INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS) AND HANDLING OF PERSONAL DATA

White paper ISMS (ISO/IEC 27001) and GDPR

INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS) AND HANDLING OF PERSONAL DATA

White paper ISMS (ISO/IEC 27001) and GDPR

Veriscan
Publishing date: 2017-01-28
Minor language update: 2019-04-26
Update on standards: 2017-09-15, v1.1.0 (Annex B etc.)
Publisher: Veriscan Security AB
Document ID: White paper
Version 1.1.0
Information class: Public

Table of content

Notes

ABOUT
This white paper is written with a background in the work conducted within ISO/IEC JTC1/SC27 and practical interpretations of an ISMS and privacy. It is intended as supportive information for anyone that has an ISMS according to ISO/IEC 27001:2013 and faces GDPR regulations.

This white paper shall not be used as any reference for fulfilment of either the ISO/IEC 27001 requirements and/or the GDPR. For this purpose the original standards and the GDPR applies.

It is anticipated that the reader has a good knowledge of ISO/IEC 27001 and its requirements and usage as well as a general understanding of GDPR.

Veriscan has been part of the standardization work within ISO SC27 since 2004 and are working with information security in Sweden as well as other countries. This paper is not written for the situation in Sweden but is intended as a general approach.

Please note that standards use the term privacy and GDPR use the term personal data protection and this white paper uses both terms depending on context.

ABSTRACT
This white paper presents a five layer principle on how to use ISO/IEC 27001 (ISMS) when addressing GDPR.
For organizations that have an ISMS in place, the GDPR requirements and intentions can be handled within an ISMS with a few additions/adaptations. These additions/adaptations are mainly to do with scoping of the processes and adaptation or adding specific controls. This is explained by the five layers and there are a number of Annexes that go a bit deeper. The Annexes especially provide information on what aspects that should be considered in order to extend information security to privacy data protection as well as controls. By using an ISMS for addressing GDPR efforts, resources can be saved compared to handling GDPR as a separate process.

CONTRIBUTORS
This white paper is written by Veriscan Security AB.
Further contributions were made by Rune Ask Veriscan Security Norway and Jeremy Evans Veriscan Security UK.
A special thanks to Raquel Porciúncula Ozona Consulting, co- editor of ISO/IEC 27003 first revision, for her support, reflections and inputs.

1 Information Security Management System and the handling of personal data

1.1 Introduction

The starting question of this white paper is:

"Can an information security management system (ISMS) ISO/IEC 27001 support the handling of personal data according to the new EU general data protection regulation (GDPR)?"

In principle if the ISMS is well-functioning - the answer should be "yes" to the above question. However not all ISMS implementations are done in such a way that the answer "yes" is obvious. Even if the ISMS is well-functioning there are some things to consider. This white paper will try to answer the question from the basis that an ISMS should be well-functioning and consider the requirements of ISO/IEC 27001:2013 including Annex A. It is intended to be applicable either to organizations that have an ISMS or who are implementing one.

This paper will be in general terms and is intended to be used by any of our clients or partners regardless if they use Veriscan services or tools.

There will also be another white paper presenting Veriscan's view of how to solve the GDPR and privacy data issue based upon Veriscan solutions and tools.

1.2 GDPR principle content

Let's start with the privacy bit and then in particular what GDPR says regarding personal data protection. In Article 32 it is stated that "the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

- The pseudonymisation and encryption of personal data;
- The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- A process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing."

Out of these four bullet points it is evident that both the concept of evaluating and continually improving the information security management system as per the basic purpose of ISO/IEC 27001 as well as the core information security aspects, (confidentiality, integrity, availability), support the GDPR requirements in general terms.

Further in article 5 the principles of GDPR are as follows:

"Principles relating to processing of personal data

1. Personal data shall be:
    a. processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');
    b. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');
    c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
    d. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');
    e. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organizational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');
    f. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures ('integrity and confidentiality').
2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')." Source: Regulation (EU) 2016/679

These principles are interesting to note particularly in relation to an ISMS, as GDPR lays down similar and in some cases different aspects that have to be considered in comparison to traditional information security aspects. These will be discussed more in detail later but principally the following should be highlighted and should be addressed within an ISMS as required:

- Basic definition is that information is an interpretation of data. Personal data is then part of information. Information security should subsequently cover personal data which should be the general and basic approach.
- Item 1 a) states that the laws have to be applied which is part of the requirements of an ISMS (ISO/IEC 27001 Clause 4)
- Items 1 b) and 1 c) are not directly information security requirements or requirements in ISO/IEC 27001
- Item 1 d) has its origin as an information security aspect
- Item 1 e) is pointing out a specific requirement that an ISMS should cover by applying sufficient organizational and technical controls
- Item 1 f) is definitely an information security requirement
- Item 2 is a requirement that should be identified and handled by an ISMS

Regarding GDPR it should be noted that EU regards these principles as requirements and violating them will increase the likelihood of being non-compliant.

“The data protection reform will strengthen citizens' rights and build trust. The new rules address these concerns through:

- A "right to be forgotten": When an individual no longer wants her/his data to be processed, and provided that there are no legitimate grounds for retaining it, the data will be deleted. This is about protecting the privacy of individuals, not about erasing past events or restricting freedom of the press.

- Easier access to one's data: Individuals will have more information on how their data is processed and this information should be available in a clear and understandable way. A right to data portability will make it easier for individuals to transfer personal data between service providers.

- The right to know when one's data has been hacked (note: it is not the data as such that is hacked but the “system” and data can then be disclosed): Companies and organizations must notify the national supervisory authority of data breaches which put individuals at risk and communicate to the data subject all high risk breaches as soon as possible so that users can take appropriate measures.

- Data protection by design and by default: ‘Data protection by design’ and ‘Data protection by default’ are now essential elements in EU data protection rules. Data protection safeguards will be built into products and services from the earliest stage of development, and privacy-friendly default settings will be the norm – for example on social networks or mobile apps.”

Source: http://europa.eu/rapid/press-release_MEMO-15-6385_en.htm

Figure 1 gives a quick overview of GDPR with the main issues.

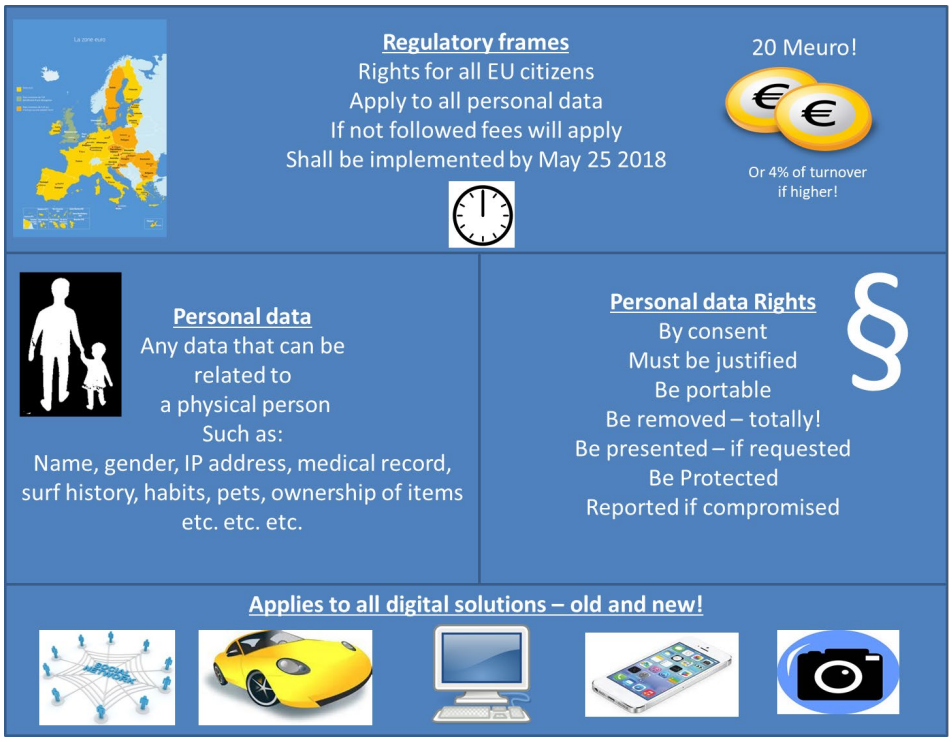

Figure 1 shows an overview of the main GDPR content (source Veriscan)

