of the platform. As such, it focuses on network-level privacy risks related to deployments of IoT and smart devices as shaped by such security threats as Distributed Denial of Service, SQL injection, zero-day exploits and malware.

To accomplish this goal, the normative and technical frameworks that surround and determine ANASTACIA's privacy-enhancing efforts were analysed in detail, aiming to develop a cross-referenced and synthetic set of personal data protection requirements. Following this effort, the document details relevant privacy vulnerabilities and security threats that shape the seven privacy risks to be monitored by ANASTACIA, namely:

1. Unauthorized access or disclosure of personal data.
2. Unauthorized modification of personal data.
3. Unauthorized or inappropriate linking of personal data.
4. Unauthorized removal or deletion of personal data.
5. Excessive collection or retention of personal data.
6. Lacking protection of traffic information and location data.
7. Impairment of data subject's rights.

The document then performs a ISO-based risk analysis process to identify the consequences, threats, impact and likelihood of the identified privacy risks and finally recommends detection, protection, mitigation and contingency actions for each. These are further specified for their implementation in use-cases related to Internet of Things (IoT), Building Energy Management System (BEMS) and Multi-access Edge Computing (MEC).

The models and contingency mechanisms developed in this document will be tested and further specified in the upcoming months. The results of this process will be detailed in ANASTACIA Deliverable 2.7 "Privacy Risk Modelling and Contingency Final Report" [M28].

1 Introduction

1.1 Aims of the document

This document aims to model relevant privacy risks to be addressed by ANASTACIA and to develop the contingencies for such risks. This task is threefold and adopted a systematic and sequenced methodology. It started by analysing the potential risk for privacy from a systemic perspective. It then analysed the new European General Data Protection Regulation (GDPR) rights and obligations to extract and to translate them into a set of key requirements. The requirements eventually guided the risk analysis and risk modelling. For each identified risk, measurement points as well as contingency measures are to be identified to mitigate the risk.

1.2 Applicable and reference documents

This document refers to the following documents:

- ANASTACIA D.1.1 "Holistic Security Context Analysis."
- ANASTACIA D1.2 "User Centred Requirements Initial Analysis."
- ANASTACIA D1.3 "Initial architectural design."
- ANASTACIA D2.2 "Attacks Threats Analysis and Contingency Actions."
- ANASTACIA D5.1 "Dynamic Privacy and Security Seal Model Analysis"

1.3 Revision History

Version	Date	Author	Description
0.1	19/02/2018	Adrian Quesada Rodriguez	Initial draft of new version of the deliverable
0.2	02/02/2018	Adrian Quesada Rodriguez	Completed Introduction to GDPR/e-Privacy directive and Requirements
0.3	12/02/2018	Adrian Quesada Rodriguez	Risk identification complete
0.4	16/02/2018	Adrian Quesada Rodriguez; Cédric Crettaz	Review of threat agents and risk analysis
0.5	27/02/2018	Adrian Quesada Rodriguez	Initial draft completed to Section 5.3
0.6	20/03/2018	Adrian Quesada Rodriguez; Pasquale Annicchino	Compiled feedback from partners, added PDP information on monitoring and contingency
0.7	4/04/2018	Adrian Quesada Rodriguez; Cédric Crettaz	Detailed contingency and mitigation elements of section 5.4 and enabler definition
0.8	10/04/2018	Adrian Quesada Rodriguez	Finalized section 5, stylistic changes and insertion of figures/tables.
0.9	13/04/2018	Adrian Quesada Rodriguez	Completed draft for peer review

0.95	18/04/2018	Stefano Bianchi	Feedback from peer review
1.0	26/04/2018	Adrian Quesada Rodriguez	Final version of the deliverable

1.4 List of Acronyms

Acronym	Meaning
API	Application Programming Interface
BMS	Building Management System
CPS	Cyber-Physical System
DBMS	Database management system
DDoS	Distributed Denial of Service
DoS	Denial of Service
DSPS	Dynamic Security and Privacy Seal
eIDAS	Electronic Identification and Trust Services (eIDAS) Regulation
ENISA	European Union Agency for Network and Information Security
ETSI	European Telecommunications Standards Institute
GDPR	General Data Protection Regulation
GUI	Graphical User Interphase
HSPL	High-level Security Policy Language
ICT	Information and Communication Technologies
IDS	Intrusion Detection System
IoT	Internet of Things
IPS	Intrusion Protection System
ITU	International Telecommunications Union
MEC	Mobile Edge Computing/Multi-access Edge Computing
MitM	Man-in-the-Middle

Acronym	Meaning
MSPL	Medium-level Security Policy Language
NIST	National Institute of Standards and Technology
PDP	Personal Data Protection
SDN	Software-defined networking
SQL	Structured Query Language

1.5 Terms and Definitions

Term	Definition
Audit	This refers to a systematic, independent and documented process for obtaining audit evidence [records, statements of fact or other information which are relevant and verifiable] and evaluating it objectively to determine the extent to which the audit criteria (including policies, procedures or other requirements) are fulfilled. (International Organization for Standardization, 2011)
Certification	This Refers to the provision by an independent body of written assurance (a seal or certificate) that the product, service or system in question meets specific requirements.
Cyber-physical systems	ICT system able to interact in continuous way with the physical system it operates in. The system is composed of physical elements equipped with computational capabilities and it presents three characteristics ("the three C"): computational capabilities, communication and control capabilities. (Cambiaso, Mongelli, et al., 2017, p. 3)
Cybersecurity:	Field of the computer science working on threat analysis, vulnerabilities identification and management and to the risk associated to ICT assets, with the aim of protect such systems from (internal or external) cyber-attacks potentially able to create (direct or indirect) damages with impact higher than a pre-defined threshold (e.g. economic, reputation, socio-politics damages, etc.) (Cambiaso, Mongelli, et al., 2017, p. 3)
Information security management systems	This refers to a systematic approach to managing sensitive company information so that it remains secure. It includes people, processes and IT systems by applying a risk management process. (International Organization for Standardization, 2013).
Information Technology Security	Is the process of implementing measures and systems designed to securely protect and safeguard information (business and personal data, voice conversations, still images, motion pictures, multimedia presentations, including those not yet conceived) utilizing various forms of technology developed to create, store, use and exchange such information against any unauthorized access, misuse, malfunction, modification, destruction, or improper disclosure, thereby preserving the value, confidentiality, integrity, availability, intended use and its ability to perform their permitted critical functions. (www.sans.org)

Internet of Things	Common life objects (e.g. fridge, TV, door sensor, video-cameras, light bulbs, weather stations, etc.) are able to communicate among themselves and with the environment by exploiting an Internet connection to exchange data in real time, without requiring external devices demanded to manage the communication. (Cambiaso, Mongelli, et al., 2017, p. 3). IoT has been defined as a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies. (International Telecommunications Union, 2012)
Middleware	Middleware is a software layer that sits between the low-level layer of devices and the high-level application layer. It usually provides a common interface and a standard data exchange structure to abstract the complex and various lower-level details of the hardware. When the middleware receives a request from a higher-layer application, it converts the high-level standardized resources access request to the corresponding device-specific methods. When the device responds back to the application, the middleware processes the low-level methods and data transformations, and then sends the related abstract commands and data back to the application. (Lin & Bergmann, 2016)
Network function virtualization	Network architecture concept using IT virtualization technologies to virtualize entire classes of functions in order to design, deploy and manage networking services. (Cambiaso, Mongelli, et al., 2017, p. 3)
Personal data	Any information relating to an identified or identifiable natural person ('Data Subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. (EU Data Protection Directive (95/46/EC))
Privacy impact assessment	A privacy impact assessment is an instrument for assessing the potential impacts on privacy of a process, information system, programme, software module, device or other initiative which processes personally identifiable information and, in consultation with stakeholders, for taking actions as necessary in order to treat privacy risk. (ISO)
Risk	Effect of uncertainty on objectives (ISO Guide 73)
Software-defined networking	Approach used in the computer network fields to provide network administrators the ability to initialize, control, update and manage in a dynamic way the network configuration through apposite interfaces and protocols and by abstracting low level functionalities of the network nodes. (Cambiaso, Mongelli, et al., 2017, p. 3)
Threat	Potential cause of an unwanted incident, which might result in harm to a system or organisation (ISO/IEC 27000:2016).

2 Methodology and Approach

An exhaustive and comprehensive analysis process was carried out towards synthetizing the requirements, analysing the risks and developing the contingency models presented in this deliverable. This was supported by continuous feedback received from the partners involved in ANASTACIA WP2 and WP5. The analysis methodology implemented throughout this deliverable was focused on the successive completion of seven stages along with scheduled scrutiny of previous stages in light with the results of the analysis efforts performed. The stages followed were:

1. **Background research:** Based on the extensive research on privacy and personal data protection, including (but not limited to) currently applicable norms and regulations[1], relevant standards and technical recommendations, including ISO Standards[2]; ITU Recommendations[3]; ETSI Standards[4]; and NIST Standards[5].
2. **Normative synthetization and cross-referencing:** Effort aimed to concretely identify the relevant privacy and personal data protection requirements found in the GDPR and the e-Privacy Regulation and to cross-reference them with those requirements identified by ANASTACIA Deliverable 1.3, along with any relevant technical standard and recommendation identified in the *Background research* stage. Finally, the ten requirements were clarified in relation to the nine use-cases detailed by ANASTACIA deliverable 1.2.
3. **Vulnerability, monitored threat and privacy risk identification:** a non-exhaustive list of potential privacy vulnerabilities that could affect monitored systems (and which could be monitored by the system) was developed. This process was accompanied by the identification of the security threats monitored by the system as declared by D2.2. Both these elements served to inform the identification process of the seven privacy risks to be addressed by the ANASTACIA platform[6].
4. **Risk analysis:** an ISO-based risk analysis process was performed to determine the potential consequences, threats, impacts and likelihood associated with the seven privacy risks that are to be addressed by ANASTACIA.
5. **Alignment with attack threats analysis:** A joint effort with partners to identify the enablers and monitoring capabilities which might be most relevant for determining the privacy status of a monitored system was followed. This process was informed directly by the developments and inputs provided by partners to D2.2.
6. **Generic contingency modelling:** This stage specified generic technical and organizational activities (protection, detection, mitigation and contingency) to be introduced for each privacy risk along with a contingency verification strategy to monitor the implementation of the organizational activities necessary to comply with personal data protection requirements.
7. **Specific contingency modelling:** Specific approaches (including attack description, protection approach, detection plan, mitigation plan) were developed for the four ANASTACIA use-cases selected by the ANASTACIA consortium for the first demonstrator of the platform.

[1] Including the General Data Protection Regulation (GDPR); the Directive 2002/58/EC (ePrivacy Directive); the Directive 2016/1148 (NIS Directive); and Regulation on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market (EIDAS Regulation).

[2] Examining particularly ISO/IEC 15408:2009; ISO/IEC 17030:2003; ISO/IEC 18045:2005; ISO/IEC 24760:2016; ISO/IEC 27000:2016; 27001:2013; ISO/IEC 27002:2013; ISO/IEC 29100:2011; ISO/IEC 29101:2013; ISO/IEC 29134:2017; and ISO/IEC 29190:2015.

[3] Considering, among others, the following ITU-T recommendations: X.805 (10/2003); X.810 (11/1995); X.816 (11/1995); X.1056 (01/2009); X.1171 (02/2009); X.1205 (04/2008); X.1206 (04/2008); X.1208 (01/2014); X.1209 (12/2010); X.1311 (02/2011); X.1312 (02/2011); X.1313 (10/2012); X.1314 (11/2014); Y.2060 (06/2012); Y.2201 (09/2009); Y.3051 (03/2017); Y.3052 (03/2017); Y.4050 (07/2012); Y.4100 (06/2014); Y.4101 (04/2014); and Y.4401 (03/2015).

[4] Particularly ETSI TR 103 304; and ETSI TR 103 305.

[5] Including the Framework for Improving Critical Infrastructure Cybersecurity; IR 7628 R1; IR 8062; IR 8114; SP 800-53 R4; SP 800-82; SP 800-122; SP 800-147; SP 800-150; and SP 800-161.

[6] Potential application-level privacy risks will be outside the scope of this deliverable given ANASTACIA's focus on network-level event, vulnerability, and threat detection/mitigation.

3 INITIAL CHARACTERIZATION OF ANASTACIA'S CAPABILITIES

"ANASTACIA is a framework for the management of complex networks and systems. Following technologies and scenarios are in particular addressed: Internet of Things (IoT), Software Defined Networks (SDN), Building Energy Management System (BEMS), Multi-access Edge Computing (MEC), also considering Network Function Virtualization (NFV) and Policy Based Management aspects." (Cambiaso, Mongelli, et al., 2017, p. 2). Considering the necessity to guarantee secure data transmissions and the sensitive nature of the information shared by the network, ANASTACIA aims to provide holistic and innovative tools for the detection, prevention and management of both security and privacy threats.

ANASTACIA's interest on IoT Security and Privacy is more than necessary: *"as the connectivity of objects exponentially increases, so are the possibilities for hacking into the system. It is noted that IoT covers a huge scope of diverse markets and the needs of security and privacy vary depending on the types of services. In order to find general requirements from the user perspective, we focus on the common risks coming from the IoT communication patterns that apply to heterogeneous IoT services and applications"*(Cambiaso, Mongelli, et al., 2017, p. 13). As such, the system's focus will be the detection of threats at a network-level to overcome the large range of possible attack vectors in the realm of IoT deployments[7].

"Cyber-security can be seen as a purely ICT related issue or as a legislative and regulation compliance problem. Nevertheless, it needs a new approach able to consider all the components of the system, in order to define a security plan able to effectively protect the commercial interests, the immaterial assets and the infrastructure of the organization, by protecting them from risks and threats that may potentially target the system." (Cambiaso, Mongelli, et al., 2017, p. 4). As this is particularly true when addressing privacy risks, ANASTACIA will incorporate network-level privacy enhancing mechanisms[8] which will make use of the functionalities listed above to address the security of processing requirements found in current personal data protection legislation, while incorporating human-based privacy impact verifications whenever necessary to ensure compliance and the protection of the rights of data subjects.

In order to achieve this goal, ANASTACIA will rely on a technical framework of "*policy-based network and security management to deal with cyber-attacks in CPS-IoT scenarios through SDN and NFV."* (Cambiaso, Mongelli, et al., 2017, p. 17). It will detect security and privacy vulnerabilities and react accordingly to mitigate both active[9] and passive[10] cyberattacks to the IoT/CPS deployments through one or more of the following functionalities:

a) Basic Security mechanisms for Software-defined networking (SDN)

- Traffic flow forwarding
- Traffic flow dropping
- Traffic flow mirroring

[7] *"network-level security can be implemented across the entire range of IoT devices, rather than device-level security that is specific to a particular device; unlike device-level security that is embedded into devices and is hence difficult to upgrade, network-level security can be implemented in the cloud, and can be enhanced on a continuous basis; network-level security can be offered by a third-party who has expertise in this specific area, rather than by the device manufacturer who may not have the drive or the skills to implement security properly; network-level security adds an extra layer of protection that can augment any device-level security implemented by the manufacturer"* (Sivaraman, Gharakheili, Vishwanath, Boreli, & Mehani, 2015, p. 2).

[8] *"(…) In order to detect and resolve security/privacy issues for IoT, we propose an external entity (…) that develops, customizes, and delivers to the user extra safeguards at the network level for the IoT devices in their household. A simple example might involve (…) adding the appropriate access control rules that protect a specific IoT device, while a more complex example might involve dynamic policies that change access control depending on the context (e.g. the family members being present or absent from the house)"*(Sivaraman et al., 2015, p. 2).

[9]Which include packet crafting attacks (such as replay attacks, masquerading, malware and zero-day attacks); packet alteration attack (such as Man-in-the-Middle attacks); and service compromising attacks (such as SQL injection attacks, Denial of Service (DoS) and Distributed Denial of Service Attacks (DDoS), and their new modalities like Slow DoS (Cambiaso, Papaleo, Chiola, & Aiello, 2013), and Slowcomm (Cambiaso, Papaleo, & Aiello, 2017).

[10] Data interception attacks, including traffic analysis, sniffing/eavesdropping and keyloggers.

- Traffic flow bandwidth reduction

b) **Basic security mechanisms for IoT**
   - Power management
   - Interface management
   - Traffic protection management

c) **Network Function Virtualization (NFV)**
   - Virtual firewall
   - Virtual Intrusion Detection System (IDS)
   - Virtual Intrusion Prevention System (IPS)
   - Virtual switch/router
   - Virtual honeypot/honeynet
   - Virtual secure web proxy
   - Virtual private network (VPN)
   - Virtual bandwidth control

These functionalities will be enriched by ANASTACIA's monitoring enablers:

- Montimage Monitoring Tool (MMT): software able to analyse network traffic and extract protocols metadata. By using Deep Packet and Flow Inspection techniques (DPI/DFI)[11], the tool is capable of extrapolating metadata[12] given in input to other modules of ANASTACIA and implement novel algorithms and systems able to counter cyber-attacks.
- ATOS Security Incident and Event Management (XL-SIEM): These solutions provide cross-level cybersecurity event and information management capabilities. Different types of security systems can be integrated, correlating events across multiple layers and identifying anomalies in real-time. Its core capacities enable the decentralized compilation and distribution of sensor events[13] and

[11] The DPI/DFI technique used by MMT Probe allows accessing the raw packets that are traversing the network. In this sense, the Probe is capable of identifying different communication protocols at different layers of the IP stack, extracting information from each one of them. The following list is not exhaustive, and it gives an example of the recognized protocols, but MMT Probe is capable of recognizing a long list of protocols:

- Layer 2-related protocols: Ethernet (mac addresses, payload size).
- Layer 3-related protocols: IPv4, IPv6 (IP addresses, Fragments, flags of the packet, among others).
- Layer 4-related protocols: TCP (port numbers, sequence/acknowledgement numbers, control bits, window size), UDP (port numbers, packet length).
- Upper layers protocols: RTP (sequence numbers, timestamps, synchronization information, etc.), HTTP, and many more.

[12] Among the many types of report available in the MMT software, the tool can provide insights into system information, general statistics of the data transmitted, the protocols and applications used, and even providing reports containing information extracted from the HTTP headers of the detected flow (such as the User agent, the server response time, accessed URL, number of requests associated with this flow, etc.); information extrapolated despite usage of SSL encryption (application Family (Web, P2P, etc.), the content type (text, video, etc.), among other fields); information about RTP usage for streaming multimedia (packet loss rate, the packet burstiness and jitter); and FTP-related information (user name used in the session, their password, the file name, etc.).

[13] The following information is included in the normalized event sent from the XL-SIEM agent to the XL-SIEM server:

- Date: Timestamp of the event received.
- Sensor: Name of the agent submitting the event.
- Triggered Signature: Text describing the event received.
- Category and Subcategory: Type of event based on the plugin processing the event.
- Data Source Name: Name identifying the type of event for the plugin processing the event.
- Product Name (optional): Name of the product related to the plugin processing the event.
- Source Address: IP address of the sensor producing the event.
- Source Port (optional): Port used to send the event.
- Destination Address: IP address of the entity receiving the event (generally the XL-SIEM agent).
- Protocol: Protocol used to transmit the event.
- User defined data (1..n): Custom user data containing additional information included in the event.

For every event processed by the XL-Agent a unique event ID is assigned. Additionally, for every event there is a preliminary analysis which results in several properties:

- Priority: This parameter determines the importance of the event processed, which is used for the XL-SIEM server to assign more resources to its processing.

provide strong correlation capabilities for the generation of alarms, providing the user with a vision of the security status of the deployed infrastructure.

- UTRC Agents: Which will be providing anomaly-based intrusion detection[14] that will be used to build a data-driven model based on collected operational data of the machines. This model will continuously monitor and analyse newly collected data in order to detect if a severe deviation from expected behaviour can be noticed.

As will be discussed throughout supra section 5, the functionalities provided by these and other security-driven enablers will be fundamental towards the monitoring and prevention of security threats, which in turn shall enrich ANASTACIA's efforts to secure personal data.

- Reliability: This parameter determines how trustworthy is the information contained in the event. The reliability level is based on the sensor producing it, which is set by the system administrator depending on the importance of the sensor or the infrastructure being monitored.
- Risk: This parameter determines the security threat that the processed event might entail.

The flexibility of the XL-SIEM model allows the integration of the Montimage Monitoring Tool and the UTRC agents as additional sources of information, using their events or alerts as an additional input when correlating events and generating more accurate alarms.

[14] This process can be divided in two phases:

- Offline: the system builds and learns the model, based on collected and processed data to represent the normal system behaviour.
- Online: the built model is used to continuously monitor and evaluate the newly collected data in order to state if there are any signs of an attack taking place from the point of the of sensor data.

Initially the agent undergoes an offline phase, also referred to as training period, when a data-driven model is built. This model consists of features and a set of relations among them to capture normal system behaviour. By system behaviour we mean collection of system states, where a state is defined by the attributes of the features of the model that are derived from the operational data. The agent collects operational data from the physical IoT devices and performs cleaning, aggregation, filtering. Feature extraction is performed on this data, capturing system behaviour over time, through identifying relations among one or more features. These features themselves already describe the monitored systems state but in order to better capture global behaviour relations between features are also created. From the collection of features relations are built between them that capture the normal and already observed system states. A threshold is learned that is used as a measurement to state whether a new system state is considered normal or not. In case of anomaly the threshold is also capable to provide a measurement of deviation of expected and actual system state. After initial constructing this model it is evaluated and updated based on its performance until it reaches a specified performance.

After learning the model that represent the behaviour of the system it is used in the online phase where the operational data is continuously monitored, collected and processed. The Agent collects the available operational data, maps it to the features used by the model and feeds them accordingly. The model then decides if the received system state can be classified as normal behaviour. When a system state derived from a collection of operational data is deviating significantly from the previously observed behaviour, the agent flags the specified state as an anomaly and reports it with the explanation to XL-SIEM component. The agent is able to provide further details what sensor or collection sensors caused the deviation and how severe it is, that is, how much it deviated from the expected system behaviour.

