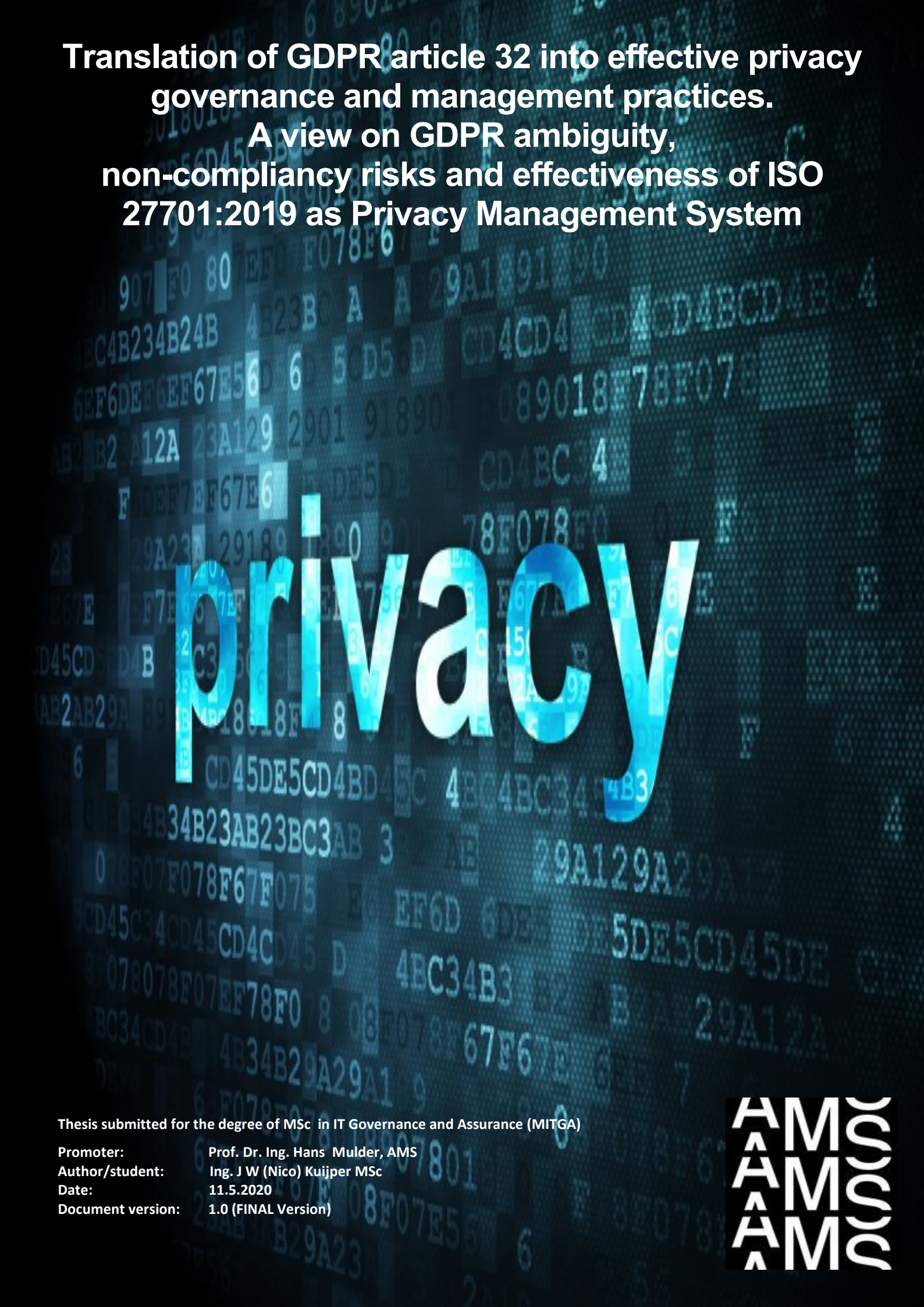
Translation of GDPR article 32 into effective privacy governance and management practices. A view on GDPR ambiguity, non-compliancy risks and effectiveness of ISO 27701:2019 as Privacy Management System



Thesis submitted for the degree of MSc in IT Governance and Assurance (MITGA)

Promoter:	Prof. Dr. Ing. Hans Mulder, AMS
Author/student:	Ing. J W (Nico) Kuijper MSc
Date:	11.5.2020
Document version:	1.0 (FINAL Version)

Abstract

Background and research question

Many organizations seem to struggle to translate the GDPR legislation into specific and effective (data privacy) governance, management & operational activities. The GDPR Enforcement Tracker (Law firm C|M|S, 2020) reported that the European Data Privacy Authorities fined non-compliance with the GDPR (up to 03.2020) with a total cumulative fine of € 332.000.000, a substantial materialized risk. Organizations with a focus on privacy risk mitigation often turn to worldwide accepted standards for guidance.
A new ISO standard that has been released in 2019, ISO 27701:2019, aims to deliver specific guidance for the setup of a PIMS (Privacy Information Management System).
This context has led to the formulation of the main research question of this paper:

What are the most violated GDPR articles/aspects in combination with the highest fines? What are the (perceived) risks, ambiguities, the required governance and (change) management activities of this most violated article and are these effectively addressed in ISO 27701 as Privacy Information Management System?

Research approach

The limited availability of literature on e.g. the case of GDPR violations and on ISO standard ISO 27701 led to the choice to select the “exploratory case study” as research methodology. We started with a quantitative analysis of the GDPR violations in order to identify the most violated GDPR articles, the violation aspects & hotspots and highest financial implications. We applied literature research to analyse the ontology of the most violated GDPR article, its specific legislative requirements and the related privacy governance and management activities (COBIT perspective). Additionally we analysed are possible ambiguities in the legislative text, the change management aspects and the privacy architecture view.
A questionnaire has been used to collect the view of privacy professionals on these topics. The consolidated findings are used as input for the “fit/gap” analysis of ISO 27701:2019.

Findings

- **Most violated article** is article *32* (secure data processing). It is linked to the highest cumulative fines and is the 2nd most violated GDPR article (period 04.2018 – 03.2020).
- **Violation hotspots** according the article 32 ontological domain classifications, combined with the analysis of the DPA rulings, are: failing to realize ongoing confidentiality and integrity of data processing, failing to realize resilience of systems / services.
- **Privacy activities.** The ontology of article 32 reveals the COBIT activities: data privacy risk analysis & instructions (governance) and risk mitigation/monitoring (management).
- **Violation risks area’s and root causes:** the authorities mainly fined the article 32 violation symptoms; failing or ineffective privacy management activities like PLAN-BUILD-RUN-MONITOR without clarifying the possible underlying root causes.
- **Perceived risks:** the questionnaire respondents identified the privacy improvements and risks mainly on governance level (COBIT activities EVALUATE and DIRECT).
- **Change management risks** identified on privacy governance & management level are:
  - Change clarity – the ambiguity (reduction) of the GDPR requires a contextual analysis
  - Change ability – security & privacy requires different skills, knowledge and frameworks
  - Change willingness - expect resistance (divergent interests, roles and cognitive views)
- **A (privacy) governance system** (GRC) should cover the complex and ongoing alignment of processes, organizational structures, policies and procedures, information flows, culture and behaviours, skills, and infrastructure. (COBIT 2019 components).
- **(Privacy) architecture** addresses the function construction gap – the inability to bridge the gap between “know *what* to do” (function) to “know *how* to do this” (construction). Both the GDPR & ISO 27701 describe the function, not the construction of that function.

Conclusions and recommendation

ISO 27701:2019 has a predominant focus on data security however data security covers only one of the seven privacy principles mentioned in GDPR. ISO 27701 need to be improved to fullfill the roles as PIMS. Security and privacy require (additional) approaches that must be merged into consistent and aligned privacy governance and management activities. Identification and mitigation of (common) operational risk (article 32 violation hotspots) could be more emphasized in the ISO 27701 guidance.This exploratory case study contributed to the identification of relevant privacy governance and management aspects, but it leaves questions unanswered like e.g. what are the factual root causes of GDPR violation cases? Current affairs like the failure to develop a privacy proof COVID19 app shows the limited systematic approach applied in this context. Further research is needed!

Acknowledgements

Je gaat het pas zien als je het door hebt – Johan Cruijff

I would like to thank my promoter Prof. Dr. Ing. Hans Mulder for his friendly and valuable guidance and support.
I am also using this opportunity to express my gratitude to everyone who supported me throughout the course of this research project, especially my wife and daughter, fellow students, respondents and the expert reviewers Dr. Sandro Lovisa and Dr. Anderson Santana de Oliveira who gave all useful expert feedback regarding the formulated improvements.
All your comments were very valuable and improved the quality of the manuscript.

Nico J W Kuijper,
Amsterdam, May 2020

Disclaimer

This thesis is prepared for the executive Master of IT Governance & Assurance (MITGA) at the Antwerp Management School (AMS), the business school of the University of Antwerp. The opinions, conclusions and recommendations presented herein are those of the author and do not necessarily reflect those of the Antwerp Management School or any of the in this research involved parties and experts.

INDEX

1. An introduction to the research

§ 1.1 Background of the research

On May 25, 2018 the GDPR (General Data Protection Regulation, (European Union, 2018)) legislation came into force across the European Union. Now more than two years after the GDPR was enacted, different research reports (e.g. that of the Ponemon institute[1]) indicate that enterprises across the world are still struggling to comply with the GDPR.

But what are some of the factors that make companies struggling to comply with the GDPR?

One of the reasons why it seems so difficult to "implement" the GDPR is that the legislation is not always defined in black and white rules (ambiguous in its guidance and description) and therefore there are different ways of interpreting and implementing some parts of the GDPR. The 99 GDPR articles are often not prescriptive in many areas, but rather descriptive in nature - a detailed "how to" is often not clearly outlined. However, many companies are looking for more detailed guidance on the "what, when, how and who" when it comes to implementing the GDPR, especially those in the organization responsible for the implementation and monitoring of GDPR compliancy.

On one hand ambiguity is unavoidable – the GDPR has been written to be future-proof so that it can keep up with the fast(er) advancing technology. Therefore some parts of the GDPR are more or less formulated in a "technology agnostic" and directive way, and as a consequence of that some ambiguity is introduced in the GDPR. The good thing about that approach is that you can apply GDPR governance *principles* (instead of detailed, prescriptive and possible quickly outdated hard "rules") to many different software solutions, applications, data sources, cloud solutions, the way data privacy is handled in different technological constellations etc. etc.