1.3 High level conclusion on ISMS and GDPR

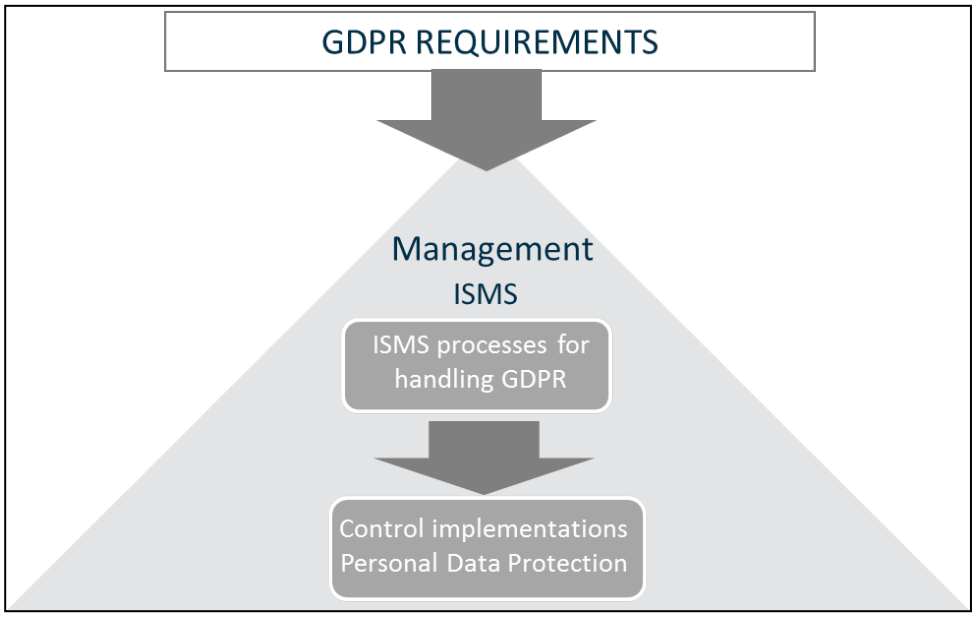

Figure 2 shows the organization view that GDPR is a new regulation that an ISMS should address (source Veriscan)

The organization faces a new regulation in the form of GDPR. Management realises that this is a concern for the organization that must be addressed. As GDPR is about data protection a judgement can be made by the management that this issue must relate to information security and that the ISMS implemented should be able to support the organization to handle GDPR. The basis for this judgement is shown in principle in the figure above.

But "why" this judgement can be made may still be the question and the following is the main arguments:

- An ISMS is supportive of protecting personal data if its implementation covers the aspects stated in GDPR.
- Many of the security controls in ISO/IEC 27001 Annex A and subsequently ISO/IEC 27002 can be directly used. (Note there are other controls that can be added from other standardisation work; see e.g. Annex B in this white paper.)

Many of the ISMS processes can be used for the requirements in GDPR such as the processes for information security risk management, auditing, measurements, incidents and non-conformities.

But if there seems to be so much similarity between an ISMS and GDPR - why write this paper?

- There are three main reasons:
  - Top management of any organization may not know or realize that an ISMS can be used to solve GDPR requirements – they are not subject matter experts.
  - The idea that an ISMS also can be used to support the handling of personal data needs to be explained to those not familiar with an ISMS.
  - An ISMS has to be partly adopted to cover protection of personal data and those who work with or manage an ISMS have to know that.

So an ISMS which incorporates personal data as defined by GDPR should manage the risk and mitigating controls to that personal data without the need for an additional similar information protection process just for GDPR.

The rest of this paper provides more specific information as well as information on ISO standard development to support the work within the organization using the ISMS to handle GDPR, see a simplified view in the figure below.

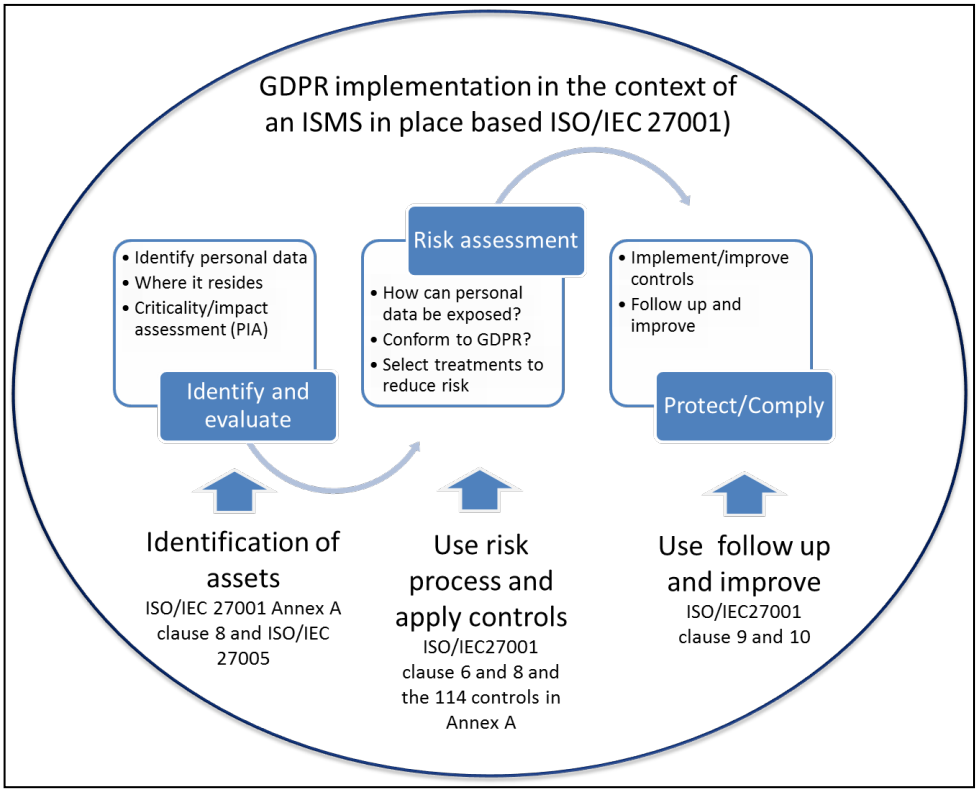

Figure 3 shows the principle linkage of ISO/IEC 27001 for GDPR (source Veriscan)

There is much knowledge to gain from standardisation efforts to support an organization to resolve GDPR issues, even if there is not just "one privacy" standard to use. ISO/IEC 27001 (ISMS) is the starting point and then other standards will be utilized as they apply to the organization. This white paper will continue to make references to standards with the priority of those published or to be published within 6 months (FDIS stage).

It should also be mentioned that the basis for much of the work on information security by organizations is ISO/IEC 27002 on controls (and indirectly ISO/IEC 27001 Annex A). To use the ISMS processes and controls is the basic starting point to link using the ISMS to handle personal data in general terms and personal data protection from a management point of view.

Annex B describes how ISO/JTC1/SC27 works with standardisation in relation to privacy and the linkage to ISO/IEC 27001. This information might be useful when considering GDPR and supporting the ISMS from a general standard view.

Furthermore, Annex A provides definitions of information and privacy aspects in order to review similarities and differences in more detail. The Annexes C, D and E in this white paper contain a more detailed evaluation about the privacy aspects and characteristics, indicating if and how they can be addressed from an information security approach or not as well as in the control perspective more generally.

2 Factors in a well-functioning ISMS supports handling of personal data

2.1 Defining the structure

Even if a general judgement is made that an ISMS can address GDPR concerns, as described earlier, there are still issues to handle in order to make this work. In principle there are five layers of an ISMS that need to be adapted to cover privacy and GDPR.

1) The ISMS as whole as described in clauses 4-10 in the standard ISO/IEC 27001
2) The specific processes used in an ISMS. These can be used addressing GDPR as well but then have to incorporate GDPR as part of the requirements of an ISMS
3) Which of the 114 controls in Annex A that are relevant for GDPR as well
4) Adjustment of some of the 114 controls to address GDPR requirements
5) Additional controls to the 114 to address specific GDPR requirements

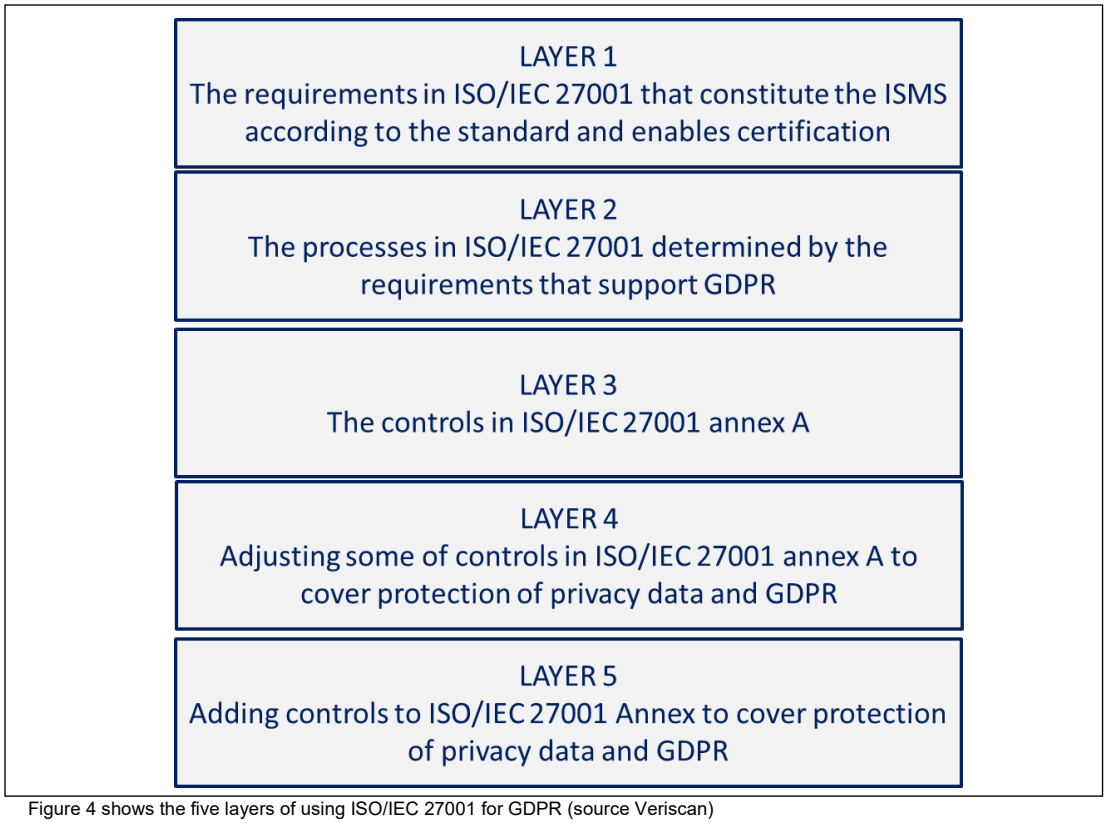

Figure 4 shows the five layers of using ISO/IEC 27001 for GDPR (source Veriscan)