4 Applicable Personal Data Protection Requirements

This section aims to examine the applicable legal framework that will shape the risks and contingencies to be addressed by ANASTACIA. It will examine the GDPR and the e-Privacy regulation, from which it will extract a set of condensed personal data protection requirements which will be accompanied with relevant references from other applicable sources. Then it will introduce the nine use-cases to be addressed by ANASTACIA while seeking to characterize their implications vis-à-vis the identified requirements.

4.1 European Personal Data Protection: The GDPR and the e-Privacy Regulation

Personal Data Protection (PDP) has been enshrined in the normative framework of the European Union by a substantial amount of treaties, regulations and directives which have clearly developed its status as a human right for residents of the Union. Among these, two sources are of the highest relevance for the protection of end-users: the General Data Protection Regulation (European Parliament & European Council, 2016) and the upcoming Privacy and Electronic communications Regulation (ePrivacy Regulation).

The General Data Protection Regulation

Designed to update the dispositions of the Data Protection Directive (95/46/EC) and to harmonize the approaches to PDP across Europe, the GDPR was adopted in 2016 to be enforceable on 25 May 2018. Among its key features, the GDPR enshrines a number of guiding principles and dispositions that are to be implemented whenever Personal Data is compiled, stored, processed, disclosed or otherwise handled.

Namely the Regulation builds upon the principles of:

- **Lawfulness:** Processing should take place in the context of express consent by the data subject (or one of the necessity scenarios found in Article 6 of the GDPR)
- **Fairness:** Processing must account for the protection of children and other vulnerable individuals.
- **Transparency:** Any information and communication relating to the processing of personal data should be easily accessible, easy to understand and presented using clear and plain language.
- **Purpose limitation:** Personal Data should be collected for specified, explicit and legitimate purposes and not subjected to further processing incompatible with those purposes.
- **Data minimisation:** Collected data should be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- **Accuracy:** Data are to be kept up to date and reasonable steps should be taken to ensure the erasure or rectification of inaccurate data.
- **Storage limitation:** Data must be stored in manners which permit the identification of data subjects only for the minimum necessary timeframes to perform the purposes of collection/processing (longer periods are sometimes possible according to Article 5 of the GDPR).
- **Integrity:** Technical and organizational measures must be implemented to prevent unauthorized or accidental modification and erasure of Personal Data.
- **Confidentiality:** Technical and organizational measures should be implemented to prevent unauthorized or accidental access and disclosure of Personal Data.
- **Accountability:** Compliance with these principles, and in general with the normative framework that surrounds personal data is the responsibility of the controller, as is the burden to demonstrate compliance.

The GDPR includes several specific requirements which have been considered by the following subsection of this deliverable, including but not limited to: Requirements for consent (Art. 7), protection of underage persons (Art. 8) and processing of special categories of data (Art. 9); dispositions on the facilitation of exercise of the data subject's rights of information (Arts. 13 and 14), access to personal data (Art. 15), rectification (Art. 16) and erasure (Art. 17); explicit regulations regarding data portability (Art. 20); Protection of the individual vis-à-vis automated decision-making mechanisms (Art. 22); the adoption of data protection by design and by default and requirements to guide data controllers and processors (Arts. 24-31); and Further regulation of transfers of data to countries outside the European Union and those countries which do not ensure equivalent levels of protection to personal information (Arts. 44-50).

While most of these requirements are fundamentally organizational in nature (as they pertain chiefly to the organizational structure and data management capabilities of personal data controllers and processors); they are intrinsically related (and sometimes explicitly so, as in the case of Articles 24-31) to the introduction of strong security measures. In this regard, the GDPR closes the traditional divide between privacy and security while enhancing user's rights through the incorporation of not only a privacy and privacy-by-design and privacy-by-default approach, but also by expressly introducing some security considerations and practices to the legal framework of personal data protection, and, most importantly, to the rights available to the end-user.

The e-Privacy Directive

Best known for expressly regulating the use of Cookies and other tracking devices[15] in IT systems, the e-Privacy Directive (European Parliament & European Council, 2009) complimented Directive 95/46/EC as it was aimed fundamentally at maximizing the protection of the rights of end-users of the electronic communications sector. As such, it included express dispositions on the security requirements to be implemented from a technical and organizational point of view by providers of publicly available electronic communications services; confidentiality of communications[16]; protection of traffic data; billing, call identification and restriction; protection of location data; subscriber directories and unsolicited communications.

The dispositions made by the e-Privacy Directive are currently being reviewed as it will soon be replaced by the regulation[17]. The latest proposal version available to the public (European Council, 2017) shows that the new Regulation will be aimed towards particularising and complimenting the dispositions of the GDPR: *"[…] the e-Privacy proposal is a lex specialis to the GDPR as regards electronic communications data that are personal data. The e-privacy also seeks to ensure and protect the right to the confidentiality of communications enshrined in Article 7 of the Charter and Article 8 of the European Convention of Human Rights"*(Lauristin, 2017, p. 91).

[15] As it declares, starting from its Recital 24 that *"Terminal equipment of users of electronic communications networks and any information stored on such equipment are part of the private sphere of the users"* (European Parliament & European Council, 2009), and requires that any program installed on such equipment to be based on legitimate purposes. This is further expanded by Recital 25, which states that these legitimate purposes include the provision of information society services, and as such *"their use should be allowed on condition that users are provided with clear and precise information (…) so as to ensure that users are made aware of information being placed on the terminal equipment they are using"* (European Parliament & European Council, 2009). Additionally, the recital requires that the user is given the right to refuse, and that any information is provided in a user-friendly manner. The contents of these recitals are synthetized and further clarified by article 5.3 of the directive, which formally introduces these limitations to the applicable body of law of the European Union) (in direct connection to the dispositions mentioned in supra note 16).

[16] Confidentiality of the communications was protected by the Directive's article 5, which required member states to introduce safeguards on their national legislation to *"prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned (…) this paragraph shall not prevent technical storage which is necessary for the conveyance of a communication (…)"* (European Parliament & European Council, 2009).

[17] Infra Section 4.2 considers only the requirements of the GDPR and the e-Privacy Directive as no final version of the e-Privacy Regulation has been published so far. Future revisions of this document might address any changes introduced by the Regulation if necessary.

The proposed regulation presents significant updates vis-à-vis the e-privacy directive and reflects not only the many ways in which technology has evolved, but also to respond flexibly to the needs of the industry while safeguarding end-user rights. For IoT[18] end-users the proposed regulation will ultimately grant a more granular level of control over their personal data by setting higher conditions to the processing of electronic communications data (article 6); the storage and erasure of data and metadata (article 7); the protection of information stored in terminal equipment of end-users and related to or processed by or emitted by such equipment (article 8); and the information and options for privacy settings to be provided to the end user (article 10).

4.2 Identification of Personal Data Protection Requirements

This section will synthetically characterize the most relevant privacy requirements that should be monitored by ANASTACIA. It will build upon the privacy requirements identified by D1.3, as well as upon relevant dispositions in both the GDPR and the e-Privacy directive, to define the most relevant privacy requirements to be examined in a monitored system, as possible considering ANASTACIA's capabilities. This will not only serve to characterize the privacy of the monitored system, but will also facilitate the minimization of any risks to personal data which could be generated throughout ANASTACIA's monitoring and reaction mechanisms.

An effort will be made to provide not only the summary description of the requirement, but also an initial set of considerations for ANASTACIA's potential implementation of these requirements (both internally and on the monitored system). Additional references[19] will be provided for each, including the associated requirement in ANASTACIA D1.3, the location of each requirement in the relevant normative framework, and any related indications found in technical standards which could enrich its context.

Req-1 Enable privacy safeguards by default

Summary description:

Privacy safeguards shall be enabled by default, without requiring further intervention by the user. This requirement stems from the GDPR, which states that "*The controller shall implement appropriate technical and organizational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage, and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons*"(European Parliament & European Council, 2016).

[18] The e-Privacy Regulation addresses IoT directly. Recital 12 of the latest draft notes that *"The use of machine -to-machine services, that is to say services involving an automated transfer of data and information between devices or software- based applications with limited or no human interaction, is emerging. While the services provided at the application -layer of such services do normally not qualify as an electronic communications service as defined in the [Directive establishing the European Electronic Communications Code], the transmission services used for the provision of machine -to-machine communications services regularly involves the conveyance of signals via an electronic communications network and, hence, normally constitutes an electronic communications service. In order to ensure full protection of the rights to privacy and confidentiality of communications, and to promote a trusted and secure Internet of Things in the digital single market, it is necessary to clarify that this Regulation, in particular the requirement s relating to the confidentiality of communications, should apply to the transmission of machine- to-machine electronic communications where carried out via an electronic communications service"* (European Council, 2017). In accordance with this approach, article 5(2) of the proposed regulation recognizes that *"Confidentiality of electronic communications data shall apply to the transmission of machine -to-machine electronic communications where carried out via an electronic communications service."* (European Council, 2017)

[19] These references will be of great utility if presented to the system administrator and Data Protection Officers by the DSPS as they will further define the measures they should implement to protect their systems or to follow when applying the recommended contingencies.

ANASTACIA's internal data management processes and systems should be designed to protect end-user privacy. Furthermore, when performing the examination of the monitored system, ANASTACIA should examine the status of all data protection safeguards available to the monitoring and reaction components and ensure that they are enabled by default.

Associated D1.3 requirement:

- PR.1

Requirement location:

- GDPR: Art. 25, Recital 78

Related indications:

- ISO/IEC 29151:2017: A.6
- ITU-T X.805: 6.8
- ITU-T Y.2060: 7.2
- ITU-T Y.2066: 7.5 / 7.7 / 8.8
- NIST SP 800-82r2: 6.2.19

Req-2 Identification of data categories, non-processing of special categories, and protection of traffic and location data

Summary description:

The GDPR prohibits *"Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation"* (European Parliament & European Council, 2016, p. 38) unless one of specific exceptions apply.

Furthermore, the e-Privacy directive[20] calls for the special protection electronic communications data, namely traffic[21] and location[22] data. This protection reflects the potential of these categories of information to affect the data subject's fundamental right of confidentiality of communications. *"Communication types in IoT systems include end-device to end-device (e.g., sensor node to sensor node, sensor node to actuator, etc.), end-device to gateway, gateway to central devices (e.g., cloud server, IoT platform servers, etc.), and/or central devices to application servers. The network communications for IoT services and applications naturally embed the traditional security and privacy risks[23]".* (Cambiaso, Mongelli, et al., 2017, p. 13)

ANASTACIA should incorporate express organizational and technical measures to avoid the processing of sensitive data and/or the identification of sensitive data from any of the datasets and measurements available to the system (apply the data minimization principle and storage limitation principles, among

[20] Protection that will most likely be extended under the upcoming e-Privacy Regulation.

[21] *"Traffic data may include any translation of this information by the network over which the communication is transmitted for the purpose of carrying out the transmission. Traffic data may, inter alia, consist of data referring to the routing, duration, time or volume of a communication, to the protocol used, to the location of the terminal equipment of the sender or recipient, to the network on which the communication originates or terminates, to the beginning, end or duration of a connection. They may also consist of the format in which the communication is conveyed by the network"(European Parliament & European Council, 2009).*

[22] *"Location data may refer to the latitude, longitude and altitude of the user's terminal equipment, to the direction of travel, to the level of accuracy of the location information, to the identification of the network cell in which the terminal equipment is located at a certain point in time and to the time the location information was recorded" (European Parliament & European Council, 2009).*

[23] *"such as session hijacking, DDoS attack, denial service, IP spoofing, man-in-the-middle, etc. What brings more cautious on IoT in security and privacy is the vulnerability of IoT devices. It is well known that the low-powered sensor nodes and their communication protocols are much vulnerable on security attacks. In addition to it, privacy related data such as location info is often included for IoT services, which brings the needs of careful privacy design."*(Cambiaso, Mongelli, et al., 2017, p. 13).

others). Special care must be taken to identify the categories of data which might have been involved in a potential breach in the monitored system, to ensure that the correct remedial and informational measures are adopted.

Associated D1.3 requirement:

- PR.1

Requirement location:

- GDPR: Art. 9, Art. 14, Art. 30, Art. 31, Art. 37, Art. 47, Art. 83
- Directive 2002/58/EC: Art. 5, Art. 6, Art. 9

Related indications:

- ETSI TR 103 305: CSC 17
- ISO/IEC 27001:2013: A.8.2.1; A.8.2.3; A.12.1.1; A.14.1; A.14.1.1; A.16; etc.
- ISO/IEC 29151:2017: 8.2
- ITU-T X.805: 6.8
- ITU-T Y.2060: 7.2
- ITU-T Y.2066: 7.5 / 7.7 / 8.8
- NIST SP 800-82r2: 6.2.19

Req-3 Data management and respect of data subject rights (information/access/rectification/restriction/objection/deletion)

Summary description:

This requirement aims to fulfil several of the rights granted by the GDPR to data subjects, including the rights of access, rectification, opposition and deletion of personal data.

In the specific context of ANASTACIA and the systems that it monitors, it relates to the need to ensure that any non-anonymized personal data undergoing processing is made available through the system GUI, which shall be developed in a way that enables data subject's rights to access, rectify, delete or block contested or non-factual/irrelevant personal data.

This requirement has several additional implications: a) In compliance with the right of information, the data subject is to be informed as soon as possible after a breach to his/her personal data has taken place; b) the right of access entails also the requirement to ensure that the system upon which such right is to be exercised is available as soon as possible after facing a data breach, so as to ensure the data subject remains in control of his personal data. Finally, all necessary measures are to be incorporated to ensure that whenever a request for deletion has been received from the data subject, any controllers or processors which possess copies of the information should be informed, asked to comply with such request.

Associated D1.3 requirements:

- PR-1; PR-6; PR-8; PR-12; PR-14

Requirement location:

- GDPR: Art. 15, 16, 17

Related indications:

- ETSI TR 103 305: CSC 17
- ITU-T X.1171: Annex A
- ISO/IEC 27001:2013: 6.1.2; A.8.1.1; A.8.2.1; A.9; A.12.1.1; A.13.2.1; A.14.1.1; A. 18.1.1; A.18.1.3.

- ISO/IEC 29151:2017: A.9; A.10
- PIA Methodology for France: P. 13; GP- 1.6; GP-1.7
- ITU-T X.805: 6.8
- ITU-T Y.2060: 7.2
- ITU-T Y.2066: 7.5 / 7.7 / 8.8
- NIST SP 800-53 R4: Appendix J: DM-1
- NIST SP 800-82r2: 6.2.19

Req-4 Data retention

Summary description:

A reasonable retention period should be set, after the expiration of which, data should be erased or de-identified. Unnecessary personal data should be erased by the system without undue delays.

ANASTACIA D1.3 states in PR-13 that *"The default personal data retention period is set at one (1) month, without prejudice to other conflicting legal obligations, which will be appraised on a case by case basis on motivated request by the data controller (e.g. in case of different retention period for internet traffic data mandated by specific law on detection and prevention of crime)"*.

The exceptions to the one-month retention policy set above may derive from the implementation of Article 15(1) of the e-Privacy Directive (Directive 2002/58/EC) at national level. Such Directive provides that: *"Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period"* when it is necessary to safeguard *"national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system"*. (Trapero et al., 2017).

All processes related to ANASTACIA end-users should utilize reasonable or non-extensive data retention periods as well as implement any technical measures as necessary to ensure that unnecessary personal data are neither requested nor registered by the system (storage limitation and data minimization principles). Effective deletion of the data should be ensured and transparency on the followed procedures kept towards the end-users.

Associated D1.3 requirements:

- PR-13

Requirement location:

- GDPR: Art. 17; Art. 25
- Directive 2002/58/EC: Art. 15(1)

Related indications:

- ETSI TR 103 305: CSC 17
- ISO/IEC 27001:2013: 6; 6.1.2; A.8.3.2; A.9; A.12.3; A14.1.1; A.16; Annex A
- ISO/IEC 29151:2017: A.7
- ITU-T X.805: 6.8
- ITU-T Y.2060: 7.2
- ITU-T Y.2066: 7.5 / 7.7 / 8.8
- NIST SP 800-53 R4: Appendix J: DM-1; UL-1
- NIST SP 800-82r2: 6.2.19

Req-5 Deidentification of Personal Data (Anonymization, Pseudonymization, Non-identifiability)

Summary description:

The GDPR recognizes that the rights of access, rectification and erasure (including the right to be forgotten), restriction of processing, and data portability shall no longer be applicable when the controller of personal data is able to demonstrate that it is not able to identify a data subject. This requirement then focuses on the information and practices that are necessary to ensure that identifiability[24] is no longer possible.

Whenever data from the monitored system (be it sensor, database, device or network usage information, etc.) is further processed by the system for security reasons, ANASTACIA must anonymize[25] or pseudonymize[26] any information which could potentially be linked to an end-user.

Associated D1.3 requirement:

- PR.1

Requirement location:

- GDPR: Art. 11, Art. 32

Related indications:

- ETSI TR 103 305: CSC 17
- ISO/TS 25237:2008: p2-5
- ISO/IEC 27001:2013: 6.1.2; 8.2; 8.3; A.7.1; A.8.2.1; A.8.2.3; A.14.1.1; etc.
- ISO/IEC 29151:2017: 12.1.5; A.6
- ITU-T X.1171: 10.6
- ITU-T X.805: 6.8
- ITU-T X.816: 7.3.1
- ITU-T Y.2060: 7.2
- ITU-T Y.2066: 7.5 / 7.7 / 8.8
- NIST SP 800-122: 4.2.2
- NIST SP 800-53 R4: Appendix J: AR-7
- NIST SP 800-82r2: 6.2.19
- PIA Methodology for France: P. 13; GP-1.8; GP-1.9; GP-3

Req-6 Records and audit of processing activities and disclosures

Summary description:

This requirement should be introduced and considered for all monitoring activities for which ANASTACIA is utilized *"based on the assumption that the ANASTACIA framework would be deployed in the context of*

[24] De-identification is a *"General term for any process of removing the association between a set of identifying data and the data subject"*(International Organization for Standardization, 2008, p. 3).

[25] Anonymization is the *"process that removes the association between the identifying dataset and the data subject"*(International Organization for Standardization, 2008, p. 2). Anonymized information is defined as previously identifiable information that has been de-identified and for which a code or other association for re-identification no longer exists. This can be performed by the application of statistical disclosure limitation techniques, such as: generalizing the data, substitution, shuffling, number and date variance, encryption, nulling out or deletion, masking out, additional complex rules, etc.

[26] Pseudonymization is a *"particular type of anonymization that both removes the association with the data subjects and adds an association between a particular set of characteristics relating to the data subject and one or more pseudonyms"*(International Organization for Standardization, 2008, p. 5).

personal data processing activities which are not defined by ANASTACIA itself, yet by the entity deploying ANASTACIA's system as a service; in that regard, ANASTACIA will typically fulfil the tasks of a Data Processor, and in so doing it provides some means to achieve the purposes set by another entity, the Data Controller"(Bianchi et al., 2017, p. 62).

Records of the diverse processing activities, containing at minimum the following elements are to be kept: name and contact details of the controller, joint controller, controller representative and data protection officer; purposes of the processing; description of the categories of data subjects, of personal data and of recipients of disclosures; data related to transfers of personal data to third countries; the envisaged time limits for erasure; and the descriptions of the technical and organizational security measures (European Parliament & European Council, 2016).

Additionally, records of any personal data disclosures should be kept so as to ensure the implementation of the principle of accountability and to enable the performance of the notifications and communications found throughout these privacy requirements. These records should be available to the system manager on the GUI to enable the performance of the notifications and communications required after a data breach has taken place. Finally, audits should be performed on the organization, programs, information systems and applications; particularly as they collect, maintain, process and disclose personal information to ensure they comply with the applicable legal and contractual security and privacy requirements.

Associated D1.3 requirement:

- N.A.

Requirement location:

- GDPR: Art. 30

Related indications:

- ETSI TR 103 305: CSC 17
- ISO/IEC 27001:2013: 7.5
- ISO/IEC 29151:2017: A.8, A.9
- ITU-T X.805: 6.8
- ITU-T X.816: 7.3.1
- ITU-T Y.2060: 7.2
- ITU-T Y.2066: 7.5 / 7.7 / 8.8
- NIST SP 800-53 R4: Appendix J: AR-4, AR-8
- NIST SP 800-82r2: 6.2.19

Req-7 Security of processing (prevention of unauthorized access, alteration, disclosure and destruction of personal data)

Summary description:

According to the GDPR, technical and organizational measures to ensure the security, confidentiality, integrity, availability and resilience of processing systems and services should be introduced *"Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself (…)"*(European Parliament & European Council, 2016, p. 48).

This high-level requirement aims to ensure the introduction of technical and organizational security safeguards to protect personal data by both the monitored IT systems and ANASTACIA. From an organizational point of view, the requirement addresses the need to define, implement (and update) security mechanisms and policies to the very design of the system. From a technical point of view, it requires such measures[27] as the introduction of strong identification, authentication and authorization mechanisms, audit and accountability tools, configuration and information management, prevision of the need for continuity of operations, and protection of system communications and information integrity capabilities for the system.

Considering ANASTACIA's capabilities[28], monitoring should attempt to identify potential privacy risks caused by imperfections or vulnerabilities in the security measures implemented at the network layer (and at the application layer, whenever possible). Furthermore, it should attempt to prevent the alteration of PII; to ensure the accountability of any internal parties which might have caused such alterations; to account for the risk of disclosure of personal data and take preventive measures to avoid any potential affectations to the rights of data subjects.