A downside however of having legislative *directive principles* is that a cascaded GDPR translation / interpretation process is needed to translate the *legislation* to *company policies (IT governance)*, the policies on its turn must be translated to *procedures and guidelines* (IT management) that are tailored & *implemented to operate in specific IT* solutions. In this process many GDPR principles and guidelines could be lost or misinterpreted.

Many companies are using standards like ISO 27001 and 2 (ISO, 2019) or other frameworks like COBIT (ISACA, 2020) to guide them and building up knowledge regarding ICT governance and management activities related to specific challenges. The GDPR legislation however is a relatively young legislation (active since May 2018) and internationally accepted standards regarding the implementation of GDPR guidelines are still under development and/or partly applied in practice.

§ 1.2 Problem statement

Based on the previous introduction of the factors that make companies struggling to comply with the GDPR on IT governance, management and operational level, we can formulate the general problem statement in the following way:

> Many companies seem to struggle to translate the GDPR legislation into specific IT (data privacy) governance, management & operational activities. This is partly caused by the perceived ambiguity in the GDPR legislative texts, a lack of specific guidance regarding GDPR relevant ICT governance and change management risks, specific activities and relevant IT standards. Is ISO 27701 indeed a privacy framework that covers the relevant GDPR aspects and thus "fit for purpose"?

Applying new legislation, like the GDPR, top-down to the organization requires a lot of change management. Different change management aspects of Meyer's change management 'mind the gap' model (Meyer, 2019), see figure 1) are used as the basis in this paper to identify some of the common (GDPR) change management challenges.

[1] See: https://mcdermott-will-emery-2793.docs.contently.com/v/keeping-pace-in-the-gdpr-race-a-global-view-of-gdpr-progress-in-the-united-states-europe-china-and-japan (Retrieved at 05.2020)

§ 1.3 Challenges in translating the GDPR legislation into effective ICT operations

Many of the aspects mentioned in Meyer's change management model can be linked to people management aspects. However, even if the employees are 100% committed to comply with the GDPR, without understanding the "what, when how and who" outlined in the GDPR (the specificity ambiguity) it becomes difficult to formulate and materialize the relevant (ICT related GDPR) governance and management measures.

In short: building up understanding regarding the expected "what, when, how and who" (Clarity, reducing ambiguity) and learning how to apply this knowledge the organizational context are vital for every change, therefore also for the GDPR relevant IT measures in your organization.

Figure 1: Change management aspects. Figure reused from Meyer's Management Models, 'Mind the Gap', (Meyer, 2019): https://blog.antwerpmanagementschool.be/en/ron-meyer-episode-1-mind-the-gap (Retrieved at 05.2020)

Based on this change model of Meijer (Meyer, 2019), the organization first of all need to understand what "the right things to do" are before it can "do the things right".
One frequently used instrument to build up knowledge about "the right things to do" is by using (international) standards as a "knowledge and guidance framework".
The use of widely accepted standards or frameworks, like ISO or COBIT, etc. can be very helpful as a kick-start instrument to build up the relevant knowledge and practical guidance.
Knowledge subsequently can deliver guidance regarding "do the things right".

§ 1.4 The development of GDPR related IT standards and certifications

NEN/ISO is such a worldwide organization that develops and publishes International Standards (22.000+ so far) in order to "provide in standards that underpin the technology we rely on and ensure the quality that we expect"[2].
Are there currently internationally accepted ISO standards and certifications available supporting and demonstrating the successful implementation of the GDPR?
Interestingly enough, GDPR related ISO standards are still under development or just recently became available.
The Dutch Data Privacy Authority confirms that a GDPR certification mechanism has been described by the GDPR, however in 2019 no organization in the Netherlands has the accreditation to provide in a certification for products, processes or organizations to demonstrate GDPR compliancy.[3] This demonstrates that GDPR certification standards are officially not available yet (at 03.2020).
Regarding the availability of ISO standards for implementing the GDPR: these are not yet widely spread. Just recently, in August 2019, NEN/ISO released the first GDPR specific NEN/ISO standard that covers (a part of) the GDPR, namely the new ISO 27701 standard[4].

[2] See: https://www.iso.org/standards.html (Retrieved at 05.2020)
[3] See: https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-waarschuwt-voor-misleidend-avg-keurmerk and https://www.agconnect.nl/artikel/avg-gedragscodes-en-certificeringen-wat-voegen-ze-toe (05.2020)
[4] See: https://www.iso.org/news/ref2419.html (Retrieved at 05.2020)

Many new ISO 27XXX industry specific privacy standards are currently being developed by ISO[5] and in August 2019 NEN/ISO has released ISO 27701:2019 as a new standard for PIMS (Privacy Information Management System).
The aim of this research is to investigate if ISO 27701:2019 guidelines are effective in the translation of GDPR requirements to clear ICT governance and management activities and if it addresses common privacy gaps identified in the GDPR violation tracker and in the questionnaire regarding this topic. Is ISO 27701 indeed a privacy framework that covers the relevant GDPR aspects and thus "fit for purpose"?
Based on the problem statement the following research (sub)questions are formulated:

§ 1.5 Research questions

What are the most violated GDPR articles/aspects in combination with the highest fines? What are the (perceived) risks, ambiguities, the required governance and (change) management activities of this most violated article and are these effectively addressed in ISO 27701 as Privacy Information Management System?

The research question has been split up into the following sub questions:

- Quantitative analysis - what are the GDPR violations registered up to 03.2020?
- What are the most violated GDPR articles and what aspects are violated?
- What are the most violated GDPR articles with the highest financial implications?
- What could be possible root causes for these violations?
- What are the ICT governance and -management requirements, guidelines and activities described by this GDPR article?
- What are the perceived (data privacy) governance and change management challenges / risks and gaps companies could / are facing?
- What are the possible ambiguities in the legislative text of this GDPR article and how to address them?
- How are companies perceiving IT related GDPR change management ambiguities, risks & challenges and are (ISO) standards be of added value in that process?
- Are the identified non-compliancy risks and perceived GDPR governance and (change) management aspects of this article effectively addressed in the ISO 27701:2019[6] (new privacy extension to ISO27001 published in October 2019)?
- What are possible improvements we can identify (based on literature research, GDPR violations statistics and questionnaires/interviews) that could be applied to ISO 27701:2019 regarding improved data privacy governance and management?

Schematically seen we aim to investigate the effectiveness and gaps regarding privacy governance aspects (privacy requirements, risks, effectiveness of frameworks) and how this is cascaded to concrete and effective privacy management activities and operations.

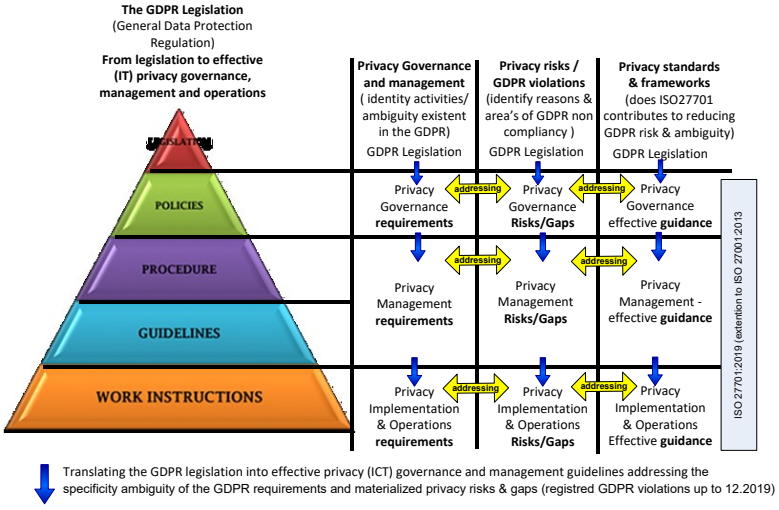


Figure 2 : Contextual research framework.
(Privacy governance & management requirements, risks/gaps and ISO standards view)

[5] See: https://www.iso.org/committee/45306/x/catalogue/p/0/u/1/w/0/d/0 Like ISO/IEC 27014 / 27045 / etc.)
[6] See: https://www.iso.org/obp/ui/#iso:std:iso-iec:27701:ed-1:v1:en (Retrieved at 05.2020)

§ 1.6 Research scope, objectives, approach and limitations

Scope and objective of the research.
As the research questions suggest, many companies are struggling with the process of translating the GDPR legislation into effective IT governance, management and operations. In that process, the use of worldwide accepted standards and frameworks like 27701:2019 could deliver the right contextual knowledge and guidance.
Aim of this research is to identify the different GDPR specific ICT governance and management requirements, guidelines and activities – and identify possible ambiguities and learning barriers perceived by organizations - including the way organizations perceive the practical value of standards as an instrument to comply with the GDPR legislation.

Overall methodological approach:

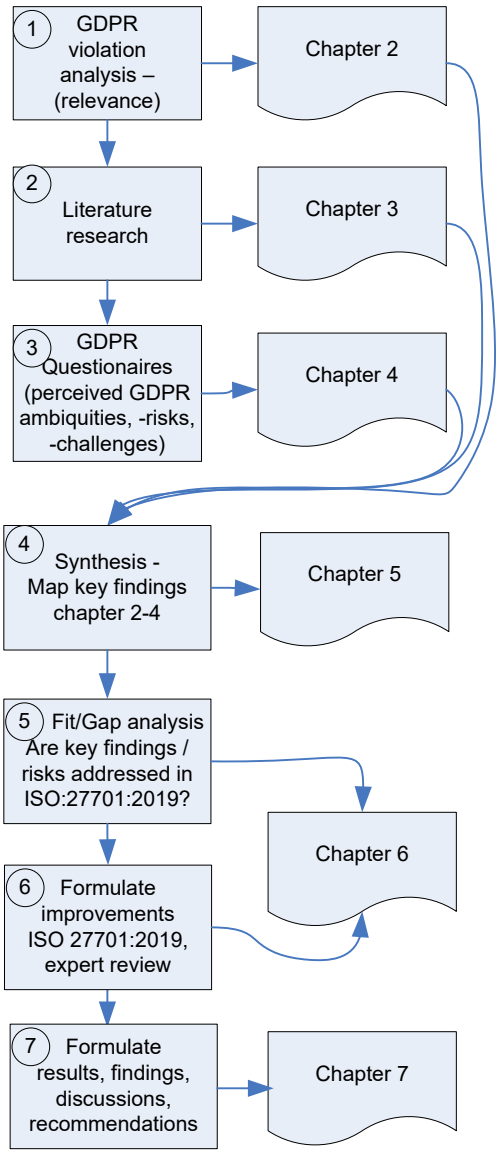


Figure 3: the research steps

Step 1. Quantitative analysis of GDPR violations).
What are the GDPR violations registered up to 12.2019, what are the most violated articles & related aspects?
What are the highest (cumulative) fined articles?

