B.7 –Technical guidance report on data security

Support Centre for Data Sharing

DG CONNECT

SMART 2018/1009

Authors		
Dr. Kyriakos Stefanidis	Fraunhofer FOKUS	DE
Tomas Kusber	Fraunhofer FOKUS	DE
Reviewers		
Adrian Belmonte	ENISA	EU
Nicolas Castellon	Capgemini	NL
Prof. Christos Douligeris	University of Piraeus	GR
Dr. Leire Orue-Echevarria Arrieta	TECNALIA	ES
Prof. Dimitrios Serpanos	University of Patras	GR

Table of Contents

1 Introduction

Data sharing can have many benefits for organisations, businesses, and individuals. However, the sustainability and acceptance of any data sharing arrangement depends crucially on the level of trust that the involved parties have in the applied instruments, processes, and policies. Data security is a core mechanism to proliferate such trust.

This guide presents a unified view on how to achieve data security in the context of data sharing. It builds on well-established, state of the art standards and best practices from thought-leading bodies, such as ISO, ENISA, and OWASP. These bodies have issued a multitude of security-related recommendations on controls that should be followed and implemented to ensure the security of IT systems in general.

The purpose of this document is to structure these recommendations based on the specific needs and requirements that data sharing practitioners have. Its objective is to serve as a reference document for practitioners, helping them to set up secure data sharing systems, policies, and procedures.

To achieve this, this guide presents a detailed view of the most important aspects (i.e. building blocks) of data sharing as well as the fundamental data security aspects and mechanisms. These two dimensions are eventually joined together in a dedicated section that explains which security aspects fit into each building block, and which controls need to be taken into account.

The remainder of this document is structured as follows:

Chapter 2 gives an introduction on the notion of data sharing and its various forms depending on the type of data concerned. The bulk of the chapter is dedicated to the dissection of the notion of data sharing into building blocks, i.e. fundamental processes that take place in a data sharing scenario, and a detailed presentation of each one of them. It should be noted that not all those building blocks are necessary, or even desirable, in all real-world data-sharing scenarios – but they can occur depending on the specific case.

Chapter 3 gives an overview on the topic of data security. It presents the basic concepts such as CIA (Confidentiality, Integrity and Availability), threats and vulnerabilities, risk assessment as well as continuity. The main content of this chapter is dedicated to the detailed presentation of the security aspects for each dimension such as architectural design, IT-security, maintenance, and security policies.

Chapter 4 presents a practical view on how these security aspects fit into the data sharing building blocks. It gives a concrete list of the controls that need to be considered for the adoption of state-of-the-art technologies and standards in data security in order to fulfil the relevant security requirements. Those guidelines are drawn from various sources such as standards, white papers, and regulatory information.

2 Data sharing aspects

2.1 Data sharing in a nutshell

Data sharing, in today's environment of interconnected services, is a process that comes as a natural requirement for each organization, business or service provider that wants to connect with its peers and get results based on large and/or diversified sets of information. Across all sectors of the economy, organisations such as research organizations, trade and exchange companies, small and large enterprises, government departments, and highly specialized intelligence organizations see the benefits, and in most cases the need, to exchange data with other relevant peers.

Depending on the type of data, the sensitivity of data, and the technological level of the organization, there are a multitude of considerations that need to be considered before the actual sharing and exchange can take place. The data needs to be stored somewhere, and be accessible, formatted accordingly and signed if needed, protected and discoverable depending on the terms of usage and licenses.

Allowing data to be accessible by external entities is a type of exposure that warrants asking questions such as "who has access", "for how long", "how should this data be used", "what personal information does this data contain", "how much does it cost", and "is there any liability"? In order to be able to answer these questions, the data needs to be structured accordingly.

A practical way to highlight the issues that arise with the decision to share data is to describe a typical example of the steps that need to be taken during the preparation of the data and the considerations (mainly in terms of security) that arise in each step.

Figure 1 shows an example for such a sequential consideration, containing all the usual steps like formatting the data, adding licence information, ensuring proper data protection, defining access control, and others.

Note that not all the steps are necessary or even relevant for all types of data or all data sharing scenarios. While the example describes the appropriate steps for confidential and proprietary data, in case of other types of data (like open data or public personal data) some of the steps can be ignored while others (e.g. data storage) must always be present. Chances are that in most non-trivial data sharing scenarios, most of these steps are mandatory and, given their generic nature, can be considered as building blocks for a well-designed data-sharing preparation.

The rest of the section is dedicated to the detailed description of each data sharing building block.

Data Sharing Blocks	Data Security Aspects Examples
Data Storage	Confidentiality protection, e.g. keep data encrypted (establish secure key management and recovery), or provide only link to data on the sharing platform and store data itself (encrypted) on premise.
Ownership or control over data	Ensure the authenticity of shared data, e.g. by providing a qualified digital seal (according to eIDAS) of the data; prepare delivered copy of data (e.g. include recipient data and seal document); ensure the shared data does not violate any licences of contained third party elements (e.g. figure, diagrams, etc.).
Anonymization	Analyse if data contains personal or confidential information that can be masked without losing value / utility for sharing. If yes, apply anonymisation/filtering/pseudonimisation to data.
Ethics Check	Receive an approval for data sharing from an ethics expert, ethics committee or comparable body.
Licensing	Define a licence for the data to be shared.
Data Security	Check the security maturity of the sharing platform (e.g. security certificate acc. to ISO 27001, passed audits, etc). Get approval from the Data Protection Officer.
Discoverability	Describe data to be shared, protect authenticity by creating a link between metadata and data itself, link master document and its visualizations (e.g. fingerprints (hash), use strong crypto-algorithms); link the metadata to underlying shared data (fingerprinting).
Data access	Ensure secure (encrypted) access to data, encrypted transfer of data and encrypted storage of data; define authentication level in order to access the data (e.g. usage of assurance levels defined by eIDAS); define data access model and restrictions: e.g. no download of data allowed and access only in a dedicated (virtual) terminal; provide mutual authentication (provider and consumer).

Figure 1 Example of data sharing building blocks

2.2 Data sharing building blocks

2.2.1 Data storage

The first building block in a data-sharing scenario is the storing of the actual data. Quite a few considerations need to be made regarding the storage of data that need to be shared. The first consideration is that data has different types of value for the organization that owns it and, given that storage solutions come at a cost, a cost-benefit analysis needs to be conducted. Apart from the business value of the data, sensitivity is an aspect that needs to be addressed. Financial records and trade secrets are inherently more sensitive than e.g. promotional material – and, therefore, need to be stored with the according access and use permissions.

In addition to the value of data, compliance with data retention regulations is often a requirement. In such cases, the data storage solution needs to be adequate in terms of long-term storage capability and redundancy.

Many organizations opt into procuring a cloud service for their main data storage instead of their local infrastructure. While this is a viable approach, given that the cloud service provider offers adequate redundancy, it comes with the risk of losing the full control of the data and, in cases where the data is neither encrypted in transit nor at rest, unauthorized access to the data by the provider is likely. There are also scenarios where regulations do not allow the data to be stored off-premises or even in different regions, although in EU the regulation of free flow for non-personal data establishes that there are no data localization restrictions with a few exceptions.

Regardless of the chosen storage solution, and depending on the type of data, an access control mechanism needs to be deployed either on the sharing platform or on the storage solution itself and, preferably, the data needs to be stored in an encrypted form. More about access control and security mechanisms can be found in sections 2.2.9 and 2.2.7 respectively.

2.2.2 Ownership or control over data

It is often desirable or mandatory to be able to verify the integrity of the shared datasets. When there is a reasonable concern that the shared data can be tampered with, the recipient needs to be able to verify that the datasets are the ones that the owner or the holder of the data intended to share.

Electronic signatures and seals are the most common security solutions for this problem. The eIDAS [eIDAS] regulation defines the framework and the requirements for electronic transactions which include the notion of data sharing. There are also initiatives like MyData[1] that act complementary to electronic IDs by allowing individuals to control the usage and sharing restrictions of their personal data.

Another concern is the intellectual property rights of the shared data, especially in cases where the sharing organisation does not own the entire dataset. Similar to the distribution of software source code, any dataset could contain information defining what is allowed to be used but what is not allowed to be shared or distributed. Therefore, each dataset needs to be checked for third-party material. Additionally, it must be clarified whether the licence for this material allows further distribution (see also section 2.2.6).

One last consideration, which is particularly relevant to the environments of the data markets, is the data provenance capabilities of the employed sharing environments or platforms. It is often desirable to have the ability to trace-back the origin and all the predecessors of a dataset and track changes to datasets and documents. Electronic signatures offer a partial solution. However, when dealing with

[1] https://mydata.org/

intermediate analysis results as part of the original dataset, more strict data-sharing platforms, that are able to regulate the flow of information between entities, are required.

2.2.3 Data format

Finding the right data and metadata formats for shared data is a recurring challenge in many knowledge-based sectors like research, modern industry, and even government. Depending on the sector, there are a multitude of standards and recommendations on how a dataset should be structured to be easily analysed by external entities.

From a practical point of view, the original format of the data is probably the most useful format. The conversion effort is usually on the recipient side, exporting useful information from the dataset via some conversion software. For most of the cases where the source format is well known (e.g. timeseries in CSV) the conversion is simple and straightforward. For more complex scenarios, there is a need to use and support a specific data exchange language that supports the notion of schemas and semantic verification. XML for web resources and RDF for metadata are two well-known examples. Many modern applications rely on JSON or YAML as alternatives to the verbosity of XML for data exchange.

Regarding open data in particular, the European Data Portal (EDP)[2], which is one of Europe's biggest aggregators of metadata from open datasets, adopts the DCAT Application Profile for data portals in Europe [DCAT-AP] as the de-facto standard for metadata. Specifically, for portals sharing public sector datasets within the EU, DCAT-AP is the de-facto specification promoted by ISA2[3] regarding the structure of the metadata records. DCAT-AP defines the structure of the catalogues to describe dataset collections, thereby improving semantic interoperability and allowing aggregators to gather descriptions into a single point of access.

Regarding industrial datasets, the information model defined by the Industrial Data Space Association[4] can be used for the description, publication and discovery of data products and data processing software within the participating organizations. This model is implemented as an ontology, using RDF as the underlying description language.

2.2.4 Anonymization

Sometimes the data to be shared contains personal or confidential information. In these cases, it needs to be checked whether the owner of the data has the right to share those parts of the data or whether those parts need to be removed or masked in some way. This is called data anonymization.

Personal or confidential information in this context usually refers to the following types

- Personal data such as names, addresses, id numbers
- Financial or other sensitive data on natural persons or legal entities
- Identifiers and data that can lead back, by aggregation, to the true identity of an individual such as an IP address in combination with a timestamp
- Special categories of personal data such as "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, ... genetic data, biometric data ...[that] uniquely identify... a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation" as per Article 9[5] of the GDPR.

[2] https://www.europeandataportal.eu/elearning/en/module9/#/id/co-01
[3] https://ec.europa.eu/isa2/home_en
[4] http://ids.semantic-interoperability.org/
[5] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e2051-1-1

The simplest course of action is to remove these fields from the data before publication. There are cases though where the simple removal results in the loss of utility and value of the data up to a point where sharing is no longer desirable. Therefore, various approaches to anonymize data exist, depending on the intended usage scenario. The most common approaches are:

- Redaction: This is the simplest of all the approaches. In redaction, the relevant fields are simply deleted from the data. This approach is valid for scenarios where the rest of the data hold the actual value for the external entity and the personal or confidential data are just unneeded parts of the initial dataset.
- Pseudonymization: In this approach, the relevant data are being converted to random strings but there is still a correlation between the initial and resulting values. This can be achieved, for example, via hash functions without salting. This approach is useful to scenarios where the shared data needs to be analysed against the relevant fields without having access to the real values of those fields. One common example is network traffic analysis.
- Generalization (k-anonymity): Generalization is a similar approach to pseudonymization. In generalization, a portion of the relevant fields is removed and replaced by common values. For example, replacing all the phone numbers by the same sequence of numbers while keeping the area codes intact. This approach is most often implemented by using the method of k-anonymity, a technique for hiding the identity of individuals in equally sized groups of similar people or data points[6].
- Differential privacy: For differential privacy, noise is added in response to specific queries on the respective data. Noise can be added by altering the values of the personal or confidential data and by adding random values to them (e.g. rounding). So, different from k-anonymity (and the other methods described before), differential privacy does not create one single, "static" view on the anonymised data set, but the anonymisation is effectively adapted in response to every query on the data. This makes it difficult to assert whether an individual or entity is part of the dataset while keeping the utility and value of the dataset relatively high.

It is important to stress that the appropriateness of each approach is dictated by the type of data and the regulations that are applicable to these types. There are scenarios where a heavy redaction of the relevant fields is the only alternative regardless of the resulting loss of value to the dataset.

2.2.5 Ethics checks

In some cases, shared datasets contain personal information. For example, if research requires obtaining data from people, the organizations involved are expected to maintain high ethical standards such as those recommended by professional bodies, institutions and funding organisations, both during processing and sharing. Datasets, even when they contain personal or confidential data, can be shared ethically and legally as long as the organization pays enough attention to the following important aspects:

- The persons' identity must be protected (this is required almost in every case).
- The provision for data sharing must be included while gaining informed consent.
- The controlled access to the shared data should be taken into consideration.

These measures should be considered even when data sharing is not planned.

Data collected from and about people could contain personal or confidential information. However, this does not mean that all the data collected this way is personal or confidential.