Associated D. 1.3 requirement:

- PR-16

Requirement location:

- GDPR: Art. 32
- Directive 2002/58/EC: Art. 9
- Directive 2016/1148: Art. 16

Related indications:

- ETSI TR 103 305: CSC 17
- ISO/IEC 27001:2013: 8.2; 8.3; Annex A
- ISO/IEC 29151:2017: 11, 12, 13, 16

[27] The exact extent of the technical measures to be implemented is unclear in the text of the GDPR, as it is understood that they will depend on the nature and associated risks of the system that is to be protected. In the specific realm of IoT devices, a State of the Art examination by NXP and the law firm Arthur's Legal identified a large number of such measures, namely:

- *"User / Human Factor: Privacy by design; Risk Assessment on privacy / threat analysis; no PII by default; avoid personal data collection or creation; design and engineer ecosystems in IoT as-if these will process personal data; de-identify or delete personal data; secure user identity; data minimization, isolation and transparency; data retention and deletion; address the personal data lifecycle; consider data as dynamic; data encryption by default; data accountability; single point of contact; management of the use and access to applications and data; safety critical assessment; inclusive environment; education of users/awareness.*
- *Data: data integrity, confidentiality, encryption by default (on application layer); secure exchange of data; data portability; data assessment and classification; data control; compliance with data processing regulations; anonymization, pseudonymization and de-identification; data ownership (proof of origin); personal data verification (true, fabricated, altered).*
- *Service: availability; safety of disconnected devices; updatability/service life-cycle management; support; autonomic services provisioning; incident response model & management; recovery model; sunset model.*
- *Software/application: Security design and coding principles; end-to-end security; secure integrity of applications; role based access control for applications; command verification based on context; Software protection, maintenance, update and life cycle management; interoperability of components and communication protocols; identity cross-authentication; message authentication; vulnerability handling and information sharing; app authentication (including source authentication); secure application download; secure OS; reset mechanism; logging and monitoring; firewall /SDP architecture; software and app isolation.*
- *Hardware: risk assessment; security by design; device integrity/individual device ID; secure deployment, management, maintenance, and end-of-life; security review; attack surface minimization; secure communication channels; secure boot; secure firmware update; 3rd party evaluation and testing; supplier verification; device capabilities specification; inventory management.*
- *Authentication: use of strong authentication; authorized access to data; identification after authorization, secure key storage; revocation process; management of administrator privileges; data processing authorizations; certificate evaluation.*
- *Architecture/network: Transparency of security architecture, use of cryptographic principles and key management; root authority; state of the art, standard and proven protocols; network isolation; proximity detection; cloud security; strong authentication; and restrictive communications."*(Kruse Brandao, 2017, pp. 12–18).

[28] See supra Section 5.1.2.

- TU-T X.1171: 10.6
- ITU-T X.1205: 8.1
- ITU-T X.805: 6.8
- ITU-T X.816: 7.3.1
- ITU-T Y.2060: 7.2
- ITU-T Y.2066: 7.5 / 7.7 / 8.8
- ITU-T Y.3051: 7.2
- ITU-T Y.3052: 8.2
- NIST IR 7628 R1: D-3.7
- NIST IR 8114: 2.4
- NIST SP 800-53 R4:   Appendix J: AR-4, AR-7, AR-8
- NIST SP 800-82r2: 6.2.19
- PIA Methodology for France: P. 13; GP-1.8; GP-1.9; GP-3

Req-8 Data breach information

Summary description:

In direct relation with the transparency and accountability principles enshrined by the GDPR, the ANASTACIA system must immediately inform its users of any breach to personal data leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed, in order to enable that user to fulfil its obligations to notify data breaches to competent Data Protection Authorities and concerned data subjects.

Beyond its intended capabilities of providing insights and information on threats to the monitored systems through its Dynamic Privacy and Security Seal, ANASTACIA should seek to comply with this requirement by providing information to end-users and system administrators of both any data breach that takes place within ANASTACIA's core services, to maintain end-user's trust in the system.

Associated D1.3 requirement:

- PR-10

Requirement location:

- GDPR: Art. 33, 34

Related indications:

- ETSI TR 103 305: CSC 17
- ISO/IEC 27001:2013: A.16; A.18.1.4
- ITU-T Y.2060: 7.2
- ITU-T Y.2066: 7.5 / 7.7 / 8.8

Req-9 Encryption of personal data by default

Summary description:

All personal data should be encrypted whenever it is stored or transferred, and strong encryption mechanisms[29] should be used at all times.

On this, D1.3 states that *"Encryption will be applied to all stages of handling data, including in communication, storage of data at rest, storage of keys, identification, access, as well as for secure boot*

[29] Cryptographic protocols: TLS, IPsec, Kerberos, PPP with ECP, ZRTP, etc.

process. The legal source of this requirement is Article 32 of the GDPR, whereby it mandates the controllers and processors to ensure a level of security appropriate to the risk, including measures that have the "ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services"." (Trapero et al., 2017).

This is a shared security requirement with special relevance for Personal Data Protection due to its specific inclusion in the text of the GDPR. "Organizations can protect the confidentiality of PII at rest, which refers to information stored on a secondary storage device, such as a hard drive or backup tape. This is usually accomplished by encrypting the stored information." (McCallister, Grance, & Scarfone, 2010, pp. 4–8). While ANASTACIA will most likely be unable to determine the encryption of data at rest, it should focus its monitoring and reaction capabilities towards ensuring that the monitored system properly encrypts any data it transmits.

Associated D1.3 requirement:

- PR-11

Requirement location:

- GDPR: Art. 30, 32

Related indications:

- ETSI TR 103 305: CSC 17
- ISO/IEC 27001:2013: 7.5, 8.2; 8.3; Annex A
- ISO/IEC 29151:2017: 10.1
- ITU-T X.1171: 10.6
- ITU-T X.805: 6.8
- ITU-T X.816: 7.3.1
- ITU-T Y.2060: 7.2
- ITU-T Y.2066: 7.5 / 7.7 / 8.8
- NIST IR 7628 R1: D-3.7
- NIST SP 800-122: 4.2.1
- NIST SP 800-53 R4: Appendix J: AR-4, AR-7, AR-8
- NIST SP 800-82r2: 6.2.19
- PIA Methodology for France: P. 13; GP-1.8; GP-1.9; GP-3
- PIA Methodology for United Kingdom: P. 27

Req-10 Update and review privacy measures

Summary description:

Technical and organizational measures to ensure the privacy of end-users should be implemented and periodically updated/reviewed as necessary to ensure their effectiveness. Organizational and technical processes to ensure the effectiveness of security measures are required by the GDPR and constitute part of ANASTACIA's principal objectives. Generally, this requirement calls for audits and cross-verification of the security measures that have been implemented, and of the verification mechanisms themselves to maximize accountability and transparency and ensure the security and confidentiality of personal data.

This requirement extends to the organizational efforts that will surround ANASTACIA's implementation. Particularly, it relates to the necessary updates that are to be introduced to the risk analysis and contingency plans generated by the organization when implementing ANASTACIA. For ANASTACIA, the requirement introduces the need to perform timely updates to the monitoring and reaction services to maximize their potential for addressing new privacy risks.

Associated D1.3 requirement:

- PR-9

Requirement location:

- GDPR: Art. 24

Related indications:

- ETSI TR 103 305: CSC 17
- ISO/IEC 27001:2013: 4; 5; 6; 7; 8; 8.2; 8.3; 9; 10; Annex A
- ITU-T X.1171: 10.6
- ITU-T X.1205: 8.1
- ITU-T X.805: 6.8
- ITU-T Y.2060: 7.2
- ITU-T Y.2066: 7.5 / 7.7 / 8.8
- ITU-T Y.3052: 8.3
- NIST IR 7628 R1: D-3.7
- NIST SP 800-53 R4: Appendix J: AR-1
- NIST SP 800-82r2: 6.2.19
- PIA Methodology for France: P. 13; GP-1.8; GP-1.9; GP-3

4.3 Characterization of Use Cases vis-à-vis Personal Data Protection Requirements

This section aims to introduce the ANASTACIA use cases and to further specify the personal data protection requirements identified throughout the previous section by providing some clarifying remarks whenever relevant.

UC_0.1 - Secure/privacy-compliant Campus ICT infrastructure management

> *"The Keamanan Campus is renowned for having a sophisticated* ***ICT/IoT infrastructure that controls all main buildings and facilities in the Campus****, which are under the direct responsibility of the Campus Manager, Mr Cahaya Budi.*
>
> *In parallel to several BMS tools, Mr Budy has a brand new installation of an ANASTACIA-powered security & privacy monitoring solution, which allows him to have an immediate view of the status of the monitored infrastructure without the burden of checking different dashboards and inspecting technical logs: a nice Dynamic Security & Privacy Seal (DSPS) change its status according to detected threats, whereas a simplified UI summarizes the* ***main mitigation actions autonomously undertaken by the system****. The DSPS is green since the ANASTACIA-powered solutions was installed, several months ago, when Mr Budi also easily configured the main security policies according to the internal Campus regulations.*
>
> *Yet, on a sunny Monday morning, an* ***anomalous traffic*** *is detected coming from a part of the network devoted to the management of* ***CCTV security cameras****, that* ***register videos from many different places*** *and forward them to a proxy server,* ***where streaming are pre-processed before relevant information (i.e. video***

> ***sections in which people access restricted labs) are sent for storage and further inspection*** *to the CED in the central control room.*
>
> *The potential threat is immediately detected by the system that, according to the security policies currently deployed, notifies Mr Budi changing the colour of the DSPS (from green to orange), suggesting* ***potential privacy breaches*** *that should be further investigated and starting the* ***definition of a mitigation plan*** *meant to limit any potential damage.*
>
> *The ANASTACIA-powered system takes action at three different levels:*
>
> *1) as for IoT devices under potential attack (this time, the CCTV cameras), the system momentarily* ***shuts them down to limit any further problem****;*
>
> *2) at security level, by means of dedicated security VNFs, the system automatically* ***deploys several different virtual appliances (a firewall, an AAA server, an Intrusion Detection System)*** *in order to intensify the monitoring and reinforce the overall security level;*
>
> *3) at network level, the system reconfigures the whole setup in order to leverage SDN functionalities and* ***temporarily isolate the part of the network under attack****,* ***redirecting the traffic to a duplicated pre-processing edge server*** *according to the newly defined network.* ***Cameras are then gradually reactivated****, in order to verify which specific device has been hacked or if the detected anomalous traffic has to be considered somehow a "false positive".*
>
> *Mr Budi, who is not a network expert and ignores most of the sophisticated network/security technologies that are used by the system to define and enforce the mitigation plan, gets a simplified report of the main actions undertaken.*
>
> *Furthermore, he also receives a* ***notice on potential privacy issues*** *that should be further investigated, since he is also the Campus Data Controller: in particular, the* ***identified threats****, impacting on a server that processes video streaming captured when access to restricted labs are detected by motion sensors, might have caused a* ***data leakage related to sensitive information****, and deserve further attention by the ICT staff, that is thus immediately summoned for an* ***internal meeting to verify any data leakage****.*
>
> *Notwithstanding the mitigation actions were successfully undertaken and all functionalities were efficiently restored, the* ***DPSP stays orange, until a manual confirmation that also privacy issues have been duly addressed*** *is provided by Mr Budi and the ICT staff – both* ***security and privacy are then fully restored****."*
>
> *ANASTACIA D1.2 "User Centred Requirements Initial Analysis."* (2017, p. 18)

The first use-case described above includes relevant elements of all of the identified requirements, as such compliance analysis should consider:

- **Req-1: Enable privacy safeguards by default:** The case mentions both preventive elements (safeguards) and corrective actions to be undertaken. In order to ensure that the system complies with this requirement, these elements should be tailored to ensure that these elements are not only enabled by default, but also tailored to the specific needs of the monitored system (i.e. previous identification of privacy risks of security cameras per location, correct definition of policies and corrective actions to be performed by ANASTACIA, proper methodology, and documentation of the privacy impact assessment to be performed by staff members).
- **Req-2 Identification of data categories, non-processing of special categories, and protection of traffic and location data:** Compliance with Req-2 is only possible through an initial identification of data categories compiled and processed by the system that permits the introduction of additional

security measures for those IoT devices which might process personal data (particularly if the data in question is of a sensitive nature).

- **Req-3 Data management and respect of data subject rights:** While data subjects are not directly involved in this use-case, the system should ensure the respect of the data management requirement and particularly should respect the data subject's right to access and information: The system should ensure service continuity to enable end-user's performance of their rights. Furthermore, following the performance of the privacy impact assessment by staff members, the DSPS system should request the DPO's inputs on compliance with this requirement before returning the privacy status of the system to green.
- **Req-4 Data retention:** Storage of personal information should meet both the purpose and storage limitation principles, as such, the verification activities undertaken by the staff after a breach should ensure that no data exceeding the retention period remains on the affected system and that relevant data erasure configurations on the system have not been altered by the breach.
- **Req-5 Deidentification of Personal Data:** The requirement relates to the purpose limitation and data minimization principles as it involves the necessity to ensure that the processing server is capable of anonymizing or pseudonymizing any information which could serve to identify a person, if that information is not strictly necessary for the specified purpose for which it is processed and stored.
- **Req-6 Records and audit of processing activities and disclosures:** Logs kept by the CCTC security cameras and the proxy servers that perform the pre-processing and storage of the information should be examined to maximize ANASTACIA's privacy breach identification potential.
- **Req-7 Security of processing:** This requirement shall be achieved through the correct implementation of all the security safeguards detailed in ANASTACIA D2.2. Whenever possible, the system should provide additional security towards those elements that are in particular risk due to the data categories processed or compiled by them.
- **Req-8 Data breach information:** Both the system and its administrator should correctly identify the need to inform data subjects of breaches to their personal data. In the present use case, this task should be recommended by ANASTACIA to the Campus Data Controller and included in the mitigation plan.
- **Req-9 Encryption of personal data by default:** All personal data transmitted to/from the network and the security cameras should be encrypted by default to minimize the possibility of unauthorized access or disclosure. If such encryption does not take place, ANASTACIA should introduce the necessary channel protection mechanisms by default.
- **Req-10 Update and review privacy measures:** Both ANASTACIA's policies and controls and the defined mitigation plans should be updated and reviewed after a breach takes place to maximize future efficiency and efficacy.

UC_MEC.1 - Spoofing attack on the security camera system

*"A smart **security camera system** was installed in a city to prevent illegal actions. The recorded videos are sent to nearby MEC servers which can operate **a data pre-treatment before sending interesting information to the Cloud. A group of hackers wants to have access to the unprocessed videos to obtain critical information about citizens, in order to blackmail them**. They want to use **a spoofing technique** to make the cameras believe their servers are the MEC servers. **They managed to get the IP address of the server and they are able to use it**.*

*To prevent this attack, Bob, the Administrator, will use ANASTACIA to ensure that the security camera systems **allows data exchange only between trusted equipment, by using secure protocols, authentication, correct network access***

> ***controls and system design****. ANASTACIA will be used to monitor and use Penetration Testing modules to quickly react in order to eliminate this intrusion. ANASTACIA will be used to provide a quality-of-security seal that ensures that systems are correctly patched against such technique and will deploy Firewalls with DPI capability VNF in the proper locations."*
>
> *ANASTACIA D1.2 "User Centred Requirements Initial Analysis."* (2017, p. 22)

This use-case relates mainly to the following requirements:

- **Req-2 Identification of data categories, non-processing of special categories, and protection of traffic and location data:** The categories of personal data that could be captured by the cameras and further processed should be clearly identified. In the context of ANASTACIA, this requirement signifies that the system should be capable of identifying the devices involved in the capture, processing and storage of video data.
- **Req-6 Records and audit of processing activities and disclosures:** All the devices on the network should be able to compile activity logs to ensure that the remedial activities performed after a breach are able to correctly identify the dates when the system were vulnerated and correctly inform the affected parties. This functionality should be examined by ANASTACIA and provided as part of the system's accountability tools.
- **Req-7 Security of processing:** The system should introduce additional security measures to prevent unauthorized access to the video streams. This includes ANASTACIA-based functionalities such as IDS/IPS.
- **Req-8 Data breach information:** A report of any breach/potential breach should be immediately generated by ANASTACIA's DSPS (based upon the information received from the Monitoring and Reaction components) to ensure the DPO and other organizational actors are aware of potential breaches to personal data and to ensure swift compliance with the notification requirements of the GDPR if necessary.
- **Req-9 Encryption of personal data by default:** All traffic to/from the network should be automatically encrypted to minimize the potential of personal data breaches (thus removing the possibility of unprocessed videos being accessed by malicious actors even if they were to manage to spoof the server's IP address).

UC_MEC.2 - Man-in-the middle attack on the MEC server scenario

> *"A SME offers* ***security camera systems*** *to its clients by proposing* ***Mobile Edge Computing Solutions****. Eve is a* ***disgruntled employee*** *who wants to damage the company's image, by* ***spreading on the internet sensitive security videos from its employer's biggest client****. Their* ***security cameras are sending all of the recorded videos to MEC servers****, deployed by the security SME in its client sites, to operate the* ***information processing****. As Eve was working in this biggest client security cameras project,* ***she illegally kept all the credentials and certificates enabling her to decrypt the transmission between the MEC server and the cameras****, which allows her to organize a* ***man-in-the-middle attack****, and* ***download the videos*** *on her home computer.*
>
> *However, Bob, the administrator will use ANASTACIA to ensure that the system can react to minimize such attacks. ANASTACIA will assist BOB to provide an enforced network access policy and allow him to protect the change of credentials."*
>
> *ANASTACIA D1.2 "User Centred Requirements Initial Analysis."* (2017, p. 26).

This use-case involves three main interactions with the identified requirements that we should consider, particularly as relates to the identification of data categories, security of processing and encryption of personal data:

- **Req-2 Identification of data categories, non-processing of special categories, and protection of traffic and location data:** The case notes that all recorded videos are submitted to the MEC servers. This element makes sense in consideration to the purpose of the processing that is to be performed (security), however before processing takes place, the categories of data that might be involved should be considered along with the possibility of incurring in unauthorized processing of special categories of personal data due to the constant and indiscriminate transmission and processing of the video feeds.
- **Req-7 Security of processing:** In line with our note on Req-2, all technical and organizational measures should be undertaken to minimize the risk of unauthorized access and disclosure of personal data. These measures include, but are not limited to: the performance of Privacy Impact Assessments by the SME (during deployment of the security cameras to ensure correct compliance with applicable requirements on consent and prevent processing of sensitive data); the introduction of strong identification, authentication, authorization mechanisms throughout the deployment; implementing firewalls and other network traffic tools to ensure that only certain IP addresses are able to access the feed, etc.
- **Req-9 Encryption of personal data by default:** the encryption of all communications to/from the network, client and the security cameras, so as to prevent potential privacy breaches through Man-in-the-Middle attacks, eavesdropping and other techniques.[30]

UC_MEC.3 - DoS/DDoS attacks using smart cameras and IoT devices

> *"The smart security cameras and IoTs can be used for a **massive distributed denial-of-service (DDoS)** as the attack that disrupted U.S. internet traffic on the October 21th 2016, where the attacks were made possible by the large number of unsecured internet-connected digital devices, such as **home routers** and **surveillance cameras**. Even though some of these devices are not powerful computers, they can generate massive amounts of bogus traffic, especially using a large numbers of IoT devices.*
>
> *All these bogus traffic are sent to targeted servers. In the MEC architecture these traffic will **pass through the MEC server**, since this server is situated at the access.*
>
> *To prevent this attack, Bob, the Administrator, will use ANASTACIA to ensure that MEC server will detect the attack and react to mitigate it. Moreover, ANASTACIA will be used to monitor and use Penetration Testing modules to quickly react in order to eliminate this intrusion. ANASTACIA will be used to provide a quality of security seal that ensures that systems are correctly patched against such technique and will deploy the adequate number of VNF security functions such as Firewalls and DPI in the proper locations."*
>
> *ANASTACIA D1.2 "User Centred Requirements Initial Analysis."* (2017, p. 29).

This use case has two main implications:

- **Req-3 Data management and respect of data subject rights:** From the point of view of this requirement, the extensive traffic that will pass through the MEC server will most likely affect the continuity of organizational services. As the goal of this requirement is to ensure that the data

[30] This relates as well to Req-5, as deidentification techniques should be used to prevent potential traffic analysis attacks which might extrapolate personal data out of the network usage.

subject remains in control of his/her personal data, any possible affectation to the service might impact the data management tools that enable the exercise of the rights to information, access, rectification, restriction, objection, and deletion.

- **Req-7 Security of processing:** on the other side presents us with a complementary need: that to prevent unauthorized access, alteration, disclosure and destruction of personal data, which might take place through the methods that have enabled the attackers to take control over the devices to perform the DoS/DDoS attack. As such, it introduces the need to perform all preventative and corrective measures to prevent this from happening (including, but not limited to disabling the devices/services in a temporary or controlled manner). While performing these steps however, all possible means should be introduced to ensure compliance with Req-3.

UC_MEC.4 - IoT-based attack in the MEC Scenario

> *"Telco networks are experiencing a drastic revolution embracing the opportunity to deploy Cloud Edge environments to host third-party services near to IoT devices. Edge-based service deployment can provide reduced latency compared to* ***Cloud-based provisioning and offer location-based contextual data awareness****. In this vein, a SME which provides security video surveillance via camera systems is interested in enhancing the* ***video pre-processing by leveraging the resources provided by the MEC environments.*** *Furthermore, accounting for the increased number of attacks related to IoT devices, the SME would require a higher level of security for their surveillance services, monitoring the traffic generated by its cameras and mitigating potential security threats.*
>
> *To guarantee the required security features, the Telco provider will adopt the ANASTACIA framework within its system, by appropriately integrating it with the existing network and service mechanisms, such as SDN, NFV, and cloud edge computing technologies. In this way, the Telco provider will be able to offer advanced Security-as-a-Service solutions, exploiting its capillary and flexible cloud-based network infrastructure. To meet the security requirements of the video surveillance SME, appropriate virtual instances of detection systems (e.g., IDS) will be deployed in the edge environment and will analyse the traffic generated by the cameras.*
>
> *In this scenario, a group of* ***hackers*** *aims at* ***exploiting vulnerabilities in the cameras used by the video surveillance SME to generate attacks*** *(such as DoS, scanning, etc.) against sensitive servers, which can be either the MEC hosting servers to create an* ***interruption in the processing of security videos or external third-party Internet servers.*** *The monitoring modules deployed by the ANASTACIA framework are able to fast detect the on-going attacks and to trigger the orchestration of appropriate countermeasures, such as isolating the compromised cameras by modifying the forwarding paths of software-based networks."*
>
> *ANASTACIA D1.2 "User Centred Requirements Initial Analysis."* (2017, p. 33)

Requirements 2 and 3 are particularly relevant for this use-case:

- **Req-2 Identification of data categories, non-processing of special categories, and protection of traffic and location data:** The case mentions several categories of data which could be relevant when protecting the personal data of monitored subjects, namely it recognizes that Edge-based services offer location-based contextual data awareness. The specific capabilities of such a system should be well considered when generating a set of privacy policies for the ANASTACIA-monitored system, so as to enrich the monitoring tool's privacy reports and to ensure the DPOs in charge of a PIA are aware of the potential affectation to the data subjects rights.