Step 2. (Literature research – GDPR text analysis).
What are the ICT governance and (change) management requirements and activities mentioned by the GDPR?
Wat are potential ambiguities we can find in the text and how to handle that?
What are the perceived (data privacy) governance and management challenges / risks and gaps companies could or are facing?

Step 3. (Questionnaire): What are the specific GDPR challenges & risks (aspects GDPR knowledge translating to IT governance/management activities) you are facing?
What are the (ISO and other) standards used in organizations and the perceived effectiveness of those standards to fulfil the GDPR requirements?
What are the perceived fit/gaps between the GDPR and IT standards (like COBIT, ISO, etc.)?

Step 4. (Synthesis of the results of step 1-3)
The outcome of the literature research and questionnaires are consolidated in an overview of the previous chapters and a synthesis of them.

Step 5. Mapping the findings of step 4 (the synthesis) to the 27701:2019 frameworks to see if there is a fit/gap between the findings and the aspects addressed in ISO 27701:2019

Step 6. (Formulate improvements)
Formulate improvements (based on the outcome of step 5) that could be used to improve (ISO) standards, guidelines or the way of working. Request experts to review the findings.

Step 7. Formulate findings, recommendations, conclusions, Discussions, etc.

§ 1.7 Research methodology

There has been very limited literature available on many of the research sub questions at the time of starting the research since the ISO standard ISO 27701:2019 we try to review has been released very recently and not many companies have extensive experience applying it. The same is valid for the detailed analysis of the type of GDPR violations. Therefore we have chosen for the research methodology type “Exploratory case study” as the best fit as research methodology.

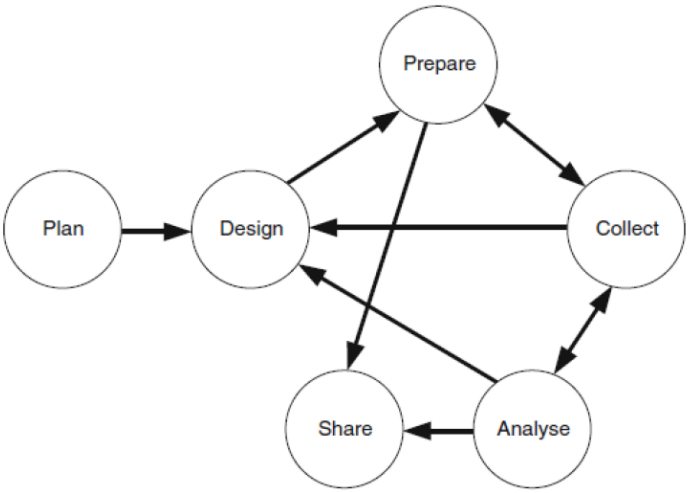


Figure 4: Exploratory case study scheme, Scientific Research in Information Systems (Recker, 2013)

(Recker, 2013)[7] shaped the exploratory case study research methodology as pictured above and that approach have been followed in this research.

First a research plan was drafted. The design phase exists of multiple steps like as a first step a quantitative analysis of the actual GDPR violations to identify the GDPR articles that were violated the most and with the highest financial implications. Subsequently a literature research will be performed on the ontology of a specific GDPR article, including the related governance and management risks and activities. As a third step a set of questions was designed to use in the questionnaire send to GDPR experts with experience in applying (ISO 2700X and other) standards.
As preparation the experts were chosen based on their expertise and experience with applying the GDPR in their working environment. The experts were given a few weeks to deliver their results (Collect phase).

A consolidation was done of the information collected (GDPR violation statistics, literature research, results of questionnaire, etc.) that is used as input for the next analysis: a fit/gap analysis of the ISO standard ISO 27701:2019 against the consolidated findings.

The recommendations for ISO 27701:2019 improvements and for further research will be formulated. These recommendations and findings will be shared with a small group of experts to give feedback on the formulated findings.

Limitations of the research
There are a limited amount of experts consulted to review the product of this research – this is not a representative set of data to draw final conclusions. The feedback of the experts on the suggested improvements is merely used as a first validation on the relevancy and practical use of the proposed improvements on ISO 27701:2019 (ISO, 2019).
Due to these limitations it is recommendable to further continue this research in order to gather more validated data.

[7] Source: Recker, Jan (2013) Scientific Research in Information Systems A Beginner's Guide [Book]. pp. 95-97) : Springer, 2013

2. GDPR violation risks – An analysis of the violation context and aspects

§ 2.1 Introduction

In this chapter we aim to give an answer to the following research sub questions:

- Quantitative analysis - what are the registered GDPR violations up to 03.2020?
- What are the most violated GDPR articles?
- What are the most violated GDPR articles with the highest financial implications?

Violation context:

- What are the ICT governance and -management requirements, guidelines and activities described by this GDPR article?
- What are the GDPR article aspects that are violated the most?
- What could be the possible root-cause for these violations seen from the ontology of the relevant GDPR article?

Complying with the GDPR requires in many cases a risk assessment regarding the way organizations are processing privacy relevant data and possible areas of non-compliancy. The difficulty with risk assessments in general is often determining the possible rate of the (risk) occurrence and (financial) impact of a materialized risk since statistical information is not always available on past incidents.
Fortunately we had at the moment this paper has been written, +/- 22 months after May 2018 when the GDPR can into force, useful statistical information available on how the Data Privacy Authorities (DPA) judged/fined non-compliance with specific GDPR articles so far. What lessons can we draw from these prior Data Privacy Authorities (DPA) enforcement actions? In this chapter we study the DPA's interpretation of the GDPR articles by closely scrutinizing its enforcement actions of the past years in order to identify the most frequent occurring GDPR violations with the highest financial implications, including the possible root causes seen from a data governance and management perspective.

§ 2.2 Analysis of materialized GDPR violation risk - analysis steps outlined

In order to get more visibility on the most violated GDPR articles/ & aspects so far we performed the following research steps:

1. Analyse the most common GDPR violations (period 4.2018 – 3.2020) published by the EU data protection authorities (DPA's) based on the GDPR Enforcement tracker.
2. Identify the most significant GDPR violations (period 4.2018 – 3.2020) in terms of the number of violations and highest fines imposed by the DPA's including the related GDPR articles that were violated. Select the GDPR article that is most frequently violated and with the most significant financial implications (highest sum of fines).
3. Analyse the text of this GDPR article using the ontological domain classification to identify the entities, their properties, rules and the relations between them described in the legislative text.
4. Map the description of the GDPR article violations described in the GDPR Enforcement tracker (period 4.2018 – 3.2020) against the ontological classification to identify the GDPR article *aspects* that were violated the most.
5. Identify possible root causes seen from a data governance and management perspective that could have led to the violation of this particular GDPR article/aspect.

§ 2.3 Data source of the history of GDPR violations/statistics

As main source of statistical data on GDPR violations and the related GDPR articles we used the "GDPR Enforcement Tracker" (https://www.enforcementtracker.com) (Law firm C|M|S, 2020) containing a list of fines and penalties which data protection authorities within the EU have imposed under GDPR.
Note that not all GDPR fines are made public, therefore the used data source can never be 100% complete – however it will give a good impression of GDPR violations in the EU.
Other data sources[8] are verified as well, however we selected the "GDPR Enforcement Tracker" (Law firm C|M|S, 2020) as the main source of information since it contains 230+

[8] See: https://www.privacyaffairs.com/gdpr-fines/ and (Retrieved at 05.2020) https://www.twobirds.com/en/in-focus/general-data-protection-regulation/gdpr-tracker/penalties

registered GDPR violations, including a good description of the GDPR articles violated and a brief description of the DPA violation findings and legal motivation.

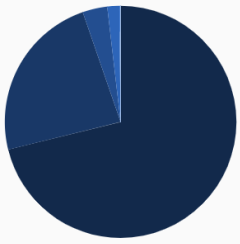
We will use the GDPR violation tracker [9] (Law firm C|M|S, 2020) for the further analysis of the GDPR violation (root)causes in terms of the identification of missing or failing (data) governance and (change) management activities.

§ 2.4 An first analysis of GDPR violations between 07.2018 and 03.2020

A summarised overview of the type of GDPR violation area's that seems to occur frequently can be found in the graph below. This overview shows the violation area versus the highest materialized financial risk per violation type.

Statistics: Fines by type of violation
The following statistics show how many fines and what sum of fines have been imposed per type of GDPR violation to date.

1. By total sum of fines:



Violation	Sum of Fines
Insufficient technical and organisational measures to ensure information security	**€ 332,845,127** (at 57 fines)
Insufficient legal basis for data processing	**€ 110,158,147** (at 95 fines)
Non-compliance with general data processing principles	**€ 16,165,370** (at 37 fines)
Insufficient fulfilment of data subjects rights	**€ 7,797,787** (at 22 fines)
Insufficient fulfilment of information obligations	**€ 557,265** (at 15 fines)
Insufficient fulfilment of data breach notification obligations	**€ 158,425** (at 6 fines)
Lack of appointment of data protection officer	**€ 61,000** (at 2 fines)
Insufficient cooperation with supervisory authority	**€ 48,511** (at 7 fines)
Insufficient data processing agreement	**€ 14,380** (at 2 fines)
Unknown	**€ 500** (at 1 fines)

Figure 5: GDPR Fines imposed by **type of violation and sum of fines** (status as per 03.2020)
Source: https://www.enforcementtracker.com/?insights viewed at 03.2020.

§ 2.5 Set research relevance & scope: GDPR article 32 / information security

The type of GDPR violation that occurred the *most frequently* up to 03.2020 seems to be "insufficient legal basis for data processing" (article 6), however the type of GDPR violation that has the highest sum of (publically published) fines imposed since the enforcement of the GDPR up to 03.2020 seems to be "insufficient technical and organizational measures to ensure information security" (article 32) see figure above.