[6] https://policies.google.com/technologies/anonymization?hl=en

The particular strategy for handling the confidentiality strongly depends on the nature of the corresponding processing of the data. In any case, the strategy must reflect the organization's ethical and legal obligations, for which the fundamental framework is the [GDPR]. Depending on where the organization that plans to collect, process and store the data is located, some national regulations may have to be considered in addition to the GDPR. In Germany, for instance, the national regulation to be obeyed is [BDSG].

In order to be compliant to the above regulation framework, the organizations are expected to have sought and received the informed consent from the individuals whose data was collected. The consent should also, as much as possible, take into account the future uses of data. This could be for instance:

- Sharing the collected data.
- Sharing of analytical results based on this data.
- Preservation of the data and their usage for a long term.

The consent should at least permit data sharing as well as deletion of the data which is no longer required. The organisations are obliged to at least:

- Keep the participants whose data is/has been collected informed on the modalities used to maintain the confidentiality,
- inform the participants how the collected data will be stored, processed and used in the long term, and
- gain written informed consent for the sharing of data (in some cases a verbal consent could also be sufficient, see below).

The most important aspect of the consent is its existence. For this purpose, there has to be an active communication between the parties. The consent has to be given freely and contain sufficient information on all aspects of the intended collection and planned data usage.

In case of detailed interviews or research, where personal data are collected, the following aspects should be taken into consideration:

- Written consent is recommended (compliance with [GDPR]).
- Consent should be clearly stated in the form of an information sheet signed by the participants.
- Alternatively, a verbal consent agreement could be audio or video recorded.

If the information to be collected does not relate to personal data, or personal identifiers are removed from the data, *written* consent may not be required. Nevertheless, research participants have to be informed on the detailed nature and scope of the research, the identity of the researcher and on the potential handling of the collected data (including any intended action on data sharing).

Other aspects of the consent are the **one-off** and **process consent** approaches:

- One-off: Simple and practical approach that avoids multiple requests to participants and assures the compliance with the GDPR [GDPR],
- Ongoing process: informed consent from participants is ensured repeatedly throughout the research project. Different parts of the consent, e.g. participation in research for primary data use and for data sharing can be handled at particular stages of the research project. This gives participants a clearer view on the details of their participation, i.e. which data is collected and how this data is handled in the project.

In most cases, collected data (containing personal information) has to be detached from personal references (e.g. individuals, organisations, businesses, etc.) before it can be published or shared with other entities. One way of achieving this is the approach of **anonymization** of the data (cf. section

2.2.4). Based on the underlying informed consent the reasons for applying the anonymization could be:

- Ethical reasons – protecting people's identities.
- Legal reasons – not disclosing personal data.
- Commercial reasons.

It can be time consuming and expensive to anonymise some types of data, e.g. textual data, or audio-visual data. Therefore, it is strongly recommended to have anonymization already planned in the very early phase of the process and to consider its influence on the design of the surveys and format of research data to be collected as well as the particular content of the informed consent such as the intended use and scope of the collected data.

2.2.6 Licensing

In terms of licensing, two topics need to be addressed:

- Copyright – Who owns the right to make copies of a creative work?
- Licensing – How can copyright owners licence others to use their intellectual property?

Discussing copyright implies the assumption that the work the copyright should apply to is original and fixed in a material form (e.g. written, recorded, etc.). The originators of the data in digital form (e.g. publications, spreadsheets, computer programs or different types of reports etc.) are usually the copyright holders. Their contribution falls under literary work and is thus protected by copyright. The author of the work is automatically the first holder of the copyright, unless there is some other legal construct in place that transfers the copyright to a third party (e.g. an employer). In case of derived data or results of collaborative work, various authors or institutions could hold a copyright cooperatively. In these cases, it is important to correctly apply the copyright to the particular parts of the entire dataset.

Any secondary users have to obtain clearance from the copyright holder before using the data. Various ways exist to license the reuse of copyrighted data:

- Open data: Secondary users are allowed to access the data fully and free-of-charge. In many cases of free access, the owner of the data wants to be acknowledged.
- Non-open data: Access to data is subject to certain conditions such as:
    - A fee is required to access the data.
    - A licence that forbids the re-use of the data including the use of "no derivatives" requirements.
    - There is a time-limit on the access to the datasets or resources,
    - Prior registration or explicit request is required to access the data.

Especially when dealing with open data, the European Data Portal offers a comprehensive licensing assistant[7] that helps with choosing the correct open data licence among the multitude of options such as:

- Creative Commons (CC)
- European Union Public Licence (EUPL)
- GNU Free Documentation License (GFDL)
- Open Data Commons License (ODC)
- Open Government Licence (OGL)

[7] https://www.europeandataportal.eu/en/training/licensing-assistant

2.2.7 Data security

The appropriate handling of data security is a key aspect in data sharing. The delivery of authentic data that only contains the appropriate personal or confidential information and applies fully to the underlying licence is one of the most common requirements when data is shared (cf. section 2.2.6). The receiver of the shared data needs to be sure that the received information comes from a particular source and has not been manipulated on the way.

Data security can be divided into three main topics: physical, network, and systems security.

Physical security deals with the physical access to, and protection of, the relevant buildings and rooms in which data is stored, the secure handling of hardware (e.g. access, maintenance), and the secure hardware and software administrative processes. The main goal is to provide a secure foundation for setting up the environment of the sharing platform (i.e. hardware, software, processes).

Network security deals with the protection of the underlying systems, especially ringfencing them against the risks related to the communication between systems over the internet (e.g. the implementation of network firewalls and DMZs).

Systems security ensures the adequate handling of the security requirements implemented on the computer systems especially at the user level. Among others, it includes:

- Password handling (e.g. how long they should be, how often they should be changed);
- Implementing suitable access control mechanisms (e.g. RBAC);
- Implementing appropriate encryption;
- Monitoring and filtering transmitted data (e.g. filtering of personal data (cf. section 2.2.4), only allowing encrypted transfer of data);
- Destruction of the data in a secure manner (the destroyed data cannot be recovered);
- Secure processing of the shared data including traceability of changes.

The current state of the implementation of relevant IT-security measures should be confirmed by the corresponding certifications and audits, e.g. in accordance with [ISO27001].

2.2.8 Discoverability

In order to enable the shared data to be broadly discovered and reused the data has to be prepared. It would not be sufficient to collect and provide data to potential users. Instead, it is crucial to describe (document) the data to be shared in a discoverable and understandable way, which is accessible by external users. Data documentation covers technical and business aspects; such as how data was created, what it means, its structure and content (e.g. origin, purpose, time reference, geographic location, creator, access conditions and terms of use of the data collection). Documentation of data is done via the use of metadata.

Providing structured and well-defined searchable information helps the users find and classify the data underneath. Therefore, metadata for online data catalogues or discovery portals is often structured according to international standards or schemes (e.g. the Dublin Core (cf. [ISO15836-1]) or the Metadata Encoding and Transmission Standards (METS)[8] etc.).

Documenting data is vital when creating, organising, and managing data due to its importance not only for data discovery but also for (long-term) data preservation.

---

8 See http://www.loc.gov/standards/mets/

2.2.9 Data access

As already mentioned in section 2.2.5, the applicable ethical standards also affect the level of access control to data. Under certain conditions, personal or confidential data can be protected by restricting access and/or granting regulated access to such data. Usually, data collected is not in the public domain, e.g. during research projects and kept in data centres and/or archives. Usage is restricted by both user registration and the informed consent signed by the research participants. Re-users of data have to accept and obey the conditions imposed by the applicable licence (cf. section 2.2.6) in order to gain access to the shared data.

However, access to confidential data can be additionally regulated by addressing further aspects such as:

- Requirements for usage of specific authentication/authorisation procedures.
- Limiting access to approved users.
- Limiting access by only enabling remote analysis, but not the download and local processing of data.
- Removal of confidential data at least for the given period.

Which access type and corresponding regulations should apply in general depends on the mutual agreement between the user and the data owner, which should be documented in a particular licence format (cf. section 2.2.6). Access regulations should always be proportionate to the kind of data involved and the required confidentiality.

3 Data security: An Overview

3.1 Important concepts

Security is an integral part of everyday life, given the progress of globalisation, growing mobility and increasing importance of (or even dependence on) information and technology. Increased vulnerabilities and substantial financial losses as a result of IT security deficits are common. Actions that seek to minimise the prevailing risks and prevent the resulting damage are therefore of increased importance. An active security management process should be part of the general management process; such an approach is mirrored in various laws and regulations that organizations have to follow.

It is widely accepted that the implementation of the necessary IT security safeguards comes with a high investment and requires highly skilled personnel. However, the success of many (national and international) standards, guidelines and supporting information prove, that well-understood processes accompanied by well-informed, autonomous, and expert staff can achieve very good results. Effective measures in IT security, with the correct use of robust open source software, can be implemented at an affordable level regardless of the size of the organization.

Important but often underrepresented is the fact that IT security is not a static condition. In addition to setting up safeguards in order to protect IT systems it is necessary to analyse and evaluate the impact and effectiveness of the installed safeguards on security on a regular basis. This includes calculating the remaining risks and implementing additional measures in order to close any security gaps found. Usually, this is done by the development of different threat scenarios as well as evaluating their consequences and probabilities of occurrence. Typical scenarios could be:

- What would happen if confidential information became available to third parties?
- What would happen if there was undetected tampering of the information by third parties?

The successful implementation and operation of a well-working IT security management system can benefit organisations in multiple ways. The analysis and documentation of the underlying processes allows getting a better and clearer view on the business, which can lead to more reliable and higher quality work. In addition, successfully implemented IT security can result in higher trust from customers and end users.

According to the basics of IT security the following three fundamental CIA values characterise the field:

- Confidentiality – describes the need to protect information against unauthorized access and disclosure.
- Integrity – considers the aspects of unwanted modification and of authenticity[9] of the provided information.
- Availability – describes the required level, the information and services that should be available to the users.

[9] In some cases, there could be a need to separate the authenticity from integrity, but as a rule, it is a part of the integrity.

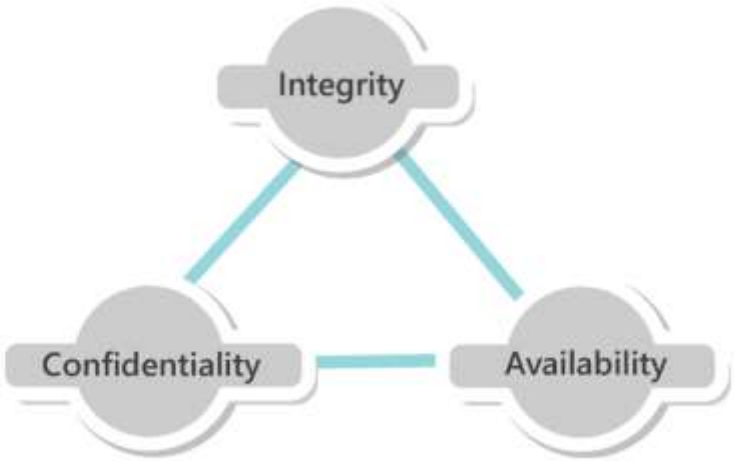

Figure 2: The three fundamental values of the IT security

The following sections will introduce the most important aspects of IT security and give a short description on each one of these aspects.

3.2 Data security aspects

In order to introduce the most important aspects of the IT security, six groups have been identified and will be described in the following subsections. The identified groups are:

1. Security architecture design and operation
2. IT-Systems security
3. Communications
4. The human factor
5. IT-Systems maintenance
6. Security policies

Each security aspect is numbered using the R-### pattern. A general description for each aspect can be found in the following subsections.

Not all security aspects are relevant to all data sharing building blocks. Section 4 details which security aspect is relevant to what data sharing building block and how these aspects are applied to their respective building blocks.

3.2.1 Security architecture design and operation

R-101	IT security aspects must be adequately considered early on in the project lifetime.

When designing the architecture, the policies and procedures of a product or service, security should be a priority in the design process rather than an afterthought or an add-on. More often than not, security mechanisms and policies belong to a crosscutting section of the overall design and, therefore, need to be considered at the start of the high-level design.

This approach is referred to as “security by design” and aims to produce services and products that are robust against the ever-increasing number of threats that even isolated systems are exposed to. Especially in a data-sharing environment, at least some of the services are bound to be exposed to the internet, or at least available remotely, which makes the whole system open to abuse by adversaries.

As stated in the OWASP “Security by design principles” [OWASP_SDP], “Applications without security architecture are as bridges constructed without finite element analysis and wind tunnel testing. Sure, they

look like bridges, but they will fall down at the first flutter of a butterfly's wings. The need for application security in the form of security architecture is every bit as great as in building or bridge construction".

R-102	Alternative approaches should be considered when necessary resources are limited.

Implementation of security mechanisms and/or policies always comes at a cost. This can be the cost of procurement of specialized software and hardware, the cost of development and integration of custom solutions into the system, and the cost of operating and maintaining those mechanisms. Finding a compromise between available funds and costs of implementing security measures is key.

Since no project comes with an unlimited budget, in practice every security architect will face the challenge of keeping the result cost effective without compromising on the basic security principles that have been put into place during the early design steps.

While the basic security requirements must be fulfilled, the actual implementation of the mechanisms that fulfil those requirements are subject to cost-benefit analyses. As a result of such analyses, it is possible to come up with alternative solutions that can achieve the same level of security but at different costs. Usually, those alternatives have trade-offs in terms of usability, support or brand trust, and, more often than not, might incur unforeseen costs in the future. One example that warrants careful consideration of the alternatives is the use of open-source software. While there are excellent security products that are open-source and free for even commercial use, there is always the risk of those projects ceasing development or unforeseen costs of adoption due to lack of required APIs or documentation.