- **Req-3 Data management and respect of data subject rights:** The case recognizes the possibility of a DoS attack, which could lead to the affectation of the end-user's rights to access and information. Countermeasures undertaken by ANASTACIA should be mindful of this possibility and take a prioritized approach to minimize system downtime.
- **Req-5 Deidentification of Personal Data:** As scanning (sniffing and traffic analysis) attacks might be involved in the case, the use of secure channels is recommended in order to comply with this requirement. ANASTACIA should implement technical mechanisms to aggregate network traffic and introduce sufficient variables to minimize the risk of personal data extrapolation through traffic analysis.

UC_BMS.1 Cyber-attack at a hospital building

> *"Annihilos is a criminal gang who takes credit in destroying the reputation of big businesses. They are targeting BetterDays, a large international healthcare provider. The operations of BetterDays include owning and operating several hospitals worldwide, providing health insurance, and running ambulance and emergency services in many countries.*
>
> *Annihilos intends to* ***exploit a zero-day vulnerability*** *in the building management system that BetterDays uses in a large city hospital. The vulnerability allows the building management system to accept an external internet-based emergency web service message that will bring elevators and escalators in emergency mode to designated floors and overriding automatic operations of HVAC systems. But the emergency mode will also activate the fire safety services in the respective floors too. Annihilos plans to activate emergency in several floors simultaneously using several lifts. Since the fire-safety system listens, activates and responds to the emergency by activating the sprinklers and foams, it is possible to increase the risk of structural damage to the building and threat of lives in the hospitals. The false alarm could be escalated throughout the BetterDays hospital building as well as invite the city's fire-brigade response. Moreover, by accessing the HVAC network, Annihilos could switch-off emergency terminal units, overwrite heating and cooling set-points in various floors, stress the heating equipment towards damage, etc. Annihilos could increase the energy consumption, utility and HVAC maintenance costs of BetterDays hospital building.*
>
> *In addition, during the panic,* ***Annihilos gang members plan to gain physical unauthorized access to the data-centre of the hospital whose secure doors will be disengaged during an emergency. Annihilos could install rogue applications in the datacentre workstations to transfer or transmit sensitive data of their business and private data of their clients. Subsequent to the emergency, the rogue applications in data-centre workstations will allow Annihilos to launch a remote attack (e.g., via SQL injection) on the servers that host the hospital document management system.***
>
> *Chris, the hospital manager, can use ANASTACIA to ensure that BetterDays is safe from any such attack from Annihilos, as described in the following session."*
>
> *ANASTACIA D1.2 "User Centred Requirements Initial Analysis."* (2017, p. 36)

Due to the high risk to the life and well-being of the data subjects identified in this use-case, the following elements should be considered when interpreting the identified requirements:

- **Req-1: Enable privacy safeguards by default:** As part of the privacy-by-design approach, all personal data should be securely stored, and all necessary security mechanisms should be enabled by default in the system. While the necessary implementation of this requirement precedes the installation of ANASTACIA, the design elements of the system, including the location of the personal data and the potential vulnerabilities of the deployment should be considered when developing both the privacy and security policies.
- **Req-2 Identification of data categories, non-processing of special categories, and protection of traffic and location data:** Data categories involved in the case are potentially sensitive. For this reason, security policies should be maximized, and proper configuration of ANASTACIA is fundamental to ensure the system is capable of minimizing the threats.
- **Req-4 Data retention:** Data retention policies in the health industry are usually greatly extended due to the need to provide and care for patients in the long-term, as such the systems involved should implement strong data storage security measures and ANASTACIA should provide special priority to prevent unauthorized access to any physical repositories of personal data and to enhance oversight of the data flows from any digital repositories.
- **Req-6 Records and audit of processing activities and disclosures:** Records of processing activities and disclosures should be constantly updated and directly inform the security and privacy policies introduced to ANASTACIA to ensure special protection is granted to internal critical resources and that the data flows to/from the partners/subjects of disclosure require a higher level of security (and that ANASTACIA keeps track of such data flows to detect any anomalies).
- **Req-7 Security of processing:** Security is especially relevant to the use-case due to the threats to the life and well-being of the data subjects it identifies. Furthermore, due to the nature of the institution and the categories of data that are handled to provide its services, special care should be taken to ensure that correct organizational and technical mechanisms are introduced to the very design of the system. For ANASTACIA this situation implies the necessity of careful and exhaustive monitoring of the system, which might be translated as higher Key Performance Indicators (KPIs) or stronger privacy and security policies.
- **Req-8 Data breach information:** Data breach information and alerts should be immediately presented after any event to ensure that the system administrator is well-aware of the system's status. Due to the sensitive nature of the information and the critical nature of the infrastructure, the reports presented might be tailored to conform to applicable national standards or regulations regarding threat information sharing (e.g.: introducing verbose logging, adopting specific data export formats or implementing immediate alert submission to governmental authorities – or CSIRTs- as defined by the system's administrator.)
- **Req-9 Encryption of personal data by default:** Due to the sensitive nature of the data stored and processed in the system, ANASTACIA should require or introduce the strongest possible encryption mechanisms.
- **Req-10 Update and review privacy measures:** Privacy and security policies should be regularly reviewed and updated to ensure their alignment with the higher-standards of security that are expected from the system. This is particularly true when addressing the privacy and security updates after a data breach has occurred or whenever indicated by a PIA.

UC_BMS.2 Insider attack on the fire suppression system

> *"Adam, the operations technician, is a* ***disgruntled employee*** *who intends to cause economic* ***cost to his employer by damaging building assets such as electronic controllers, servers, CCTV cameras, furniture, etc****. To carry out his sinister motive, he intends to exploit the building operations workstation he is*

> *entrusted with. The workstation is used to manage the fire-alarm panel input/output. He could compromise the workstation* ***by installing malware via a USB drive.*** *This* ***workstation has network access beyond the reach of much of the network access controls such as firewalls and authentication, authorization, and accounting mechanisms deployed upstream****. Adams's intention is to use the* ***malware to exploit an unpatched application*** *that controls the fire alarm panel in order to activate unauthorised release of pressurized water or gas suppressants to flood and damage the building.*
>
> *Bob, the operations manager, will use ANASTACIA to ensure that appropriate network and system design, implementation, monitoring and reaction are considered to* ***minimise such an insider attack.*** *ANASTACIA will assist Bob to provide a quality of security seal that ensures that systems within the building are correctly* ***patched against known malware and that proper deployment of firewalls with deep packet inspection capability that act as points of demarcation between back-end workstations and IoT/CPS controllers****. More importantly, ANASTACIA will assure Bob that should pressurized fire suppressants are released to areas vulnerable to fire, other building operations such as evacuation of occupants, alerting of wardens and responders, elevator and escalator operations, ventilation, etc., follow the emergency operation mode."*
>
> *ANASTACIA D1.2 "User Centred Requirements Initial Analysis."* (2017, p. 41)

While the use-case is focused on the potential damages to the building caused by an insider threat, the high-level of network access granted to the vulnerable workstation implies potential risks to the personal data of both persons accessing the building infrastructure (and thus being recorded by the security systems) and to those data subjects found in corporate databases connected to the building's network. As such, the following requirements are of particular relevance:

- **Req-3 Data management and respect of data subject rights:** while legitimate, ANASTACIA's implementation of Deep Packet Inspection capabilities could lead to privacy concerns by users of the networks. Any deployment of the ANASTACIA system should then be accompanied by a communication campaign aimed at informing users of monitored networks of the nature and privacy safeguards involved in these mechanisms.
- **Req-6 Records and audit of processing activities and disclosures:** In line with the previous point, correct records and audit mechanisms should be introduced to ANASTACIA to ensure the system's accountability regarding personal data protection.
- **Req-7 Security of processing:** Given the extended access level of the vulnerable workstation and the malicious nature of the insider motivations, ANASTACIA's role in minimizing attacks (through enforcement of access policies, prevention of malware and traffic control) are fundamental to the protection of personal data in the network.

UC_BMS.3 Remote attack on the building energy microgrid

> *"Clara is an ex-colleague of David who is the plant manager at Eisen Inc., a steel producer. Clara is now a security contractor for the competitor of Eisen Inc. Not surprisingly, Clara is aware of the existence of a misconfigured network path (any source IP address) for a utility provider (trusted IP address) of Eisen Inc.* ***This allows the external energy provider to directly interface with the SCADA (supervisory control and data acquisition)*** *system of the Eisen Inc's energy microgrid. But the* ***SCADA data historian is accessible due to an unpatched bug in the networking middleware that allows a privileged***

> ***escalation of access**. Clara will exploit this bug to launch a remote attack (e.g., via SQL injection) on the database servers that host the SCADA data historian. She could **steal Eisen Inc.'s business credentials**, overwrite boiler setpoints, rewrite activation ratios between generators and battery, fake network demands, etc. Clara could increase the energy consumption and utility costs of Eisen, stress the generators and boilers towards damage, and disable the shut-down capability of the blast-furnace.*
>
> *David will use ANASTACIA to ensure that the Eisen Inc.'s network access policy enforcement is not compromised. Further, ANASTACIA will help David to detect insecure operations of the processes, equipment or controllers. David will rest assured that the reactive and resilient features of ANASTACIA will activate safe-mode of operations should abnormalities occur."*
>
> *ANASTACIA D1.2 "User Centred Requirements Initial Analysis."* (2017, p. 45)

This use-case does not directly relate to end-user privacy, and as such the requirements could only become relevant if certain assumptions beyond the detailed elements are made to maximize the potential impact of the attack. Accordingly, the unauthorized connection to Eisen's system and the associated privilege escalation of access could be assumed to be extensive enough to enable access to worker and client personal information available in other systems of the network (particularly through the use of stolen business credentials).

Under this eventual situation, the following requirements would be of special relevance:

- **Req-4 Data retention:** The company should implement strong data minimization policies to ensure that any data breach does not negatively impact their personnel / customer's rights. ANASTACIA should point out this element as part of the contingency measures to be examined by a DPO after a breach.
- **Req-7 Security of processing:** ANASTACIA should enforce the access policies defined by the organization and detect insecure or unexpected operation of processes, equipment or controllers, as these could lead to further escalation of the breach and to access to sensitive information available in the network.

UC_BMS.4 Cascade attack on a megatall building

> *"FoulGame is a notorious group of **criminal hackers** who specialize in attacks on internet-connected services of global brands. They have set their eyes **to destroy the brand name of Hilltop Group who owns many iconic hotels worldwide**. FoulGame intends to use internet-connectivity of the buildings operations to create **an emergency in a mega-tall hotel building**. They hope that the **emergency will generate panic, trap the guests in escape elevators, activate fire-suppression sprinklers, confuse first-responders, etc.***
>
> *FoulGame wants to exploit a **zero-day vulnerability of the HVAC system network that allows an external service such as an internet-service or original equipment manufacturer (OEM) to set default values (e.g., -40 ºC) to temperature sensors.** For practical reasons, HVAC zonal temperatures are also monitored by the fire safety systems as a precaution. But if the temperature exceeds a threshold (e.g., +80 ºC), an emergency is activated. This could cascade to alarms and sprinklers activating, air-handlers stopping, elevators becoming disabled, fire-doors and corridors closing, etc. **Risk to lives of occupants due to activation of fire-suppression systems, depletion of oxygen in the air, and rush and stampede in the stairwells will be catastrophic**.*

> *Hilltop Group can use ANASTACIA to* ***identify and rate cyber-security security vulnerabilities automatically for the entire building.*** *ANASTACIA will use system design and operational data to discover dependencies between cyber-physical systems and operations for the entire megatall structure. Hilltop Group will use ANASTACIA to predict potential security consequences of interacting operations between subsystems and* ***generate threat isolation strategies****. ANASTACIA will continuously* ***enforce access and security policies*** *and resilient control strategies comprehensively at various cyber-physical levels, viz. the temperature sensors, fire-panels, elevator system managers, air-handling unit controllers, fire-suppression sprinkler systems, etc."*
>
> *ANASTACIA D1.2 "User Centred Requirements Initial Analysis."* (2017, p. 48)

The final case focuses on potential threats to the life and security of the inhabitants of a mega-tall building. In this context, the requirements identified should focus on minimizing the potential impact of the security breaches towards the end-user and, generally speaking, avoiding any escalation of the privacy risks. As such, the identified requirements should be considered as follows:

- **Req-7 Security of processing:** This requirement is of the greatest importance to this use-case considering the immediate and evident risks to the lives of inhabitants of the monitored building. While performing the general security checks necessary to prevent the potential impact on human well-being, ANASTACIA should maintain a strong vigilance on access-rights and the protection of any personal data available on the buildings intranet. This can be performed in different ways. For example, upon detection of the use of a Zero-day attack by a malicious actor, the system could reinforce any tasks aimed at identifying other varieties of these attacks in the systems.
- **Req-10 Update and review privacy measures:** Following the security breaches, all privacy measures and policies should be re-examined to determine whether they provide sufficient protection to the personal data on the monitored system.

5 Privacy Risk Assessment and Contingency Planning

According to ISO 31000/2009, *"Risk assessment is the overall process of risk identification, risk analysis and risk evaluation"* (International Organization for Standardization, 2009, p. 17). This section will be subdivided in accordance to this definition and shall follow ISO/IEC 31010 guidance on the risk assessment techniques to be implemented. Once risks have been correctly assessed, a set of contingencies based on current ANASTACIA reaction capabilities will be described.

5.1 Identification of Privacy Vulnerabilities, Risks and Measurement Points

The first step in performing an assessment is the generation of "*a comprehensive list of risks based on those events that might create, enhance, prevent, degrade, accelerate or delay the achievement of objectives (…) Identification should include risks whether or not their source is under the control of the organization, even though the risk source or cause may not be evident. Risk identification should include examination of the knock-on effects of particular consequences, including cascade and cumulative effects. It should also consider a wide range of consequences even if the risk source or cause may not be evident. As well as identifying what might happen, it is necessary to consider possible causes and scenarios that show what consequences can occur. All significant causes and consequences should be considered"* (International Organization for Standardization, 2009, p. 17).

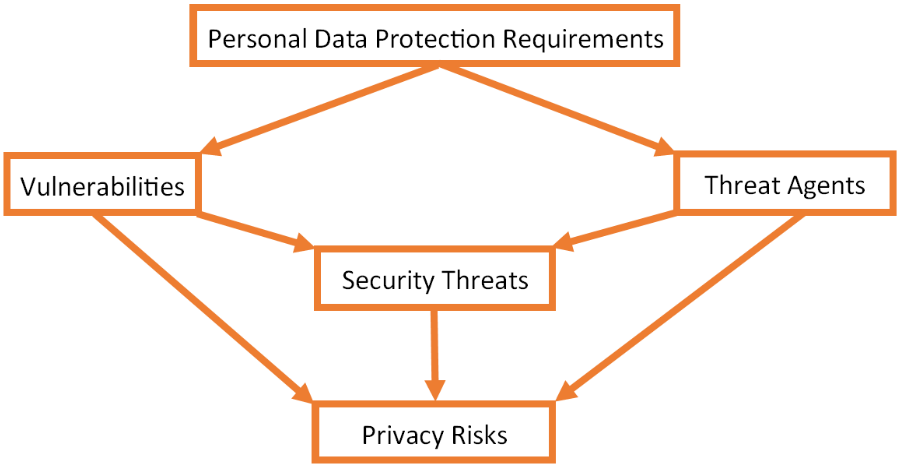

Figure 1 Privacy risk identification process

As noted in figure 1, to identify the most relevant privacy risks that should be considered by ANASTACIA, this section will initially define a set of potential privacy vulnerabilities that might affect an IoT/CPS system. Next, a review of the security threats that are to be monitored by ANASTACIA will be performed to better understand those risk elements related to the Security of Processing requirement which are already monitored by the system. Finally, the relevant privacy risks will be specified along with the measurement points that are necessary for their identification in a system. All of the previous elements will be cross-referenced between themselves to ensure clarity in their potential interdependencies, and a list of potential (or actual) threat agents[31] will be included so as to facilitate the risk analysis and evaluation that is to take place in the following sections.

5.1.1 Potential Privacy Vulnerabilities (PV)

The following is a list of common vulnerabilities which might affect an IoT/CPS system, and which might be addressed or prevented by ANASTACIA. This list is not intended to be exhaustive[32], but rather aims to provide a baseline to enrich and contextualize the identified privacy risks. For this reason, the summary description provided will be accompanied with a list of the threat agents that could exploit such vulnerabilities to generate the associated risks.

PV-1 Disclosure of personal information in transport layer

Summary description:

The first privacy vulnerability that must be considered by ANASTACIA relates to the possibility of disclosure of personal information in the transport layer. This vulnerability relates primarily to the lack or partial use of the Transport Layer Security (TLS) cryptographic protocols[33] or other channel-protection mechanisms (such as VPNs, etc.) when transmitting or receiving data. In the case of IoT devices, a potential attacker could utilize eavesdropping, sniffing or keylogger techniques to access the contents of the unencrypted communications, thus exposing personal information. Secondarily, this vulnerability relates to the possibility of extrapolating personal information through traffic analysis leading to the identification of trends in the encrypted data streams which could lead to the re-identification of data subjects (Apthorpe, Reisman, Sundaresan, Narayanan, & Feamster, 2017). Finally a hop-by-hop trace back attacks (Shaikh et al., 2010) could affect network privacy[34] by re-identifying a sensor (or its location in the network[35]) through the analysis of the path followed by the data packets within a network.

Potential threat agents

- Commercial establishments, marketing companies, online service providers, malicious attackers (hackers), States, IoT service providers, IoT device providers

Associated Risks:

- 1, 2, 3, 4, 6

[31] Intel's library of threat agents and defining attributes available in (Casey, 2007) provides further specification of the capabilities and motivations of many of these actors.

[32] Given the constant technological evolution and the ingenuity of threat agents, the generation of an exhaustive list of vulnerabilities is unfeasible. Regardless of this fact, the identification of vulnerabilities is of great significance to the correct functioning of ANASTACIA's privacy features. For this reason, it is expected that this exercise is to be carried out by the operators of the monitored systems and its results addressed through the inclusion of sufficient privacy policies to address the risks generated by the system's vulnerabilities.

[33] As described by IETF RFC 5246 (Rescorla, 2008) and it's updates.

[34] *"network level privacy has often been categorized into four sub-categories:*

1. *Sensor node identity privacy: no intermediate node can get any information about who is sending the packets except the source, its immediate neighbours and the destination,*
2. *Sender node location privacy: no intermediate node can have any information about the location (in terms of physical distance or number of hops) about the sender node except the source, its immediate neighbours and the destination,*
3. *Route privacy: no node can predict the information about the complete path (from source to destination). Also, a mobile adversary gets no clue to trace back the source node either from the contents and/or directional information of the capture packets(s), and*
4. *Data packet privacy: no node can see the information inside in a payload of the data packet except the source and the destination"* (Shaikh et al., 2010, p. 1447).

[35] See (Rios, López, & Cuellar, 2016), (Jian Ren & Di Tang, 2011), and (Niu et al., 2016).

PV-2 Lacking/insecure encryption at device/gateway/middleware level

Summary description:

A second privacy vulnerability opens the possibility of accessing personal information directly from the devices, gateways and/or middleware that enable the correct functioning of the IoT/CPS deployment. This vulnerability relates to both Req-9 (Encryption of personal data by default) as potential threats relate mainly to the use of obsolete/unsecure encryption protocols by the devices and the potential breaches that are possible through the exploitation of optional or partial certificate verification by the web-apps that are incorporated in the devices (which are worsened due to lack of continuous support/updates). As such, this vulnerability also relates to eavesdropping/sniffing, keylogger and traffic analysis attacks.

Potential threat agent:

- Commercial establishments, marketing companies, online service providers, malicious attackers (hackers), States, IoT service providers, IoT device providers.

Associated risks:

- 1, 2, 3, 4, 6, 7

PV-3 Lacking Network Isolation

Summary description:

The third privacy vulnerability relates to the possible exchange of unnecessary data between the networks that support and control the IoT/CPS deployment and publicly accessible networks, which could serve as a first step towards accessing or controlling devices in the network or as an access point for attacks and malware. This could be the result of improperly configured Virtual Local Area Networks or firewalls and could make personal data available to unauthorized individuals.

Potential threat agent:

- Malicious attackers (hackers), insider threats

Associated risks:

- 1, 2, 3, 4, 6

PV-4 Missing identification, authentication and authorization mechanisms

The fourth vulnerability in our list raises the potential of unauthorized access, alteration, disclosure and destruction of personal information in the system due to lacking or missing identification[36], authentication[37], and authorization[38] mechanisms and policies for both users and devices in the network. This vulnerability relates to several of the personal data protection requirements[39], as these mechanisms are fundamental to the correct implementation of access control by the network and IoT/CPS systems monitored by ANASTACIA.

Identification, authentication and authorization mechanisms are basic security requirements of IT systems and have special relevance for personal data protection. Once a classification of the personal data that is processed by a system is performed, sufficient tools must be implemented to ensure that only authorized individuals and devices are granted access to this information[40]. Furthermore, these are fundamental

[36] Process by which a subject or device claims an identity.
[37] Process by which a subject or device proves their identity.
[38] Process by which access to certain objects or resources are granted to an identified and authenticated subject or device.
[39] Namely, requirements 1, 2, 3, 4, 6, 7, and 10.
[40] This relates not only to the need for ensuring that policies in place properly assign the diverse privileges available in the system to the authorized users or devices, as some classes of information should not be available to non-privileged users; but also seeks to

elements in the design of a secure network, as properly identifying the devices part of the network is the first step towards protecting the network from attacks. As such, this vulnerability exposes the system to many security threats (Malware, Man-in-the-middle attacks, masquerading, replay attacks, sniffing/eavesdropping, keyloggers, and SQL Injection attacks, among others) which could directly compromise the data subject's rights.