When we review the motivation of the DPA's on what the specific GDPR articles are that are violated (see excel sheet of the GDPR enforcement tracker above for details), we see that the DPA's ruled that article 5 (1) f) and predominantly article 32 of the GDPR (European Union, 2018) were violated when they refer to the "insufficient technical and organizational measures to ensure information security".

Scope limitation and relevance: in order to limit the scope of this research we focus mainly on the analysis of the context around **GDPR article 32** (information security) since violation of GDPR article 32 has led to the highest cumulated fine of € 332.000.000+ (01.03.2020). This makes a better understanding of the requirements / context of article 32 very relevant.
Note: in the annex you find the data of the 53 article 32 violation cases we selected for this research from the GDPR violation database (Law firm C|M|S, 2020).

What are the specific requirements described in article 32?
We can find a full description of the legislative text here: https://gdpr-info.eu/art-32-gdpr/

Suitable recitals (detailed clarifications on law articles) of GDPR article 32 are:
(75) Risks to the Rights/Freedoms of Natural Persons, https://gdpr-info.eu/recitals/no-75/
(76) Risk Assessment, https://gdpr-info.eu/recitals/no-76/
(77) Risk Assessment Guidelines, https://gdpr-info.eu/recitals/no-77/
(78) Appropriate Technical & Organisational Measures, https://gdpr-info.eu/recitals/no-78/
(79) Allocation of the Responsibilities, https://gdpr-info.eu/recitals/no-79/
(83) Security of Processing, https://gdpr-info.eu/recitals/no-83/

[9] GDPR violation database collected and maintained by law firm C|M|S, see: (https://www.enforcementtracker.com)

§ 2.6 Requirements of GDPR article 32 identified using the GDPRtEXT ontology

Since the statistics have shown that GDPR article 32 has been violated frequently and resulted in a significant cumulative fine of € 332.000.000+ up to 01.03.2020, it is useful to understand more in detail what "Insufficient technical and organizational measures to ensure information security" actually means in practice. What are the *specific aspects* that were violated and how can we avoid it that we will face the same situation?

Just reading the legislative text of GDPR article 32 and the related recitals 75-79 and 83 will not always be sufficient for policy makers and management to actually *understand what is required*, what the *risks* are and how to *enforce and control the legislative requirements*.
A schematic (ontological) representation of the legislative text can be useful to clarify this.

One way to schematically represent information regarding a specific subject is by using a **domain ontology**. Domain ontology can be defined as a concept relevant to a particular topic, domain of discourse, or area of interest[10]
The **GDPRtEXT ontology,** developed by Pandit (Pandit, 2020)[11], and published in the open science community space, aims to provide in a way to refer and use concepts defined by the GDPR. SKOS - Simple Knowledge Organization System[12] – is used by Pandit to provide in "a model for expressing the basic structure and content of concept schemes".

The core expressions defined in the GDPRtEXT ontology are obligations and activities[13]:
Obligation -> These are the obligations specified by the GDPR.
Activity -> An activity signifies some process(es) or step(s) towards specific deed(s), action(s), function(s), or sphere(s) of action.

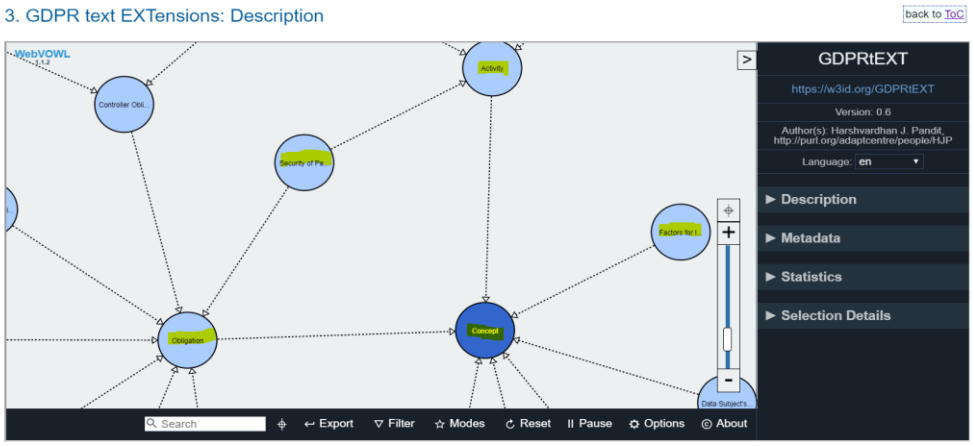


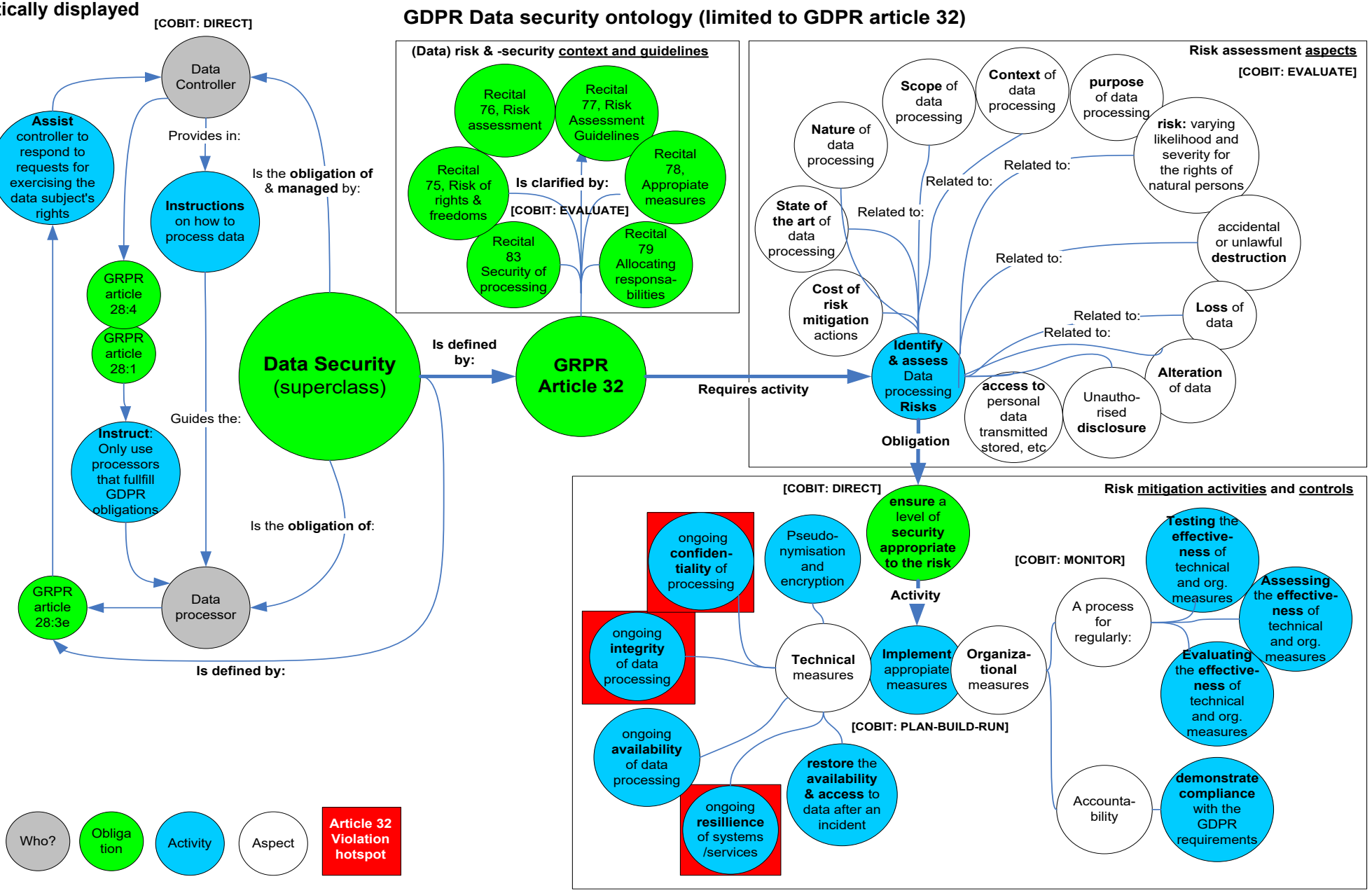
Figure 6**:** The GDPR ontology (Pandit, 2020) displayed as WebOWL
Source: https://openscience.adaptcentre.ie/ontologies/GDPRtEXT/deliverables/docs/ontology

Note: enterprise ontology (Dietz & Mulder, Enterprise Ontology, A Human-Centric Approach to Understanding the Essence of Organisation, 2020) and the DEMO model, lectured at the Antwerp Management School, are focused on the *enterprise and its transactions and processes*.
In this paper however we applied the concept of **domain ontology** as an instrument to break down and categorize the *legislative obligations, requirements and related activities* in a model for expressing and structuring the requirements of GDPR article 32.

We used the GDPRtEXT ontology (Pandit, 2020) as a basis to perform a further breakdown and enrichment of the structure, requirements, rules, etc. of GDPR article 32 (see next page). We have added some more contextual relations and objects to the GDPRtEXT ontology like "clarified by", "aspect", "defined by", etc. in order to provide in more contextual clarification.

[10] Source: https://en.wikipedia.org/wiki/Ontology_(information_science) and https://en.wikipedia.org/wiki/Ontology#Types
[11] Source: https://openscience.adaptcentre.ie/ontologies/GDPRtEXT/deliverables/docs/ontology (05.2020)
[12] Source: https://www.w3.org/TR/skos-primer/ (Retrieved at 05.2020)
[13] Source: https://openscience.adaptcentre.ie/ontologies/GDPRtEXT/deliverables/docs/ontology#DataSecurity

§ 2.7 The ontological view of GDPR article 32 schematically displayed



GDPR Data security ontology - developed based on GDPR ontology as published on https://openscience.adaptcentre.ie/ontologies/GDPRtEXT/deliverables/docs/ontology#DataSecurity

The GDPR article 32 ontology as displayed on the previous page helps us to break down and display the concrete article 32 obligations, activities, definitions, clarifications, actors and relations between them in a more schematic way.

This is probably useful to help policy makers and executive management to actually understand what is required in a more simplified and schematic way.
However, knowing **what** to do is often not sufficient. In the next step we try to categorize the GDPR article 32 obligations and activities in terms of **who** (governance and management roles) should do what (activities).