R-103	IT security requirements must be clearly specified.

The basis for the design and implementation of the security architecture of a service or a product are the requirements of that service/product. A number of requirements fit into almost all software products that are exposed to public networks (the most common scenario in a system that supports data sharing). However, the granularity and strictness of those requirements can vary widely depending on factors such as the nature of the data or the attack surface of the product. For example, open data usually does not come with the strict privacy requirements that personal data has. Likewise, systems deployed in computer emergency response teams (CERTs) have more physical security requirements than an SME's advertisement publication services.

Therefore, the definition of security requirements needs to be both complete and precise in terms of granularity and scope. This safeguards against vulnerable implementations that are fulfilling the requirements only in contractual terms and against unexpected cost increases.

R-104	Appropriate controls should be implemented for every security requirement and associated mechanism.

Like software testing the implementation of a security mechanism that fulfils a given requirement should always be verifiable. Hence, appropriate controls should be implemented to allow for the quick verification of the correct fulfilment of the security requirements (e.g. all external communications should be encrypted).

Those controls can be either automatic or manual. Some examples of automatic controls include regular network scanning for unauthorized communications and regular automatic penetration tests. Manual audits should also be part of the standard operational procedures.

R-105	Full security management should be a long-term objective.

Apart from a suitable security architecture design and implementation, the correct operation and maintenance of the implemented system is of equal importance. Therefore, these operational procedures should be part of a full security management plan that includes classification of the system components and possibly the organization's assets, as well as threat assessment and risk management.

A valuable tool for this task is a well-defined and enforced set of security policies. More details can be found in section 3.2.6.

R-106	Security mechanisms should be selected according to the relevant requirements.

A usual caveat during the design of a secure system is the selection of security mechanisms only based on the past experience of the organization or the level of experience of the architect, without the careful consideration whether those mechanisms are sufficient or necessary given the specific needs and requirements of the product.

This practice can either lead to the under-fulfilment of the security requirements or to an unnecessary complexity of the resulting architecture. Therefore, just as a security architecture should follow the principles of minimal attack surface and least privilege, the choice of security mechanisms should be based on the principles of simple, yet coherent design and least overlap.

Many security mechanisms or solutions offer a multitude of features that cover a wide range of needs. Choosing solutions that have feature overlaps could result in an unnecessary increase of complexity during the integration and operation of the system without any gains in the robustness of the overall system. In practice, integrating solutions without properly configuring features that are not needed can even introduce additional vulnerabilities or increasing the attack surface of the overall system (e.g. by leaving exposed services with their default, and usually vulnerable, configuration).

3.2.2 IT-Systems Security

R-201	Existing protection mechanisms in the used application should be used.

Many applications that are used in a common IT operation today ship with a variety of very good quality IT security mechanisms. It is very important to know, understand, and ultimately use these provided functionalities. The addressed security functions have to be analysed, understood (especially with regards to the configuration possibilities) and used correctly.

Because the vendors of the various applications tend to implement these mechanisms by themselves, the existing protection mechanisms usually provide a good understanding of the application results as well as a good knowledge of potential weaknesses. Therefore, they can also provide a solid mechanism to protect the application against attacks which are tailored to use these weaknesses.

R-202	Usage of anti-malware software must be implemented throughout the organisation.

One of the most common and very important aspects of IT security is the protection against malware (e.g. viruses, spyware, adware, rootkits, ransomwares, trojan horses). Every day, hundreds of thousands new malware and potentially unwanted applications are registered[10].

[10] https://www.av-test.org/en/statistics/malware/

The common propagation mechanism of malware is the Internet (e.g. malicious e-mails, visiting of web pages). However, systems which are operated offline can also be infected via alternative ways such as media storage devices. This means that every system should be protected by anti-virus programs, even if it is operating offline.

In order to speed up the investigation efforts of the anti-virus programs, some of the tasks are performed centrally (e.g. checking of the incoming e-mail or monitoring of the internet traffic), whereas others are computed locally (e.g. monitoring of the executable files or scripts, checking of the macros and content of the mounted external storage devices like a pen drives or external hard disks). The local monitoring should be performed continuously on the fly, but scans of the whole system should be periodically performed in regular intervals as well. Finally, the most important thing is to keep the anti-virus programs, especially their malware description database, constantly updated.

Even if the malware protection program (including the malware recognition database) is kept constantly up-to-date and the malware protection strategy includes almost all the requirements mentioned above, there are still additional risks that cannot be mitigated in this way. Therefore, it is still important to combine this approach with others, such as the requirements described in section 3.2.4.

R-203	Data access should be restricted to the minimum level needed.

One of the most important rules of IT security is the “need-to-know” principle. In other words, users (including a privileged one – i.e. an administrator or a root) should only have access to those features/programs and information, which are necessary for their everyday work. By using state-of-the-art approaches that implement role-based access control (RBAC) the implementation of this rule can be achieved without huge expenses. According to RBAC, the particular access rights are connected directly to corresponding roles. A set of roles can be combined in a group. A specific role/roles or group/groups can be assigned to a user and by doing so, the users would indirectly be allowed to execute specific actions in the system and access dedicated information as derived from their individual access rights.

A suitable access management allows the ongoing monitoring of the current concentration of access rights as well as the elaboration of strategies for its minimization. Regular checks are necessary. Especially business processes implicating a change of business roles (e.g. transfer to other organisational unit implies assignment of new access rights but also deletion of the rights, which are not needed any more) should be a major focus. Another important point which is commonly neglected is the revocation of the permissions for staff that leaves a company.

R-204	Roles and profiles must be assigned to all system users.

Access authorization should not be assigned to individual persons or groups directly. When large numbers of persons have to be administered, this approach inevitably requires substantive administrative effort, is highly complex, and therefore highly susceptible to errors. Almost all standard applications offer the possibility to define appropriate authorisation profiles and creating suitable roles. Every user (and every administrator) is assigned one or more permissible roles, which can be assumed during work. This not only permits simpler (and therefore more secure) authorisation management; it also enables more flexibility, as the same person can assume different roles depending on the particular tasks or activities currently performed.

R-205	Administrator privileges should be restricted to the minimum.

Many system administrators work under an administrative role which is subject to virtually no restrictions and enables extensive system privileges. The administrator could abuse this fact while also raising the risk of successful privilege escalation by unauthorised third parties. Therefore, if possible, different

administrative functions should be defined. For example, depending on the administrative role, it is possible for one administrator to manage only the printers, another to create new users and a third to be responsible for backups. Ideally, there would even be a separate administrator to analyse logged data and monitor the other administrators' work.

It is an observed tendency that the concertation of the access rights especially by the members of those groups could lead to disastrous consequences. Centrify's survey[11] of 1.000 IT decision makers in the U.S. and U.K. found out that 74% of breaches involved access to a privileged account. A functional and effective Privileged Access Management (PAM), as a part of Access management (AM) as a whole, is of great importance.

R-206	Application privileges should be restricted to the minimum.

Executable programs, as well as the users themselves, have certain access rights and system privileges assigned to them. In many cases, a program will simply inherit the permissions of the user who executes it. Sometimes these authorisations are not sufficient such as the case of server processes, which often have to be configured with extensive privileges. In such cases, programs sometimes possess permissions of dedicated privileged users (e.g. "root") and can use all the accessible system resources. If such programs are used by an aggressor in a way in which they were not intended to be used, the aggressor will inherit all the permissions that go with the misused program. Thus, programs should also only be assigned the access rights required for them to work properly.

R-207	The standard (default) vendor configuration needs to be changed.

Most of the IT systems come with a pre-set manufacturer configuration. By doing so, the freshly installed system can be used in a smooth and convenient manner directly after its installation. Unfortunately, the convenience and security are two opposing concepts and IT security aspects do not always play the main role in the choice of the default values by the vendors. The out-of-the-box installations come usually with as few restrictions as possible in their default configuration. This means that weak and broadly known default passwords (also for the administrator), default users and relative unrestricted communication with the application (not sufficient secured interfaces and broadly open interfaces) are in place. These have to be adjusted in order to avoid possible misuse. A freshly installed system must not be released for production if the underlying configuration has not been customized and the system sufficiently secured.

Very often, the systems which are of higher importance for the business must be subject to additional hardening measures, such as:

- Only the minimum number of administrative accounts is active
- No default users are active
- Default usernames and passwords have been changed
- Only the absolutely necessary functionality is active
- Only the absolutely necessary interfaces are enabled
- Sufficient authentication and authorisation measures are implemented
- No other systems are installed on the same node (separation)
- The appropriate regular maintenance processes are in place
- The provided update strategies have been implemented

11 https://www.centrify.com/resources/centrify-privileged-access-management-in-the-modern-threatscape-2019/

R-208	Product manuals and documentation should be read in time.

An experienced administrator will often be in a position to boot up a system without reading the operating manuals in advance. However, this is often unreliable. For example, manufacturer warnings can be overlooked resulting in unexpected problems later on, such as incompatibilities, system crashes or undetected vulnerabilities. It would be prudent not to ignore the guidance provided by the manufacturer and, thus, create unnecessary risks.

R-209	Detailed documentation of the installation and the system itself must be created and regularly updated.

It is advisable to document all the operator actions performed prior to, during and after an installation, in writing. This will make it possible to recover more quickly from potential problems and to locate the possible causes. It is also important that the system documentation can be understood by third parties (e.g. by a "stand-in" administrator when the main administrators are away from office). This reduces the risk of failures in the event that the full-time administrator is suddenly no longer available. Moreover, if an attack is carried out, unauthorised changes to the system will be identified more quickly.

3.2.3 Networks

R-301	Networks should be protected by appropriate security mechanisms (firewall, NIDS, clustering, etc.)

No computer used for business purposes should be connected to the Internet without the protection of a suitable firewall. Even within relatively large internal networks, there are usually several subnets with different user groups and different security requirements. Therefore, it is often necessary to protect one's "own" subnet against adjacent networks to ward off threats, which may be qualitatively similar to threats from the Internet (e.g. isolation of the Human Resources department from the rest of the organisation). Therefore, appropriate protection mechanisms should be installed on those networks.

R-302	Implemented network security mechanisms must satisfy certain minimum requirements.

To protect the internal network against other, less trusted networks, an appropriate firewall type must be selected. The design of the firewall architecture, firewall installation and the internal intrusion detection systems should be done by specialists.

Generally, a multi-level firewall concept is recommended, under which additional filter elements (for example routers) are positioned in the upstream and downstream communication. If there is only a single computer or a complex firewall system is not feasible, it is recommended to install a personal firewall on the computer to be protected and, thereby providing at least basic protection.

The filter rules in firewalls tend to grow and become more complicated with time. Most of the times, the firewall administrators comply with requests from users all too lightly, thus watering down the rules. However, there should be no security exceptions regardless of their position in the company. It is therefore necessary to check at regular intervals, whether the existing filter rules are still consistent, whether they can be simplified and whether they are sufficiently restrictive. Moreover, checks should be carried out periodically as to whether the existing firewall design can still cope with communications protocols that have already been introduced or are expected to be used in the near future. Finally, new technologies can pose additional challenges to existing firewall concepts.

Even the security enabling systems like firewalls can fall victim to a successful cyber-attack. Defence strategies that are designed with multiple levels are necessary in order to be able to maintain a minimum amount of protection even when one firewall component has been compromised.

Apart from the firewalls, networks need to be monitored and the logs need to be securely stored and processed in a manner that ensures traceability of all network related incidents.

R-303	Data accessible by outsiders should be restricted to the minimum.

A lot of confidential information is provided to authorised users over open networks. This means that provided data can be accessed from outside the system. In this case, data protection depends solely on reliable authentication and authorisation mechanisms. However, if these mechanisms are configured/implemented incorrectly or they contain a vulnerability, information requiring protection can easily fall into unauthorized hands. It is therefore necessary to always check whether data that requires protection has to be made available and processed outside the organisation's own network individually.

R-304	Services and application features accessible by outsiders should be restricted to the minimum.

Every service or open communication port that is offered to the outside world increases the risk of a possible security loophole. Therefore, it is important to carefully check whether services need to be enabled, thereby possible exposing an attack vector. The associated security risk can vary depending on the relevant technology and implementation. With existing installations, regular checks should be carried out as to whether individual services or functions have not simply been enabled by mistake or out of convenience without an actual use case. The time gained by the reduction in administrative effort that results from such measures can then the be directed into the security administration of the remaining processes.

R-305	Particular caution should be exercised when handling web browsers; risky actions should be strictly prohibited.

Only active content, scripting languages and multimedia plug-ins that are essential for the work to be performed should be enabled in web browsers. In particular, risky scripting languages should be disabled, without exception.

R-306	Particular caution should be exercised regarding e-mail attachments.

The file attachments appended to incoming e-mails can contain damaging functionality if executed. No user should innocently open such attachments without checking them first. It is imperative to use a virus protection program. If in doubt, the recipient should check with the originator before opening an attachment. One particular problem is that certain e-mail programs open and execute attachments directly without asking the user for confirmation. Automatic opening of e-mail attachments can be technically prevented by selecting an e-mail program that does not have this functionality, by implementing appropriate configuration settings, or by installing add-on programs.

R-307	A stand-alone internet appliance used for surfing could be a low-cost solution for most security problems related to the use of the Internet.