Potential threat agent:

- Malicious attackers (hackers), insider threats

Associated risks:

- 1, 2, 3, 4, 7

PV-5 Sharing or re-purposing personal data with third parties without the consent of the data subject

A fifth potential vulnerability relates to the devices and sensors that are to be monitored by ANASTACIA and the possibility of them sharing or repurposing data without the consent of the data subject. *"On the one hand, people demand richer experiences through more customized services being provided by any smart object. On the other hand, companies require highly sensitive information from users (e.g., location) in order to provide more satisfactory services"*(Hernández-Ramos, Bernabe, Moreno, & Skarmeta, 2015). This dichotomy has led to the inclusion of automated reporting mechanisms which share user data for security/marketing purposes and the increasing integration of social network apps/tools[41] in consumer devices (Smart TVs, smart refrigerators, etc.) by some IoT providers.

Indeed *"many smart home devices have always-on sensors that capture users' offline activities in their living spaces and transmit information about these activities outside of the home, typically to cloud services run by device manufacturers. Examples of offline activities recorded by currently available smart home devices include sleeping patterns, exercise routines, child behaviours, medical information, and sexual activity. Even if a smart home device is not designed to capture privacy sensitive activities, such activities may indirectly influence information collected by device sensors, allowing them to be identified by inference techniques."* (Apthorpe et al., 2017, p. 1).

As such, the direct threats related to this vulnerability include not only the breach of the basic principles of personal data protection (particularly data minimization and purpose limitation) by IoT providers, but the potential exposure of user data to unauthorized processing by third parties. Furthermore, the many ways in which this information is shared will create new attack vectors which could be exploited by malicious attackers, online service providers and internet service providers, and even States[42].

Associated Risks:

- 1, 3, 4, 5, 7

Potential threat agent:

- Commercial establishments, marketing companies, Internet service providers, malicious attackers (hackers), States, Insider threats

limit the possibility of overcollection or unauthorized processing of personal information by not enforcing correct session termination mechanisms in the diverse devices.

[41] This vulnerability could be identified by unauthorized communications between smart devices and social media sites, see (Shaikh et al., 2010).

[42] It is important to remember that the GDPR permits personal data transfers to a third country subject to compliance with several conditions, including the adequacy of its Personal Data Protection legislation. See (European Parliament & European Council, 2016, Chapter V).

PV-6 Unnecessary ports/services enabled in devices

The last vulnerability that should be monitored by ANASTACIA is characteristic of IoT/CPS deployments, as it revolves around potential attack vectors open due to the physical exposure of the objects/sensors that feed the network. The existence of unused or vulnerable ports and services[43] in these devices grants attackers an opportunity to obtain personal data directly from the internal memory[44] of the objects by exploiting unpatched vulnerabilities, introducing malware, deploying man-in-the-middle attacks or simply hijacking the device to attack or gain unauthorized access to the network: Hijacked physically exposed and unattended objects might be used to masquerade as a client or application server to send data and perform operations. In an IoT context this might lead to vulnerabilities of physical facilities, and direct privacy impacts (i.e. remotely compromised doors lead to break-ins).

Associated risks:

- 1, 2, 3, 4, 5, 6, 7

Potential threat agent:

- Commercial establishments, marketing companies, online service providers, malicious attackers (hackers), States, IoT service providers, IoT device providers

5.1.2 ANASTACIA-Monitored Security Threats (MST)

According with Deliverable 2.2 (Cambiaso et al., 2018), the following Security Threats will be monitored and addressed through ANASTACIA. As Req-7 discussed, the deployment of monitoring systems capable of implementing technical contingencies to minimize security risks is key to the protection of the rights and interests of subjects of personal data. In the context of this deliverable, this list will serve to understand the set of potential vulnerabilities that will shape the privacy risks identified in infra Section 5.1.3. Furthermore, in conjunction with the contents of Deliverable 2.2 and the capabilities listed in supra section 3, this list will inform the risk analysis process carried out in infra section 5.2.

MST-1 Zero-day Attacks

Summary Description:

“Zero-day vulnerabilities (also known as "0-days") concerns the exploitation of unknown software vulnerabilities never appeared in networks before. Because of this, their knowledge is extremely limited, usually only to a restricted number of malicious users (even not knowing/communicating among them). In virtue of this, since most of the times even the software producer is not aware of the vulnerability, appropriate patches are not available, and the affected system is vulnerable. Until appropriate patches are deployed on the vulnerable systems, hosts afflicted with such vulnerabilities are exposed to cyber-attacks that may even cause serious damage to the system.”(Cambiaso et al., 2018, p. 7).

Threat agent:

Malicious attackers (hackers), insider threats, States.

[43] Speedtest.net has compiled a list of known vulnerabilities associated with diverse ports (speedguide.net, 2018).

[44] This vulnerability must also consider the possibility of backdoors within the device/sensor/object which could be exploited by an attacker to obtain unencrypted information from the device.

MST-2 DDoS attacks

Summary Description:

"A Distributed Denial of Service (DDoS) threat is a simultaneous attack executed by different coordinated nodes against commonly targeted services offered by the victims. The services under attack can be classified in primary victims, where the targeted service is the one that the attacker wishes to make inaccessible, and third victims, where third-party hosts or services are exploited to execute the attack against the primary victims (real targets). Instead, the use of secondary victims during a DDoS attack provides the attacker the ability to exploit (usually infected) zombies/bots to amplify the attack power by remaining anonymous" (Cambiaso et al., 2018, p. 8).

Threat agent:

- Malicious attacker (hacker, script-kiddies), insider threat, States.

MST-3 DoS attacks

Summary Description:

"In a denial of service attack, an attacker exploits the network connection to make the services offered by the victim unavailable, by simply flooding the victim with several packets (e.g., flooding, amplification and reflection DoS), or by exploiting some sort of vulnerability (e.g., low-rate or exploit based DoS). Denial of service attacks cause significant damage each year, making it essential to implement and develop innovative techniques for detection and protection against this attack. In order to develop innovative protection techniques, a thorough knowledge of the dynamics of the attack is required. Being a well-known attack with vast potentials, it is considered one of the most dangerous cyber-attacks"(Cambiaso et al., 2018, p. 8).

Threat agent:

- Malicious attacker (hacker, script-kiddies), insider threats, States.

MST-4 Malware

Summary Description:

"Malware are malicious files or software running on infected hosts. The malware category includes several kinds of malicious programs such as computer viruses, worms, trojan horses, spyware, and ransomware. These programs aim to attack users' devices for different malicious reasons. For example, they can steal user sensitive data, encrypt data to request an unlock ransom, or directly delete them to cause damage to the victim." (Cambiaso et al., 2018, p. 7).

Threat agent:

- Malicious attacker (hacker), insider threat, State

MST-5 Man in the middle attacks

Summary Description:

"A man-in-the-middle attack is implemented to access private data exchanged in a communication session or to modify packets thus violating session integrity. This attack is executed in real-time, which means that the attack occurs during the communication session between two network devices. Data can be read, edited

and stored when the attacker is able to access the session. The attacker will know the contents of the message before the intended recipient receives it or changes the message along the path. The attacker could adopt different well-known techniques, could put himself in the middle of the communication between two hosts pretending to be the respective recipients of the session." (Cambiaso et al., 2018, p. 7)

Threat agent:

- Malicious attacker (hacker), insider threat, State

MST-6 Masquerading

Summary Description:

"During a masquerading attack, the attacker assumes the identity of another user of the system to gain access to specific information. It is a technique used by a malicious user to pretend to be an authorized person to gain access to confidential information (e.g., by executing some sort of privilege escalation) in an illegal way." (Cambiaso et al., 2018, p. 7).

Threat agent:

- Malicious attacker (hacker), insider threat, State

MST-7 Replay attacks

Summary Description:

"A replay attack is intended to postpone or replay the transmission of a package to get a victim's disservice or to obtain information that it would not have access to. An attacker acquires data that he previously had no access to and uses them for his (malicious) purposes. For instance, by repeating a connection packet seizing some sort of resource on the victim, it would be possible to seize all the available resources, hence creating a disservice." (Cambiaso et al., 2018, p. 7)

Threat agent:

- Malicious attacker (hacker), insider threat

MST-8 Sniffing attacks

Summary Description:

"In general, if network communications occur in plain text, hence exchanged data are not encrypted, it is possible for a malicious user to intercept exchanged information and process them. In this case, it may be required to the attacker to place the malicious host between the two nodes of the communication (see MiTM attack (…)). For instance, this is possible for a network administrator, by using mirroring ports of network switches, or for an insider threat, by placing a tap on the network. The interception action is generally referred as sniffing or spoofing. The ability of an attacker to monitor the network is generally one of the main problems that users have to deal with, especially if unknown networks (e.g. public access points) are adopted, since, without enabling strong and effective encryption algorithms, data can be read and stored by malicious users." (Cambiaso et al., 2018, p. 9)

Threat agent:

- Internet Service Providers, Insider threat

MST-9 Keyloggers

Summary Description:

"Keyloggers run in the background on the infected system, recording key press and executed commends. Keyloggers can be software based or physical devices attached between the keyboard and the motherboard of the garget. Concerning software based keyloggers, once the data are stored, they are hidden memory areas for later retrieval, or directly sent in background to the attacker on the Internet. Once the malicious payload is retrieved, the attacker may find passwords or other sensitive data that could be used to compromise the system, for personification, or for social engineering attacks." (Cambiaso et al., 2018, p. 9)

Threat agent:

- Malicious attacker (hacker), Insider threat

MST- 10 SQL Injection attacks

Summary Description:

"Structured Query Language (SQL) injection is a computer attack that involves the injection of malicious SQL code to target a web application directly connected to a database management system (DBMS) and to access/steal or inject illegitimate data. During this attack, the attacker usually crafts a portion of the SQL statement by passing it to the server into an HTTP request, in order to alter the initial query and gain access to the database." (Cambiaso et al., 2018, p. 8).

Threat agent:

- Malicious attacker (hackers), Insider threat, State

MST-11 Traffic analysis attacks

Summary Description:

"Traffic analysis is a process of intercepting and analysing packets exchanged in a network in order to infer the exchanged content. This kind of threat can also be executed if analysed packets are encrypted and decryption is not possible. In general (but not always), more packets are exchanged on the network, more information can be extrapolated from the captured traffic." (Cambiaso et al., 2018, p. 9)

Threat agent:

- Malicious attacker, insider threat, Internet Service Providers, marketing companies, States

5.1.3 Privacy Risk Identification and Measurement Point Definition

The first step towards identifying potential privacy risks is the definition of risk criteria which *"should reflect the (…) values, objectives and resources. Some criteria can be imposed by, or derived from, legal and regulatory requirements"* (International Organization for Standardization, 2009, p. 17). As defined throughout previous sections of this research, relevant criteria in the context of ANASTACIA are given by the GDPR[45] (and secondarily by the e-Privacy regulation). The GDPR clearly focusses on one type of risk:

[45] This criterion has been further expanded by the Art. 29 Working Party (WP 248) to enable the identification of high risk processing. According to this document, high risk processing includes "*Systematic monitoring: processing used to observe, monitor or control data subjects, including data collected through "a systematic monitoring of a publicly accessible area" (Article 35(3)(c)).(…) Sensitive data: this includes special categories of data as defined in Article 9 (…) This criterion also includes data which*

adverse risk to the individual. The risks to the rights and freedoms of individuals of “varying likelihood and severity” may result from personal data processing which could lead to “physical, material or non-material damage” (European Parliament & European Council, 2016, Recital 75).

In this context, he following list aims to identify the most relevant privacy risks (taking place at the network-level[46]) which could be addressed through ANASTACIA.

Risk 1: Unauthorized access or disclosure of personal data (loss of confidentiality)

Summary description:

Access or disclosure to/of personal data generated or held by a device or object, by an unauthorized user or device.

Associated requirements:

- 1, 2, 7, 9, 10

Measurement points:

- Detection of any of the monitored security threats
- Unusual account or device activity (as determined by time of the access, IP address, amount of data transferred, port used, etc.)
- Unauthorized connections to external networks/servers

Risk 2: Unauthorized modification of personal data (loss of integrity)

Summary description:

Modification or affectation to the integrity of the personal data generated or held by a device or object, by an unauthorized user or device.

Associated requirements:

- 1, 2, 7, 9, 10

Measurement points:

- Detection of any of the monitored security threats
- Unusual database access/modification, including but not limited to access/modification of system logs, timestamps, etc.

may more generally be considered as increasing the possible risk to the rights and freedoms of individuals, such as electronic communication data, location data (…)Datasets that have been matched or combined, for example originating from two or more data processing operations performed for different purposes and/or by different data controllers in a way that would exceed the reasonable expectations of the data subject (…) Innovative use or applying technological or organisational solutions: (…) (Article 35(1) and recitals 89 and 91) (…) the use of such technology can involve novel forms of data collection and usage, possibly with a high risk to individuals' rights and freedom. Indeed, the personal and social consequences of the deployment of a new technology may be unknown. (…). For example, certain “Internet of Things” applications could have a significant impact on individuals' daily lives and privacy (…). [and finally] When the processing in itself “prevents data subjects from exercising a right or using a service or a contract” (Article 22 and recital 91). (…)(Article 29 Data Protection Working Party, 2017, p. 8).

[46] See supra note 6.

Risk 3: Unauthorized or inappropriate linking of personal data (Potential for data re-identification)

Summary description:

Unauthorized interconnection of two or more data sources by a device, object or user in the network.

Associated requirements:

- 1, 5

Measurement points

- Unusual data flows between network devices (particularly as supported by information obtained through previous classification of device capabilities and categories of personal data provided by each device).

Risk 4: Unauthorized removal or deletion of personal data (loss of availability)

Summary description:

Personal data is removed or deleted by an unauthorized user or device.

Associated requirements:

- 1, 2, 7, 9, 10

Measurement points:

- Detection of any of the monitored security threats
- Sudden memory loss registered in device/object system logs
- Loss of system logs
- Unexpected disconnection of authorized device or object from the network

Risk 5: Excessive collection or retention of personal data (loss of operational control)

Summary description:

Devices or objects do not respect restrictions on collection/retention of data defined by policies/configuration.

Associated requirements:

- 1, 2, 3, 4, 5, 6, 7

Measurement points

- Devices/objects do not execute scheduled internal memory purges
- Devices/objects are always active regardless of policies requesting disconnection when authorized users/devices are on the network

Risk 6: Lacking protection of traffic information and location data

Summary description:

Information associated with device usage and/or location is disclosed or incorrectly protected.

Associated requirements:

- 1, 2, 7

Measurement Points:

- Unencrypted data streams to/from devices and/or network detected.
- Brute-force attacks on encrypted devices/data streams (high number of access attempts)
- Usage of insecure communication channels
- Lacking traffic shaping mechanisms in encrypted communications through public networks
- Unauthorized devices identified on the network
- Improper assignment of device IDs (which might enable an attacker to identify the location of a device)

Risk 7: Impairment of data subject's rights

Summary description:

Downtime or loss of control of the platform prevents information, access, rectification, restriction, objection and deletion processes by data subject.

Associated requirements:

- 3, 7, 8

Measurement points:

- Detection of any of the monitored security threats (particularly DoS and DDoS)
- Downtime in the system's GUI
- System or devices not generating/saving logs

5.2 Risk Analysis

"Risk analysis involves developing an understanding of the risk. [it] provides an input to risk evaluation and to decisions on whether risks need to be treated, and on the most appropriate risk treatment strategies and methods. (…) Risk is analysed by determining consequences and their likelihood, and other attributes of the risk. An event can have multiple consequences and can affect multiple objectives. Existing controls and their effectiveness and efficiency should also be taken into account. (…) consequences and their likelihood can be determined by modelling the outcomes of an event or set of events, or by extrapolation from experimental studies or from available data. Consequences can be expressed in terms of tangible and intangible impacts."(International Organization for Standardization, 2009, p. 18).

This supports what ISO/IEC 29134 defines as the objective of privacy risk analysis: "to analyse the potential consequences and threats of the privacy risks identified, and to estimate their respective levels of impact and likelihood".

5.2.1 Consequences

To examine the consequences of any potential data breach, two types of consequences will be identified:

- Organizational consequences (for informative purposes only): which will follow the dispositions of article 83[47] of the GDPR to identify three levels of potential consequences for each risk: 1) None: No consequences arise from the identified infringement; 2) Low: Infringements which might carry a fine up to €10 million or 2% of the company's global annual turnover as defined by the GDPR; 3) High: Infringements which might carry a higher level of fine (up to €20 million or 4% of the company's global annual turnover) as defined by the GDPR.
- Data subject consequences: Which will examine the potential impact of the data breach towards the data subject.
  1. *"Negligible: PII principals either will not be affected or may encounter a few inconveniences, which they will overcome without any problem (time spent re-entering information, annoyances, irritations, etc.).*
  2. *Limited: PII principals may encounter significant inconveniences, which they will be able to overcome despite a few difficulties (extra costs, denial of access to business services, fear, lack of understanding, stress, minor physical ailments, etc.).*
  3. *Significant: PII principals may encounter significant consequences, which they should be able to overcome albeit with serious difficulties (misappropriation of funds, blacklisting by banks, property damage, loss of employment, subpoena, worsening of state of health, etc.).*
  4. *Maximum: PII principals may encounter significant, or even irreversible, consequences, which they may not overcome (financial distress such as unserviceable debt or inability to work, long-term psychological or physical ailments, death, etc.)."*(International Organization for Standardization, 2017, p. 32)

Consequences vary depending on the severity of the breach (i.e. amount of information extracted, classes of personal data affected by the breach, etc.) and *"may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned."*(European Parliament & European Council, 2016, Recital 85). This being considered, we will begin our examination of the identified risks by detailing their potential consequences in each of the ANASTACIA use cases:

Use Case	Risk 1	Risk 2	Risk 3	Risk 4	Risk 5	Risk 6	Risk 7
UC_0.1	Significant (3)	Negligible (1)	Significant (3)	Negligible (1)	Negligible (1)	Significant (3)	Negligible (1)

[47] *"4. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 10,000,000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:*

(a) the obligations of the controller and the processor pursuant to Articles 8, 11, 25 to 39 and 42 and 43;
(b) the obligations of the certification body pursuant to Articles 42 and 43;
(c) the obligations of the monitoring body pursuant to Article 41(4).

5. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20,000,000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:

(a) the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9;
(b) the data subjects' rights pursuant to Articles 12 to 22;
(c) the transfers of personal data to a recipient in a third country or an international organisation pursuant to Articles 44 to 49;
(d) any obligations pursuant to Member State law adopted under Chapter IX;
(e) non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority pursuant to Article 58(2) or failure to provide access in violation of Article 58(1).

6. Non-compliance with an order by the supervisory authority as referred to in Article 58(2) shall, in accordance with paragraph 2 of this Article, be subject to administrative fines up to 20,000,000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher. (…)"(European Parliament & European Council, 2016).

UC_MEC.1	Significant (3)	Negligible (1)	Significant (3)	Limited (2)	Limited (2)	Significant (3)	Negligible (1)
UC_MEC.2	Significant (3)	Negligible (1)	Significant (3)	Limited (2)	Negligible (1)	Significant (3)	Negligible (1)
UC_MEC.3	Limited (2)	Limited (2)	Negligible (1)	Limited (2)	Negligible (1)	Limited (2)	Significant (3)
UC_MEC.4	Limited (2)	Limited (2)	Limited (2)	Limited (2)	Negligible (1)	Limited (2)	Significant (3)
UC_BMS.1	Maximum (4)	Maximum (4)	Maximum (4)	Maximum (4)	Maximum (4)	Maximum (4)	Maximum (4)
UC_BMS.2	Maximum (4)	Maximum (4)	Significant (3)	Maximum (4)	Limited (2)	Limited (2)	Significant (3)
UC_BMS.3	Significant (3)	Significant (3)	Significant (3)	Maximum (4)	Limited (2)	Significant (3)	Significant (3)
UC_BMS.4	Significant (3)	Significant (3)	Significant (3)	Significant (3)	Significant (3)	Significant (3)	Significant (3)
Consequences (Average)	Significant (3)	Limited (2)	Significant (3)	Significant (3)	Limited (2)	Significant (3)	Limited (2)

Table 1: Risk Analysis - Consequences per use case

In summary, the identified risks carry the following consequences:

Risk	Affected Requirement(s)	Average Data subject consequences	Organizational consequences
Risk-1	1, 2, 7, 9, 10	Significant (3)	High (3)
Risk-2	1, 2, 7, 9, 10	Limited (2)	High (3)
Risk-3	1, 5	Significant (3)	Low (2)
Risk-4	1, 2, 7, 9, 10	Significant (3)	High (3)
Risk-5	1, 2, 3, 4, 5, 6, 7	Limited (2)	High (3)
Risk-6	1, 2, 7	Significant (3)	High (3)
Risk-7	3, 7, 8	Limited (2)	High (3)

Table 2: Risk analysis - Consequences

5.2.2 Threats

Secondarily, the monitored security threats potentially involved in each risk will be accounted for and a grade will be given depending on the results.

1. Negligible: No security threat is directly related to or could lead to the identified privacy risk
2. Limited: 6 or Less than 6 of the monitored security threats could lead to the identified privacy risk
3. Significant: More than 7 of the monitored security threats could lead to the identified privacy risk
4. Maximum: All monitored security threats could lead to the identified privacy risk.

Risk	Related Security Threats	Threat level
Risk-1	1, 4, 5, 6, 7, 8, 9, 10, 11	Significant (3)
Risk-2	1, 4, 5, 6, 7, 8, 10, 11	Significant (3)
Risk-3	1, 4, 5, 7, 9, 10, 11	Significant (3)

Risk-4	1, 4, 5, 6, 7, 8, 10, 11	Significant (3)
Risk-5	4	Limited (2)
Risk-6	1, 4, 5, 7, 8, 10, 11	Significant (3)
Risk-7	2, 3	Limited (2)

Table 3: Risk analysis – Threats

5.2.3 Impact

According to ISO, to estimate the level of impact, the consequences and planned or implemented controls should be considered to determine the potential damage caused by each identified risk. The following table summarizes the results of this process in the specific context of the ANASTACIA platform and the use cases detailed in this deliverable.