§ 2.8 Governance and management activities categorised using COBIT

There are different ways to categorize governance and management activities.
In this chapter we use ISACA's framework COBIT (ISACA, 2020) for the definition of governance and management activities, roles and responsibilities.
According COBIT one can classify governance and management in the following way:

Governance: *ensures* that enterprise objectives are achieved by *evaluating* stakeholder needs, conditions and options, *setting direction* through *prioritisation* and *decision making*, and *monitoring* performance, compliance, and progress against plans.
In most enterprises, governance is the responsibility of the board of directors under the leadership of the chairperson.

Management: *plans, builds, runs and monitors activities* in alignment with the direction set by the governance body to achieve the enterprise objectives. In most enterprises, management is the responsibility of the executive management under the leadership of the CEO.

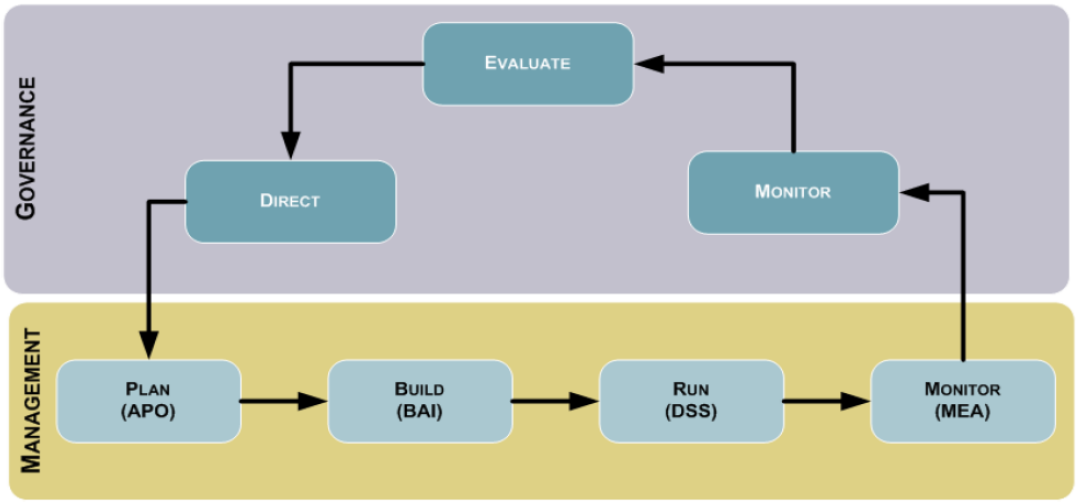


Figure 8: COBIT (ISACA, 2020) - Separation and interaction of governance and management [14]

When we applied the above mentioned COBIT definitions of governance and management activities to the enriched GDPRtEXT ontology (Pandit, 2020) in § 2.7 we can identify and map the specific COBIT governance and management activities mentioned in article 32.

It is interesting to see that some of the (governance and management) activity wordings used in COBIT, like "evaluate", "monitor" etc. are also used in the GDPR text.
We used that where possible to apply the related COBIT governance and management activity wording used to article 32 phrases (marked in green in the table on the next page).

Note: Although we can apply the governance and management *activities* defined in COBIT to the GDPR ontology, we will identify in chapter 3 if the governance and management *focus* mentioned in COBIT (serve enterprise objectives) are the same as formulated in the GDPR.

[14] Source ISACA: COBIT, governance and management - key roles and related activities (Retrieved at 05.2020) https://www.academia.edu/22135776/Governance_and_Management_in_COBIT_5_Key_Roles_Activities_and_Relationships

§ 2.9 Article 32 violations mapped against the ontology to find violation hotspots

In this step we have combined the GDPR article 32 ontology (as defined in § 2.7) and the categorization of COBIT governance and management activities (§ 2.8) in the table below.

Subsequently we have analysed the detailed article 32 violation case descriptions - 53 cases of article 32 violations in total - to identify the specific aspect(s) that have been violated.
In the annex you can find the violation case description (Law firm C|M|S, 2020) we used in the analysis. A detailed analysis of the violation case description gives us more insight regarding the specific article 32 violation aspects and their occurrence (hotspots - marked in orange).

GDPR article	**Obligations** (high level)	**Activities** (high level)	**Aspects** (contextual details regarding aspects to be considered when executing the activities)	**# of violations of article 32** reported (6.2018 – 2.2020) – see excel/annex	
				# Violations (per aspect)	**Case number** (see annex)
Article 32:1, 2 **Recital 75-79**	**(Governance)** **[EVALUATE]** **Identify & assess** data processing risks	**(Governance)** **[MONITOR EVALUATE]** **Identify / assess** data processing **risks** related to the following aspects:	**Cost of risk mitigation** actions		
			State of the art of data processing		
			Nature of data processing		
			Scope of data processing	1	33
			Context of data processing	1	33
			Purpose of data processing	1	33
			varying **likelihood and severity** for (violating) the rights of natural persons		
			Accidental or unlawful **destruction**		
			Loss of data		
			Alteration of data		
			Unauthorised **disclosure**		
			Access to personal data transmitted, stored, etc.		
Article 32:1a-c **Recital 83** **Recital 75-79**	**(Governance)** **[DIRECT]** **Ensure** a level of security appropriate to the risk	**(Management & operations)** **[PLAN,BUILD, RUN, MONITOR]** **Implement** appropriate **technical** measures, like:	Pseudonymisation, anonymization/encryption	1	38
			Implement ongoing **confidentiality** of processing	**43**	1,2,4-10, 12-16, 18, 20-23, 25-36, 38-48, 51-53
			Implement ongoing **integrity** of data processing	**14**	1,3,6,11,13,17,21,22, 35,36,38,40,42,47,48.
			Implement ongoing **availability** of data	2	18,19
			Implement ongoing **resilience** of systems / services	**8**	9,26,29,30,35,36,39,46, 53
			The **ability to restore** the **availability and access** to personal data after an incident		
Article 32:1d **Recital 75-79**		**(Governance)** **[MONITOR, EVALUATE]** **Implement** appropriate **organizational** measures	**Testing** the **effectiveness** of technical and org. measures	1	7
			Assessing the **effectiveness** of technical and org. measures	1	7
			Evaluating the **effectiveness** of technical and org. measures	1	7
Article 32:3			**Demonstrate compliance** with the GDPR requirements	1	1
Article 32:4 **Recital 75-79**		**(Governance)** **[DIRECT, MONITOR]** Provide in data processing instructions and oversight	Data controller **instructs (in writing)** the processor on **how to process the data**	1	15
			Data controller must **ensure** that **processor processes the data according instructions**	1	15

Table 1: the domain *ontology* of GDPR article 32 mapped to the *violation aspects* / cases of article 32
Annex: data (53 cases) used for the analysis of article 32 violation hotspots.
Orange marked = Article 32 violation hotspots (high number of violation occurrences)

Based on the 53 case rulings describing the context of the article 32 violation more in detail, we have isolated the top 3 of most occurring violation aspects (hotspots). These are:

1. Failing to realize ongoing **confidentiality** of processing: 43 violations
2. Failing to realize ongoing **integrity** of data processing: 14 violation
3. Failing to realize ongoing **resilience of systems / services**: 8 violation

We have updated the ontological scheme of article 32 in § 2.6 with these "violation hotspots".

Looking at the *type of activities* (according the categorization governance or management activities as used by COBIT (ISACA, 2020)) we see that the violations are mainly concentrated around (failing or ineffective) management activities like PLAN-BUILD-RUN-MONITOR.

Please note that the mapping of the violation aspects mentioned in the DPA ruling to the ontological scheme and COBIT categorization of type of activities (governance or management activities) is a matter of interpretation of the case text (see Annex).
In this process we try to map carefully specific wordings used in the ruling text to similar wording used in the ontology / GDPR text and COBIT.

Classification of (type of) governance and management activities according COBIT		Type of activities that failed per violation case
Governance activities (COBIT view)	[MONITOR]	4
	[EVALUATE]	
	[DIRECT]	
Management activities (COBIT view)	[PLAN]	50
	[BUILD]	
	[RUN]	
	[MONITOR]	

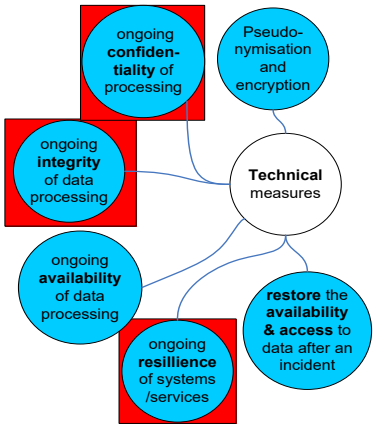


Table 2**:** Article 32 violation – type of activities (COBIT) and violation hotspots (Ontological view)

Now we have isolated the top 3 of most frequently violated aspects of article 32 (failing to realize ongoing **confidentiality, integrity and resilience of systems and services)**, it is useful to specify more in detail what those terms means in practice. A whitepaper of ISACA "how to audit GDPR" [15] provides in a good clarification of those terms:

Confidentiality (of privacy relevant data/data-processing).
In the context of GDPR, confidentiality is about privacy. The purpose of this principle is to ensure that data are accessible only to people who are authorized to access it.
For example, a patient's medical history is something the patient normally wants kept private, so only a few people, such as a doctor treating the patient, should have access to it.

Integrity (of privacy relevant data/data-processing).
GDPR requires data to be accurate and up to date. Enterprises should avoid making multiple copies of the data where possible and should also be wary of *enriching the data in a way that extends beyond the stated purpose of the data's collection and processing*. The requirement that the controller should be able to demonstrate that the purpose has not been extended adds an extra facet.

Resilience (of systems/processes used to process privacy relevant data).
Resilience of a system allows it to cope with security threats, rather than failing critically. Systems and processes should be designed and operate in a way that they are resilient to events that can cause a breach of GDPR data privacy principles like data availability, integrity, confidentiality, etc.

[15] Source: https://www.isaca.org/bookstore/bookstore-wht_papers-digital/whphag (Retrieved at 05.2020)

§ 2.10 Lagging & leading indicators: from symptom back to the possible root cause(s)

It is interesting to see that +/- 92,5% of the 53 cases describing article 32 violations are classified as "failing to *implement* appropriate technical measures" (*management* activities). In only 4 out of 53 cases listed in § 2.8, the DPA points to the violation of activities that can be related to *governance* like "failing to give instructions", "failing to test, assess, evaluate and document the effectiveness of measures taken" or "failing to assess risks related to the scope, context or purpose of data processing".