One simple and cheap way of reducing the number of risks associated with surfing on the Internet is to set up a stand-alone appliance (such as a PC), which is not connected to the internal network. This can be used for internet research without having to give up functionality and convenience. Downloaded files can be checked for viruses on this dedicated system and then be passed on via data media or via other dedicated mechanisms into the internal network. This approach is only suitable for highly secured environments and cannot be adopted easily by the majority of organizations due to cost and convenience.

3.2.4 The human factor

R-401	Security policy and requirements must be followed.

Security policies can only help if users follow them. Even the best security functions and programs are of no benefit if they are used infrequently or not at all. The consistent observance of all the necessary security requirements is a learning process for every individual in the underlying organisation and only works in the long-term once it becomes routine.

The entire staff should have a basic understanding of IT security, be able to follow the relevant lines of argument and assess the dangers. Even the most sophisticated security policy cannot cover every security aspect of the daily working life.

R-402	Order should dominate at the workplace and no personal or confidentail information should be freely accessible.

In the context of IT security orderliness is without doubt an excellent way of avoiding additional risks.

Confidential files should be securely locked in a cabinet or safe at the end of the day. Data storage devices such as external hard disks or USB sticks containing confidential material should never be left lying around. If necessary, they should be properly disposed of to prevent unauthorised persons from reconstructing the data that was stored on them.

Confidential printouts should be shredded and not thrown in the normal waste paper basket. Data media such as hard disks or CD-ROMs must be securely deleted or destroyed.

Of course, the implementation of this safeguard depends on data and files having been rated as personal or confidential in the context of an assessment of protection requirements and staff being familiar with these requirements.

R-403	Special precautions should be taken in the case of maintenance and repair work.

When computers or individual hard disks are repaired or thrown away, it is possible for unauthorised people to view or reconstruct confidential data (and normally even on defective data media). Service technicians should therefore never be left unsupervised while working on IT systems or private branch exchanges. When data media is to be taken off-site, all data must be wiped beforehand or the necessary confidentiality agreements should be signed.

Files which are deleted in the conventional way can subsequently be read either solely or partially using special tools. Important files must therefore be "securely deleted". Add-on programs are available for this purpose for all standard operating systems.

R-404	Staff has to participate in regular training.

Many mistakes arise because of ignorance or lack of awareness on the potential threats or hazards. This statement obviously applies to IT security as well. Thus, regular training is essential for administrators and IT security managers. When budgeting it is important not to be frugal with training, even if expensive options such as attending outside seminars are not possible. Purchasing high quality technical literature can quickly pay off.

However, training should not just cover technical topics. Often, the weakest link in the security chain are the employees that can be tricked to reveal confidential information or give access to privileged systems via social engineering.

Safeguards should therefore be taken at regular intervals to increase security awareness among all the staff concerned. This can be done in a variety of ways: internal lectures, training courses, circulated memos, posters, graphic examples, publication of security incidents etc.

It is also important to inform staff of the channels available for communicating with business partners: Who are the contacts? What competence level do they have? Which process must be followed for authorisation? Which information may be forwarded to external parties?

Lines of communication, too, need to be explained: What data may be exchanged via e-mail? What are the business partners' correct phone numbers and URLs?

R-405	Only an honest self-assessment will help: sometimes it is necessary to call in the experts for advice.

The necessary technical knowledge on all aspects of IT security will not always be available within the organisation. qualification safeguards are often not sufficient, as the people concerned may not have the resources required for mastering all technical requirements. Here it is necessary to rethink and redefine responsibilities. It may be wise to call on external help or to outsource technical tasks to service providers. The overestimation of one's own capabilities can have adverse consequences.

R-406	Audits should be arranged for all existing security objectives.

Comprehension, acceptance and willingness on the part of the staff with regard to all the required security safeguards is always the uppermost aim. However, these requirements can be ignored for a number of reasons. Deliberate disregard is the exception rather than the rule, while mistakes and carelessness are the most common causes. Risk avoidance through suitable safeguards is in the interests of everyone. For this reason, it is necessary to consider how compliance can be monitored for every security objective. For example, monitoring may entail the use of technical tools or dedicated auditors, through analysis of logged data or spot checks by managers etc. Equally important is offering the possibility of self-regulation should be offered, for example by giving suitable checklists to staff (cf. section **Fehler! Verweisquelle konnte nicht gefunden werden.**). Optionally, such completed checklists can then be signed and passed on to the administration.

R-407	The consequences of security breaches should be described and published.

All those involved should be aware that (intentional or unintentional) disregard of security requirements will incur disciplinary safeguards. It should be clearly noted (for example, in the organisation's security policy) what these consequences will be.

R-408	Detected security breaches should have consequences.

If any security breaches are discovered the line manager needs to deal with the guilty party in an appropriate manner. Tough sanctions for mild breaches would be inappropriate, especially if it is the first such occasion. However, it is equally wrong not to act in case of more serious breaches or persistent offenders, since this could lead to a lack of obedience in the long run. Therefore, an appropriate response is required where necessary. The fact that breaches will incur disciplinary action must be communicated to everyone, as far as the particular business environment permits.

3.2.5 IT-Systems Maintenance

R-501	Security updates must be regularly installed

Given how fast new viruses can spread, implementing anti-virus software security updates must be a top priority. Updates of web browsers, e-mail programs and operating systems should likewise be carried out at regular intervals. Moreover, other application software and particular hardware components also have to be regularly maintained.

In larger organizations, the use of update roll-out tools that push out patches (e.g. MS SCCM) can be a valuable addition to ensuring correct maintenance. Apart from security updates, central configuration management tools can help in preventing and responding to vulnerabilities and internal incidents.

R-502	Detailed research on the security characteristics of the applications used should be carried out periodically.

It is vital to stay informed of newly identified vulnerabilities and tools when protecting IT systems. The latest recommendations on the Internet and technical articles can assist here. New program versions (e.g. of browsers) often eliminate known security-relevant vulnerabilities. However, this does not obviate the need to consider this matter on an individual basis, as new versions usually contain new functions and bugs that bring other risks.

Every system manager should regularly take time for appropriate searching/investigating as well as exchanging information with professional colleagues. A number of information services that are free of charge exist.

Moreover, the abundance of updates and security patches that are constantly being published requires a selection process. Usually not all are installed, especially as an immediate safeguard. Therefore, an advanced agreement should be put in place on the selection criteria to be applied when deciding which updates can or must be installed and with what time delay.

R-503	An action plan for installing necessary security updates should be created.

Even if the system manager does not install important security updates, this does not mean that the system automatically stands still or that a malicious hacker attack will take place immediately. This makes clear that the installation of updates requires considerable discipline and must be laid down as a process in advance. In the case of anti-virus software, the fastest possible installation of updates should become the routine.

R-504	Software changes should be tested.

In theory, every software change to productive systems should be exhaustively checked in advance in a test environment, thereby ensuring that all systems will still function as expected once the change is implemented. This applies to both architectural and implementation levels.

For instance, a virus protection program update can paralyse corporate networks if in-house software is incorrectly identified as a new virus and subsequently disabled.

Testing important security updates usually takes place under time pressure, as they need to be installed as soon as possible. Administrators must therefore carefully weigh the IT security requirements against the available resources and derive reasonable compromises.

3.2.6 Security policies

R-601	A security policy should be properly documented in the corresponding security concept.

The document(s) that bind together an organization's system operations and human activities in terms of information security is called security policy. A security policy contains the roles and responsibilities as well as the rules and procedures for each individual that is using the organizations assets or resources. While the actual document structure and scope is heavily dependent on the organization's size and needs, standards such as ISO 27001 [ISO27001] and the security policy requirements as dictated in NIST Special Publication 800-35 [NIST800-35] can be valuable tools for the composition of a complete and, in case it is needed, compliant security policy. The security policy should be approved and supported by the security officer and the organization management and should be known and clear to all of the organization staff.

R-602	A sensible password policy should be adopted.

The password policy is one of the standard policies that should be implemented and enforced in an organization. Due to the increase of processing power that can be used for password cracking, strong passwords are mandatory for the robustness of the access control mechanisms of the organization's hosts and services.

One trade-off that should be considered is the possibility that a very strict password policy could potentially result in passwords that are not easy to be remembered by the users, who in turn write them down and leave them in easily accessible places. The same holds true for high frequency password reset policies. Sometimes it is preferable to make sure that the policy allows the use of high entropy passwords containing easy to use phrases even if those passwords stay valid for longer periods of time [HIC2016]

Apart from passwords, authentication can be enhanced by a second factor such as a hardware token or OTPs sent to mobile devices. Such 2-factor authentication is becoming the default policy for systems that process personal or confidential data.

R-603	Workstations should be secured in the absence of their owner by a password-protected screensaver.

Physical access to a user's host machine is one of the attack vectors that cannot be easily covered by the usual cyber-security mechanisms. The impact of such a breach is proportional to the access level of the user whose station is compromised. Therefore, for the hosts that are available to users with a higher access level, the default policy should be a screen lock with a short time threshold and mandatory password protection. This ensures the minimum amount of time that a host remains unprotected remains as low as possible.

R-604	Sensitive data and systems must be protected according to their asset value.

The systems and services that require protection within an organization (i.e. the assets) have a different "value" assigned to them depending on the type of data or operations that they host or process. Since the implementation of a security policy does not come without cost, the amount of protection, in the form of deployed security mechanisms and implemented security operations that each asset warrants, should be decided based on the asset's perceived value. The result can be that, for example, accessing specific systems requires 2-factor authentication or that changes to specific data are tracked up to 1 month.

R-605	Responsibilities must be clearly defined and assigned.

One important part of a well-designed security policy is the clear definition of actors, roles and responsibilities within the system's operational environment. While the redundancy of actors is a good property for the continuous operation of the system, the redundancy in responsibilities often leads to a lower accountability and to longer reaction times during a security incident.

As a rule, each role should have a small number of clearly defined responsibilities without any overlaps between roles. In addition, the number of actors for each role should be adequate to ensure the continuous operation of the system. Lastly, the number of roles per actor should be equal to the number of non-overlapping responsibilities for each actor.

R-606	IT security should be audited regularly.

The correct implementation of the security policies is of equal importance as its correct design. Security audits conducted by internal or external experts are one of the main controls that ensure the continuous correct implementation of said policies. Part of the design of security policies should be the documentation of the controls that are to be used during audits. While external audits are sometimes the only way of proving the correct operation of the system to an external regulator, depending on the access level the organization is willing to give to external entities during an audit, some parts of the system can only be audited by internal yet autonomous security experts. A well-documented auditing procedure is therefore vital for proving the system's trustworthiness to an external regulator. This holds true especially in the context of systems that handle and share personal or confidential data.

4 Secure data sharing

This section discusses how to achieve data security in the context of data sharing. It is where the two dimensions of data sharing building blocks and data security aspects are combined. For each data sharing building block sub-section, we show which security aspects are applicable and we present a list of security recommendations based on these aspects.

To further elaborate on how each recommendation should be implemented, this section contains a matrix with the mapping between the previously presented recommendations and security controls specified by ISO, ENISA, BSIGSK, and OWASP. The controls specify the practical measures that should be considered for implementing the stated recommendations. Therefore, they give specific guidance on what needs to be done, and/or considered, during the implementation of a recommendation. The appropriate measures can be technical, physical, procedural, or policy-specific.

Finally, each data sharing building block sub-section contains a checklist that provides a series of questions that should be considered in order to ensure security in the context of each respective building block.

4.1 Data storage

As discussed in the previous sections, data storage security is the first building block for a secure data sharing environment. This section will present how the generic security aspects can be applied specifically to data storage, which controls should be taken into account, and what a practical checklist for data storage should look like.

4.1.1 Security recommendations on data storage

To ensure proper data storage security, the responsible practitioners should make certain that the following measures are taken:

- R-101 – When designing the architecture of the data storage subsystems, the required security mechanisms should be taken into account from the start of the design process. The "security by design" approach should be part of this process.
- R-102 – Since the security mechanisms that should be built in and around the storage subsystems come at a cost, there should be alternative solutions that can fulfil the security requirements at lower costs. The trade-off will usually come as lack of usability, difficulty in maintenance, or smaller long-term integrity guaranties. It should be noted that for long term storage systems, integrity is a high priority requirement.
- R-105 – Apart from the security design, the operational and maintenance procedures of the storage subsystems and the stored data should be clearly defined as part of the full security management plan.
- R-106 – The security mechanisms to be deployed with the storage subsystem should be selected according to the security requirements of the system and not follow a one-size-fits-all approach. Depending on the sensitivity of the data in terms of secrecy, value, and availability, the security mechanisms should be chosen accordingly. For example, for high availability of non-confidential data, a cloud storage solution behind a CDN is sufficient. For scenarios which involve processing of medical data, the solution should be housed on-premise and all processing should be done within the organization itself.
- R-201 – There are a multitude of local or cloud storage solutions, most of which come with their own standard security mechanisms. Those mechanisms should, after careful evaluation, be prioritised. Introducing custom-made mechanisms which have not been subjected to rigorous integration tests should be avoided. In general, the offered security mechanisms of

a storage solution should play a prominent part in the evaluation of the solution itself and, given the adoption of the solution, should be used as directed.