2.2 Layer 1 – Clause 4-10 and how they can be used for GDPR

2.2.1 Layer 1 - Overview

There are a number of ISMS items in ISO/IEC 27001 that indirectly or directly support personal data protection according to GDPR. These are in particular:

1) The context set according to clause 4.1 and 4.2
    a. The business purpose and structure should give the purpose of handling personal data for the organization and should include the interested parties.
    b. The EU directive (GDPR) is part of the external context as this is a regulation that the organization has to consider for its ISMS. This can be seen as a new regulation if not included already. (Note: There might be existing national laws for privacy.)
2) Leadership and responsibilities should ensure responsibility and involvement according to clause 5
    a. Enables the distinction between information security responsibilities and privacy responsibilities within the organization.
    b. The need for top management commitment regarding the protection of personal data is evident as the financial and reputational risk of non-compliance is substantial
3) Planning as set forth in clause 6.1 is very much about risk and controls.
    a. Risk assessment for information security should cover privacy information
    b. Control selection is already there as part of the protection
    c. Identification is part of the controls in Annex A clause 8
4) The resource allocated in clause 7 that balances the risks etc. is applicable to privacy as well.
    a. Additional resources can be allocated for privacy if needed according to the ISMS process. Especially if the ISMS process is integrated in the overall business management process (which it should be)
5) Operation and running risk and control applications for information security should incorporate personal data protection as well.
    a. When doing a risk assessment for information security it is more natural to see personal data as information that should be protected than trying to keep it separate as some other kind of information.
6) Performance evaluation in clause 9 is ideal to use for keeping track of also the performance of protecting personal data.
    a. The extent, need and nature of the personal data in the organization should influence the design of measurements and audits.
    b. Management review for information security should incorporate privacy aspects as a natural element.
7) The continual improvement of protection of personal data is applicable as the natural outcome, just as for other aspects of the ISMS.

2.2.2 Layer 1 - Specifics

Even if the items described previously can be utilized for personal data protection within an ISMS, there are specific considerations as well in order to support GDPR requirements. A more specific link to the requirements in clauses of the standard with references can be seen below:

The requirements in ISO/IEC 27001 to address personal data protection according to GDPR are in particular but not limited to the following:

- All requirements in clause 4-10 must be applied to have a well-functioning ISMS and in particular:

- 4.1 Understanding the organization and its context
  - To understand the external issues and to realize that the protection of personal data is one of them, as well as acknowledging GDPR as an applicable law
- 4.2 Understanding the needs and expectations of interested parties
  - to have the ”owner” of personal data included as an interested party and to meet his or her expectations
- 4.3 Determining the scope of the ISMS
  - Considering the activities performed by other organizations that relate to the personal data
- 5.1 Leadership and commitment
  - Determine if the protection of personal data is one of the information security objectives as part of the strategic direction of the organization
  - Ensuring that protection of personal data according to the GDPR is integrated into the organization’s processes
- 5.2 Policy
  - The GDPR should be one of the requirements that is considered when establishing the information security policy
- 5.3 Organizational roles, responsibilities and authorities
  - A privacy officer should be appointed as part of the organizational roles and given the responsibility and authority according to GDPR
  - How this role relates to other information security roles should also be determined
- 6.1 Actions to address risk and opportunities
  - Personal data should be part of the overall risk assessment process for information security
- 6.1.3 Information security risk treatment
  - Additional controls for privacy may need to be added as part of the risk treatment plan and the Statement of Applicability (SoA) and thus the scope is widened from information security to incorporate additional privacy aspects too.
- 6.2 Information security objectives and planning to achieve them
  - Privacy and GDPR might be the subject of explicit objectives stated
- 7.2 Competence
  - As personal data protection is similar to information security, the need for relevant competence should be determined and attained
- 7.5 Documented information
  - As GDPR requires certain documentation this should be deemed necessary by the organization

- 9.1 Monitoring, measurement, analysis and evaluation
  - The effectiveness of the ISMS regarding these activities should also cover protecting personal data
- 9.2 Internal Audit
  - The scope of the internal audit program should cover privacy controls and GDPR requirements as well
- 9.3 Management review
  - Privacy issues should be included as this is a follow up on all requirements. Preferably this should be done as part of the information security scope but for clarity personal data protection may have a separate focus in the reporting etc.
- 10.1 Non-conformity and corrective actions
  - Depending on the size of the organization these requirements might be on a strategic level. Non-conformity and corrective action should focus on the need for the ISMS to support compliance with the requirements in GDPR as well as other ISMS compliance issues. Any non-conformity directly related to personal data must be dealt with in a structured and consistent manner.

2.2.3 Layer 1 - What considerations to be taken in the aspect of personal data protection?

There are number of privacy specific aspects that must be handled within the ISMS, but it shall be remembered that protecting personal data information and information security has more in common than differences. The commonalities shall be the focus in order to have an efficient handling of GDPR requirements as well as utilizing the investment in the ISMS as described previously. The gains can be several, but in principle, processes and tools already in place with the ISMS just needs to be broadened to cover the privacy bit to the full extent. Money and time for of the organization can be saved and focus on the business can be kept.

The basis for determining how privacy requirements come into play may be difficult to grasp from an information security viewpoint only and also understanding laws such as GDPR. The principle as stated in ISO/IEC 29100 can be a good starting point for understanding and then seeing how information security will address privacy. The principle from ISO/IEC 29100 is basically explained in 11 bullets as:

- Consent and choice
- Purpose legitimacy and specification
- Collection limitation
- Data minimization
- Use, retention and disclosure limitation
- Accuracy and quality
- Openness, transparency and notice
- Individual participation and access
- Accountability
- Information security
- Privacy compliance

An ISMS according to ISO/IEC 27001 generally covers compliance and also accountability that can compromise personal data. In order to have the ISMS to support the above principle there are four conceptual issues that information security has to have a broader approach to:

- The use of information security as CIA (Confidentiality, Integrity and Availability) is not exactly the same for privacy. (See Annex A for definitions of aspects.)
- The impact of privacy breach is set primarily for the individual, not the organization
- The controls that mitigate privacy risks can be different from traditional controls aimed at information security (CIA), thus adjusting and adding controls is needed to reduce risks with regard to personal data protection
- There are distinctive roles and responsibilities specified for privacy information

Layer 1 – ISMS and GDPR - Needs that are not directly information security related

The GDPR is a new regulation building on previous privacy regulations. It further strengthens the citizens' rights and builds trust. In short GDPR introduces:

a) The "right to be forgotten";
b) Easier access to one's data;
c) The right to know when one's data has been “hacked” (note: it is not the data as such that is hacked but the “system” and data can then be disclosed); and
d) Data protection by design and by default

All these “new” four rules have to be addressed; how this is done is in strategic terms a layer one issue for the ISMS and can be exemplified as follows:

a) The right to be forgotten is highly related to what kind of business the organization is conducting and how that business can or needs to adapt to the “Right to be forgotten” rule. (Note: There might also be other laws that overrule this basic GDPR rule and thus it might be a legal reason why this rule should not apply.)
b) The burden imposed by the requirement to provide easier access to one’s data under GDPR may be reduced as the strategic benefit of business digitalisation increases
c) Depending on the business organizational and supplier structure, the “hacking” incident reporting and communication responsibilities might need to be coordinated better. This is not necessarily a disadvantage for the business; on the contrary, it can be an opportunity for better control. It might also be that internal and external parties are identified as an unacceptable “hacking” related risk as a result of the risk management process.
d) The design of data protection is a long term advantage if done by default. The design of an extended control set based upon ISO/IEC 27001 Annex A is important, as new controls and/or adjusted controls to adapt to GDPR will form a basis for design by default. Organizations and their suppliers will both in the future benefit from design by default as this will reduce risk of loss of business and can increase long term efficiency.

These rules will be an implicit part of an ISMS handling GDPR as well.

2.3 LAYER 2 - ISMS PROCESSES

2.3.1 Layer 2 - Which can be used and why – ISMS processes

General: Information security and personal data protection should be considered within the business context and scope as part of the ISMS requirements.
As mentioned before the overall processes in ISO/IEC 27001 apply but there are three specific processes that have to be looked into more closely:

a) The definition and classification of assets based upon ISO/IEC 27001 Annex A control objective 8 (and the additional guiding text in ISO/IEC 27002 as this process relates to controls). This process will both create an inventory of "information relating to an identified or identifiable natural person" as well as the impact on privacy aspects and the basic need for personal data protection.
b) The risk process as in clause 6.1. This process will determine actions needed to address risks related to GDPR (i.e. selection and applying controls as risk treatment.)
c) The overall evaluation of the compliance process. Compliance is part of the performance evaluation process as stated in clause 9 through both audits and performance measurements.