The DPA's rulings summarized: the DPA mainly fines the **visible symptoms** of GDPR non-compliancy (materialized risks - not having the appropriate technical measures mentioned in article 32 in place) rather than describing the underlying root cause of those symptoms like e.g. failing privacy governance or ineffective management activities.
The DPA basically *measures the performance* (output) of GDPR compliance against the KPI's defined in article 32, but not the root cause (input) leading to GDPR non-compliancy.

For an organization it is relevant to understand the *root cause leading to* non-compliance or under-performance instead of focussing only on and repairing the visible symptoms.

The performance management theory often refers to "lagging" and "leading" indicators. (Poel, 2012)[16] describes that lagging indicators are typically "output" oriented, easy to measure (like a GDPR violation) but hard to improve or influence.
Leading indicators are typically input oriented, hard to measure and easy to influence.

If we combine the ontological view of article 32, COBITs classification of governance and management activities with the "lagging" and "leading" indicators, we can see some correlations in the following picture below that can help us to identify the possible root cause(s) leading to non-compliance with the GDPR (under-performance).

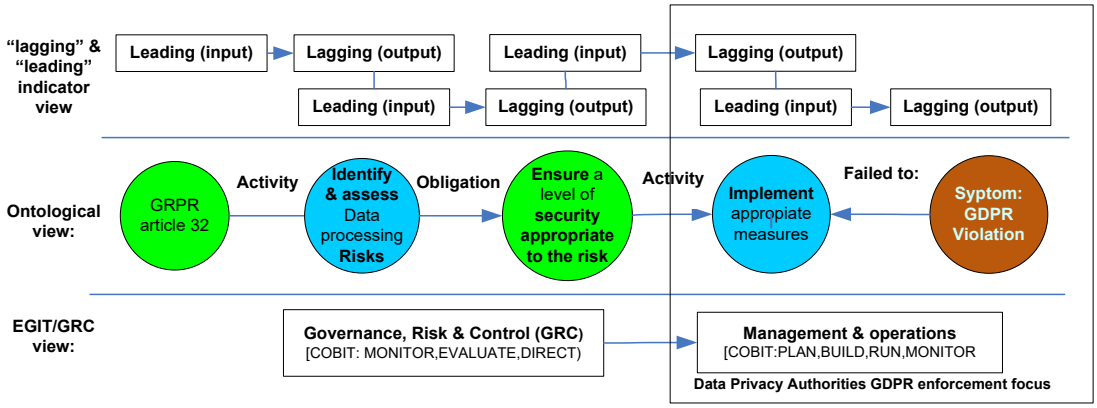


Figure 9**:** mapping KPIs, governance and management activities to the high level GDPRtEXT ontology

Leading indicators are often related to the (under)performance of activities undertaken by employees. In our example of the **visible symptoms** of GDPR non-compliancy, we can verify the different (cascaded) leading indicators that leaded to this symptom.
The relevant leading indicators for not having **effective technical or organizational (risk mitigating) measures** *could* be the underperformance of one or more of the following aspects: missing or failing **governance** (direction) and/or **controls** (assurance).
The relevant leading indicators for not having governance (direction) and/or controls & assurance in place *could* be a failing or missing **risk assessment** possibly triggered on its turn by a failing governance process.
The **root cause chain** could for example in some cases look like this: failing governance could lead to no or insufficient risk identification (no GDPR risk awareness) that on its turn leads to no drive to focus on risk mitigation and risk controls that on its turn probably results in not having implemented the appropriate GDPR measures at all that on its turn could lead to non-compliancy / fines. The root cause chain is likely to be a complex set of interconnected factors that could lead to non-compliancy. In the next chapters we will focus on the identifications of the different possible root causes and "lagging" and "leading" indicators for relevant governance and management activities.

[16] See: https://kpilibrary.com/topics/lagging-and-leading-indicators (Retrieved at 05.2020)

§ 2.11 Chapter summary

In this chapter we answered the following research sub question:

Question 1
Quantitative analysis - what are the GDPR violations registered up to 02.2020?
Summarized findings: the GDPR violations (period 6.2018 – 3.2020) published by the EU data protection authorities (DPA's) can be identified in the GDPR enforcement tracker published by law firm C|M|S. 236 violations are published by the different data privacy authorities in the EU according C|M|S in this timeframe although this is not a complete list of all violations. Not all DPA rulings are available to the public or centrally registered.

Question 2
What are the most violated GDPR articles?
Summarized findings: the type of GDPR violation that occurred the *most frequently* up to 03.2020 seems to be "insufficient legal basis for data processing" (article 6).

Question 3
What are the most violated GDPR articles with the highest financial implications?
Summarized findings: C|M|S grouped the GDPR violations by types of violations, like "insufficient legal basis for data processing" and refers to the related GDPR articles that were violated. C|M|S also documented the imposed fines (*materialized* financial risk) per violation. Based on that information we could identify that the type of violation ("insufficient technical and organizational measures to ensure information security") referring to the violation of GDPR articles 5 and 32 has led to the highest cumulated fine of € 332.000.000+ (at 01.03.2020).
These findings basically determined the further scope limitation and focus (relevance) of our research. A better understanding of the requirements / context of article 32 can contribute to the reduction of (high financial) risks related to the violation of article 32.

Question 4
What are the ICT governance and -management requirements, guidelines and activities described by this GDPR article?
Summarized findings: based on the analysis of the GDPR ontology we could identify a list of detailed activities and the aspects to consider. We have categorized these according the by COBIT defined governance and management (type of) activities:

1. [Governance] [MONITOR, EVALUATE]
   Identify / assess data processing risks related to different aspects
2. [Governance] [DIRECT]
   Ensure a level of security appropriate to the risk
3. [Management] [PLAN,BUILD, RUN, MONITOR]
   Implement appropriate technical measures
4. [Governance] [MONITOR, EVALUATE]
   Test, assess, evaluate the effectiveness of technical and org. measures
5. [Governance] [DIRECT, MONITOR, EVALUATE]
   Instruct (in writing) how to process the data and **ensure** this is done accordingly

In this overview of article 32 activities we clearly recognize the Plan-Do-Act-Evaluate cycle.

Question 5
What are the article aspects that were violated most frequently?
Summarized findings: Just reading the legislative text of GDPR article 32 and the related recitals 75-79 and 83 will not always be sufficient for policy makers and management to actually understand what is required and what the risks (mitigation) aspects are.
A more schematic representation of the legislative text can be very useful to visualize this and we applied/enriched the GDPRtEXT ontology to break down and categorize the concrete article 32 obligations, activities, definitions, clarifications, actors and relations between them.

Subsequently we have analysed the C|M|S violation database detailed case description to identify and map the ontological article 32 *aspect(s)* that have been violated in detail.

Of the 53 cases describing the violation of article 32 in detail we isolated the top 3 of most occurring violation aspects hotspots mentioned in the rulings of the DPA's.

Failing **confidentiality** of processing: **43 violations**
Failing ongoing **integrity** of data processing: **14 violations**
Failing ongoing **resilience** of systems / services: **8 violations**
Based on the case description, we identified that 50 (of 53 cases) can be related to failing or ineffective) privacy **management** activities like PLAN-BUILD-RUN-MONITOR (COBIT view).

Question 6
What could be the possible root-cause for these violations seen from the ontology of GDPR article 32?

Summarized findings: the DPA's mainly fines the **visible symptoms** of GDPR non-compliancy (materialized risks - not having implemented the appropriate technical measures mentioned in article 32) rather than fining and describing the underlying root cause of those symptoms.
Looking at the *type of activities* (according the governance or management activity classification as used by COBIT) we see that the violations are mainly concentrated around (failing or ineffective) **privacy management** activities like PLAN-BUILD-RUN-MONITOR.

In order to identify the possible root-causes, we identified the possible different (cascaded or chained) leading & lagging indicators that possibly have led to the (operational) violation.

The relevant leading indicators for not having implemented the technical measures *could* be missing governance (direction) and/or governance and/or technical controls (assurance).
The relevant leading indicators for not having governance (direction) and/or controls & assurance in place *could* be a result of failing or absent risk assessment (no risk awareness).

In the next chapters we will focus on the identifications of the different possible root causes and change management aspects for relevant governance and management activities.

3. GDPR article 32 – Analysis of potential change management risks related to privacy governance and management activities

§ 3.1 Introduction

In chapter 2 we identified that the article 32 aspects that were violated most frequently were "failing to ensure ongoing **confidentiality, integrity** of data processing and **resilience** of systems / services" leading to an accumulated fine up to of € 332.000.000+ (measured at 01.03.2020). We also identified that the data privacy authorities (DPA's) mainly fines the **visible symptoms** of GDPR non-compliancy (the *materialized* risks) rather than fining and/or describing the underlying root cause(s) of those non-compliancy symptoms like e.g. failing to analyse the data processing risks, a lack of governance or controls, etc..

In this chapter we aim to give an answer to the following research sub questions:

- What are the perceived (data privacy) governance and change management challenges / risks and gaps companies could / are facing?
- What are the possible ambiguities in the legislative text of this GDPR article and how to address them?
- What could be the possible root-causes for the occurred violations?

§ 3.2 Compliance with the GDPR seen from a change management perspective

In this chapter we aim to learn more about the *specific* privacy governance and (change) management risks and pitfalls, the specific guidance provided by the GDPR legislative text and if possible ambiguities in the legislative text that could contribute to non-compliancy.

We applied elements of the "mind the gap" change management model pictured below to identify certain change management aspects and pitfalls (both on governance and management or operational level). Change management in general is an important factor for successfully changing the organization, thus also in the context of GDPR.
We used Meyers "mind the gap" model below, with a focus on the red boxed aspects.