- R-203 – Almost all storage solutions offer some form of access control. The default configuration of the access control at the storage level should follow the deny-by-default and least privilege approach. In the case where user access control is performed at application level, the data storage services should only be accessible by explicitly configured applications.
- R-204 – Every user account in the database should be assigned roles that allow the minimum required access to the data. Generally, users should not have direct database accounts. The applications that have access to the database should not use administrator accounts.
- R-207 – Database and storage solutions are shipped with a minimum default configuration that includes default administrator accounts and default network configuration. The default configuration needs to be changed before the system goes into production.
- R-209 – Configuration of the storage subsystem as well as deployment of databases and their schemas should be documented on both operation and application levels. This ensures that there are no forgotten or misconfigured databases and/or API endpoints that could be used as a vector for a data breach.
- R-401 – Access to the stored data is governed by the deployed access control mechanism and the security policy in effect. This policy should be communicated clearly to anyone that has any kind of access to data and should be followed accordingly.
- R-403 – One probable breach vector for data centres and/or subsystems are maintenance windows. In terms of availability, maintenance should not result in complete loss of data access, especially without prior configuration of application servers (i.e. the usual systems that have direct access to the data subsystem) to use redundant databases. In terms of confidentiality, old and broken hard disks could be used by malicious entities to access insecurely deleted data. The maintenance personnel - especially if they belong to external vendors - should not perform any kind of datacentre work unsupervised.
- R-603 – Apart from data centres, personal or confidential data can also exist in individual employee workstations. Even if there is no provision for long term storage of data in a workstation, caching could create temporary copies. Therefore, the workstation should be password-protected and unattended workstations should be locked automatically.
- R-604 – The strictness of the security mechanisms and policies for the stored data should be equivalent to their value and sensitivity.

4.1.2 Applicable Controls

The controls specify the practical measures that should be considered to implement the stated recommendations. Therefore, the controls give specific guidance on what needs to be done and/or considered during the implementation of a recommendation. The appropriate measures can be technical, physical, procedural, or policy-specific.

The following matrix gives an overview of how security controls specified by ISO, ENISA, BSIGSK, OWASP and other external resources apply to the previously mentioned requirements and recommendations. The controls are on the horizontal axis (blue shade) and the requirements on the vertical axis (yellow shade).

	ISO27001, 8.1	ISO27002, 9.4.1	ISO27002, 8.2.1	ISO27002, 10.1.1	ISO27002, 12.3.1	ISO27002, 12.4.1	BSIGSK, M 2.161	BSIGSK, M 2.162	ENISA1, 7.2.3	ENISA1, 7.2.4	ENISA2, 4.1.1.3	ENISA2, 4.2.3	ENISA2, 4.2.5	ENISA2, 4.2.8	ENISA3, SO18	ENISA3, SO19	ENISA3, SO23	ENISA4, 4.5	ENISA4, 4.9.2	ENISA4, 4.9.4	OWASP_ASVS, V6	OWASP_ASVS, V12	OWASP_SDP, 5.3
R-101							X	X													X	X	X
R-102							X	X															
R-105	X	X	X	X																			
R-106						X			X	X	X	X	X	X	X	X	X	X	X	X			
R-201						X			X	X					X	X	X						
R-203			X			X					X					X							X
R-204			X			X					X					X							X
R-207				X	X	X							X	X		X							
R-209	X	X																					
R-401			X			X					X					X							X
R-403	X				X								X	X	X								
R-603									X	X		X					X		X				
R-604						X			X	X	X	X	X	X	X	X	X	X	X	X			

Table 1: Data Storage: Relationship between the identified IT-security recommendations and the available controls

As shown in

	ISO27001, 8.1	ISO27002, 9.4.1	ISO27002, 8.2.1	ISO27002, 10.1.1	ISO27002, 12.3.1	ISO27002, 12.4.1	BSIGSK, M 2.161	BSIGSK, M 2.162	ENISA1, 7.2.3	ENISA1, 7.2.4	ENISA2, 4.1.1.3	ENISA2, 4.2.3	ENISA2, 4.2.5	ENISA2, 4.2.8	ENISA3, SO18	ENISA3, SO19	ENISA3, SO23	ENISA4, 4.5	ENISA4, 4.9.2	ENISA4, 4.9.4	OWASP_ASVS, V6	OWASP_ASVS, V12	OWASP_SDP, 5.3
R-101							X	X													X	X	X
R-102							X	X															
R-105	X	X	X	X																			
R-106						X			X	X	X	X	X	X	X	X	X	X	X	X			
R-201						X			X	X					X	X	X						
R-203			X			X					X					X							X
R-204			X			X					X					X							X
R-207				X	X	X							X	X		X							
R-209	X	X																					
R-401			X			X					X					X							X
R-403	X				X								X	X	X								
R-603									X	X		X					X		X				
R-604						X			X	X	X	X	X	X	X	X	X	X	X	X			

Table 1, the most important controls that should be applied for the managing, controlling, and implementation of the above-mentioned security aspects are:

- Operational planning and control - [ISO27001] chapter 8.1
- Information access restriction - [ISO27002] control 9.4.1
- Classification of information - [ISO27002] control 8.2.1
- Policy on the use of cryptographic controls - [ISO27002] control 10.1.1

- Information backup - [ISO27002] control 12.3.1
- Event logging - [ISO27002] control 12.4.1
- Development of a cryptographic concept - [BSIGSK] M 2.161
- Selection of a suitable cryptographic procedure - [BSIGSK] M 2.162
- Files and records encryption - [ENISA1] chapter 7.2.3
- Storage encryption - [ENISA1] chapter 7.2.4
- Access control policy - [ENISA2] – chapter 4.1.1.3
- Security of data at rest - [ENISA2] chapter 4.2.3
- Back-ups - [ENISA2] chapter 4.2.5
- Data deletion/disposal - [ENISA2] chapter 4.2.8
- Disaster recovery capabilities - [ENISA3] SO18
- Monitoring and logging - [ENISA3] SO19
- Security of data at rest - [ENISA3] SO23
- Privacy in databases - [ENISA4] chapter 4.5
- Local encrypted storage - [ENISA4] chapter 4.9.2
- Secure remote storage - [ENISA4] chapter 4.9.4
- Stored cryptography verification requirements – [OWASP_ASVS] V6
- File and resources verification requirements - [OWASP_ASVS] V12
- Principle of Least privilege - [OWASP_SDP]chapter 5.3

4.1.3 Practical checklist

The following checklist provides a series of questions and considerations that should be taken into account to ensure secure data storage in data sharing scenarios. These are based on the previously cited requirements as well as the respective recommendations and controls.

Does the storage subsystem provide redundancy against data loss?	
Does the storage subsystem provide redundancy for data availability?	
Is the confidential data encrypted at rest?	
Is all communication with databases and storage subsystem encrypted?	
Is network access of the storage subsystem protected by firewall?	
Is there a defined back-up procedure and solution as part of the security management plan?	
Is authenticated access to the storage subsystem allowed to the smallest number of users?	
Do all storage endpoints and database access endpoints require authenticated access?	
Are vendor-specific storage security mechanisms configured properly?	
Are all default passwords, accounts and configurations removed or updated?	
Is workstation access authenticated?	
Are workstations full-disk encrypted?	
Are all user accounts in the databases accounted for and documented?	
Are maintenance procedures documented as part of the security management plan?	
Do storage maintenance procedures mandate supervised-only access to maintenance personnel?	
Does the storage subsystem provide sufficient security mechanisms?	

Is physical security of the storage subsystem ensured?	
Is access to the storage subsystem monitored?	
Does the storage subsystem allow traceability of changes?	

4.2 Ownership or control over data

As discussed above, part of a common data sharing scenario is to establish the ownership information as well as the authenticity of the shared datasets. This section will present how the generic security aspects can be applied specifically to data ownership, which controls should be taken into account, and what a practical checklist for data ownership should look like.

4.2.1 Security recommendations on ownership or control over data

To ensure a proper data storage security, the responsible practitioners should make certain that the following measures are taken:

- R-105– A full security management plan should include procedures for the proper digital signing of outgoing data, either via the organization's sharing services and portal or via direct exchange of data between individuals. Apart from the signatures, IPR information and any applicable licences should accompany the data whenever necessary. This should be explicitly specified in the security management plan.
- R-303– The data that is made accessible to external entities should contain proper identifiers denoting the ownership, intellectual property rights, and applicable licence. Its authenticity should also be verifiable. This additional information should be added as accompanying metadata and its authenticity and ownership should be attested via digital signatures.
- R-401– Since the exchange of data often takes place directly between individuals (for example via email), the mandatory signing of data should be an explicit part of the organization's security policy and should be followed by the individuals.
- R-601 & R-605– The security policy regarding signing outgoing data and adding applicable licences should be properly documented. The policy should describe the signing procedure and contain an explicit enumeration on the types of data that can be excluded from the procedure. It should also contain the contact details of the responsible individual for licence information and intellectual property rights.
- R-604– There are always categories of data that do not have to follow the security policy. Those exceptions are documented in the policy, and for those exceptions the security mechanisms and procedures are much more relaxed. In general, the level of protection depends on the sensitivity and value of the data.

4.2.2 Applicable Controls

The controls specify the practical measures that should be considered to implement the stated recommendations. Therefore, the controls give specific guidance on what needs to be done and/or considered during the implementation of a recommendation. The appropriate measures can be technical, physical, procedural, or policy-specific.

The following matrix gives an overview of how security controls specified by ISO, ENISA, BSIGSK, OWASP and other external resources apply to the previously mentioned requirements and recommendations. Controls are in the horizontal axis (blue shade) and requirements in the vertical axis (yellow shade).

	ISO27001, 8.1	ISO27001, 7.5	ISO27002, 6.1.5	ISO27002, 8.2.1	ISO27002, 18.1.1	ISO27002, 18.1.2	ENISA1, 5.2.2	ENISA2, 2.3.1	ENISA3, SO26	ENISA4, 4.2	ENISA4, 4.12
R-105	X		X	X				X			
R-303		X		X	X	X			X	X	X
R-401	X		X	X			X				
R-601	X		X	X			X				
R-604	X			X							
R-605	X		X	X			X				

Table 2: Ownership: Relationship between the identified IT-security recommendations and the available controls

As shown in Table 2, the most important controls that should be applied for the managing, controlling, and implementation of the above-mentioned security aspects are:

- Operational planning and control - [ISO27001] chapter 8.1
- Documented information - [ISO27001] chapter 7.5
- Information security in project management - [ISO27002] control 6.1.5
- Classification of information - [ISO27002] control 8.2.1
- Identification of applicable legislation and contractual requirements – [ISO27002] control 18.1.1
- Intellectual property rights - [ISO27002] control 18.1.2
- Personal data breach notification - [ENISA1] chapter 5.2.2
- Security obligations in GDPR - [ENISA2] chapter 2.3.1
- Interoperability and portability - [ENISA3] SO26
- Attribute based credentials - [ENISA4] chapter 4.2
- Intervenability-enhancing techniques - [ENISA4] chapter 4.12

4.2.3 Practical checklist

The following checklist provides a series of questions and considerations that should be taken into account to ensure proper ownership in data sharing scenarios. These are based on the previously cited requirements as well as the respective recommendations and controls.

Do all organization individuals have a digital signature?	
Are all available datasets signed by the owning organization?	

Do all available datasets contain accompanying owner information as well as licence and IPR information?	
Is mandatory data and email signing part of the security policy?	
Are the types of data that are excluded from the mandatory signing explicitly enumerated?	
Are provisions of transferring control over data documented in the licence or accompanying ownership information?	
Is there a defined incident response/data breach procedure?	
Is there an impact assessment for the loss/publication of confidential data?	

4.3 Anonymization

As discussed previously, an important aspect of the shared data protection is anonymization. This section will present how the generic security aspects can be applied specifically to anonymization, which controls should be taken into account, and what a practical checklist for anonymization should look like.

4.3.1 Security recommendations on anonymization

To ensure proper anonymization responsible practitioners should make certain that the following measures are taken:

- R-102 & R-106 & R-604– Depending on the type of data that needs to be anonymized and the usage scenario of this data, there are many anonymization approaches to be considered. An overview of the different approaches, such as tabular data protection, query perturbation, and k-Anonymity, can be found in [ENISA4] chapter 4.6.
- R-203 & R-303– Regardless of the anonymization approach the amount of information an external entity is allowed to access should be kept to the minimum. This applies not only to the access allowed to the datasets but also to the level of aggregation of the data available for processing.
- R-204– There should be preconfigured anonymization rules for each available user role; especially for roles assigned to external individuals. This allows for fine-grained control on the field and property level for each dataset. The rules should be designed following the approach of providing the highest usable level of aggregation by default. Only when explicitly needed, should a user or group have more detailed access to data.
- R-209– The anonymization rules, as well as any dataset specific configuration, should be documented and kept together with the rest of the system documentation for easy reference and audit. The documentation should be kept up to date.
- R-406– Anonymization is one of the important security objectives of an organization intending to share personal or confidential data. Therefore, security audits should include checks on the state of outgoing data by monitoring either the logs (automatic anonymization) or the data itself (manual anonymization).

4.3.2 Applicable Controls

The controls specify practical measures that should be considered to implement the stated recommendations. Therefore, the controls give specific guidance on what needs to be done and/or considered during the implementation of a recommendation. The appropriate measures can be technical, physical, procedural, or policy-specific.

The following matrix gives an overview of how security controls specified by ISO, ENISA, BSIGSK, OWASP and other external resources apply to the previously mentioned requirements and recommendations. The controls are in the horizontal axis (blue shade) and the requirements in the vertical axis (yellow shade).