Impact	Consequences[48]	Controls	Impact level
Risk-1	Significant (3)	Appropriate (3): IDS/IPS, virtual honeypot/honeynet; other controls introduced by ANASTACIA 2.2.	Limited (2)
Risk-2	Limited (2)	Appropriate (3): IDS/IPS, virtual honeypot/honeynet; other controls introduced by ANASTACIA 2.2.	Limited (2)
Risk-3	Significant (3)	Limited (2): Encryption, VPN.	Significant (3)
Risk-4	Significant (3)	Appropriate (3): IDS/IPS, virtual honeypot/honeynet; other controls introduced by ANASTACIA 2.2.	Limited (2)
Risk-5	Limited (2)	Limited (2): Power management, interface management.	Limited (2)
Risk-6	Significant (3)	Appropriate (3): traffic flow bandwidth reduction; VPN, virtual bandwidth control.	Limited (2)
Risk-7	Limited (2)	Appropriate (3): Traffic flow dropping, traffic flow bandwidth reduction.	Limited (2)

Table 4: Risk analysis – Impact

5.2.4 Likelihood

Estimating the likelihood should take into account the vulnerabilities of the supporting assets and the capabilities of risk sources to exploit them. The following reference classification is provided by ISO/IEC 29134 to clarify the likelihood of an event.

1. *Negligible: Carrying out a threat by exploiting the properties of supporting assets does not appear possible for the selected risk sources (…).*
2. *Limited: Carrying out a threat by exploiting the properties of supporting assets appears to be difficult for the selected risk sources (…).*
3. *Significant: Carrying out a threat by exploiting the properties of supporting assets appears to be possible for the selected risk sources (…).*
4. *Maximum: Carrying out a threat by exploiting the properties of supporting assets appears to be extremely easy for the selected risk sources (…).*(International Organization for Standardization, 2017, p. 33).

[48] See supra section 5.2.1.

Following the identification of relevant threat agents performed throughout Sections 5.1.1 and 5.1.2, identification of the capabilities of the potential threat can be performed. Following the methodology and results of (Casey, 2007), threat agent capabilities will be assigned in accordance with the following classification:

1. None
2. Minimal
3. Operational
4. Adept

Based on this classification, the following threat capabilities can be identified as relevant:

Threat Agent	Capabilities (Max skills)
Commercial establishments	Adept (4)
Insider threat	Operational (3)
IoT device providers	Operational (3)
IoT service providers	Operational (3)
Malicious attacker (Hacker)	Adept (4)
Malicious attacker (Script kiddy)	Minimal (2)
Marketing companies	Operational (3)
Online service providers	Operational (3)
State	Adept (4)

Table 5: Capabilities per threat agent

Finally, likelihood can be determined by ascertaining the relevant risks in each use case and the capabilities of the involved Threat agent.

Use Case	Relevant Risks	Relevant Risk Sources	Capabilities	Likelihood[49]
UC_0.1	1, 2, 3, 4	(unknown)	Adept (4) [50]	Maximum (4)
UC_MEC.1	1	Malicious attacker (Hacker)	Adept (4)	Maximum (4)
UC_MEC.2	1, 2, 3, 6	Insider threat	Operational (3)	Maximum (4)
UC_MEC.3	7	Malicious Attacker (Hacker / Script kiddies)	Adept (4)[51]	Maximum (4)
UC_MEC.4	1, 2, 4, 5, 6, 7	Malicious attacker (Hacker)	Adept (4)	Maximum (4)
UC_BMS.1	1, 2, 3, 4, 5, 6, 7	Malicious attacker (Hacker)	Adept (4)	Maximum (4)
UC_BMS.2	1, 2, 3, 4, 5, 6, 7	Insider threat	Operational (3)	Maximum (4)
UC_BMS.3	1, 2, 4	Insider threat	Operational (3)	Maximum (4)
UC_BMS.4	1, 6, 7	Malicious attacker (Hacker)	Adept (4)	Maximum (4)

Table 6: Risk analysis – Likelihood

[49] These values will vary depending on the specific circumstances of each analysed IoT/CPS deployment that is to be examined by ANASTACIA. In the case of the use cases examined by this deliverable, the likelihood value will always be maximum due to the fictitious and certain nature of the described attacks.

[50] The maximum likelihood is to be assumed in case of an unknown threat agent, as preventive and corrective measures should be deployed regardless of the assumed likelihood of an ongoing event.

[51] While DoS/DDoS attacks can be theoretically performed by malicious attackers with diverse skill levels, the maximum capability level is assumed as the use case denotes a massive attack.

5.3 Risk Evaluation

"The purpose of risk evaluation is to assist in making decisions, based on the outcomes of risk analysis, about which risks need treatment and the priority for treatment implementation. Risk evaluation involves comparing the level of risk found during the analysis process with risk criteria established when the context was considered. Based on this comparison, the need for treatment can be considered. (…) In some circumstances, the risk evaluation can lead to a decision to undertake further analysis." (International Organization for Standardization, 2009, p. 18)

The following table synthetizes the risk analysis performed and provides a final characterization of the risk level in accordance with the following classification:

1. Negligible: total does not exceed 4/16
2. Limited: total between 5/16 and 8/16
3. Significant: total between 9/16 and 12/16
4. Maximum: total between 13/16 and 16/16

Risk	Consequences	Threats	Impact	Likelihood	Level of risk
Risk-1	Significant (3)	Significant (3)	Limited (2)	Maximum (4)	Significant (12/16)
Risk-2	Limited (2)	Significant (3)	Limited (2)	Maximum (4)	Significant (11/16)
Risk-3	Significant (3)	Limited (2)	Significant (3)	Maximum (4)	Significant (12/16)
Risk-4	Significant (3)	Significant (3)	Limited (2)	Maximum (4)	Significant (12/16)
Risk-5	Limited (2)	Limited (2)	Limited (2)	Maximum (4)	Significant (10/16)
Risk-6	Significant (3)	Limited (3)	Limited (2)	Maximum (4)	Significant (12/16)
Risk-7	Limited (2)	Limited (1)	Limited (2)	Maximum (4)	Significant (9/16)

Table 7: Risk analysis - Results

Based on the results of the analysis of the identified risks, all are to be considered as significant. In the context of the use cases examined throughout this deliverable however, three priority levels can be identified among the identified risks:

Risk	Level of risk	Priority for treatment implementation
Risk-1	Significant (12/16)	1
Risk-3	Significant (12/16)	1
Risk-4	Significant (12/16)	1
Risk-6	Significant (12/16)	1
Risk-2	Significant (11/16)	2
Risk-5	Significant (10/16)	2
Risk-7	Significant (9/16)	3

Table 8: Risk evaluation - Priority classification

Having considered the high level of significance of the identified risks and the nature of the information potentially affected by them, it is recommended that all instances of such risks are followed by human-based verification of potential breaches to the rights of the data subjects involved.

5.4 Contingency Modelling

The task of modelling the contingency elements necessary to address each of the identified risks will involve three main elements:

A) The definition of the technical activities required to prevent and mitigate risk impact.

B) The definition of any human-based verification activities that are to be followed by the Data Protection Officer (DPO) to ensure organizational compliance with the identified requirements.

C) A strategy[52] for verifying the implementation of both sets of activities in order to inform the ANASTACIA DSPS of changes to the system's privacy.

This section will aim to develop the high-level technical and human-based protection, detection, mitigation and contingency activities necessary to address each identified risk. Following this, the strategy for verifying the implementation of these elements will be detailed. Further specification of the activities and strategy will take place in a case-to-case basis, as will be demonstrated throughout Section **Errore. L'origine riferimento non è stata trovata.** and future research activities leading to ANASTACIA Deliverable 2.7.

Risks 1, 2 and 4: Unauthorized access, modification or removal of personal data (loss of confidentiality, integrity and availability)

The risks of unauthorized access, modification or removal of personal data are closely related to the security of the monitored systems (see Req-7) and the ANASTACIA-monitored security threats identified in section 5.1.2. For this reason, all security-related tasks performed by ANASTACIA to protect the network will serve to minimize the potential impact of these risks.

Protection:	**Detection:**

[52] *"A strategy which embeds the protection of personal data – also in terms of security – into the design and functioning of the systems, needs therefore to be devised and followed. The strategy should incorporate the following elements: a) clear allocation of roles within the personal data processing, in order to: a. identify the data controller, the data processor(s) and the persons processing personal data under the authority of the controller or processor; b. formally bind the data processor(s) to guarantee a certain level of safeguards for personal data; c. map any potential stakeholder that may process personal data outside the European Union and formally bind it to guarantee a certain level of safeguards for personal data; d. assign the relevant authorization and authentication profiles to the persons processing personal data under the authority of the controller or processor. b) appointment of a Data Protection Officer, where necessary, in the light of the business and related data processing activities carried out by the data controller and/or processor; c) a Data Protection Impact Assessment (DPIA), where necessary; this process is anyway recommended for services, applications, systems that process personal data, even though they do not seem risky at the outset. The DPIA is a crucial step to ascertain whether personal data run risks in terms of security, and what the remedies are to those risks; d) implementation of the principles of data protection by design and by default throughout the whole data lifecycle; e) policies and procedures to periodically test the security resilience of a system (e.g., penetration tests, vulnerability assessments, etc.) and carry out the relevant remediation activities; f) adherence to codes of conduct and /or certification mechanisms for security of personal data g) a well-defined internal procedure to cope with any data breaches and notification thereof: a. to the competent Data Protection Authority, within 72 hours after having become aware of it; b. to the data subjects involved, without undue delay, unless any of the following conditions are met: i. the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption; ii. the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise; iii. it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner."* (Cambiaso, Mongelli, et al., 2017, pp. 36–37).

• Initial audit performed before implementation of ANASTACIA to ensure system complies with personal data protection principles and requirements • Implement security of processing requirement (verification of all WP2.2 attacks and mitigation) • Identify categories of personal data handled by devices in the network (this identification might take place under pseudonyms within ANASTACIA to minimize the threat of re-identification) • Ensure strict access control policy enforcement	• Use VNF AAA Architecture for detection
Mitigation: • Virtual secure Web proxy, virtual firewall and router, SDN The access control policy enforcement could be achieved through: • Definition of which resources can be accessed by which user/elements through HSPL policies. For instance, the IoT resources (Temperature, Humidity…) which will be accessible by a specific user. • Translating the MSPL policies to XACML. • Deploying access control architecture components on demand as VNFs. For instance, it could be the Policy Decision point. • Applying the configurations through the access control architecture. • Ensuring devices do not have unnecessary services/ports enabled <u>Example Policies:</u> • **Access control:** Subject no_/authorise_access resource/[TYPEOF]_traffic. Enablers involved in policy implementation: • AAA architecture, XACML, SDN Controller, Virtual Router, Firewall configuration • **Firewalls:** Subject no_/authorise_access resource/[TYPEOF]_traffic, Subject Enable/remove resource. Enablers involved in policy implementation: • SDN, VR; Firewall configuration	**Contingency:** • Execution of a privacy impact assessment by the DPO (Following case-specific instructions). • Update and review of privacy policies and mechanisms in accordance to results of the DPIA. • Update ANASTACIA privacy and security policies if necessary.

• **Boundary Protection:** “Subject enable/remove IDS_IPS, Subject no_/authorise_access resource/[TYPEOF]_traffic”. Enablers involved in policy implementation: • SDN, VR, Firewall configuration	

Table 9 Contingency model - Risks 1, 2 and 4

Risk 3: Unauthorized or inappropriate linking of personal data (Potential for data re-identification)

In the specific context of the systems and networks that are to be analysed and protected with ANASTACIA, this risk relates mainly to the potential privacy vulnerabilities arising out of inappropriate implementation of encryption mechanisms and vulnerabilities in the anonymization/pseudonymization techniques used by the system). As such, protection, detection and mitigation approaches should build upon the security strategies setup by ANASTACIA to identify and prevent such threats as keyloggers and man in the middle attacks (as these would be able to gather unencrypted information from the network and eventually vulnerate the measures undertaken to anonymize personal data).

Protection:	**Detection:**
• Initial audit performed before implementation of ANASTACIA to ensure system complies with personal data protection principles and requirements • Definition of strong channel protection and anonymity policies. • Requiring encryption of all communications by default. • Ensuring ANASTACIA does not unnecessarily release/utilize non-anonymized data from the system.	• Use VNF AAA Architecture; IDS/IPS for detection in accordance to security detection plans
Mitigation: • Mitigation through SDN, firewall, VPN and TLS The channel protection policy enforcement could be achieved through: • Defining channel protection policies using HSPL. For instance, enabling the DTLS communication between the IoT Controller and a specific IoT device. • Getting the Enabler/VNF configuration from the policy refinement and translation. • Deploying if required or configuring the security VNFs capable to provide channel protection between the requested path. For instance, it could be achieved enabling DTL/TLS capabilities or deploying a DTL/TLS	**Contingency:** • Execution of a privacy impact assessment by the DPO (Following case-specific instructions). • Update and review of privacy policies and mechanisms in accordance to results of the DPIA. • Update ANASTACIA privacy and security policies if necessary.

proxy. • Applying the configuration to the VNFs. Enforcement of anonimity policies could take place through: • Definition of anonymity policies using HSPL. For instance, aggregating the specific measurements of an IoT device with the data received from its neighbours. • Getting the Enabler/VNF configuration from the policy refinement and translation. • Deploying if required or configuring the security VNFs capable to provide anonymity. • Applying the configuration to the VNFs. Example Policies: • **Anonymity** "Subject" enable anonymity • **Channel protection** "Subject" prot_conf_integr [TYPEOF]Traffic	

Table 10 Contingency model - Risk 3

Risk 5: Excessive collection or retention of personal data (loss of operational control)

This risk can be generated by external or internal factors to ANASTACIA. From an external point of view, it relates to the possibility of a malicious party manages to modify network or device configuration to disable data minimization measures (through a 0day attack for example) or to actively collect personal data (through malware that prevents automatic deletion of data collected on sensors/networked devices, for example, or through a traffic analysis attack implemented through vulnerable/unauthorized devices on the network). On an internal perspective, it relates to the possibility of attackers exploiting ANASTACIA's own tools and enablers (Deep Packet Inspection and Deep Network Inspection tools, for example). As such, protection measures to address this risk should include technical checks to ensure the security of ANASTACIA itself and detection and mitigation should build upon the security mechanisms and policies introduced to prevent unauthorized access to the network and devices.

Protection:	**Detection:**
• Initial audit performed before implementation of ANASTACIA to ensure system complies with personal data protection principles and requirements • Determination of strong data deletion / minimization policies for both ANASTACIA and monitored devices, and continuous enforcement of these policies. • Strong anonymity policies implemented by	• Audit over ANASTACIA DPI tools and continuous intra-ANASTACIA security reviews to identify compliance with data deletion / retention policies. • Traffic inspection to identify anomalous data streams in accordance to security detection plans • Use Intrusion Detection Systems and AAA Architecture to identify unauthorized devices in

default • Securing only anonymized event information in ANASTACIA DSPS logs.	the network which could be compiling personal information. • Examine the security logs of all monitored devices to determine failure to delete unnecessary data from internal memory.
Mitigation: • Implement access control policies to block those devices which could be gathering information from the network. • Ensuring all communications in the network are encrypted. Example Policies: • **Access control:** Subject no_/authorise_access resource/[TYPEOF]_traffic Enablers involved in policy implementation: AAA architecture, XACML, SDN Controller, Virtual Router, Firewall configuration • **Channel protection** "Subject" prot_conf_integr [TYPEOF]Traffic	**Contingency:** • Execution of a privacy impact assessment by the DPO (Following case-specific instructions). • Update and review of privacy policies and mechanisms in accordance to results of the DPIA. • Update ANASTACIA privacy and security policies if necessary.

Table 11 Contingency model - Risk 5

Risk 6: Lacking protection of traffic information and location data

In the ANASTACIA context, this risk relates mainly to the potential usage of traffic attacks to extrapolate traffic or location information out of the network or its encrypted communications[53]. As such, this risk should be addressed through the better addressed through the aggregation of communications and the introduction of traffic shaping mechanisms to the encrypted channels to minimize the potential impact of this attack.

Protection: • Initial audit performed before implementation of ANASTACIA to ensure system complies with personal data protection principles and requirements • Definition of strong policies for channel protection • Ensuring ANASTACIA itself is not vulnerable to	**Detection:** • Use MMT DPI/DFI, virtual IDS/IPS, XL-SIEM and UTRC agents for detection of unaggregated data streams in accordance to security detection plans

[53] As mentioned by (Apthorpe, Reisman, Sundaresan, Narayanan, & Feamster, 2017).

attacks	
Mitigation: • Mitigation through SDN traffic flow management, virtual firewall, virtual switch/router, configuration of IDS/IPS; TLS The virtual proxy data aggregator enabler could be implemented in parallel to other tools (such as VPN and AAA) to minimize the potential impact of this risk. Any unnecessary outbound connection of the monitored devices beyond the local network could be blocked unless explicitly whitelisted by the end-user. Necessary or whitelisted outbound connections should use a VPN and traffic shaping mechanisms to ensure that the traffic information is not easily extrapolated by a malicious attacker.	**Contingency:** • Execution of a privacy impact assessment by the DPO (Following case-specific instructions). • Update and review of privacy policies and mechanisms in accordance to results of the DPIA. • Update ANASTACIA privacy and security policies if necessary.

Table 12 Contingency model - Risk 6

Risk 7: Impairment of data subject's rights

Since ANASTACIA is only capable of compiling information and addressing threats at a network-level, DoS and DDoS attacks are the prime example of threats which might generate the kind of affectations to the data subjects related to this risk. For this reason, IDS/IPS and firewalls are fundamental elements for the prevention and mitigation of system downtime and other limits to the right of access to personal data.

Protection:	**Detection:**
• Initial audit performed before implementation of ANASTACIA to ensure system complies with personal data protection principles and requirements • Definition of organizational policies and measures to ensure continuity of service and implementation of technical measures to this end (backup/redundant servers, etc.) • Denial of service protection: through strong filtering/forwarding policies on both the internal system and on the sites/places where information on user rights are being displayed (in order to ensure possibility of exercising rights of information, access/rectification/restriction/objection/deletion). • Deployment of virtual honeypots/honeynets by	• Use IDS/IPS, MMT DPI/DFI for detection in accordance with security detection plans

ANASTACIA • Notifying third parties regarding rectification, erasure or deletion requests • Keep records and audits of all processing operations and of disclosure activities performed by ANASTACIA	
Mitigation: • Mitigation through IDS/IPS and virtual firewall for DDoS attack protection The filtering/forwarding policy enforcement could be achieved through: • Defining filtering/forwarding policies using HSPL. For instance, denying the Internet access to a IoT device or redirecting the traffic to a VNF. • Getting the Enabler/VNF configuration from the policy refinement and translation. • Deploying if required new security VNFs capable to enforce the policies over the specified network segment. • Applying the configuration to the VNFs. Example Policies: • **Denial-of-service protection** Subject enable/remove IDS_IPS, Subject enable/remove DDos_Attack_protection, Subject no_/authorise_access resource/[TYPEOF]_traffic Enablers Involved: ○ SDN, VR, Firewall configuration	**Contingency:** • Execution of a privacy impact assessment by the DPO (Following case-specific instructions). • Update and review of privacy policies and mechanisms in accordance to results of the DPIA. • Update ANASTACIA privacy and security policies if necessary.

Table 13 Contingency model - Risk 7

Contingency verification strategy for ANASTACIA

As defined at the beginning of Section 5.4, the last element to be considered when shaping contingencies for the privacy risks addressed by ANASTACIA is the strategy to ensure that both technical detection, protection and mitigation mechanisms are well aligned with the human-based contingency activities which are necessary to ensure compliance with the GDPR's dispositions.

The following strategy has been shaped in consideration of the information available to ANASTACIA and the capabilities of the envisioned system[54]. The general steps that are to be followed to ensure proper integration of the technical and organizational mechanisms are:

a) **Initial system privacy and security verification:** as defined in ANASTACIA Deliverable 5.1, a privacy and security verification should take place before the system is set in place. This step aims to develop the necessary baselines to detect whether a privacy breach has taken place and to perform the organizational tasks required to identify and authenticate the system administrator and data protection officer which will be performing any human-based activities.

b) **Policy definition:** task to be completed jointly by ANASTACIA representatives, the system administrator and the DPO. This task should be aligned to the organization's privacy policies, legal requirements and data flows, and should be accompanied by the identification of the devices or network elements which are particularly vulnerable to privacy risks (due to the types of data compiled and processed for example).

c) **Detection and automatic mitigation of privacy and security threats:** security threats identified by the system will automatically raise alarms to the DSPS. Policy-defined mitigation activities will be performed by ANASTACIA to reduce the impact of the privacy and security threats.

d) **Recommended human-based contingencies displayed:** The DSPS will update its status automatically to reflect any changes in system security and privacy and will alert the system administrator of potential risks to the system. Its GUI will also present instructions to the DPO on recommended contingencies to be implemented by considering the types of affected devices, the duration and impact of the attack and the effectiveness of the mitigation activities.

e) **DPO input required to DSPS before restoration of privacy seal:** while the security elements of the DSPS will be automatically updated to reflect the restoration of normal system behaviour, those elements of the DSPS[55] which reflect personal data protection in the system will continue to reflect the potential breaches until the DPO certifies[56] that human-based contingencies have taken place and that the technical and organizational review (and update, if necessary) has been performed.

This strategy might be further adapted or specified as the system is developed. A final version will be presented as part of ANASTACIA Deliverable 2.7 "Privacy Risk Modelling and Contingency Final Report" [M28].

[54] It is necessary to recognize that the personal data protection requirements identified through section 4 (and as further defined by the GDPR) included elements which are not addressable through ANASTACIA. As such, the risks and associated contingency mechanisms identified throughout this deliverable should be closely examined by the DPO in charge of the system that is monitored by ANASTACIA. The DPO should be well aware of ANASTACIA's capabilities and limitations, and dully perform the system/data verification that might be beyond ANASTACIA's capabilities to properly determine whether a breach of personal data has taken place.