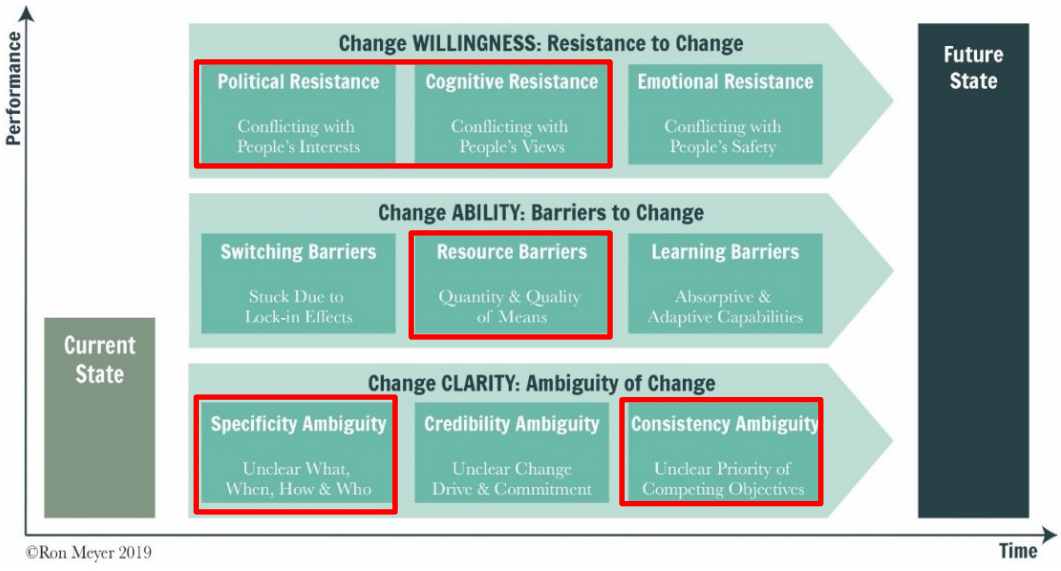


Figure 10 : Change management aspects. Figure reused from Meyer's Management Models.
Mind the Gap', (Meyer, 2019):https://blog.antwerpmanagementschool.be/en/ron-meyer-episode-1-mind-the-gap

Meyer identified different change barriers (Meyer, 2019) that could also influence the road to compliance with the GDPR and we will therefore have a look at the following change management aspects:

Specificity ambiguity.
Often the change itself (comply with the GDPR) hasn't been made tangible enough to act upon. It is unclear what needs to be done, when, how and by whom.

Consistency ambiguity.
GDPR related changes may also be inconsistent with the stakeholders' other priorities. This can lead to un-clarity as to what (competing) objectives should be given priority to.

Resource barriers.
Organizations may lack the necessary tangible resources, e.g. money, and/or intangible resources, e.g. (GDPR implementation) knowledge, skills, relations and mind-set.

Political resistance.
Going along with the changes may not be in people's perceived interest.
Their resistance is then a rational and calculated response to a potential loss.

Cognitive resistance. Going along with the changes may go against people's views on what should be done. They resist because they believe the proposed changes don't make sense.

---

§ 3.3 Change willingness - The principle / agent theory

When we want to answer the sub question - What are the perceived (data privacy) *governance* and (change) management *challenges / gaps* companies could face? – it might be useful to have a look at the history of corporate governance in general and the different types of governance risks including the role and influence stakeholders have in the context of corporate risk.

(Dallas, 2004) [17] addresses the problem of "agency risk" (or "principle-agent-problem"). According Dalles, in the early years of the Industrial Revolution, ownership and management were often inseparable - one single 'principle' steered the 'agents'.

However, in larger and complex organizations the founder-owner-manager combination nowadays hardly exists – we often can identify multiple 'principles' and as well as 'agents'. As a practical matter, ownership and management are separated. Retail and institutional investors own stocks in enterprises, but they do not exercise effective supervision or oversight of those enterprises – that's the task of C-level executives who on their turn steer the operational activities of the organization using one or multiple management layers.

Dallas also distinguished two categories of corporate governance risk:

- **Internal and firm-specific** — this type of risk focusses on takeover defences, shareholder voting and shareholder rights, audit and accounting issues, board independence, executive pay, risk management, etc.

- **External and systemic** —this category addresses law/legislation, compliance, the structure of ownership, policies with respect to labour and product markets, and so on.

Although the "principle-agent-problem" theory has been criticized in different ways (e.g. you can't control every risk with contractual agreements), the theory did have an ongoing and influential role as a framework for establishing the roles of principals (those setting directions and driving changes) and agents and, in turn, for managing policy development and

---

[17] Source: Dallas, G.S. (2004). Governance and Risk: An Analytical Handbook for Investors, Managers, Directors, and Stakeholders. https://www.semanticscholar.org/paper/Governance-and-Risk%3A-An-Analytical-Handbook-for-and-Dallas/c980bbb058c4d5a4c052e8b493489160932439f4 (Retrieved at 05.2020)

implementation. We used the principle-agent framework and the categories of corporate governance risk as an viewpoint to look at the complexities related to the governance and management of data security and privacy in organizations.

Corporate governance risks - increase of external and systemic risk factors.
In the context of the rise of new data privacy legislations like the GDPR, CCPA, etc. we can indeed say that the *external and systematic* (corporate governance) risks of e.g. non-compliance with new privacy legislation has increased over time, including the financial risks in terms of high GDPR fines imposed since May 2018 as discussed in chapter 2.
Data privacy governance is clearly a relevant (corporate) governance topic, but how to look at the relevant stakeholders in this context?

The "principle-agent-problem" mapped to data security and data privacy
A well-known 'agent' serving the digital interest of *the company* (the 'principle') by protecting the companies digital assets is often the CISO (Corporate Information Security Officer). However, due to new legislation like the GDPR we also see a new type of 'agent-principle' relationship occurring, namely the *individual* gaining more influence (via legislation like the GDPR) on how companies must handle their digital assets in case it contains privacy relevant personal information – a more outward looking view.

Due to these new kind of stakeholders, backed by a 'super principle' (the legislator), we also have seen new roles (or 'agents') like the DPO (or Data Privacy Officer) occurring in the organization, focussed on safeguarding the interest of this new 'principle': the *individual* and its privacy rights (with the focus on conformance).

This new reality with different types of 'agents' organized in different roles like the CISO and the DPO and different 'principle's' like the company owners and/or shareholders versus the individual backed by the legislator makes (IT) governance and management much more complex and multi-faceted as displayed in the figure below.

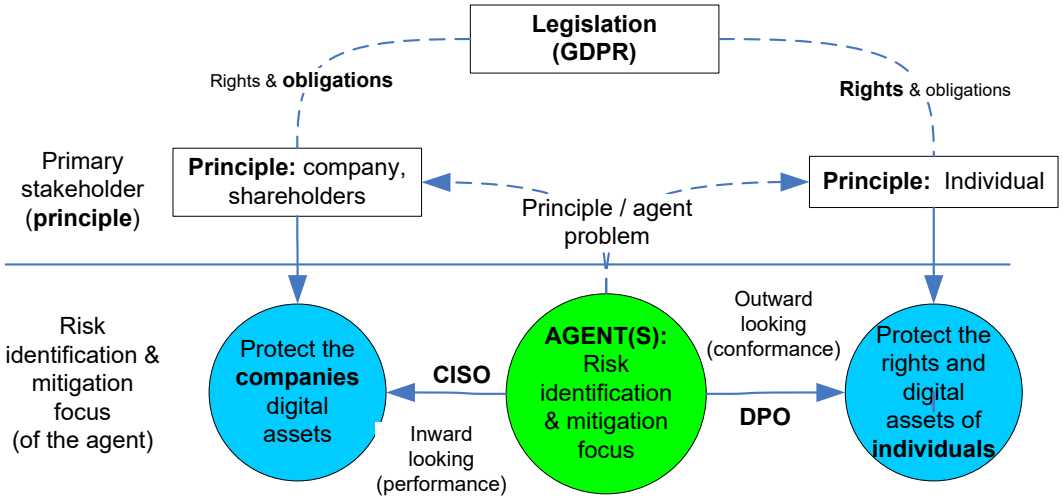


Figure 11 **:** (data) governance - more complex & multi-faceted due to multiple principle/agent relations

(Friedman & Darrell , 2010) [18] also applied the principle-agent theory to the context of Privacy and Security and stated that we can identify different "Threat Vectors" and related principles and agents. Due to new technology and legislation, new threat vectors are introduced, and old ones can be exploited in new ways.

[18] Source: Friedman.A, West,D (2010). Privacy and Security in Cloud Computing, Center for Technology Innovation at Brookings http://ent.cs.nccu.edu.tw/drupal/files/privacySecurityInCloudComputing(Brookings).pdf (Retrieved at 05.2020)

§ 3.4 Change willingness - Pairing divergent interests and risk views

The identified principle-agent problem can also being mapped to Meyer's "mind the gap" model, and we can identify here three change barriers formulated by Meyer that could influence compliance with the GDPR in a negative way:

Political resistance. Going along with the new privacy governance and management changes may not be in some people's perceived interest. Take the CISO as an example. Since the risk awareness of a CISO is often more internal and firm-specific focussed (protecting the *companies* digital assets) compared to the DPO who has a focus on risks mitigation and conformance related to the *individual* and its privacy rights, we have a risk of conflicting interests.

Cognitive resistance. When people in the organization have different perceived interests, they probably also tend to focus on different activities and changes may go against people's views on what should be done. They resist because they believe the proposed changes don't make sense from their perspective.

Consistency ambiguity. When we are facing cognitive resistance from the different stakeholders involved in achieving compliance with the GDPR we are risking consistency ambiguity both on governance as management level. This can lead to un-clarity as to what (competing) objectives should be given priority to.

Summarized: to implement a complex change successfully, like in this case complying with the GDPR, there is more needed than a technical plan on how to go from "as is" to "to be". In achieving the difficult balance between data privacy and data security, a position in which we often find ourselves at the moment, it is important to realize that we are dealing with different principal-agent relations with divergent interests (*political resistance*), different roles, tasks and cognitive views (*cognitive resistance*) as pictured at the previous page.
If we face that situation, we are at risk to steer and/or act inconsistently regarding our data privacy governance and management activities and priorities due to competing objectives of different stakeholders (consistency ambiguity).

It is of vital importance to identify these type of change management risks and take action to close these "gaps" even before you start with the implementation of a privacy program.

§ 3.5 Change clarity - Identify potential ambiguity in the text of article 32

Meyer (Meyer, 2019) also mentioned another possible change management barrier: **specificity ambiguity**. We are at risk that the change itself (e.g. comply with the GDPR) hasn't been made tangible enough to act upon. It might be unclear what needs to be done, when, how and by whom.