	ISO27002, 18.1.1	ISO27002, 18.1.4	ENISA2, 2.3.2	ENISA4, 3.2	ENISA4, 4.6	ENISA4, 4.7.1	ENISA4, 5.1	OWASP_ASVS, V6.1
R-102				X	X	X		
R-106				X	X	X		
R-203		X			X		X	X
R-204					X	X		
R-209			X					
R-303		X			X		X	X
R-406	X	X	X					
R-604				X	X	X		

Table 3: Anonymization: Relationship between the identified IT security recommendations and controls

As shown in

	ISO27002, 18.1.1	ISO27002, 18.1.4	ENISA2, 2.3.2	ENISA4, 3.2	ENISA4, 4.6	ENISA4, 4.7.1	ENISA4, 5.1	OWASP_ASVS, V6.1
R-102				X	X	X		
R-106				X	X	X		
R-203		X			X		X	X
R-204					X	X		
R-209			X					
R-303		X			X		X	X
R-406	X	X	X					
R-604				X	X	X		

Table 3, the most important controls that should be applied for the managing, controlling, and implementation of the above-mentioned security aspects are:

- Identification of applicable legislation and contractual requirements - [ISO27002] chapter 18.1.1
- Privacy and protection of personally identifiable information - [ISO27002] chapter 18.1.4
- Security risk management for the processing of personal data - [ENISA2] chapter 2.3.2
- Eight privacy design strategies - [ENISA4] chapter 3.2
- Technologies for respondent privacy: statistical disclosure control - [ENISA4] chapter 4.6
- Privacy-preserving data mining for data-hiding - [ENISA4] chapter 4.7.1
- Limits of privacy by design - [ENISA4] chapter 5.1

- Data classification - [OWASP_ASVS] V6.1

4.3.3 Practical checklist

The following checklist provides a series of questions and considerations that should be taken into account to ensure proper anonymization in data sharing scenarios. These are based on the previously cited requirements as well as on the respective recommendations and controls.

Have datasets that contain personal or confidential data and require anonymization been identified?	
Is there a defined anonymization procedure for each type of data?	
Are there pre-configured anonymization rules for each type of data?	
Are there pre-configured anonymization rules for each user role? (for data requestors)	
Are anonymization rules documented as part of the full security management plan?	
Are checks on the state of outgoing data (in terms of anonymization) part of regular audit plans?	
Do both manual and automatic anonymization procedures follow GDPR regulations?	
Are all publicly available datasets anonymized accordingly?	

4.4 Ethics checks

As discussed previously, sharing personal or derived data comes with an obligation to check that aspects such as personal identity protection, informed consent and controlled access follow the mandated ethical standards. This section will present how the generic security aspects can be applied specifically to ethics checks, which controls should be taken into account, and what a practical checklist for ethics checks should look like.

4.4.1 Security recommendations on ethics checks

To ensure proper ethics checks responsible practitioners should make certain that the following measures are taken:

- R-103 – The identified requirements on ethics need to be clearly specified and documented. Those can be derived from business strategy, regulations, legislations, given contracts, and the current and estimated information security threat environment.
- R-104 – The necessary controls to fulfil the specified ethics requirements need to be implemented. An ongoing control and improvement process must to be put in place.
- R-105 – Ethics checks should be implemented as part of a holistic approach towards IT security (security management plan). IT-security aspects bound to the ethics can only be successfully solved if they are handled as a part of a general IT security approach.
- R-303 & R-304 – Access to provided data and services, especially from outside the system, has to be limited to minimum and be compliant with contracts and rules. Corresponding technical mechanisms (e.g. role-based access control systems etc.) should be implemented and used. In order to minimize the attack surface only relevant sets of features and access rights to necessary information should be given to the users (see also recommendations below).
- R-401 – Underlying regulations (contracts, rules, policies) should be available to and followed by the users. Especially when data is propagated to other countries, general compliance as well as possible export restrictions should be considered.

- R-601 - IT security (including ethical aspects) should be documented and certified (e.g. ISO 27001 or similar). All relevant aspects relating to ethics must be documented and published internally.
- R-604 – Confidential data has to be adequately protected. This means that classification of information has to be carried out and documented. Access to confidential information must be done according to the agreed terms. The implementation of an adequate access control system can be significantly simplified by documented classification of information.
- R-605 – The list of people responsible for the aspects of ethics should be documented and published. In order to clearly define the point of contact for ethics affairs, responsible persons must be designated. Their duties include the support of the conception, the implementation, and the continuous improvement of the aspects of ethics within the IT security, according to the strategic objectives of the security policy.

4.4.2 Applicable Controls

The controls specify practical measures that should be considered to implement the stated recommendations. Therefore, the controls give specific guidance on what needs to be done and/or considered during the implementation of a recommendation. The appropriate measures can be technical, physical, procedural, or policy-specific.

The following matrix gives an overview of how security controls specified by ISO, ENISA, BSIGSK, OWASP and other external resources apply to the previously mentioned requirements and recommendations. The controls are given on the horizontal axis (blue shade) and the requirements on the vertical axis (yellow shade).

	ISO27001, 4.4	ISO27001, 8.1	ISO27001, 7.5	ISO27002, 5.1.1	ISO27002, 5.1.2	ISO27002, 6.1.1	ISO27002, 8.2.1	ISO27002, 9.1.1	ISO27002, 12.1.1	ISO27002, 18.1.1	ISO27002, 18.1.2	ISO27002, 18.2.2	BSIGSK, M 2.503	OWASP_ASVS, V1.8	ENISA2, 4.1.1.1	ENISA2, 4.1.1.2	ENISA2, 4.1.3.1
R-103			X												X		
R-104				X	X				X								
R-105		X										X					
R-303						X	X	X			X		X	X	X	X	
R-304						X		X								X	
R-401										X							
R-601	X												X				
R-604								X						X			X
R-605							X										

Table 4: Ethics Checks: Relationship between the identified IT-security recommendations and controls

As shown in Table 4, the most important controls that should be applied for the managing, controlling, and implementation of the above-mentioned security aspects are:

- Information security management system - [ISO27001] chapter 4.4
- Operational planning and control - [ISO27001] chapter 8.1
- Documented information - [ISO27001] chapter 7.5
- Policies for information security - [ISO27002] control 5.1.1
- Review of the policies for information security - [ISO27002] control 5.1.2
- Information security roles and responsibilities - [ISO27002] control 6.1.1

- Classification of information - [ISO27002] control 8.2.1
- Access control policy - [ISO27002] control 9.1.1
- Documented operating procedures - [ISO27002] control 12.1.1
- Identification of applicable legislation and contractual requirements - [ISO27002] control 18.1.1
- Intellectual property rights - [ISO27002] control 18.1.2
- Independent review of information security - [ISO27002] control 18.2.1
- Compliance with security policies and standards - [ISO27002] control 18.2.2
- Aspects of data protection concept - [BSIGSK] M 2.503
- Data protection and privacy architectural requirements - [OWASP_ASVS] chapter V1.8
- Security policy and procedures for the protection of personal data, [ENISA2] chapter 4.1.1.1
- Roles and responsibilities - [ENISA2] chapter 4.1.1.2
- Confidentiality of personnel - [ENISA2] chapter 4.1.3.1
- Training - [ENISA2] chapter 4.1.3.2

4.4.3 Practical checklist

The following checklist provides a series of questions and considerations that should be taken into account to ensure proper ethics checks in data sharing scenarios. These are based on the previously cited requirements as well as the respective recommendations and controls.

Are current ethic requirements documented as part of the security management plan?	
Have people for ethics checks been appointed and are they known to the entire organization?	
Have ethic requirements undergone an independent review since their last update?	
Is there an “ethics issues” table in place for each project?	
Is there an “ethics review procedure” in place for each type of project?	
Is there an ethics committee or a responsible individual appointed to each project?	
Is there a regular ethics audit for each project?	

4.5 Licensing

As discussed before, having clearly assigned licences for shared data is typically a requirement for data sharing, especially between organizations. This section will present how generic security aspects can be applied specifically to licensing, which controls should be taken into account, and what a practical checklist for licensing should look like.

4.5.1 Security recommendations on licensing

To ensure proper licensing, responsible practitioners should make certain that the following measures are taken:

- R-103 – Terms and conditions of a licence have to be clearly defined. In some cases it is necessary to write a custom licence text, but the recommendation is to use an existing licence text and adapt it accordingly.
- R-104 – Correctness and consistency of the defined licence terms have to be continuously verified and, if needed, adjusted. The suitability of the licence can change, e.g. if some additional third-party data has been acquired and integrated. There could be discrepancies or even contradictions between the previous and the new licences which prohibit the use of the new data without the necessary adjustments to the previous licence.

- R-105 – Handling licensing should be part of the security management plan. As with almost all IT security aspects, handling of licenses must be part of the overall concept of IT security.
- R-208 – Both license terms and security provisions of shared data must be clearly presented to the requestor in an easily accessible manner (e.g. presented on the website and using easy-to-read formats and layout).
- R-401 – Users are required to know and follow the mandated security policies and licence of the processed data.

4.5.2 Applicable Controls

The controls specify practical measures that should be considered to implement the stated recommendations. Therefore, the controls give specific guidance on what needs to be done and/or considered during the implementation of a recommendation. The appropriate measures can be technical, physical, procedural, or policy-specific.

The following matrix gives an overview of how security controls specified by ISO, ENISA, BSIGSK, OWASP and other external resources apply to the previously mentioned requirements and recommendations. The controls are shown on the horizontal axis (blue shade) and the requirements on the vertical axis (yellow shade).

	ISO27002, 5.1.1	ISO27002, 5.1.2	ISO27002, 18.1.1	ISO27002, 18.1.2	ISO27002, 18.1.4	ISO27002, 18.2.1	ISO27002, 18.2.2	BSIGSK, M 1.1	BSIGSK, M 2.205	BSIGSK, M 2.439	BSIGSK, M 2.340	ENISA3, 2.3
R-103	X			X								X
R-104	X			X		X				X		X
R-105		X	X				X					
R-208								X		X		
R-401					X				X		X	

Table 5: Licensing: Relationship between the identified IT-security recommendations and controls

As shown in Table 5, the most important controls that should be applied for the managing, controlling, and implementation of the above-mentioned security aspects are:

- Policies for information security - [ISO27002] control 5.1.1
- Review of the policies for information security - [ISO27002] control 5.1.2
- Identification of applicable legislation and contractual requirements - [ISO27002] control 18.1.1
- Intellectual property rights - [ISO27002] control 18.1.2
- Privacy and protection of personally identifiable information - [ISO27002] control 18.1.4
- Independent review of information security - [ISO27002] control 18.2.1
- Compliance with security policies and standards - [ISO27002] control 18.2.2
- Compliance with relevant standards and regulations - [BSIGSK] M 1.1
- Transmission and retrieval of personal data - [BSIGSK] M 2.205
- Design and organisation of compliance management – [BSIGSK] M 2.439
- Consideration of legal framework conditions – [BSIGSK] M 2.340
- Roles and responsibilities - [ENISA2] chapter 4.1.1.2
- Information security policy - [ENISA3] chapter 2.3

4.5.3 Practical checklist

The following checklist provides a series of questions and considerations that should be taken into account to ensure proper licensing in data sharing scenarios. These are based on the previously cited requirements as well as on the respective recommendations and controls.

Is every dataset accompanied by a licence?	
Does the structure of the dataset licence follow existing established licences?	
Has the correctness of the licences been checked after the last modification of the datasets?	
Have the licences been checked by an independent expert?	
Is handling of the licensing process defined as part of the full security management plan?	
Are licences of combined datasets compatible?	
Do you have permission to share or own all the licenced datasets?	

4.6 Data security

As discussed previously, information security in the context of data sharing is primarily addressed through measures for data security.[12] This section will present how generic security aspects can be applied specifically to data security, which controls should be taken into account, and what a practical checklist for data security should cover.

4.6.1 Security recommendations on data security

To ensure data security, responsible practitioners should ensure that the following measures are taken:

- R-101 – Policies ruling the security mechanisms have to be defined at an early stage in the project, i.e. significant IT-security-aspects should already be considered in the design phase.
- R-102 – The security implementation costs can be controlled by a wise choice of mechanisms and tools. It is recommended to get an overview of the market when planning the implementation of measures. The most advertised solution may not always the best.
- R-103 – The security architecture must be clearly defined. Only a sufficient list of IT security requirements can lead to a successful implementation. A clear IT security policy and security architecture based on these requirements are important milestones along the way.
- R-104 – The implementation of security mechanisms should be exhaustive, controlled permanently, and routinely improved. The successful implementation of the security strategy implies full compliance with the requirements. Sufficient measures must be implemented for each requirement. Only a holistic approach will lead to success. Furthermore, the status of the implementation must be constantly checked, revised and adjusted if necessary. Information can be secured cryptographically on databases or servers, but it is also important to secure the access to the premises.
- R-105 – A holistic approach according to IT security should be the long-term target. The tasks of IT security should not be seen as a one-off hurdle, but represent a continuous process that must be seen as part of a long-term strategy of the project.
- R-106 – A set of necessary security requirements should be defined and used as a base for the security mechanisms to be chosen. It is extremely important that not only all defined requirements of IT security are implemented, but also that no further unnecessary

[12] See section 2.2.7.

mechanisms are introduced. Each new mechanism increases the complexity of the system and expands the potential attack surface.