2.3.2 Layer 2 - The process for identification and classification of assets

As stated in ISO/IEC 27001 Annex A control objective 8 the organizational assets related to information security should be managed by means of an inventory, appointed ownership, classification, etc. For GDPR purposes the following can be said:

- Defining and registering personal data can be made through the asset identification, registration and protection. Even if this is not one of the main processes defined in clause 4-10 in ISO/IEC 27001 the assets have to be considered also in the risk management process.
- Maintaining a register/inventory is according to ISO/IEC 27001 Annex A 8.1.1. Note that this register should also include where the personal data resides which is often also done for any information asset any way within an ISMS, also includeing ownerships according to ISOI/IEC 27001 Annex A 8.1.2.
- Making an impact assessment of the personal data is the same as classification according to ISO/IEC 27001 Annex A 8.2, but with the different angle that this assessment should be done considering the individual that the data is connected to and not to the organization using/handling it.
- Recording what has happened/changed regarding personal data is not an ISO/IEC 27001 requirement, but can be addressed by considering the need for integrity and traceability as part of the information security classification process (ISO/IEC 27001 Annex A 8.1.1).

2.3.3 Layer 2 - The risk process of an ISMS

The risk process has to take the GDPR into consideration:

- Risk assessment in respect to GDPR will use the ISMS risk process. But the risks to be considered may differ slightly as these are related to “any information relating to an identified or identifiable natural person” as stated in GDPR.
- Risk treatment is the same basic four options (accept, avoid, reduce, transfer). However in some cases the law might have requirements on how specific risks should be handled. In these cases accept will not be an option.
- Protection as part of the risk treatment can be done using the 114 controls in 27001 but further “privacy” controls can be added such as covering “consent, “data minimization” etc.

Controls might have to be changed when considering GDPR, control application in general terms will be no different. This is then covered in Layers 3-5 in this white paper.

Combining the above (identification, impact, risk, controls) is then covering the assessment of personal data as required by GDPR (or the Privacy Information Assessment (PIA) as in ISO/IEC 29134), with the exception of compliance.

2.3.4 Layer 2 - Personal data protection compliance as part of an ISMS

The performance evaluation in ISO/IEC 27001 clause 9 as well the controls in ISO/IEC 27001 Annex A18 mean that there have to be processes in place to evaluate the performance of the ISMS and its controls as well as compliance. This can of course also be adopted to cover GDPR compliance and evaluation of related controls.

Even if performance measurements are not in themselves a verification of compliance, these can provide strong indicators for compliance evaluation and, depending on the design of the measurements, also provide compliance evidence.

2.4 Layer 3 - ISO/IEC 27001 controls

2.4.1 Layer 3 - Use of ANNEX A 114 CONTROLS

Information security according to ISO/IEC 27001 is about protecting information. Information is based upon data and knowledge. ISO/IEC 27001 also requires that legal aspects relating to information security is considered such as GDPR.

Information security therefore concerns the protection of personal data/information both in principle and as contractually and regulatory (GDPR) required.

Depending on the organization's business, risks etc. the 114 controls, from ISO/IEC 27001 Annex A, should be selected to modify information security risks and, in most cases, all or most of them will apply.

Personal data, being information, is a business asset. It should be protected by ISO/IEC 27001 Annex A based controls just as any other asset. Hence the 114 controls form a basic information security platform for treating information security risks that the business faces. Together they form a basic set of protection controls for all types of information depending on the context of the organization (regardless if it concerns personal data or other types of information).

Annexes C, D and E in this white paper give more detailed information but it should be noted that these annexes only bring up privacy specific issues.

Annex C denotes a conceptual understanding of the personal data requirements and an interpretation of what adjustment is needed. There is no reason to analyse to what extent any existing control can be excluded, if focus is on personal data protection only.

The conclusion on layer 3 related to what ISO/IEC 27001 Annex A controls could be used for personal data protection is that all of them apply (depending upon the organizational context), as good information security is a general basis for personal data protection.

2.5 LAYER 4 - ISO/IEC 27001 CONTROLS

2.5.1 Layer 4 - Adjustment of ANNEX A 114 CONTROLS

Even if all 114 controls in Annex A of ISO/IEC 27001 are applicable to information security and thus are supporting GDPR as applicable to personal data protection, not all can be directly used as described for GDPR. Especially the guidance provided in ISO/IEC 27002, it is not specifically written for privacy so this text may not be directly related to GDPR issues.
So in conclusion and in general terms the 35 control objectives are all valid as are the 114 control descriptions in principle, but the guidance in ISO/IEC 27002 may not address privacy aspects and personal data protection according to GDPR.

It should also be noted that not all personal data needs to be protected at the same level. The identification and impact processes described earlier will provide a basis for strategy. The action decision will come from the control application based upon the risk process. However all personal data still needs to be protected in such a way that it can only be used for the purpose for which it was collected. This usually implies that no personal data should be openly accessible.

Annex D in this white paper goes a bit more into details about the ISO/IEC 27001 Annex A 114 controls and how they work or how they might be adjusted for GDPR and privacy concerns.

Many of the controls can be used 'with modifications', as they are general and should also concern personal data protection. There is a difference also between those organizations that only have personal data relating to their own employees and contractors, and those that also have data related to customers and third persons. In the first case the controls handling employee and system user aspects could be adopted to handle personal data of the employees, (or "Data Subject" as in GDPR). However in the second case if the organization processes any personal data that is related to individuals that are not employed or hired by the organization, the situation become more complicated. In such a case subsequently both the number of controls needed and the need for adjustments may increase.

Also the roles given in GDPR should be considered, especially in terms of both the general requirement in clause 5.3 in ISO/IEC 27001 and the controls of the security organization in Annex A6.1(see also guidance on controls in ISO/IEC 27002 6.1). The roles in GDPR are:

- Data Subject
- Controller
- Processor
- Third Party
- Data Protection Officer

If personal data is handled by the organization itself the roles that have to be defined within the organization as part of the controls in clause ISO/IEC 27001 Annex A6.1, depend on the actual processing of data. If the data is solely processed within the organization the roles of "data subject" and "controller" need to be defined. If any part of the personal data is processed by an external party the role of processer also

needs to be defined. Certain organizations are required by GDPR to have a “Data Protection Officer”. The requirement is always applicable in the case of large scale processing of sensitive data or systematic monitoring or if the organization is a governmental body. But in general terms it might be advantageous to appoint such a role. (Note; national laws in specific European countries may be more restricted.)

The role of the “Data Protection Officer” is unique and tied to an individual that may be internal or contracted. The processor and controller are roles that are tied to organizations and are part of the responsibility of existing roles.

If the personal data at any point leaves the organization, for instance stored and/or processed by a third party, such a third party needs to be defined and personal data protection determined and applied.

It should also be noted that ISO/IEC 27018 standard on public cloud and protection of privacy information have additional guidance on clauses 5, 6, 7, 9, 10, 11, 12, 13, 16 and 18 in ISO/IEC 27002. Even if this standard is specific for public cloud providers acting as processors it gives an indication on the types of adjustment of controls that are needed.

2.5.2 Layer 4 - Specifically on supply chain controls

One of the issues that must be addressed is that if the personal data is handled by a supplier in any way this needs a specific focus in GDPR. In general the controls in ISO/IEC 27001 Annex A, A15.1 and 15.2 apply and further support can be given in ISO/IEC 27036 on supplier relationships, but also the specific requirements of roles and agreements in GDPR have to be considered. Here the roles of “Controller” and “Processor” are of specific interest as suppliers are often handling personal data especially in relation to ICT services, including cloud services.

ISO/IEC 27036 on supplier relationships also gives further support on how to generally handle suppliers from an information security perspective. Part 3 on ICT supply chain and part 4 on cloud services are very relevant for risk evaluation and designing agreements even if neither provides specific controls. The part 4 provides responsibility advice for both cloud service users and cloud service providers.

2.6 Layer 5 - Additional privacy controls

2.6.1 Layer 5 - Controls from other ISO 27000 series related standards

Annex E also refers to additional controls linked to the specific protection techniques relating to the aspects of privacy. The information in this Annex provides guidance for additional controls for privacy compared to existing or adjusted controls in ISO/IEC 27001 Annex A (ISO/IEC 27002). These additional controls could also be based upon ISO/IEC 27018 to some extent but more relevant is ISO/IEC 29151:2017.

When adding controls these should be aimed at further protecting personal data and mitigating risks, thereby increasing the ability to comply with GDPR.

Generally there might be several controls needing to be added but this is highly dependent on what personal data is collected and in what context it is handled, stored etc. Further there might be specific laws that apply that might provide a different context and other specific requirements. As with all controls in a standard due care should be made when designing and adopting them.

There is a number of protection techniques listed in Annex E, such as Separation / Isolation, Avoidance of identifiers etc. How controls can be designed to support these techniques is not just a question of stating controls but more so how and where they should be applied. Some controls might be needed for adjusting policies or procedures and others to implement technical solutions. These additional controls should of course work with existing ones as well. Hence Annex E provides general guidelines rather than specific control statements to support further guidance on what might be needed. Specific control statements are in the referenced standards such as ISO/IEC 27018, ISO/IEC 29151. It can also be concluded that these referenced standard controls may not be complete or practical for each individual situation, but rather an organization may choose to design their own controls.