[55] For more information on the DSPS, see (Quesada Rodriguez et al., 2017).

[56] DPO certification of human-based contingency activities will be performed through electronic signature (as governed by the eIDAS Regulation (Kirova, 2016)) or equivalent means capable of fulfilling the non-repudiation principle and guaranteeing that the DPO has approved the activities implemented to address the situation.

6 SPECIFIC APPROACHES FOR SELECTED USE-CASES

This section aims to conclude the deliverable through the definition of case-specific elements to be considered when implementing the generic contingencies detailed in section 5.4. As agreed by the partners, this deliverable will focus on four use-cases selected for the initial ANASTACIA demonstrator, namely:

- Use Case MEC.3
- Use Case BMS.2
- Use Case BMS.3
- Use Case BMS.4

The contents of this section will perform a closer examination of these cases and will attempt to illustrate the risks generated by the use-cases; the protection approach that is likely to have been defined by the affected organization though the definition of ANASTACIA privacy policies; the ANASTACIA tools and enablers that might detect the attacks and raise the alarm to the DPO/sysadmin of the identified privacy risks; and finally, some of the mitigation recommendations that might be presented through the DSPS.

In this context, the contents of this section will serve as a baseline for ANASTACIA Deliverable 2.7, which will aim to complete the use-cases and further specify the ways in which the system will address them, while tailoring the contingency mechanisms to developments in the system's capabilities.

6.1 UC_MEC.3

6.1.1 Attack description

As previously detailed, this scenario involves a Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks through smart cameras and IoT devices belonging to the targeted network. The following figure serves to illustrate the use-case:

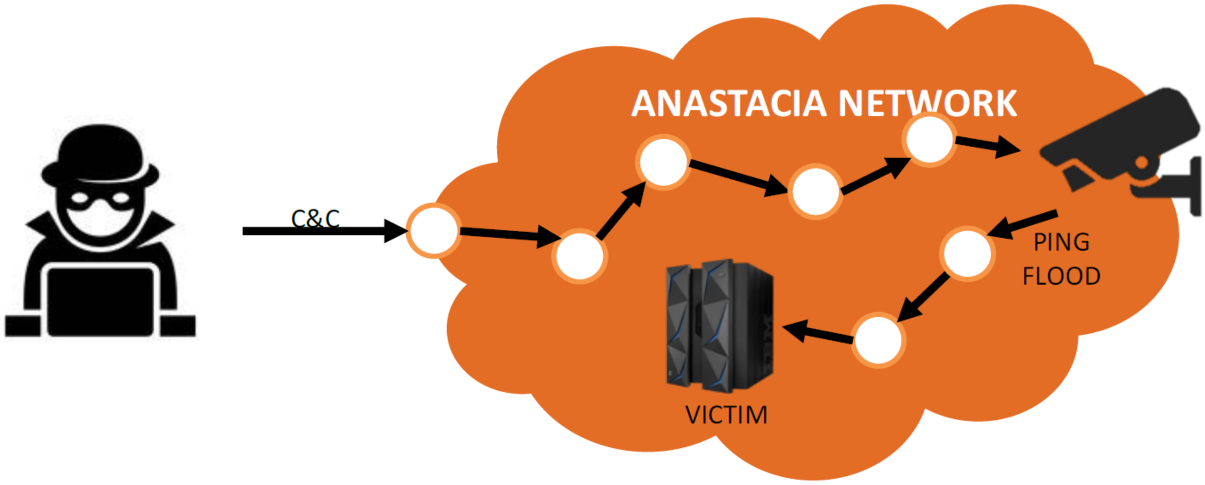

Figure 2 Representation of the MEC.3 scenario (Cambiaso et al., 2018, p. 13)

ANASTACIA Deliverable 2.2 describes the attack as follows: *"In the cyber-security panorama, Denial of service (DoS) attacks are considered a serious threat, since their aim is to compromise connectivity capabilities of an entire network or internal nodes/hosts. (…) A DoS attack can be executed autonomously by a single attacking host (…) Nevertheless (…) an attacker may execute a simultaneous and coordinated* *attack from several different nodes/hosts, willing or not to participate to the malicious activity, thus executing a Distributed DoS attack. Usually, it is quite easy to implement and run a denial of service attack, due to the vastness of tools available on the Internet.)"*(Cambiaso et al., 2018, p. 12).

As defined in supra section 4.3, from a privacy point of view, the attack will have the greatest effects in relation to Req-3 (data management and respect of data subject rights and Req-7 (security of processing), as these types of cyberattacks have the potential of limiting data subject's PDP rights (information, access, rectification, restriction objection and deletion) as defined by the GDPR.

Several characteristics of the attack as defined by Deliverable 2.2 are to be considered when determining the risks involved and their potential consequences to the fundamental rights of data subjects, namely:

- *"For our scenario, a DoS is accomplished by a malicious user with malicious goals. Although a denial of service attack could make it possible to dismantle an entire building or organization network, the use case is focused on an attack against a smart camera system. Although the severity rank of the attack is lower than in case of a target to the entire network, it should be considered that in this case the attack may be the first step of a more accurate plan (e.g. involving physical access to the building."* (Cambiaso et al., 2018, p. 12).
- *"It is possible to notice that the attacker accesses the ANASTACIA network to target the smart IP camera, which is directly connected to the network"* (Cambiaso et al., 2018, p. 12).
- *"In this scenario, an attacker, external at the network, controls a set of internal nodes/zombies and instructs them to execute a ping flood DoS attack on the network. In this case the attacking hosts are **compromised** IoT devices and smart cameras"* (Cambiaso et al., 2018, p. 13).

While the possibility of affectations to data subject's rights is clear in this use-case (Risk 7), the fact that a malicious attacker can gain access to the ANASTACIA network and effectively control compromised IoT devices and smart cameras, should also be considered as it demonstrates that the security of processing requirement has been breached. This in turn raises the potential risk of unauthorized access, disclosure, modification, removal or deletion of personal data (Risks 1, 2, and 4). While we are unable to determine the exact access or control level that has been obtained by the malicious attacker on the devices the fact that network traffic is altered by these malicious actions also points out that the network's traffic information and device location data might not be secure (Risk 6).

The following table summarizes the privacy risks and foreseeable consequences involved in this use-case[57]

Use Case	Risk 1	Risk 2	Risk 3	Risk 4	Risk 5	Risk 6	Risk 7
UC_MEC.3	Limited (2)	Limited (2)	Negligible (1)	Limited (2)	Negligible (1)	Limited (2)	Significant (3)

Table 14 UC_MEC.3 Relevant risks and foreseeable consequences

6.1.2 Protection approach

The protection approach for privacy to be followed in this use-case should consider the necessary organizational policies and due diligence that are required by the GDPR (in accordance to requirements 1, 2, 4, 5, 6, 7 and 9). These elements have been further examined in supra sections 4.2 and 4.3. Additionally, it is necessary to consider the protection elements mentioned in supra section 5.4 for each of the relevant risks. Particularly, it is recommended that the following elements are implemented:

- Security mechanisms to prevent DoS and DDoS attacks (ping packet blocking or packet limiting) as defined in ANASTACIA D.2.2 (Cambiaso et al., 2018, p. 14).
- Deployment of virtual honeypots/honeynets by ANASTACIA.

[57] As defined in supra section 5.2.1.

- Utilize ANASTACIA's IoT interface management to examine and push firmware and software updates to monitored IoT devices and security cameras.
- Use of AAA Architecture, IoT traffic protection management and firewalls to prevent unauthorized communications from potential attackers to vulnerable devices in the ANASTACIA network
- Previous identification of types of devices in the network and device classification based on personal data processed by the devices.
- Provision of alternative means for data subjects to contact the organization and to exercise their rights.

6.1.3 Detection and mitigation

Detection of the aforementioned privacy risks is based on the same mechanisms used for detecting the DoS/DDoS attack, namely: "*the proposed protection system* (ping flood packet blocking or packet limiting, upon which any infringing communications from the network would raise an alarm) (which) *should be binded on the destination address of the targeted system, to counter IP spoofing and DDoS attacks"* (Cambiaso et al., 2018, p. 14).

Short-lived DoS attacks which do not have a lasting effect on the monitored system or the services that are provided to the end-user should not be considered as potentially generating an affectation to data subject rights. For this reason, the extent of the attack or total duration of system downtime should be considered when determining the relevant privacy policies by the organization (Example: any DoS/DDoS attack that causes system downtime larger than 3 consecutive hours should trigger a privacy alert). This is particularly true as D.2.2 has mentioned the possibility of the DoS/DDoS attack being used as part of a larger attack on the network.

Mitigation of the threat should also be closely aligned with the security approach identified by D.2.2: *"After the attack is detected, the ANASTACIA platform has to react to the threat, by deploying a mitigation plan. Particularly, in this case a mitigation plan is followed in order to interrupt the attack, thus making the smart IP camera able to properly communicate on the network, independently from the fact the detection alert was triggered when the camera was able to communicate (hence, before the DoS is reached) or not (hence, under the DoS)"*. (Cambiaso et al., 2018, p. 15).

6.1.4 Contingency plan

Once a privacy risk has been identified the system should inform the system administrator and DPO of the contingencies that should be implemented at an organizational level to determine whether the threat has been materialized in an affectation to data subject's rights.

This includes:

- Determine whether the attack has had any impact on data subjects (review the alternative mechanisms to identify contact attempts by data subjects trying to exercise their rights) and whether there is a need to inform the Data Protection Authorities or the Data Subjects.
- Execution of a privacy impact assessment by the DPO considering:
    - Vulnerabilities of installed smart cameras and IoT devices
    - Location, data processed and additional capabilities (enabled or not) of devices in the network
    - Procurement policies and vendors
    - Maintenance policies
    - Post-attack debriefing of ICT team
    - Any recommendation from Data Protection Authority (if relevant)

- Update and review of organization's privacy policies and mechanisms in accordance to results of the DPIA.
- Update ANASTACIA privacy and security policies if necessary.

6.2 UC_BMS.2

6.2.1 Attack description

The use-case is focused on the injection, by an insider, of malware on the network in order to target a fire alarm application system with the aim to control a fire suppression system. The following figure depicts this situation:

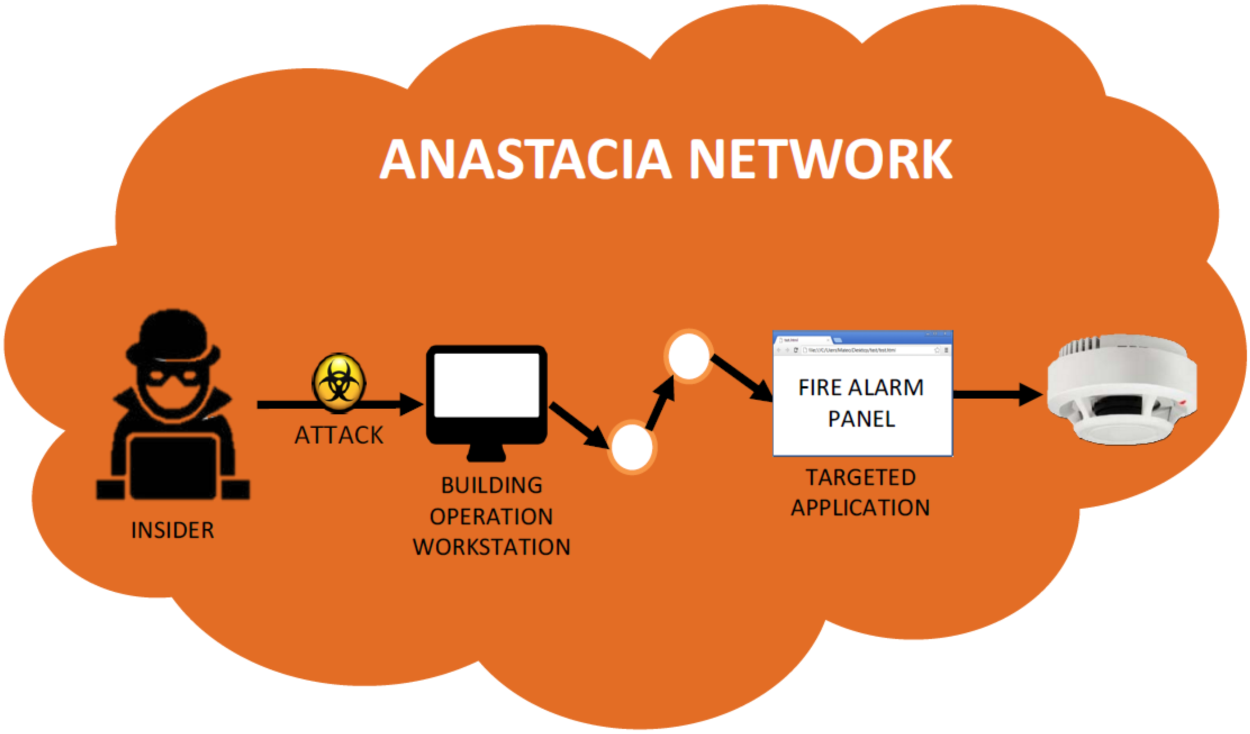

Figure 3 Representation of the BMS.2 scenario (Cambiaso et al., 2018, p. 22)

ANASTACIA D.2.2 correctly points out that the main threat in the use-case relates to the insider (and secondarily to the malware that he/she introduced to the network). *"This kind of threats is extremely dangerous, since insiders typically have advanced knowledge on the targeted system and access to restricted areas. For the selected use case, the malware is spread by using different attack vectors, such as USB infection of a building operation workstation of the malicious employee, or by exploiting wireless connectivity to access the network and spread the malware."*(Cambiaso et al., 2018, p. 22).

As defined in supra section 4.3, from a privacy point of view, the attack will have the greatest effects in relation to data protection requirements 3, 6 and 7. This because the best way to prevent insider threats involve[58] potentially invasive measures which could affect the privacy of both end-users and employees. For this reason, any measures implemented to prevent malware or intrusions into a system should respect the personal data protection principles (particularly transparency and accountability). ANASTACIA therefore

[58] *"An important consideration regarding the insider threat issue is the balance between security and employee privacy: it is generally known that there is no expectation of privacy when using an organization's network and devices, nevertheless, employee monitoring is an area that many organizations prefer to avoid. Nowadays, any computer system is attacked by malicious users, then it is necessary to implement an attack detection system and a response plan to avoid damaging the system."* (Cambiaso, Mongelli, et al., 2017, p. 6).

should meet these requirements and avoid generating any further risks when attempting to prevent security or privacy threats.

The specific attack depicted by this use case is particular as it recognizes the possibility of having malware "spread via network using a computer internal to the infrastructure of the targeted organization. The malware exploits an unpatched application of the fire suppression system to access sensitive sensors."(Cambiaso et al., 2018, p. 22). Considering both the malicious intent of the attacker and the broad potential range of impact of the malware, privacy risks 1, 2 and 4 are of maximum relevance to this use-case. A similar situation can be identified with regards to privacy risks 3 and 7, as the attacker could effectively use the same attack vectors to compile or aggregate information from multiple sources and to negatively affect the system's availability (or any other safeguards integrated at an application level to respect the rights of the data subject). Finally, while less likely given the aims and nature of the attacker, privacy risks 5 and 6 should be considered as also possible in this use-case.

The following table summarizes the privacy risks and foreseeable consequences involved in this use-case[59]:

Use Case	Risk 1	Risk 2	Risk 3	Risk 4	Risk 5	Risk 6	Risk 7
UC_BMS.2	Maximum (4)	Maximum (4)	Significant (3)	Maximum (4)	Limited (2)	Limited (2)	Significant (3)

Table 15 UC_BMS.2 Relevant risks and foreseeable consequences

6.2.2 Protection approach

Deliverable 2.2 proposed a layered approach to protecting the system from an insider/malware attack. This approach included the following elements:

- Network level protection: based on network traffic analysis to identify and drop malicious packets.
- Host level protection: based on controlling hosts and limit privileges and activities users can execute
- Application server protection: based on continuous vulnerabilities patching on both the system and its nodes and exposed applications.

From a privacy point of view, this protection approach should be complemented by the necessary organizational policies and due diligence that are required by the GDPR (in accordance to requirements 1, 2, 4, 5, 6, 7 and 9). These elements have been further examined in supra sections 4.2 and 4.3. Finally, the protection recommendations mentioned in supra section 5.4 for each of the relevant risks should be considered when designing and implementing the monitored system.

6.2.3 Detection and mitigation

The detection approach recommended by ANASTACIA D.2.2. for this use-case was based mainly on log inspection[60] accomplished by the monitoring components along with the implementation of access control rules on actions/boundaries: *"By adopting this approach, it is possible to have a complete vision of the current state of the system in order to identify the attack in time, for proper mitigation."* (Cambiaso et al., 2018, p. 23).

These same set of detection actions can be implemented to detect privacy threats:

- The AAA Architecture could be utilized to detect unauthorized or unexpected/unusual behaviour from terminals (unusually contacting devices in the network, transferring or receiving large amounts of information, using abnormal authentication credentials, etc.) particularly once the network and

[59] As defined in supra section 5.2.1.

[60] D.2.2 recommended the inspection of logs from the network, host, protection software, access, application and IoT devices.

ANASTACIA have been properly configured with a set of privacy policies which identify those network resources in which personal data could be found.

- Log inspection by the monitoring components could greatly enhance the effectiveness of this approach, particularly if access to application-level or device-level logs is possible, as this could lead to the identification of the specific resources that are being accessed.

Mitigation of these risks will depend on the implementation of SDN/NFV functionalities and enablers like MMT DPI/DFI and virtual firewalls. D.2.2. recommends the implementation of three separate approaches for mitigation (design time, run-time and continuous mitigation) at host, application and network levels. The most relevant of these from a privacy standpoint in the ANASTACIA context is the runtime-mitigation at a network level, which aims to validate users and devices accessing the network and blocking IPs which irregularly access the network.

6.2.4 Contingency plan

Once a privacy risk has been identified the system should inform the system administrator and DPO of the contingencies that should be implemented at an organizational level to determine whether the threat has been materialized or impacted the data subject.

This includes:

1. Organizational process to identify insider and report it to authorities.
2. Examine reports and logs from AAA and malware detection/prevention mechanisms at the application/host level.
3. Execution of a privacy impact assessment by the DPO considering:
   a. Human resource policies and training.
   b. Physical security mechanisms in place (to minimize risk of unauthorized access to devices in the network by insider threats)
   c. Location, data processed and additional capabilities (enabled or not) of devices in the network which might be vulnerable to similar attacks (particularly determine whether ports or services could be disabled to minimize risk potential).
   d. Maintenance policies
   e. Post-attack debriefing of ICT team
   f. Results of recent security audits
   g. Any recommendation from Data Protection Authority (if relevant)
4. Update and review of organization’s privacy policies and mechanisms in accordance to results of the DPIA.
5. Update ANASTACIA privacy and security policies if necessary.

6.3 UC_BMS.3

6.3.1 Attack description

In this situation, a malicious user targets an energy micro-grid by exploiting network nodes to violate a SCADA database through a SQL injection attack. The following figure illustrates the use-case:

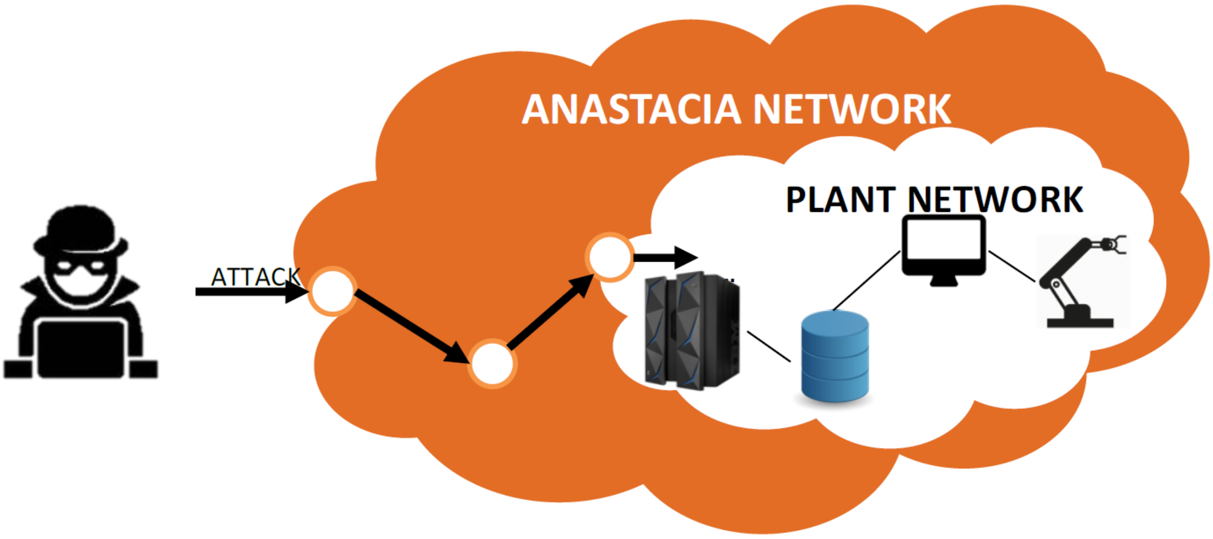

Figure 4 Representation of the BMS.3 scenario (Cambiaso et al., 2018, p. 17)

ANASTACIA D.2.2 describes SQL attacks as representing *"well-known serious threat for web applications [Halfond, 2006]. By executing such threats, an attacker is potentially able to retrieve or alter database information. Indeed, web applications vulnerable to SQL injection attacks may allow an attacker to gain complete access to the adopted databases. Usually, databases are directly accessed by web servers in order to access structured data from the (web) user interface. SQL injection attacks exploit vulnerabilities affecting web pages, often deriving from bad code quality"*(Cambiaso et al., 2018, p. 16).