- R-201 – Already existing protection mechanisms should be reused. Many of the applications used already have some security features. It is recommended to check these functions and if necessary to use them as part of your own security measures. This approach saves money and very often leads to better results because application manufacturers know their own products better and, thus, can often implement security measures more appropriately.
- R-202 – Protection against malware has to be implemented. One of the biggest threats to IT continue to be different types of malware. Use of appropriate anti-virus applications is essential. In order to increase the effectiveness of such tools, it is also recommended to use multiple programs that come from different manufacturers (multi-tool and multi-vendor strategy).
- R-209 – As an important aspect of IT security, the complete documentation of the system must be available. An undocumented system cannot be used. All functions and processing information in the system must be sufficiently documented. The documentation must be made available to the all authorized users. Furthermore, documentation provides the basis for developing, maintaining, and improving an organisation's own IT security.
- R-301 & R-302– An adequate protection of own networks is crucial. Access to own networks must be secured by the use of an appropriate firewall. It is important to change the default settings of the chosen product and to reconfigure them according to the requirements of your own IT security.
- R-306 – The e-mail communication channel has to be monitored, because of the potential to transfer the information as attachment outside of the organisation. E-mail is a channel with a substantial threat potential. It is quite possible that on the one hand through this channel various malware find their way into the system or on the other hand confidential information is transmitted unnoticed from the system to externals. This aspect must be payed adequate attention.
- R-401 – Security policies must be known and followed by everyone. The best IT security will not help if the underlying security policies are not known to everyone and not applied by everyone. Note that this is a continuous process. The knowledge must be continually refreshed, the application of which should be controlled.
- R-402 – Staff should be informed on the handling policy for the personal data. The handling of personal data is an important aspect of IT security. Failure to comply with relevant regulations can result in considerable damage. For this reason, it is important that staff is adequately trained on this issue.
- R-403 – The handling of third-party actors should be clearly defined. The conditions and procedures for dealing with outsiders within your own organization must be defined precisely. In particular, access to certain premises may result in unnoticed access to confidential data stored there.
- R-405 – Emergency contact data for external experts for particular IT security aspect should be defined and communicated. In case of an incident, it is important that the responsible persons can quickly contact the relevant experts and call them for help. In order to make this possible, the experts must be known in advance and their contact details and the associated application procedures must be communicated to staff.
- R-406 – Audits of the implemented IT security (preferably with a certification) should take place regularly. Even the best functioning system has to be constantly checked. In addition to the internal audits, audits by the external experts (auditors) must be carried out in regular

intervals. Preferably, external audits should be completed with a corresponding certification, according to a recognised IT security standard (e.g. [ISO27001]).

- R-407 & R-408 – The handling of detected security breaches has to be specified. In order to be able to respond appropriately to potential incidents and to maintain the defined security objectives in relation to the kept information, the procedures for dealing with the incidents must be defined and communicated to responsible persons.
- R-503 – A strategy for the application of security updates and a corresponding update plan have to be created. In some cases, non-upgraded applications become sources for successful IT infrastructure attacks. Such applications provide attackers with access to active vulnerabilities and allow the use of known exploits. A clear update / upgrade strategy and its consistent application reduce this threat to the necessary minimum.
- R-601 – IT security provisions should be documented and certified (e.g. ISO 27001 or similar). A security certificate according to an established international standard generally increases the maturity of the implemented IT security and is therefore strongly recommended.
- R-604 – Personal or confidential data has to be sufficiently protected. Violations of these rules will usually cause damage, both in monetary terms and in reputation.
- R-605 – Responsibilities for particular tasks have to be defined and assigned. The core of the security policy is a clear allocation of responsibilities. The security team must react quickly and actively to occurred incidents and initiate effective countermeasures. In such cases, it must be clear who is responsible for which part of the measures to be implemented.
- R-606 – IT security has to be controlled and improved (ISMS[13]) on an ongoing basis. Only a steadily maintained approach can permanently improve IT security. In this sense, it is necessary to continuously review and improve the implemented IT security system. In particular, regular audits by external auditors contribute to such improvement through their impartiality.

4.6.2 Applicable Controls

Controls specify the practical measures that should be considered to implement the stated recommendations. Therefore, the controls give specific guidance on what needs to be done and/or considered during the implementation of a recommendation. The appropriate measures can be technical, physical, procedural, or policy-specific.

The following matrix gives an overview of how security controls specified by ISO, ENISA, BSIGSK, OWASP and other external resources apply to the previously mentioned requirements and recommendations. Controls are in the horizontal (blue shade) and requirements in the vertical (yellow shade).

[13] ISMS – Information Security Management System

Table 6: Data security: Relationship between the identified IT-security recommendations and controls

As shown in Table 7, the most important controls that should be applied for the managing, controlling, and implementation of the above-mentioned security aspects are:

- Information security management system - [ISO27001] chapter 4.4
- Operational planning and control - [ISO27001] chapter 8.1
- Documented information - [ISO27001] chapter 7.5
- Policies for information security - [ISO27002] control 5.1.1
- Review of the policies for information security - [ISO27002] control 5.1.2
- Information security roles and responsibilities - [ISO27002] control 6.1.1
- Information security in project management - [ISO27002] control 6.1.5
- Information security awareness, education and training - [ISO27002] control 7.2.2
- Disciplinary process - [ISO27002] control 7.2.3
- Classification of information - [ISO27002] control 8.2.1
- Policy on the use of cryptographic controls - [ISO27002] control 10.1.1
- Physical security perimeter - [ISO27002] control 11.1.1
- Working in secure areas - [ISO27002] control 11.1.5
- Documented operating procedures - [ISO27002] control 12.1.1
- Controls against malware - [ISO27002] control 12.2.1
- Information backup - [ISO27002] control 12.3.1
- Event logging - [ISO27002] control 12.4.1
- Installation of software on operational systems - [ISO27002] control 12.5.1
- Information systems audit controls - [ISO27002] control 12.7.1
- Security of network services – [ISO27002] control 13.1.2
- Information transfer policies and procedures - [ISO27002] control 13.2.1
- Responsibilities and procedures (with regard to information security incident management) - [ISO27002] control 16.1.1
- Planning information security continuity - [ISO27002] control 17.1.1

- Identification of applicable legislation and contractual requirements – [ISO27002] control 18.1.1
- Intellectual property rights - [ISO27002] control 18.1.2
- Compliance with security policies and standards - [ISO27002] control 18.2.2
- Aspects of a data protection concept - [BSIGSK] M 2.503
- Development of a cryptographic concept - [BSIGSK] M 2.161
- Selection of a suitable cryptographic procedure - [BSIGSK] M 2.162
- Data protection and privacy architectural requirements - [OWASP_ASVS] chapter V1.8
- Communications architectural requirements - [OWASP_ASVS] chapter V1.9
- Malicious software architectural requirements - [OWASP_ASVS] chapter V1.10
- Minimize attack surface area - [OWASP_SDP] chapter 5.1
- Principle of Least privilege - [OWASP_SDP] chapter 5.3
- Security policy and procedures for the protection of personal data, [ENISA2] chapter 4.1.1.1
- Roles and responsibilities - [ENISA2] chapter 4.1.1.2
- Access control policy - [ENISA2] – chapter 4.1.1.3
- Confidentiality of personnel - [ENISA2] chapter 4.1.3.1
- Training - [ENISA2] chapter 4.1.3.2
- Access control and authentication - [ENISA2] chapter 4.2.1
- Information security policy - [ENISA3] SO 01
- Third party management - [ENISA3] SO 04
- Access control to network and information systems - [ENISA3] SO 10
- Asset management - [ENISA3] SO 14
- Monitoring and logging - [ENISA3] SO 19
- Compliance - [ENISA3] SO 22

4.6.3 Practical checklist

The following checklist provides a series of questions and considerations that should be considered to ensure data security in data sharing scenarios. These are based on the previously cited requirements as well as respective recommendations and controls.

Is someone assigned the responsibility for data security?	
Have employees received training on basic information security?	
Is there an established IT security policy?	
Do assigned department technical administrators with clear roles and responsibilities exist?	
Do established reporting protocols for indications of security breaches exist?	
Do established email handling protocols and guidelines exist?	
Does the organization provide digital IDs for email encryption and signing?	
Has the organization established back-up protocols?	
Is physical access to computer hosts protected?	
Is vision to computer hosts screens restricted from people passing by?	
Are computer hosts password protected?	
Are there established procedures for wiping data from computer hosts prior to disposal?	

Is there an established password policy?	
Are there automatic security updates on computer hosts and servers?	
Is there a regular auditing procedure of logs and indicators of compromise (IOC)?	
Are there physical access restrictions on the servers?	
Is remote access to internal services secured via VPN?	

4.7 Discoverability

As previously discussed, in order to share data, it has to be discoverable (visibility and metadata) and understood (availability in terms of formats). This section will present how the generic security aspects can be applied specifically to discoverability, which controls should be taken into account, and what a practical checklist for discoverability should look like.

4.7.1 Security recommendations on data discoverability

To ensure that data is both discoverable and secure, responsible practitioners should ensure that the following measures are taken:

- R-104 – Appropriate metadata and data format standards have to be used. The information can only be used if it has been adequately described and if it can be readily represented. In both cases, the successful fulfilment of the requirements addressed above is related to the formats used. The used formats of the so-called metadata (description) as well as the visualization must correspond to the accepted international standards as accurately as possible (cf. also section **Fehler! Verweisquelle konnte nicht gefunden werden.**).
- R-106 – Security mechanisms that ensure authenticity and integrity of data should be implemented. Mechanisms must be implemented that reliably assure integrity and authenticity of the electronic information available. The use of electronic signatures and seals is one option to achieve such assurance.
- R-303 – Only data released for the search (especially without privacy violations) should be accessible. Requirements of data protection must be respected. In particular for research purposes, data must be prepared accordingly, e.g. personal data must be removed or rendered illegible (cf. section 4.3).
- R-304 – Only search function should provide less restricted (even perhaps unrestricted) access. The search function as the first step in finding the appropriate information must be provided to the user on a (more or less) free basis. The next step (information access) should be realized according to the conditions of use for the wanted information. Free access should be kept to a minimum and applied only to absolutely necessary functions.
- R-401 – Policies for the preparation of searchable subsets of data have to be followed. The pursued strategy of how to prepare the database must be filed as part of the security policy. The approach followed must be documented in detail and this documentation must always be available to staff. The correct application of the approach must be monitored and regularly reviewed.

4.7.2 Applicable Controls

Controls specify the practical measures that should be considered to implement the stated recommendations. Therefore, the controls give specific guidance on what needs to be done and/or considered during the implementation of a recommendation. The appropriate measures can be technical, physical, procedural, or policy-specific.

The following matrix gives an overview of how security controls specified by ISO, ENISA, BSIGSK, OWASP and other external resources apply to the previously mentioned requirements and recommendations. Controls are in the horizontal (blue shade) and requirements in the vertical (yellow shade).

	ISO27002, 8.2.1	ISO27002, 8.2.2	ISO27002, 9.2.3	ISO27002, 9.4.1	ISO27002, 9.4.2	ISO27002, 10.1.1	ISO27002, 13.1.2	ISO27002, 13.2.1	ISO27002, 13.2.2	ISO27002, 13.2.4	ISO27002, 18.1.2	ISO27002, 18.2.2	BSIGSK, M 2.393	BSIGSK, M 2.504	BSIGSK, M 2.505	BSIGSK, M 2.506	BSIGSK, M 2.162	OWASP_ASVS, V1.5	ENISA3, SO 22
R-104	x	x																	
R-106			x	x	x	x						x					x	x	
R-303	x			x	x			x	x	x									
R-304				x			x	x										x	
R-401											x		x	x	x	x			x

Table 7: Discoverability: Relationship between the identified IT-security recommendations and controls

As detailed in table 4, the most important controls that should be applied for the managing, controlling, and implementation of the above-mentioned security aspects are:

- Classification of information - [ISO27002] control 8.2.1
- Labelling of information - [ISO27002] control 8.2.2
- User access provisioning - [ISO27002] control 9.2.3
- Information access restriction - [ISO27002] control 9.4.1
- Secure log-on procedures - [ISO27002] control 9.4.2
- Policy on the use of cryptographic controls - [ISO27002] control 10.1.1
- Security of network services - [ISO27002] control 13.1.2
- Information transfer policies and procedures - [ISO27002] control 13.2.1
- Agreements on information transfer - [ISO27002] control 13.2.2
- Confidentiality or non-disclosure agreements - [ISO27002] control 13.2.4
- Intellectual property rights - [ISO27002] control 18.1.2
- Compliance with security policies and standards - [ISO27002] control 18.2.2
- Regulations concerning information exchange - [BSIGSK] M 2.393
- Checking the legal framework and prior checking before processing personal data - [BSIGSK] M 2.504
- Definition of technical/organisational safeguards according to the state-of-the-art for processing of personal data - [BSIGSK] M 2.505
- Obligation/briefing of staff members for the processing of personal data – [BSIGSK] M 2.506
- Selection of a suitable cryptographic procedure - [BSIGSK] M 2.162
- Input and output architectural requirements - [OWASP_ASVS] chapter V1.5
- Compliance - [ENISA3] SO 22

4.7.3 Practical checklist

The following checklist provides a series of questions and considerations that should be taken into account to ensure data discoverability and security in data sharing scenarios. These are based on the previously cited requirements as well as respective recommendations and controls.

Do all published data include relevant metadata?	
Are metadata following an established format (like DCAT)?	
Is access to datasets granted via an authentication/authorization mechanism?	
Are all relevant data searchable via queries?	
Are search endpoints protected against abuse? (e.g. denial of service attacks)	
Are all databases protected against direct access?	
Is publicly accessible data indexed by established search engines? (e.g. Google)	
Are all API endpoints, including search functions, encrypted?	