3 Conclusions

Any organization strives to be efficient and that means both complying with laws as well as acknowledging the reality of economics. GDPR can be seen as a costly compliance activity in 2017 and 2018 but it has a long term value.

To use standards for personal data protection and getting a certificate might seem like an easy approach. But there is no standard that anyone one can be ISO certified against specifically for personal data protection. Currently ISO/IEC 27001 is the closest match as a base. However, it should also be understood that ISO standards are not written to comply with national laws etc. This is always up to the organization to interpret and use the standards to support their work with fulfilling the laws.

The drive from the users for digital solutions on more devices will reduce costs and increase possibilities of more and efficient services. To comply with the requirements in GDPR will be a strong enabler for developing compliant digital solutions based upon stable technical and organizational platforms designed for handling personal data. If we learn from history the adaptation to new technology comes before the security concerns, and GDPR can be seen as a balance in this perspective.

Even if today the awareness of privacy concern from the users for using a service may not be that evident in all cases, it will not become less in the future, rather the personal data protection will be generally expected. Thus the adaptation to GDPR is not just a matter of being legally compliant and avoiding high penalty fees, but an investment for being able to do business in the digital world of today and tomorrow.

There is also a lot of benefit within identification and access management if this can already by design address privacy issues, not only for external users but also for the internal staff. Nevertheless this must be done in a structured manner and how it is done will be a key question for many organizations now before May 25 2018 when GDPR is applicable. A correctly done adaptation of an ISMS that addresses GDPR now, will have a positive long term effect even after this date.

The cost for adapting an ISMS to GDPR on layers 1 and 2 as described in this white paper is not substantial, relatively speaking, as the ISMS already should cover most control areas. The costs will rather appear in the 3-5 layers of adopting and implementing controls if they are not in place. This is then heavily dependent on what risks are identified in layer 2 and that these risks enable the organization to identify what decisions to make.

The need of an organization for GDPR compliance within an ISMS just highlights what is needed to get control on personal data protection and makes privacy more evident as one of the key factors that an ISMS should address.

To have a structured approach that involves top management and that is risk based such as ISMS according to ISO/IEC 27001 enables the organization to encompass the protection of privacy information and GDPR. If not using an ISMS for GDPR purposes and the organization creates something separate for GDPR from their ISMS, this will not only be a failure of the ISMS, but will also drive higher costs due to dual processes and controls.

ANNEX A

Information security and privacy – definitions

In order to understand how the concept of privacy has an impact on the ISMS, a reference to the terms regarding information security and privacy is fundamental. This part of the white paper brings up the basic definitions based upon standards primarily and GDPR if that differs. This is in order to get a combined view of what aspects need to be covered for an ISMS protecting personal data according to GDPR.

Information security aspects

Information security aspects (CIA) are the basis for control application as part of the information security risk treatment. The controls are implemented to protect information security aspects of information and related resources. The impact value in terms information security classification is also made to cover the value of these aspects. Hence these aspects are the basis also for protection of privacy information. An understanding of their definition is essential for applying the ISMS to GDPR.

The definition of information security aspects (CIA) are:

- Confidentiality
  - Is defined as: property that information is not made available or disclosed to unauthorized individuals, entities, or processes (source ISO/IEC 27000:2016, 2.12)
- Integrity
  - Is defined as: property of accuracy and completeness (source ISO/IEC 27000:2016, 2.40)

    NOTE: Often this is also referred to as integrity that can be achieved by protecting information or data against unauthorised modification
- Availability
  - Is defined as: property of being accessible and usable upon demand by an authorized entity (source ISO/IEC 27000:2016, 2.9)

Further these other aspects used within information security should be mentioned:

- Traceability
  - Is defined as: property that allows the tracking of the activity of an identity, process, or an element throughout the supply chain (source ISO/IEC 27036-3:2014, 3.4)

    NOTE: The supply chain orientation is not needed to use this term in general
- Authenticity
  - Is defined as: property that an entity is what it is claims to be (source ISO/IEC 27000:2016, 2.8)
- Non-repudiation
  - Is defined as: ability to prove the occurrence of a claimed event or action and its originating entities (source ISO/IEC 27000:2016, 2.54)
- Authorization
  - Is defined as: mechanism to ensure that the entity or person or accessing information, services or a function has the authority to do so (source ISO/IEC 14762:2009, 3.13)

PRIVACY ASPECTS

- Privacy
  - Is defined as: Right of individuals to control or influence what information related to them may be collected and stored and by whom and to whom information may be disclosed. (source ISO 24534-4:2010, 3.50)

- Personal Identifilable Information (PII)
  - Is defined as: any information that (a) can be used to identify the PII principal to whom such information relates, or (b) is or might be directly or indirectly linked to a PII principal. (source ISO/IEC 29100:2011, 2.9)

    NOTE: In GDPR PII is referred to as personal data.

- Personal data
  - Is defined as: 'personal data' in GDPR and even it if it has the same basic meaning as ISO/IEC 29100 it is more explicit as it 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;

The following aspects related to privacy besides the traditional CIA aspects of information security:

- Unlinkabillity
  - Is defined as the property that privacy-relevant data cannot be linked across domains that are constituted by a common purpose and context.
  - There are a number of connected characteristics to unlinkability and these are found in Annex C.
- Transparency
  - Is defined as the property that all privacy-relevant data processing, including the legal, technical, and organizational settings can be understood and reconstructed at any time.
  - There are a number of connected characteristics to transparency and these are found in Annex C.
- Intervenability
  - Is defined as the property that intervention is possible concerning all ongoing or planned privacy-relevant data processing.
  - There are a number of connected characteristics to intervenablity and these are found in Annex C.

ANNEX B

What current work is done within the ISO standardisation regarding privacy

The basic content of the two main standards within ISO/IEC/JTC1/SC27 with a scope regarding privacy and ISMS is described in the text block below.

It should be noted that currently there is no ISO standard to be certified against for specifically personal data protection. At the time of writing ISO/IEC 27001 is the closest match.
But it should also be understood that ISO standards are not written to comply with any national laws etc. This is always up to the organization to interpret and use the standards to support their work with fulfilling the laws.

ISO/IEC 27001:2013 Information security management
It specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization. The requirements set out in ISO/IEC 27001:2013 are generic and are intended to be applicable to all organizations, regardless of type, size or nature.

ISO/IEC 29100:2011 Information technology -- Security techniques -- Privacy framework
Provides a privacy framework which specifies:

- a common privacy terminology;
- defines the actors and their roles in processing personally identifiable information (PII);
- describes privacy safeguarding considerations; and
- provides references to known privacy principles for information technology.

ISO/IEC 29100:2011 is applicable to natural persons and organizations involved in specifying, procuring, architecting, designing, developing, testing, maintaining, administering, and operating information and communication technology systems or services where privacy controls are required for the processing of PII.

NOTE: PII is Personal data in GDPR Source: www.iso.org

ISO/IEC 27001 as the ISMS standard is developed by the committee ISO/JTC1/SC27.This is done in working group 1 (WG1) and working group 5 (WG5) of the same committee is handling privacy matters of security. As the privacy related standards in WG5 are developed in the same committee as ISO/IEC 27001, naturally the WG1 standards are also addressing management aspects of information security considered in WG5 work.

Figure 1 below outlines the different WG5 standards with different focus such as management and technology. It should be noted that controls are referred to from ISO/IEC 27002 which is the WG1 standard providing guidelines of information security controls and are directly linked to the Annex A controls in the ISMS standard ISO/IEC 27001.

(The fact insertion below gives titles and status of the different standards, figure B1.)

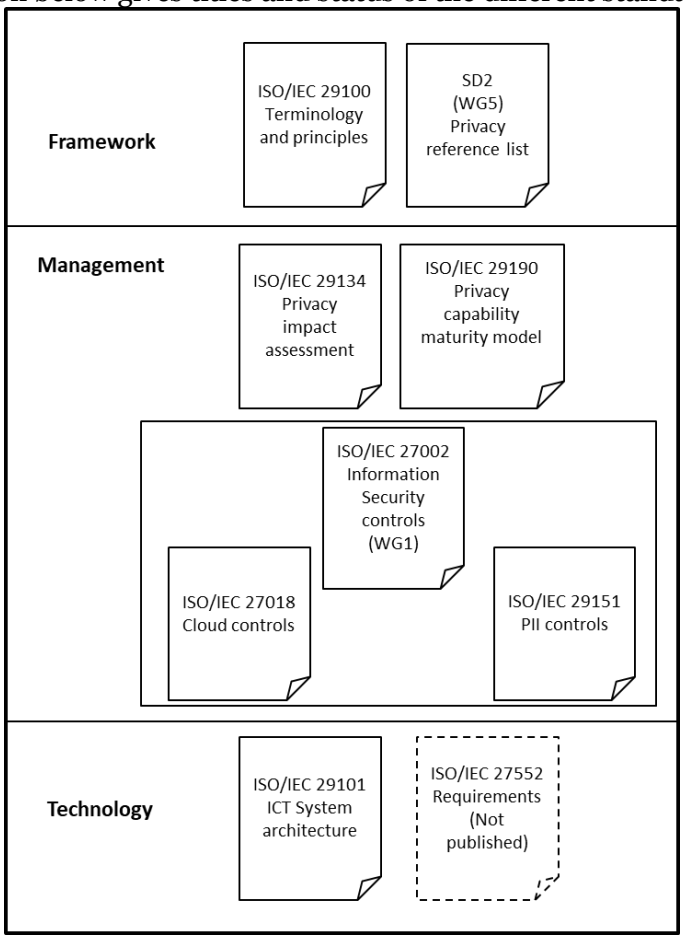

Figure B1. Showing the main different privacy standards published or under development by ISO JTC1/SC27/WG5

At this point in time the consideration in WG5 of the relationship to ISMS in ISO/IEC 27001 was not taken into account. Neither is the GDPR requirement specifically addressed as this is a regulation that only affects the EU while the ISO work is generally covering the world. It should also be clearly stated that the ISO work with standards is not for being compliant to laws/regulations as they may differ from country to country. Rather to give a common international understanding and support for organizations.