As defined in supra section 4.3, this scenario is very related to two of the identified personal data protection requirements (2 and 4) as the attacker (knowledgeable of the security mechanisms implemented and their vulnerabilities) is able to directly access the ANASTACIA-monitored network and access the plant's database, potentially stealing company credentials with which she could cause further affectations to the systems and personal data of employees and customers alike.

Several characteristics of the attack as defined by Deliverable 2.2 are to be considered when determining the risks involved and their potential consequences to the fundamental rights of data subjects, namely:

- While the attacker is external to the network, it has previously worked at the company.
- *"The attacker exploits a web page vulnerability to inject SQL malicious code in order to access or manipulate the SCADA database. Such exploitation is based on the generation of the query by using unfiltered inputs provided by the user".* (Cambiaso et al., 2018, p. 16).
- The attacker's aim may be
    - To alter/tamper the database content.
    - To bypass access restrictions (to accomplish privilege escalation).
    - To access/steal sensitive data.

In this context, the risks raised by the threat are many:

- There is an extremely high risk of unauthorized destruction of personal data (risk 4) given her express intentions to directly tamper or damage the plant's infrastructure.
- Significant risks of access, modification of personal data and affectation to data subject rights (risks 1, 2 and 7) can be identified given the type of attack launched, the attacker's ties with a competitor and the very possible downtime that is to be caused by the attack.
- Additionally, there is a significant risk (6) that even if the attacker were to be unsuccessful in further escalating her access rights, the fact she is knowledgeable of the protocols and vulnerabilities in the system will enable her to directly or indirectly (through a traffic analysis

attack, for example) obtain traffic information and device location data from the network (which could involve employee personal data).

- Finally, the attacker could exploit the network and company infrastructure to complement other attack vectors[61], thus raising the possibility of excessive collection or retention of personal data (risk 5) from unsuspecting third parties.

The following table summarizes the privacy risks identified and foreseeable consequences involved in this use-case[62]:

Use Case	Risk 1	Risk 2	Risk 3	Risk 4	Risk 5	Risk 6	Risk 7
UC_BMS.3	Significant (3)	Significant (3)	Significant (3)	Maximum (4)	Limited (2)	Significant (3)	Significant (3)

Table 16 UC_BMS.3 Relevant risks and foreseeable consequences

6.3.2 Protection approach

As with previous cases, the privacy protection approach to be introduced to this case should be well aligned with the necessary organizational policies and due diligence that are required by the GDPR (in accordance to requirements 1, 2, 4, 5, 6, 7 and 9). These elements have been further examined in supra sections 4.2 and 4.3. Finally, the protection recommendations mentioned in supra section 5.4 for each of the relevant risks should be considered when designing and implementing the monitored system.

Considering the nature of the attack however, protection efforts should include organizational activities to be undertaken in line with the data minimization principle (minimization, anonymization, etc.) and introducing input sanitization mechanisms to their systems and applications. Meanwhile, sufficiently strict access control, log inspection policies should be introduced to ANASTACIA to accomplish continuous oversight of the system's security.

6.3.3 Detection and mitigation

As defined by ANASTACIA D.2.2, detection of these attacks will depend mainly on ANASTACIA's capability to monitor the logs from three principal components: database, network, and application server. This effort should be aimed at identifying unexpected queries, network accesses and anomalous or large 1 to 1 traffic in the network (particularly as relating to those devices which have been identified as potentially containing or processing personal data). These efforts should be further enhanced by the implementation of deep-packet and flow inspection tools and the recommended detection elements identified in supra section 5.4 for the relevant risks involved in this use-case.

[61] For example, using her access to the power plant's network to exfiltrate personal data from a third party's malware infected computer. Indeed, it is possible to develop malware to use power lines to exfiltrate data from air-gapped computers. "*In this case, a malicious code running on a compromised computer can control the power consumption of the system by intentionally regulating the CPU utilization. Data is modulated, encoded, and transmitted on top of the current flow fluctuations, and then it is conducted and propagated through the power lines*" (Guri, Zadov, Bykhovsky, & Elovici, 2018). This kind of attack could be impossible to track via regular network-level monitoring (as the malware would be based in the host and could make use of a zero-day vulnerability to avoid detection) and records of the flow fluctuations (and thus, of the exfiltrated data) would be kept by the power company.

[62] As defined in supra section 5.2.1.

6.3.4 Contingency plan

Once a privacy risk has been identified the system should inform the system administrator and DPO of the contingencies that should be implemented at an organizational level to determine whether the threat has been materialized or negatively affected the data subject.

As such, the following recommendations should be presented to the DPO and the system administrator by the DSPS:

1. Determine whether the attack has had any impact on devices in the network that compile or process personal data and whether there is a need to inform the Data Protection Authorities or the Data Subjects. (special care should be taken at this step considering the broad range of risks associated to the use-case, the many possible attack vectors opened by a potential escalation of privileges and the possibility to hide privacy-compromising actions through damages to the infrastructure)
2. Execution of a privacy impact assessment by the DPO considering:
    a. Vulnerabilities of affected devices in the network.
    b. Location, data processed and additional capabilities (enabled or not) of devices in the network.
    c. Human resources policies (background checks performed and post-employment follow-up for risk assessment).
    d. Policies for revocation of access and scheduled system wide credential changes.
    e. Maintenance policies
    f. Post-attack debriefing of ICT team.
    g. Results of recent security audits.
    h. Any recommendation from Data Protection Authority (if relevant).
3. Update and review of privacy policies and mechanisms in accordance to results of the DPIA.
4. Update ANASTACIA privacy and security policies if necessary.

6.4 UC_BMS.4

6.4.1 Attack description

This use-case is based on the exploitation of the system by a malicious user to manipulate critical temperature sensors through a zero-day vulnerability to bypass signature-based intrusion detection systems and trigger fire and evacuation alarms.

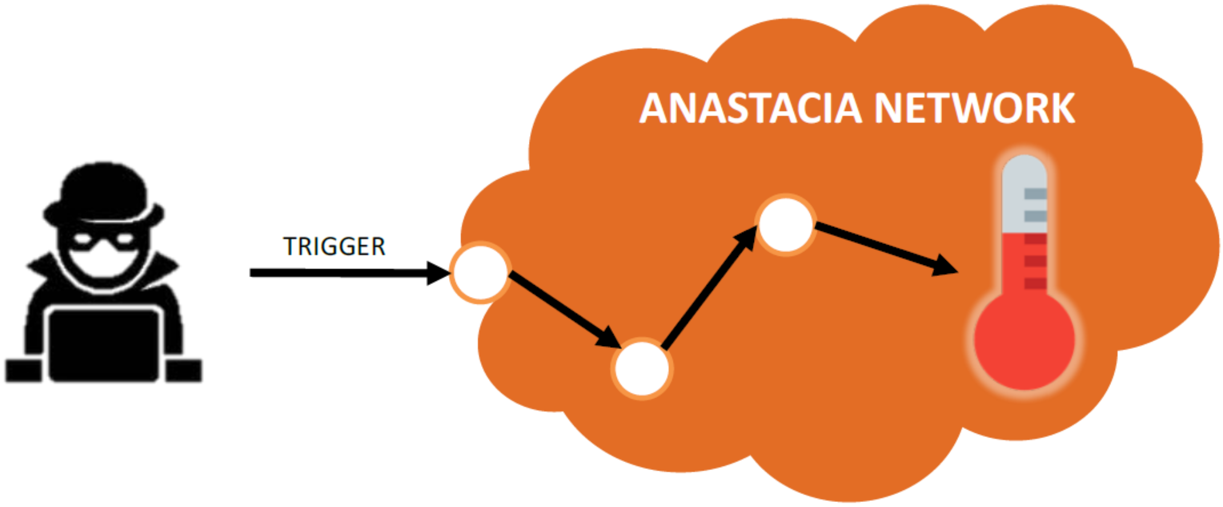

Figure 5 Representation of the BMS.4 scenario (Cambiaso et al., 2018, p. 19)

ANASTACIA D.2.2 describes the threat as follows: *"A zero-day vulnerability (0-day) is exploited by an attacker that makes use of unknown vulnerabilities on the system to target it [Bilge, 2012; Endorf, 2004]. Indeed, unlike well-known vulnerabilities, "known" by the system and often mitigated, a zero-day attack is unknown to the targeted system, usually attacked in such way for the first time. Since the vulnerability is discovered for the first time during the execution (if it is detected), there may not be known solutions or patches able to efficiently protect the system."*(Cambiaso et al., 2018, p. 19)

As defined in supra section 4.3, the attack has the potential to threaten the life and security of the inhabitants of a mega-tall building and for this reason the security requirements (Req-7 and secondarily Req-10) are fundamental to the minimization of further impacts to the individual and to avoid any further escalation of the privacy risks. As defined by Deliverable 2.2, the case involves a hacker group, *"external to the network, who exploits a zero-day vulnerability to remotely target a sensitive device, in order to access the entire network and attack the infrastructure."*(Cambiaso et al., 2018, p. 19).

The fact that the attack has been launched by a group of hackers is the most relevant element when determining the potential privacy risks involved in this scenario. As mentioned in Table 5, these groups are very adept at performing the tasks they aim to achieve. In this case, they aim to negatively impact the brand name of the hotel under attack. Considering these elements and the malicious nature of the attacker it is just as likely that they will seek to target the personal information of individuals connected to the building's vulnerable networks as it will maximize the potential impact of their current attack (achieve privilege escalation through employee identity theft) and grant them with additional attack vectors for future attacks.

In this context, all the privacy risks are to be as relevant. The fact that the tools (including knowledge of additional zero-day vulnerabilities on the system) available to the attackers to perform such attacks is unknown, along with their capabilities and motivation should be enough to raise the alarm level significantly. As such, the following table summarizes the privacy risks and foreseeable consequences involved in this use-case[63]:

Use Case	Risk 1	Risk 2	Risk 3	Risk 4	Risk 5	Risk 6	Risk 7
UC_BMS.4	Significant (3)	Significant (3)	Significant (3)	Significant (3)	Significant (3)	Significant (3)	Significant (3)

Table 17 UC_BMS.4 Relevant risks and foreseeable consequences

[63] As defined in supra section 5.2.1

6.4.2 Protection approach

As mentioned by D.2.2, there is no common and general protection plan that can be adopted to defend a system from zero-day attacks. However, certain actions like the deployment of a honeynet and continuous maintenance and training of the intrusion detection and prevention systems could help to palliate the risks involved in the scenario.

From a privacy point of view, this protection approach should be complemented by the necessary organizational policies and due diligence that are required by the GDPR (in accordance to requirements 1, 2, 4, 5, 6, 7 and 9). These elements have been further examined in supra sections 4.2 and 4.3. Finally, the protection recommendations mentioned in supra section 5.4 for each of the relevant risks should be considered when designing and implementing the monitored system.

6.4.3 Detection and mitigation

While detection and mitigation of zero-day attacks is no simple task, implementation of strong intrusion detection systems (capable of both anomaly detection and misuse or signature-based detection) is a good step to maximize the probability of detection. Furthermore, while most of the privacy risks associated to the use-case could be performed through the exploitation of a zero-day vulnerability, it is highly unlikely that the attackers will depend solely on one mechanism. For this reason, by correctly implementing the whole range of tools available to ANASTACIA, the possibility of identifying and mitigating the many security threats associated to any of the privacy risks is considerably enhanced.

6.4.4 Contingency plan

Once a privacy risk has been identified the system should inform the system administrator and DPO of the contingencies that should be implemented at an organizational level to determine whether the threat has been materialized in an affectation to data subject's rights.

This includes:

1. Determine whether the attack has had any impact on the personal data of employees or hotel visitors and inform the Data Protection Authorities due to the grave nature of the security breach.
2. Consider the need to inform the Data Subjects in light of the protection activities implemented (data minimization, anonymization, encryption, etc.) and impact to personal data.
3. Execution of a privacy impact assessment by the DPO considering:
    a. Vulnerabilities of affected devices.
    b. Location, data processed and additional capabilities (enabled or not) of devices in the network.
    c. Procurement policies and vendors.
    d. Maintenance policies.
    e. Post-attack debriefing of ICT team.
    f. Results of recent security audits.
    g. Recommendation from Data Protection Authority.
4. Update and review of privacy policies and mechanisms in accordance to results of the DPIA.
5. Update ANASTACIA privacy and security policies if necessary.

7 CONCLUSIONS

This deliverable presents the results of the first 16 months of research for ANASTACIA Task 2.3. It includes the general data protection requirements and network-level privacy risks to be addressed; the generic mitigation and contingency actions to be considered; and the specific approaches to be implemented when addressing four selected use-cases.

To accomplish this, the normative and technical frameworks that surround and determine ANASTACIA's privacy-enhancing efforts were analysed in detail. Starting from the general dispositions of the GDPR and the e-Privacy regulation, a set of synthetic personal data protection requirements were developed, commented and cross-referenced with other relevant sources. These requirements were then clarified in view of the nine use-cases to be addressed by the ANASTACIA project. Following this effort, a set of privacy vulnerabilities were identified along with the general list of security threats that will be monitored by ANASTACIA. Having considered both these elements in light of the requirements, seven privacy risks were identified, and potential measurement points associated to each.

A ISO-based risk analysis process was then followed to identify the consequences, threats, impact and likelihood of the identified privacy risks and after their evaluation a set of generic detection, protection, mitigation and contingency actions were recommended for each. Additionally, a contingency verification strategy was specified to introduce the results of the contingency actions implemented by the DPO to ANASTACIA's DSPS.

Finally, specific approaches were developed for four of the use-cases selected by the ANASTACIA consortium as relevant towards the first demonstrator of the platform. One of these cases relate to the Mobile Edge Computing/Multi-access Edge Computing (MEC) context, while three use cases concern the Building Management Systems (BMS) context. The approaches developed as part of this research described the attack involved in the scenario, recommended a protection approach to be introduced; a set of detection and mitigation activities that were to be implemented by the ANASTACIA platform; and finally a contingency plan which detailed the recommendations that should be presented to the DPO of the monitored system for further inspection and final verification of the platform's compliance with the broader (local, national or sector-specific) data protection requirements applicable to the organization.

The models and contingency mechanisms developed in this document will be tested and further specified in the following months. The results of this process will be detailed in ANASTACIA Deliverable 2.7 "Privacy Risk Modelling and Contingency Final Report" [M28].

8 REFERENCES

- Apthorpe, N., Reisman, D., Sundaresan, S., Narayanan, A., & Feamster, N. (2017). Spying on the Smart Home: Privacy Attacks and Defenses on Encrypted IoT Traffic. *ArXiv:1708.05044 [Cs]*. Retrieved from http://arxiv.org/abs/1708.05044

- Article 29 Data Protection Working Party. (2017, April 4). Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679. European Commission. Retrieved from ec.europa.eu/newsroom/document.cfm?doc_id=44137

- Bianchi, S., Troglio, G., Belabed, D., Mady, A., Farris, I., Scudiero, L., … Trapero, R. (2017, June 30). ANASTACIA D1.2 "User Centred Requirements Initial Analysis." Retrieved from http://anastacia-h2020.eu/deliverables/ANASTACIA-WP1-T1.2-SOFT-D1.2-UserCentredRequirementsInitialAnalysis-v11.pdf

- Cambiaso, E., Mongelli, M., Vaccari, I., Trapero, R., El-Din Mady, A., Belabed, D., … Scudiero, L. (2017, June 30). ANASTACIA D.1.1 "Holistic Security Context Analysis." Retrieved from http://www.anastacia-h2020.eu/deliverables/ANASTACIA-WP1-T1.1-CNR-D1.1-HolisticSecurityContextAnalysis-v0.6.pdf

- Cambiaso, E., Papaleo, G., & Aiello, M. (2017). Slowcomm: Design, development and performance evaluation of a new slow DoS attack. *Journal of Information Security and Applications*, *35*, 23–31. https://doi.org/10.1016/j.jisa.2017.05.005

- Cambiaso, E., Papaleo, G., Chiola, G., & Aiello, M. (2013). Slow DoS attacks: definition and categorisation. *International Journal of Trust Management in Computing and Communications*, *1*(3/4), 300. https://doi.org/10.1504/IJTMCC.2013.056440

- Cambiaso, E., Vaccari, I., Punta, E., Scaglione, S., Bianchi, S., Trapero, R., … Rivera, D. (2018, February 28). ANASTACIA D2.2 Attacks Threats Analysis and Contingency Actions.

- Casey, T. (2007, September). Threat Agent Library Helps Identify Information Security Risks. Intel Corporation. Retrieved from https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Intel - Threat Agent Library Helps Identify Information Security Risks.pdf

- European Council. (2017, December 5). Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications). Retrieved from https://iapp.org/media/pdf/resource_center/ePrivReg-council-draft-12-5.pdf

- European Parliament, & European Council. Directive 2002/58/EC (as ammended by Directive 2009/136/EC) concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (2009).

- European Parliament, & European Council. Regulation (EU) 2016/679 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) (2016). Retrieved from http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf

- Guri, M., Zadov, B., Bykhovsky, D., & Elovici, Y. (2018). PowerHammer: Exfiltrating Data from Air-Gapped Computers through Power Lines. *ArXiv:1804.04014 [Cs]*. Retrieved from http://arxiv.org/abs/1804.04014

- Hernández-Ramos, J. L., Bernabe, J. B., Moreno, M. V., & Skarmeta, A. F. (2015). Preserving Smart Objects Privacy through Anonymous and Accountable Access Control for a M2M-Enabled Internet of Things. *Sensors (Basel, Switzerland)*, *15*(7), 15611–15639. https://doi.org/10.3390/s150715611

- International Organization for Standardization. (2008, December). ISO/TS 25237:2008 Health informatics -- Pseudonymization. Retrieved from https://www.iso.org/standard/42807.html

- International Organization for Standardization. (2009). ISO 31000:2009(en) Risk management — Principles and guidelines. Retrieved from https://www.iso.org/iso-31000-risk-management.html

- International Organization for Standardization. (2011, November). ISO 19011:2011 Guidelines for auditing management systems. Retrieved from https://www.iso.org/standard/50675.html

- International Organization for Standardization. (2013, October). ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems -- Requirements. Retrieved from https://www.iso.org/standard/54534.html

- International Organization for Standardization. (2017, June). ISO/IEC 29134:2017 Information technology -- Security techniques -- Guidelines for privacy impact assessment. Retrieved from https://www.iso.org/standard/62289.html

- International Telecommunications Union. (2012, June 15). Recommendation Y.2060: Overview of the Internet of things. Retrieved from https://www.itu.int/rec/T-REC-Y.2060-201206-I

- Jian Ren, & Di Tang. (2011). Combining Source-Location Privacy and Routing Efficiency in Wireless Sensor Networks (pp. 1–5). IEEE. https://doi.org/10.1109/GLOCOM.2011.6134560

- Kirova, M. (2016, June). eIDAS Regulation (Regulation (EU) N°910/2014). European Commission / Futurium. Retrieved from https://ec.europa.eu/futurium/en/content/eidas-regulation-regulation-eu-ndeg9102014

- Kruse Brandao, J. (2017, September). *GDPR in the IoT: Reducing Financial Risks by Defining Standards on "Technical Measures" Required by Article 25 & 32*. Presented at the ENISA-CEN-CSCG WORKSHOP, Brussels. Retrieved from https://www.enisa.europa.eu/events/enisa-cscg-2017/presentations/kruse-brandao

- Lauristin, M. (2017, November 20). Report on the proposal for a regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications). European Parliament. Retrieved from https://iapp.org/media/pdf/publications/Lauristin-report-ePrivacyRegulation-Oct2017.pdf

- Lin, H., & Bergmann, N. (2016). IoT Privacy and Security Challenges for Smart Home Environments. *Information*, *7*(4), 44. https://doi.org/10.3390/info7030044

- McCallister, E., Grance, T., & Scarfone, K. A. (2010). *Guide to protecting the confidentiality of Personally Identifiable Information (PII)* (No. NIST SP 800-122). Gaithersburg, MD: National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-122

- Niu, X., Zhang, Y., Yao, Y., Chen, X., Jornet, J. M., & Liu, J. (2016). An energy-efficient source-anonymity protocol in surveillance systems. *Personal and Ubiquitous Computing*, *20*(5), 771–783. https://doi.org/10.1007/s00779-016-0949-1

- Quesada Rodriguez, A., Bajic, B., Menon, M., Ziegler, S., Pacheco Huamani, A. M., & Kim, E. (2017, December 31). ANASTACIA D.5.1 "Dynamic Privacy and Security Seal Model Analysis." Retrieved from http://www.anastacia-h2020.eu/deliverables/ANASTACIA-WP5-T5.1-MAND-D5.1-DynamicPrivacyAndSecuritySealModelAnalysis-v1.0.pdf

- Rescorla, E. (2008, August). The Transport Layer Security (TLS) Protocol Version 1.2. Retrieved February 18, 2018, from https://tools.ietf.org/html/rfc5246

- Rios, R., López, J., & Cuellar, J. (2016). *Location privacy in wireless sensor networks*. Boca Raton: Taylor & Francis, a CRC title, part of the Taylor & Francis imprint, a member of the Taylor & Francis Group, the academic division of T&F Informa, plc.

- Shaikh, R. A., Jameel, H., D'Auriol, B. J., Lee, H., Lee, S., & Song, Y.-J. (2010). Achieving Network Level Privacy in Wireless Sensor Networks. *Sensors*, *10*(12), 1447–1472. https://doi.org/10.3390/s100301447

- Sivaraman, V., Gharakheili, H. H., Vishwanath, A., Boreli, R., & Mehani, O. (2015). Network-level security and privacy control for smart-home IoT devices. In *2015 IEEE 11th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)* (pp. 163–167). https://doi.org/10.1109/WiMOB.2015.7347956

- speedguide.net. (2018). Vulnerable Ports. Retrieved from https://www.speedguide.net/ports_sg.php

- Trapero, R., Rivera, D., Taleb, T., Farris, I., Belabed, D., Crettaz, C., … Bianchi, S. (2017, September 31). ANASTACIA D 1.3 "Initial architectural design." Retrieved from http://anastacia-h2020.eu/deliverables/ANASTACIA-WP1-T1.3-ATOS-D1.3-InitialArchitecturalDesign-v1.0.pdf