4.8 Data access

As previously discussed, inadequate access control policies can violate the access rules as defined by the licence and restricted by the informed consent, which in turn could lead to penalties for non-compliance. This section will present how the generic security aspects can be applied specifically to access control, which controls should be taken into account, and what a practical checklist for access control should look like.

4.8.1 Security recommendations on data access

To ensure that data is both accessible and secure, responsible practitioners should ensure that the following measures are taken:

- R-101 – The data access policy should be defined in the early phases of the project (in particular while developing the rules for the sharing of collected data). Similarly, the aspect of regulated data access must already be documented at an early stage in the security policy. According to the classification of the offered data, corresponding access protection mechanisms must also be anticipated.
- R-104 – Relevant controls must be implemented (either by the owner of the shareable data or by the service provider, e.g. the sharing portal). All controls addressed in the context of the IT security concept must also be implemented. Only a full implementation of measures guarantees adequate achievement of postulated security goals and ensures a sufficiently operational access protection of information.
- R-105 – A holistic approach for security management should be designed and implemented. Even in the context of data access, its successful deployment is strongly dependent on the holistic approach to IT security. Implementation of only parts of the underlying security concept may result in one-off improvements, but will not be effective as they are likely to ignore the weak points in other areas of the overall system. The best implementation of login and access control will be useless if, for example, no firewalls are used and access controls can be bypassed.
- R-201 – Synergy effects should be considered. The access control mechanisms that are already offered by the products used can very often be retained. Reimplementing existing technology is rarely desirable. Especially complex access control mechanisms can be effectively designed and implemented by the manufacturers of such systems / products due to their extensive knowledge of the products and their underlying logics.
- R-203 – Appropriate concepts for access control have to be in place. Regardless of the implementation, the design of access control mechanisms must be completed and documented. The requirement to use such a system must be included in the security policy.

- R-204 – Especially the treatment of privileged users should be controlled and managed. Dealing with privileged users poses a particular challenge in any system. Especially with the use of personal information, this aspect is of increased importance. This needs to be included in the security policy and a corresponding plan must be drawn up.
- R-205 – Access rights of privileged users should be limited to the required minimum. Due to the fact that damages done by privileged users will generally be greater, this aspect deserves increased attention. In general, it is important to ensure that no accumulation of access rights in the case of such users can occur. The fine-grained design of appropriate roles and implementation of additional mechanisms (for example, following the four eyes principle) can help.
- R-207 – Default accounts and users should be reconfigured. There have been successful cyberattacks based on the use of default user accounts or configuration by the manufacturers. These settings must be changed before the system is taken into operation. In particular, standard administrator accounts represent a considerable threat.
- R-303 – Only necessary data should be provided for access from outside of the system. According to the minimum principle, only data necessary for the fulfilment of the preliminary task should be made available. Providing additional data doesn't help accomplishing the task but instead increases the risk that may result in breach of relevant security objectives and, thus, cause damage. Only necessary applications/services should be provided for access from outside of the system
- R-401 – The security policy, especially data access policy, should be well-known to all relevant users. The need for an implementation of adequate access control mechanism must be included in the security policy.
- R-403- Access of third-party staff to systems holding confidential data has to be regulated and limited to a minimum. Dealing with outsiders who have access to the protected premises must be clearly regulated. Measures must be developed and implemented which do not result in compromised protected information resulting from such access.
- R-404 – Regular training on security aspects of the staff has to be implemented. Staff must be continuously trained in the relevant aspects of IT security in general and access control in particular. Changes to the concepts and mechanisms must be communicated immediately. Confirmation of the knowledge transfer is recommended.
- R-501 – Necessary updates, especially security updates, should be installed immediately. As in the case of any technical system, access control systems must be continuously maintained. All necessary updates / upgrades (especially security-related) must be installed promptly. To control the correct execution of related activities, a responsible person must be named. The designation must be announced.
- R-602 – An appropriate password policy has to be established. Suitability of the passwords used determines the suitability of the underlying sign-on mechanism and, in part, the access control system. For this reason, it is important that correct handling of passwords is defined in the corresponding policy and that this policy is made available to both personnel and users. Measures should be implemented which automatically monitor compliance with the policy and, thus, rule out their violation as much as possible.
- R-606 –Implemented security mechanisms have to be audited and improved on a regular basis. Mechanisms for access control (like the other security aspects) should be checked by external experts through regular audits. This is necessary to fully meet the requirement for continuous maintenance of the specified mechanisms. The objectivity of the external auditors can help enormously in finding the uncovered security risks.

4.8.2 Applicable Controls

Controls specify the practical measures that should be considered to implement the stated recommendations. Therefore, the controls give specific guidance on what needs to be done and/or considered during the implementation of a recommendation. The appropriate measures can be technical, physical, procedural, or policy-specific.

The following matrix gives an overview of how security controls specified by ISO, ENISA, BSIGSK, OWASP and other external resources apply to the previously mentioned requirements and recommendations. Controls are in the horizontal (blue shade) and requirements in the vertical (yellow shade).

	ISO27002, 5.1.1	ISO27002, 5.1.2	ISO27002, 9.1.1	ISO27002, 9.2.1	ISO27002, 9.2.2	ISO27002, 9.2.3	ISO27002, 9.2.4	ISO27002, 9.3.1	ISO27002, 9.4.1	ISO27002, 9.4.2	ISO27002, 9.4.3	BSIGSK, M 2.503	BSIGSK, M 2.505	BSIGSK, M 2.11	BSIGSK, M 2.220	BSIGSK, M 4.133	BSIGSK, M 4.498	BSIGSK, M 1.1	BSIGSK, M 4.1	BSIGSK, M 4.7	BSIGSK, M 4.30	BSIGSK, M 2.31	BSIGSK, M 2.161	OWASP_ASVS, V1.4
R-101	X		X															X						X
R-104																		X						
R-105	X	X																	X				X	
R-201																					X			
R-203			X													X								X
R-204				X	X	X																X		
R-205				X	X	X																X		
R-207							X				X					X				X				
R-303			X	X					X			X	X					X						
R-304			X	X					X															X
R-401															X							X		
R-403													X					X						
R-404	X	X											X											
R-501																								X
R-602								X		X	X			X			X		X				X	
R-606		X																						

Table 8: Data access: Relationship between the identified IT-security recommendations and controls

As shown in table 5, the most important controls that should be applied for the managing, controlling, and implementation of the above-mentioned security aspects are:

- Policies for information security - [ISO27002] control 5.1.1
- Review of the policies for information security - [ISO27002] control 5.1.2
- Access control policy - [ISO27002] control 9.1.1
- User registration and de-registration - [ISO27002] control 9.2.1
- User access provisioning - [ISO27002] control 9.2.2
- Management of privileged access rights - [ISO27002] control 9.2.3
- Management of secret authentication information of users - [ISO27002] control 9.2.4
- Use of secret authentication information - [ISO27002] control 9.3.1
- Information access restriction - [ISO27002] control 9.4.1

- Secure log-on procedures - [ISO27002] control 9.4.2
- Password management system - [ISO27002] control 9.4.3
- Aspects of a data protection concept- [BSIGSK] M 2.503
- Definition of technical/organisational safeguards according to the state-of-the-art for processing of personal data - [BSIGSK] M 2.505
- Provisions governing the use of passwords - [BSIGSK] M 2.11
- Guidelines for access control - [BSIGSK] M 2.220
- Appropriate choice of authentication mechanisms - [BSIGSK] M 4.133
- Secure use of single sign-on - [BSIGSK] M4.498
- Compliance with relevant standards and regulations - [BSIGSK] M 1.1
- Password protection for IT systems - [BSIGSK] M 4.1
- Change of pre-set passwords - [BSIGSK] M 4.7
- Utilisation of the security functions offered in application programs - [BSIGSK] M 4.30
- Documentation of authorised users and rights profiles - [BSIGSK] M 2.31
- Development of a cryptographic concept - [BSIGSK] M 2.161
- Access control architectural requirements - [OWASP_ASVS] chapter V1.4

4.8.3 Practical checklist

The following checklist provides a series of questions and considerations that should be considered to ensure access control in data sharing scenarios. These are based on the previously cited requirements as well as respective recommendations and controls.

Has an access control policy been established as part of the IT security policy of the organization?	
Is every user account tied positively to an authorized individual?	
Is every user authorized to only access information that is required for their work duties?	
Are all non-public files only accessible via authentication/authorization mechanism?	
Is there an established audit log mechanism?	
Have employees been trained on secure handling of personal or confidential data?	
Are all databases protected by a firewall and not directly accessible from the internet?	
Do all API endpoints require authentication?	
Is the authentication/authorization mechanism up to date and secured?	
Have regular external audits and penetration tests been established?	
Are all vendor remote maintenance connections documented and secured?	
Is remote file sharing and printing disabled?	

5 Glossary

Access control	Means to ensure that access to assets is authorized and restricted based on business and security *requirements.*
Audit	Systematic, independent and documented *process* for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled.
Authenticity	Electronic data is authentic if it corresponds to the original data and the identity of an issuer (author, creator and/or sender) can be assigned to it without any doubt.
Availability	Availability refers to the ability of a user to access information or resources in a specified location and in the correct format.
Confidential data	Confidential data are data given in confidence or data agreed to be kept confidential, i.e. secret, between two parties, which are not in the public domain such as information on business operations, income, health, medical details, or political opinions and voting behaviour.
Confidentiality	Confidentiality allows authorized users to access protected data. Specific mechanisms ensure confidentiality and safeguard data from harmful intruders.
Firewall	A firewall is a hardware or software system that monitors the connection between networks and, in particular, averts attacks on the network (intranet) from the Internet. Options start with simple, sometimes free of charge computer programs ("personal firewalls") that generally only protect the computer on which they are installed. On large networks complex firewall systems that consist of several hardware and software components are used.
Integrity	Integrity refers to methods to ensure that data is real, accurate, and safeguarded from unauthorized user modification.
Measures	The management, operational, and technical controls (safeguards or countermeasures) prescribed for an information system and the security controls in place or planned to meet those requirements (also see security controls).
Personal data	According to article 4 [GDPR]: “personal data” means any information relating to an identified or identifiable natural person (“data subject”); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Privacy by design	An approach to systems engineering, initially developed by Ann Cavoukian and formalized in a joint report on privacy-enhancing technologies by a team of the Information and Privacy Commissioner of Ontario (Canada), the Dutch Data Protection Authority and the Netherlands Organisation for Applied Scientific Research in 1995. The framework was published in 2009 and adopted by the International Assembly of Privacy Commissioners and Data Protection Authorities in 2010. Privacy by design calls for privacy to be taken into account throughout the entire engineering process. The concept is an example of value sensitive design, i.e. to take human values into account in a well-defined manner throughout the whole process.
Security by design	When software is fundamentally designed to be secure this is called “security by design”. In this approach, security is built in the system from the ground up and with a robust architecture design. Security architectural design decisions are often based on well-known security tactics and patterns defined as reusable techniques for achieving specific quality levels.

6 Bibliography

[BDSG]	German Bundesdatenschutzgesetz (BDSG) is a federal data protection act, 30.07.2017, https://www.gesetze-im-internet.de/englisch_bdsg/index.html
[ENISA1]	Reinforcing trust and security in the area of electronic communications and online services: Sketching the notion of "state-of-the-art" for SMEs in security of personal data processing, ENISA, 2018, https://www.enisa.europa.eu/publications/reinforcing-trust-and-security-in-the-area-of-electronic-communications-and-online-services
[ENISA2]	Guidelines for SMEs on the security of personal data processing, ENISA, 2017, https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing
[ENISA3]	Technical Guidelines for the implementation of minimum security measures for Digital Service Providers, ENISA, 2017, https://www.enisa.europa.eu/publications/minimum-security-measures-for-digital-service-providers
[ENISA4]	Privacy and Data Protection by Design, ENISA, 2015, https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design
[GDPR]	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 4.5.2016, http://data.europa.eu/eli/reg/2016/679/oj
[ISO15836-1]	ISO 15836-1:2017. Information and documentation — The Dublin Core metadata element set — Part 1: Core elements, ISO, 2017
[ISO27001]	ISO/IEC 21001:2013 Information technology - Security Techniques - Information security management systems — Requirements, ISO, 2013
[ISO27002]	ISO/IEC 27002:2013 Code of practice for information security controls, ISO, 2013
[OWASP_ASVS]	OWASP: Application Security Verification Standard 4.0, March 2019, https://github.com/OWASP/ASVS/raw/master/4.0/OWASP%20Application%20Security%20Verification%20Standard%204.0-en.pdf
[OWASP_SDP]	OWASP: Security by Design Principles https://www.owasp.org/index.php/Security_by_Design_Principles
[HIC2016]	Password Guidance https://www.microsoft.com/en-us/research/publication/password-guidance/
[NIST800-35]	NIST Special Publication 800-35, "Guide to Information Technology Security Services" https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-35.pdf
[BSIGSK]	IT-Grundschutz-Catalogues, BSI, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/International/GSK_15_EL_EN_Draft.pdf?__blob=publicationFile&v=2
[eIDAS]	The Regulation (EU) N°910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation)

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG

[DCAT-AP] The DCAT Application Profile for data portals in Europe (DCAT-AP) https://joinup.ec.europa.eu/solution/dcat-application-profile-data-portals-europe