The WG5 work as mainly described in the figure B1 can be listed as follows:

- ISO/IEC 29100:2011
  - INFORMATION TECHNOLOGY - SECURITY TECHNIQUES - PRIVACY FRAMEWORK
- ISO/JTC1/SC27/WG5 SD2 – FREELY AVAILABLE
  - STANDING DOCUMENT – PRIVACY DOCUMENTS REFERENCE LIST
- ISO/IEC 29134–:2017
  - INFORMATION TECHNOLOGY -- SECURITY TECHNIQUES -- PRIVACY IMPACT ASSESSMENT – GUIDELINES
- ISO/IEC 29190:2015
  - INFORMATION TECHNOLOGY -- SECURITY TECHNIQUES -- PRIVACY CAPABILITY ASSESSMENT MODEL
- ISO/IEC 27018:2014
  - INFORMATION TECHNOLOGY -- SECURITY TECHNIQUES -- CODE OF PRACTICE FOR PROTECTION OF PERSONALLY IDENTIFIABLE INFORMATION (PII) IN PUBLIC CLOUDS ACTING AS PII PROCESSORS

- ISO/IEC 29151:2017
  - INFORMATION TECHNOLOGY -- SECURITY TECHNIQUES -- CODE OF PRACTICE FOR PERSONALLY IDENTIFIABLE INFORMATION PROTECTION
- ISO/IEC 29101:2013
  - INFORMATION TECHNOLOGY -- SECURITY TECHNIQUES -- PRIVACY ARCHITECTURE FRAMEWORK
- ISO/IEC 29191:2012
  - INFORMATION TECHNOLOGY -- SECURITY TECHNIQUES -- REQUIREMENTS FOR PARTIALLY ANONYMOUS, PARTIALLY UNLINKABLE AUTHENTICATION.
- ISO/JTC1/SC27/WG5 SD4
  - STANDARDS PRIVACY ASSESSMENT
- ISO/JTC1/SC27/WG5 SD5
  - GUIDELINES ON THE APPLICATION OF ISMS IN THE AREA OF PRIVACY
- ISO/IEC 27552 Information technology – NOT PUBLISHED - AT ERALY STAGE
  - SECURITY TECHNIQUES -- ENHANCEMENT TO ISO/IEC 27001 FOR PRIVACY MANAGEMENT – REQUIREMENTS

In figure B1 above ISO/IEC 27002 as mentioned in relation to controls is not a WG5 project; it is a WG1 standard that provides guidance on controls in Annex A of ISO/IEC 27001. The work within WG1 of the management standards has a general approach to cover information security and even if there are some sector specific standards in WG1 privacy has not been seen as sector specific topic and has not been addressed specially.
A number of cross WG items have evolved, for example ISO/IEC 27018 on cloud security and privacy. However at the last meeting more cross over projects related to privacy have evolved, but these are at such an early stage that they will not be released prior to May 25 2018 when GDPR shall be applied.

The JTC1/SC27/WG1 work as per 2016 in particular interest for ISMS and privacy can be listed as follows:

- ISO/IEC 27000:2016 – PUBLISHED
  - INFORMATION TECHNOLOGY -- SECURITY TECHNIQUES -- INFORMATION SECURITY MANAGEMENT SYSTEMS -- OVERVIEW AND VOCABULARY
- ISO/IEC 27001:2013 – PUBLISHED
  - INFORMATION TECHNOLOGY -- SECURITY TECHNIQUES -- INFORMATION SECURITY MANAGEMENT SYSTEMS -- REQUIREMENTS
- ISO/IEC 27002:2013 – PUBLISHED
  - INFORMATION TECHNOLOGY -- SECURITY TECHNIQUES -- CODE OF PRACTICE FOR INFORMATION SECURITY CONTROLS – PUBLISHED
- ISO/IEC 27003:2017 - PUBLISHED
  - INFORMATION TECHNOLOGY -- SECURITY TECHNIQUES -- INFORMATION SECURITY MANAGEMENT SYSTEM -- GUIDANCE
- ISO/IEC 27005:2011 – PUBLISHED
  - INFORMATION TECHNOLOGY -- SECURITY TECHNIQUES -- INFORMATION SECURITY RISK MANAGEMENT

Further there is one standard in particular of the work in JTC1/SC27/WG4 that is of interest for GDPR, even if all of the standards in WG4 support information security and thus GDPR indirectly:

- ISO/IEC 27036, PART 1-4 2015/2016 – PUBLISHED
  - INFORMATION TECHNOLOGY -- SECURITY TECHNIQUES -- INFORMATION SECURITY FOR SUPPLIER RELATIONSHIP

Annex C

Table linking personal data protection to information security and comments related to the ISMS

The table below is based upon ISO standards such as ISO/IEC 27001, 27002 and 27003, 29100, 29151. Protection goals and characteristics are taken from "Protection Goals for Privacy Engineering". (see Biography for full titles)

Table C1 describing privacy aspects and possible links to information security and ISMS

Privacy aspects	Personal data protection aspects linked characteristics	Link to information security	Comments in relation to ISMS implementation
Unlinkability	Data minimization	This is not a part of an information security aspect.	This characteristic is closely related the business purpose of the organization and the reasons for using personal data. To use data minimization can reduce the risks and thus be a general approach for reducing the need of information security even if it is not part of information security per se.
Unlinkability	Necessity / Need-to-know	The concept of need to know is frequently used in information security. It is usually considered a characteristic of confidentiality.	Regarding personal data protection this has a broader meaning. It refers to both the idea that the data is strictly necessary to have in order to use/offer a service or perform a task as well as the assumed restriction on whom and what information needs to be accessed in order to perform the service or task in question.
Unlinkability	Purpose binding	This is an extension to access control and/or usage control.	This characteristic refers to the fact that, ideally, it should not be possible to process the data for anything else than the purpose for which it was collected. However this is hard to implement as it usually requires both technical and organizational measures in order to be upheld.
Unlinkability	Separation of power	Roles and responsibilities including (information) asset ownership.	All information security responsibilities should be defined and allocated. Duties

			and areas of responsibilities that have conflict of interest should be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets. Assets maintained in the inventory should have designated owners.
Unlinkability	Unobservability	In a sense this is a question of confidentiality but with regards to activities performed rather than to the actual information.	According to common criteria (CC PART2 V3.1R4), un-observability ensures that a user may use a resource or service without others (especially third parties), being able to observe that the resource or service is being used by the user. In an ISMS this should be seen as a an aspect that should be considered in order to mitigate or reduce risks in connection with personal data and a way of avoiding creating personal data where it is not needed.
Unlinkability	Undetectability	This is partly an aspect of confidentiality with respect of existence of an item. A properly protected asset shall be undetectable to an unauthorized entity.	According to "ANON" version v034, undetectability is defined as follows: Undetectability of an Item of Interest (IoI) from an attacker's point of view means that the attacker cannot sufficiently distinguish whether it exists or not. In an ISMS this should be seen as a an aspect that should be considered in order to mitigate or reduce risks in connection with personal data and a way of avoiding creating personal data where it is not need.

Transparency	Openness	Openness is the principle that as far as possible required documents, actions and activities should be open and understandable for data subjects and/or supervisory authorities (see also governmental openness). This is not directly an information security aspect but indirectly influences all of the CIA requirements of company related information.	In an ISMS this should be handled as a requirement for all aspects of a system, service or process life cycle. It will influence necessary information security controls as well as risks and needs to be taken into consideration as part of procedural activities/controls such as classification.
Transparency	Accountability	Accountability is not related to an information security aspect. In relation to transparency it is rather the opposite, that the transparency is a prerequisite of the accountability characteristic.	This is the organization within the ISM. Roles, responsibilities and authorities with respect to e.g. asset ownership, governance, risk assessments, supplier relationships, monitoring, audit.
Transparency	Reproducibility	This is not directly an aspect of information security. This characteristic refers to the possibility to reproduce how the information has been processed and by whom.	In ISMS this will influence the requirements on documentation of processes, services and systems as well as on the level of traceability and monitoring that is needed. It will most likely also influence incidents and the incident management process. This may also, if done properly, assist in the process of business continuity planning where processes need to be described and recreated.

Transparency	Notice and Choice	There is no similar aspect of information security. Notice is usually referred to as the act of providing the data subject with information on the fact that personal data is being collected and how the data will be used and handled and thus is part of transparency. Choice, on the other hand, refers to the data subject's ability to restrict or to agree on collection and/or usage of personal data. This is then a characteristic of intervenability.	In an ISMS this should be handled as a requirement for all aspects of a system, service or process life cycle. It will influence necessary information security controls as well as risks and needs to be taken into consideration as part of procedural activities/controls such as classification.
Transparency	Auditability	Auditability is not directly related to an information security aspect as such but has a strong dependency on integrity and availability. In relation to transparency it is rather the opposite, that the transparency is a prerequisite of the auditability characteristic.	There is a similar basic requirement in the concept of ISMS that controls etc. should have auditability. However, in the ISMS case it is the possibility to audit the conformity to either the ISMS or the Standard that is in focus while in the privacy case it is the conformity to GDPR and the agreed upon handling of personal information that is the core focus. These two areas might have different requirements regarding what is needed in order to be auditable.
Intervenability	Self-determination	Self-determination can be related to the information security aspects of integrity and confidentiality. The aspect covers the rights or abilities of a data subject to be able to determine what information it is willing to release, under what conditions and for what use. It also has relations to privacy by design and data minimization.	In an ISMS this should be handled as a specific requirement for all aspects of a system, service or process life cycle. It will influence necessary information security controls as well as risks and needs to be taken into consideration as part of procedural activities/controls such as classification.

Intervenability	User control	In privacy terms this refers to the data subject's ability to control the use of personal data through e.g. configurations, flow control or other means. It also has relations to privacy by design and data minimization.	In an ISMS this should be handled as a requirement primarily for the design, development and acquisition of processes and systems and as a risk. Such a risk consideration will influence necessary information security controls as well as taken into consideration as part of procedural activities/controls such as classification.
Intervenability	Rectification and erasure of data	This is linked to both integrity and traceability. But also to the concept of correctness. In essence it requires that the data subject has the right to correct data and may have the right to delete its data.	In an ISMS this should be handled as a requirement on design, development and acquisition of systems and services as well as requirement on implementation of technical and organizational processes.
Intervenability	Consent withdrawal	This is not directly related to an information security aspect. Consent withdrawal can however be a pre-step to set requirements on integrity and availability. It will also have an impact on traceability and even confidentiality depending on the personal data involved.	In an ISMS this should be handled as a requirement that cannot be neglected for the processes and as a risk towards the business model and by that influence necessary controls as well as taken into consideration as part of procedural activities/controls such as classification.
Intervenability	Claim lodging/ Dispute raising	This is not an information security aspect as such. However traceability will be needed in order to keep track of events.	This is a formal procedural activity that might need information security controls to handle risks.
Intervenability	Process Interruption	The ability to stop or alter a process going gives a permission to change information and can then be seen both as integrity and an availability aspect of information security. But this is rather a demand than a protection of information.	This is a formal procedural activity that might need information security controls to handle the risks and possibly incidents. The controls needed follows the requirements for the ISMS related to GDPR will influence technical and organizational controls.

Annex D

Adjustments of the 114 controls

This Annex is about the ISO/IEC 27001 Annex A 114 controls and how they work or in particular how they should be adjusted for GDPR and privacy concerns. It might also address the main clauses in 27001 if so.
Protection characteristics are taken from "Protection Goals for Privacy Engineering" (see * in Biography for full title).
ISO/IEC 27018 which addresses privacy in public cloud services provides additional guidance on ISO/IEC 27002 controls and has noted 14 of the 114 controls for further guidance, please see that standard. (ISO/IEC 27018 has also 23 additional controls and these are mentioned in Annex E as well as references to ISO/IEC 29151.)

NOTE: The 14 Controls of ISO/IEC 27002 listed in ISO/IEC 27018 with further guidance are: 5.1.1, 6.2.1, 7.2.2, 9.2.1, 9.4.2, 10.1.1, 11.1.7, 12.1.4, 12.3.1, 12.4.1. 12.4.2, 13.2.1, 16.1.1, 18.2.1.

Table D1 linking personal data protection to control or requirements in ISO/IEC 27001 in particular for further development

Personal data protection aspects linked characteristics	Linked information for security protection	ISO SC27 standard ref (in principle)	Comment
Data minimization	This is not an information security protection aspect	see clause 4 of ISO/IEC 27001) (See also ISO/IEC 29100 and ISO/IEC 29151 A5, A6 a)	This is part of the external requirements if GDPR is valid for the ISMS. Will be an internal regulation to meet external requirements and should be handled through PIA and Risk process. Controls must be administrative in the first place and technical if needed.
Necessity/ Need-to-know	Access control policy	ISO/IEC 27002 9.1.1 (Note other clause 9 controls may apply) (See also ISO/IEC 29151 A4, A5, ISO/IEC 27018 9.2.1, 9.4.2)	An access control policy must cover the rules of what the basis for need-to-know is. (Several sub-policies might be needed for various services.)

Necessity/ Need-to-know	Information classification	ISO/IEC 27002 8.2.1, 8.2.2, 8.2.3 (Note many other controls may apply)	The confidentiality aspect should be determined (and controls applied accordingly)
Purpose binding	This is not an information security protection aspect	ISO/IEC 27002 18.1.1, 18.1.4 (See also ISO/IEC 29151 12.4.1, 12.4.2 and A6.1.)	This is a compliance aspect only in terms of ISO/IEC 27002 controls and purpose binding has to be included in 18.1.1 and addressed as part of 18.1.4
Separation of power	Roles and responsibilities including asset ownership. Access rights	ISO/IEC 27002 6.1.1, 6.1.2, 8.1.2, 9.2.3	These controls are linked between organizational procedures and technical implementation and the actual linkage is the adjustment that is needed to be assured.
Openness	Information Classification Confidentiality and traceability	ISO/IEC 27002 8.2.1 (See also ISO/IEC 29151 A1, A6.3, A6.4, A6.5 and A8.)	Openness is a contradiction to something being confidential but on a scale in classification this can be a categorization. Note that in order to fulfil this, the information that should be open must also to be traceable.
Accountability	Roles and responsibilities including asset ownership	ISO/IEC 27002 6.1.1, 8.1.2 (See also ISO/IEC 29151 A10.)	ISO/IEC 27002 states ownership of assets. This does not necessary mean that that role is also accountable for privacy.

Process Documentation / description	Documented information	ISO/IEC 27001 7.5	This is a more complex adjustment as it is not a control per se (or a specified required documentation in ISO/IEC 27001). It is rather a description demanded to be necessary for GDPR and thus required also by ISO/IEC 27001.
Reproducibility	Protecting application services transactions	ISO/IEC 27002 14.1.3 (See also ISO/IEC 29151 A6.3, A6.4, A6.5)	This aspect should just be a requirement as for any other information that needs to be addressed.
Notice and Choice	This is not an information security protection aspect.	(Possible ISO/IEC 27002 7.1.2, 15.1.2) (See also ISO/IEC 29151 A2, A3.2, A6.3, A8.1, A8.2)	This control needs to be added. (If only applicable to staff or hired personnel, the ISO/IEC 27002 controls can be adjusted to cover this.)
Audibility	This is part of both the ISMS requirement of internal audits as well as controls and is only a concern that it should be possible to audit.	ISO/IEC 27002 18.2 (See also ISO/IEC 29151 A6.3, A6.4, A6.5 ISO/IEC 27018 18.2.1)	The audit scope and activities for privacy have to be considered.
Self-determination	This is not an information security protection aspect.	(Possible ISO/IEC 27002 7.1.2, 15.1.2)	This control needs to be added. (If only applicable to staff or hired personnel the ISO/IEC 27002 controls can be adjusted to cover this.)

User Controls	Prior to employment During employment	ISO/IEC 27002 9.1, 9.2, 9.3, 9.4 (Possible ISO/IEC 27002 7.1, 7.2, ISO/IEC 27018 7.2.2, 9.2.1, 9.4.2)	Access and privileges have to be applied to all users. The clause 7 controls are only for employees. Users can be non-employees.
Rectification and Erasure of data	Disposal of media Ownership of assets Return of assets	ISO/IEC 27002 8.1.2, 8.1.4, 11.2.7	
Consent Withdrawal	This is not an information security protection aspect.	(Possible ISO/IEC 27002 7.3.1) (See also ISO/IEC 29151 A2, A8.1, A8.2)	This control needs to be added. (If only applicable to staff or hired personnel the ISO/IEC 27002 controls can be adjusted to cover this.)
Claim lodging/ Dispute raising	Incident process requirement	ISO/IEC 27002 16.1 (see also ISO/IEC 27018 16.1.1)	This has to be added as a step in the incident process and part of the controls.
Process Interruption	Incident process requirement	ISO/IEC 27002 16.1 (see also ISO/IEC 27018 16.1.1)	This has to be added as a step in the incident process and part of the controls.

Annex E

Techniques comparison between protecting personal data and information security for additional controls.

The table below provides a principal comment for additional controls linked to the characteristics of these aspects to reach protection of privacy in general. Protection goals and characteristics are taken from "Protection Goals for Privacy Engineering" (see * in Biography for full title).

The table E1 has a reference to ISO/IEC 29151 if found linked. Additionally a reference is also given to any of the 25 additional controls specified in SO/IEC 27018 when so seems to be relevant. But as ISO/IEC 27018 is for privacy related to public cloud these references have to be used carefully. For further details the actual standards shall be used as basis for control design when they are referred to. (Other controls and control design may of course be made as the table just presents a starting point.)

Table E1 linking protection techniques to additional control development

Protection technique For control	Control explanation	Ref to ISO/IEC 27018 and ISO/IEC 29151	Comment for control
Data avoidance /Reduction	Design data structure so that minimum data is used	ISO/IEC 29151 A.6 (See also ISO/IEC 27018 A4.1, A.7.2)	Data minimization characteristic to be achieved. This can be technical as well administrative additional control/controls.
Access control enforcement	Access controls are in general always applicable to this type of information.	x	(ISO/IEC 29151 clause 9 has additional guidance on the controls in ISO/IEC 27002 even if no additional controls are added.)
Generalisation - Anonymization/ Pseudonymization	Design data structure so that data cannot be linked to an individual	ISO/IEC 29151 A.6	This is privacy by design and an additional control and should be applied both to existing services and new ones. This can be a general control but needs to be put in place where personal data resides.
Generalisation - Abstraction	To reproduce data to a simplified representation of the whole is a way of avoiding data to be linked to an individual	ISO/IEC 29151 A.7.1 (See also ISO/IEC 27018 A10.2)	This is an additional control that might be useful depending on the purpose of the data collected.
Generalisation -	This can be applied to	(See also	This is an additional control

Derivation	ensure correctness of data from different sources. (It can also be a control for what cannot be derived.)	ISO/IEC 27018 A10.6)	that might be useful depending on the purpose and structure of the data collected.
Separation / Isolation	This can be applied to ensure data is not accessible from different sources.	x	This is an additional control that might be useful depending on the purpose of the data collected. It works well in combination with access controls in 27002. (Other 27002 related design controls of resources will support this)
Avoidance of identifiers	This will limit the possibilities that data can be linked to an individual	x	This is privacy by design and an additional control and should be applied both to existing services and new ones. This can be a general control but needs to be put in place where personal data resides.
Logging and Reporting	This is not specific	(See also ISO/IEC 27018 A10.3)	Additional controls should be applied to ensure that personal data is covered in logs to a necessary extent as well as the logs may also contain personal data and be protected.
User Notifications	This will ensure consent and manage changes that are linked to the user rights and privacy	ISO/IEC 29151 A.9.1	This is privacy by design and an additional control and should be applied both to existing services and new ones. This can be a general control but needs to be put in place where personal data resides.
Documentation	This is not specific and documentation requirements shall apply. If any specific additional control is needed this should be based on legal aspects depending on the context.	ISO/IEC 29151 A.9.2, A.7.4 (See also ISO/IEC 27018 A.9.2, A.10.9)	Specific retention controls may be needed depending on laws for keeping records that contain personal data.
Status Dashboards	This is a visualization of	x	The only additional control

	monitoring activities		that might be added is if this should be presented to the users.
Privacy Policies	This is very general and depends both on the context of personal data used as well as the context of the business. In general controls may be added to cover this specifically if this is seen as necessary	(See also ISO/IEC 27018 A2.1)	If specific controls should be added to cover a privacy policy such controls could preferably apply to existing policies or may result in specific privacy related policies. These can cover that purpose for example.
Transparency services for personal data	This is to ensure keeping control of where personal data is used etc.	ISO/IEC 29151 A.13.2 (See also ISO/IEC 27018 A11.1, A.11.2)	This is privacy by design and an additional control and should be applied both to existing services and new ones. This can be a general control but needs to be put in place where personal data resides.
Data breach notification	This could be seen as not specific – but additional procedures are most likely needed to know why, who, when and how	ISO/IEC 29151 A11.6 (see also ISO/IEC 27018 A9.1)	The procedure that needs to be in place to have notifications may result in one or several controls that might need to be implemented in several instances. These controls should apply to management as well as to the personal data owner (PII principal).
Point of contact	This is to ensure that the "user" has a clear contact for privacy matters	ISO/IEC 29151 A.10.3	Such an additional control is normally needed. (This can be a help desk or some other existing contact that will apply this control.)
Stop-Button for processes	This is to ensure that a process can be stopped but is also used for giving authority to being able to stop it.	x	Such an additional control should be determined if needed and might be part of the incident management. It is likely that several controls are needed as they have to be linked between organizational procedures and technical implementation.

Break-Glass / Alert Procedures	This is to ensure that information is possible to give under certain circumstances so that a judgement can be made if a process should be stopped, but is also used for giving authority to being able to “break the glass”	ISO/IEC 29151 A.3.2, A.10.2	Such an additional control should be determined if needed and might be part of the incident management.
Manual override of automated decisions	This is an extra precaution to ensure that an automatic process can be changed or stopped by manual decisions	x	Such an additional control should be determined if needed and might be part of the incident management. (Note that this can be a user privilege to do this.)
Supervisory authorities	This will enable clarifying roles and responsibilities (and authorities) special to privacy regulations (GDPR)	x	Such an additional control should be determined if needed and might be part of the overall information security organization.

Biography

- ISO/IEC 27000:2016 – PUBLISHED
  - INFORMATION TECHNOLOGY -- SECURITY TECHNIQUES -- INFORMATION SECURITY MANAGEMENT SYSTEMS -- OVERVIEW AND VOCABULARY
- ISO/IEC 27001:2013 – PUBLISHED
  - INFORMATION TECHNOLOGY -- SECURITY TECHNIQUES -- INFORMATION SECURITY MANAGEMENT SYSTEMS -- REQUIREMENTS
- ISO/IEC 27002:2013 – PUBLISHED
  - INFORMATION TECHNOLOGY -- SECURITY TECHNIQUES -- CODE OF PRACTICE FOR INFORMATION SECURITY CONTROLS
- ISO/IEC 27003:2017 - PUBLISHED
  - INFORMATION TECHNOLOGY -- SECURITY TECHNIQUES -- INFORMATION SECURITY MANAGEMENT SYSTEM -- GUIDANCE
- ISO/IEC 27005:2011 – PUBLISHED
  - INFORMATION TECHNOLOGY -- SECURITY TECHNIQUES -- INFORMATION SECURITY RISK MANAGEMENT
- ISO/IEC 27018:2014 - PUBLISHED
  - INFORMATION TECHNOLOGY -- SECURITY TECHNIQUES -- CODE OF PRACTICE FOR PROTECTION OF PERSONALLY IDENTIFIABLE INFORMATION (PII) IN PUBLIC CLOUDS ACTING AS PII PROCESSORS
- ISO/IEC 27036, PART 1-4 2015/2016 – PUBLISHED
  - INFORMATION TECHNOLOGY -- SECURITY TECHNIQUES -- INFORMATION SECURITY FOR SUPPLIER RELATIONSHIP
- ISO/IEC 29100:2011 – PUBLISHED
  - INFORMATION TECHNOLOGY - SECURITY TECHNIQUES - PRIVACY FRAMEWORK
- ISO/JTC1/SC27/WG5 SD2 – FREELY AVAILABLE
  - STANDING DOCUMENT – PRIVACY DOCUMENTS REFERENCE LIST
- ISO/JTC1/SC27/WG5 SD4
  - STANDARDS PRIVACY ASSESSMENT
- ISO/JTC1/SC27/WG5 SD5
  - GUIDELINES ON THE APPLICATION OF ISMS IN THE AREA OF PRIVACY
- ISO/IEC 29134.2017 – PUBLISHED
  - INFORMATION TECHNOLOGY -- SECURITY TECHNIQUES -- PRIVACY IMPACT ASSESSMENT – GUIDELINES
- ISO/IEC 29151:2017 – PUBLISHED
  - INFORMATION TECHNOLOGY -- SECURITY TECHNIQUES -- CODE OF PRACTICE FOR PERSONALLY IDENTIFIABLE INFORMATION PROTECTION
- ISO/IEC 29101:2013 – PUBLISHED
  - INFORMATION TECHNOLOGY -- SECURITY TECHNIQUES -- PRIVACY ARCHITECTURE FRAMEWORK
- ISO/IEC 29190:2015 – PUBLISHED
  - INFORMATION TECHNOLOGY -- SECURITY TECHNIQUES -- PRIVACY CAPABILITY ASSESSMENT MODEL
- ISO/IEC 29191:2012 – PUBLISHED
  - INFORMATION TECHNOLOGY -- SECURITY TECHNIQUES -- REQUIREMENTS FOR PARTIALLY ANONYMOUS, PARTIALLY UNLINKABLE AUTHENTICATION.
- *MARIT HANSEN, MEIKO JENSEN, AND MARTIN ROST, “PROTECTION GOALS FOR PRIVACY ENGINEERING”, 2015 IEEE CS SECURITY AND PRIVACY WORKSHOPS, 21 MAY 2015, SAN JOSE, CALIFORNIA, USA
- COMMON CRITERIA FOR INFORMATION TECHNOLOGY SECURITY EVALUATION, PART 2: SECURITY FUNCTIONAL COMPONENTS, SEPTEMBER 2012, VERSION 3.1, REVISION 4, CCMB-2012-09-002
- 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) OFFICIAL JOURNAL OF THE EUROPEAN UNION, L19, VOLUME 59, 24 MAY 2016