The legislative text itself is unfortunately not always helpful in understanding "what needs to be done". Take one example of a GDPR requirement in article 32 regarding the "security of processing". Article 32 simply begins with "taking into account.. the state of the art". However, what to do if you don't know the "state of the art", and who has the ability to recognise it?
Other article 32 phrases[19] like "taking into account", "varying likelihood", "severity" "appropriate measures" and "take steps" can be seen as very ambiguous and leave room for interpretation. One could ask: what does the legislator means exactly with these phrases and how can companies comply with these "requirements" that can be interpreted in different ways?
Let's start with taking a view on the possible reasons why ambiguity can be found in the legislative text of the GDPR. One reason is that the speed of technological change and innovation, including new ways to use privacy relevant data, makes it difficult to be *prescriptive in detail* about data protection (implementation) activities, since that could become outdated as soon new technologies or ways to use personal data are introduced. (Lokin, 2018)[20] describes that the language model used to formulate law articles is mainly focussed on **rights** and **obligations** of **actors** and the relevant **conditions and variables**

[19] See article 32 text: https://gdpr-info.eu/art-32-gdpr/ (Retrieved at 05.2020)
[20] See: https://research.vu.nl/en/publications/wendbaar-wetgeven (Retrieved at 05.2020)
Full dissertation: https://research.vu.nl/ws/portalfiles/portal/69432703/complete+dissertation.pdf

these are valid for (see page 159-174, wendbaar wetgeven), however there are (almost) no concrete guidelines given on *how* this should be implemented in ICT systems.
More specific regarding the way the GDPR text has been defined, Lokin writes at page 22 of the same article that the GDPR provides in **design principles** that are applicable for ICT systems used to process privacy relevant data however there are (often) no ready to use ICT solutions available that fit to these formulated design principles.

What could be a reason for the ambiguity found in the GDPR?
One reason is that some level of ambiguity is unavoidable to make the law "future proof" to some extend – the GDPR has been developed in a way it can keep up with the much fast(er) advancing technology.
As a result of that most parts of the GDPR are formulated in a "technology agnostic" way, and as a consequence of that some ambiguity has been introduced in the GDPR.
The good thing about that approach is that you can apply GDPR governance and design *principles* (instead of detailed, prescriptive and possible quickly outdated hard "rules") to the many different software solutions, applications, data sources, cloud solutions, etc. etc.

A downside however of having legislative *directive principles* is that these principles must be understood and applied correctly. This requires not only a proper understanding of the privacy principles, they must be "translated / interpreted" to *company policies (IT governance)*, the policies on its turn must be translated to *procedures and guidelines* (IT management) that are *tailored & implemented to operate in specific IT* solutions.
In this process GDPR principles and guideline aspects could be lost or misinterpreted.

§ 3.6 Change clarity - the different types of ambiguity and how to address this

How can we reduce the possible ambiguity found in the legislative text?
First of all a better understanding of the different types of ambiguity helps us a bit further.

What is ambiguity actually (not)?
One definition of ambiguity that could be used is this one: **"**ambiguity is something liable to more than one interpretation, explanation or meaning, if that meaning cannot be determined from its context"[21]. Still, when we use this definition, it is useful to investigate some nuances of the word ambiguity.
Ambiguity is similar to the idea of uncertainty but they have different aspects.
Uncertainty is when *relevant information is unavailable and unknown*, and *ambiguity* where relevant information *is available but the overall meaning is still unknown*.

This problem of ambiguity (in the design specification) is not new and well known to software engineers who need be able to reliably determine whether software requirements meet or exceed their legal obligations.
In a study conducted by (Massey , 2014) [22] it became clear that ambiguity is prevalent in legal texts, but with the use of an ambiguity taxonomy as a guideline, it is possible to recognize and classify this.
According to the definition of the Stanford Encyclopaedia of Philosophy (Sennet, 2016) [23] there are many different types of ambiguity - however we limited this to two applicable examples for our use case: **under specification** and **contextual ambiguity** found in GDPR article 32.

Context sensitivity as a type of ambiguity
The Stanford Encyclopaedia of Philosophy (Sennet, 2016) describes it like this: *context sensitivity* is the "(potential) variability in content due purely to **changes in the context** of utterance without a change in the convention of word usage".

Specificity ambiguity (under specification)
Another type of ambiguity mentioned by Stanford Encyclopaedia is **under specification.**
As an example to clarify under specification, the Stanford Encyclopaedia used this example: "If I tell you that I am going to visit one of my sisters, what I say underspecifies which sister I

[21] Source: Wikipedia, description of ambiguity: https://en.wikipedia.org/wiki/Ambiguity
[22] Source: https://doi.org/10.1109/RE.2014.6912250 (Retrieved at 05.2020)
[23] Source: Stanford Encyclopaedia of Philosophy: https://plato.stanford.edu/entries/ambiguity/#UndeSpecGene

am going to see. This can be frustrating if you are trying to figure out where I am going. But this doesn't make 'I am going to visit one of my sisters' ambiguous. Its meaning is clear. The sentence is 'sense-general'; it *fails to specify some detail* without thereby being ambiguous with respect to that detail."

If we want to reduce the perceived ambiguity in the GDPR text, we need to apply the process of **disambiguation**[24] (identifying which meaning of a word is used in context).
In the table below we classified the types of ambiguity found in article 32 and the required activities to reduce the perceived ambiguity.

Phrase used in article 32	Type of ambiguity	Disambiguation activity
"*taking into account*"	context sensitive	Perform (contextual) analysis
"varying *likelihood* of risk"	context sensitive	Perform (contextual risk) analysis
"*severity*"	context sensitive	Perform (contextual risk) analysis
"*appropriate* measures"	context sensitive and under specification	Perform (risk)analysis used to formulate concrete requirements and/or measures
"*take steps*"	under specification	Specify concrete measures addressing the before mentioned risks and context

Table 3: article 32 wording applied to YOUR specific contextual situation reduces ambiguity

Summarized: if we want to reduce the perceived ambiguity in the GDPR text, we need to apply the process of disambiguation.
The steps to reduce ambiguity are:
1) perform a (contextual/risk) analysis of **your data processing activities** and
2) formulate concrete steps that addresses the contextual usage of privacy relevant data and the **related data processing risks** relevant for your specific organization.

The GDPR domain ontology (Pandit, 2020), discussed in chapter 2, addresses all the contextual (risk)analysis aspects we need to consider.
The identified risk and data processing context can be mapped to the relevant risk mitigation activities listed in article 32. These activities on their turn must be mapped to the technological context and possibilities of the data processing systems we use in our organization.

In short: the perceived ambiguity does not occur in the semantics of the GDPR text as such. It can be found in the (to the legislator unknown) organizational *data processing context* and data processing *risks*. A proper context and company specific data processing risk assessment will reduce this ambiguity – basically putting the requirements in context.

§ 3.7 Change barriers – The gap between privacy function and -construction

Once the perceived ambiguity has been reduced and the organizational data processing context and data processing risks are identified, and we understand **what** "the right things to do" are to comply with the GDPR we might stumble upon the next barrier: **how to** implement this, what "the right things to do" are in a practical sense.

One important hurdle to translate privacy governance into effective privacy management and operations is the function construction gap – the inability to bridge the gap between "know *what* to do" (function) to "know *how* to do this" (construction).
Bridging this gap requires a different type of knowledge, mind-set and skillset and this gap can be seen as a change management "resource and cognitive barrier" (Meyer, 2019).

Resource barriers. Organizations may lack the necessary tangible resources, e.g. money, and/or intangible resources, e.g. *knowledge, skills, relations and mind-set*.

Cognitive resistance. Going along with the changes may go against *people's views on what should be done*.
(Hoogervorst, 2009)[25] also refers to this barrier or gap between governance and management: "too often, enterprise attention is limited to the functional perspective: **what**

[24] Source: Wikipedia, description of dis-ambiguity:: https://en.wikipedia.org/wiki/Disambiguation_(disambiguation) (Retrieved at 05.2020)

[25] Source: https://www.springer.com/gp/book/9783540926702 (Retrieved at 05.2020)

the enterprise should do is in focus, whereby attention for ***how*** the requirements must be realized is virtually absent. The core reason for strategic failures, confirms this observation".

Dietz[26] pictures these different cognitive perspectives in the figure below by separating the ontology and functional (requirements) view from the way the solution is constructed (Dietz, 2006).
We can apply this viewpoint also to data privacy: the **GDPR domain ontology** delivers **functional requirements** (the white box) however to the legislator, C-level executive and business it is often a black box **how the solution should be or is constructed** in the context of a particular IT environment.

Architectural processes are needed to analyse, synthesise the (GDPR) requirements, design and construct it in a way that fits to a particular system or technological context.
Here we could also face another change barrier, cognitive resistance: the different viewpoints of stakeholders responsible for the privacy function versus its construction.

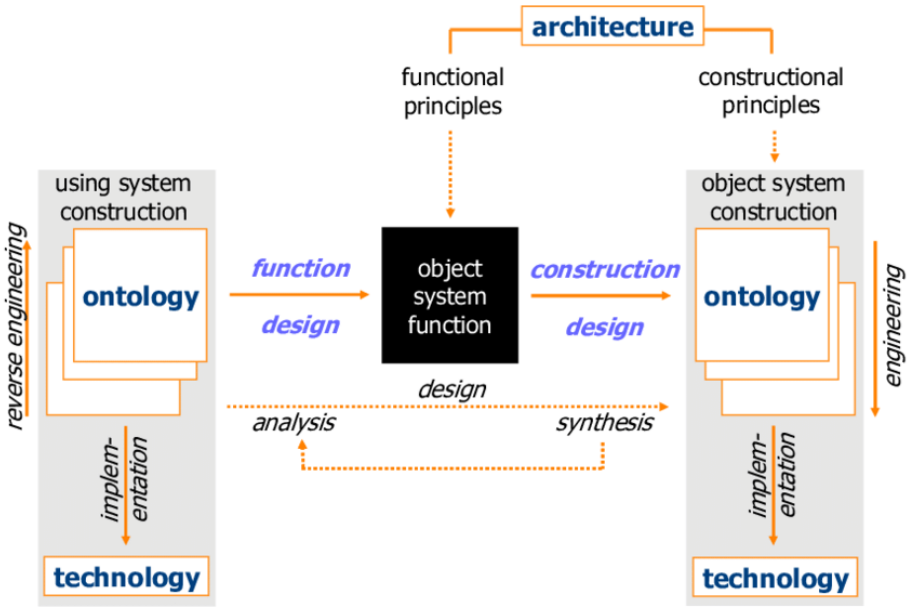


Figure 12: Design process and architecture (Dietz, 2006)

If the translation of the privacy function to its construction is not carefully aligned, it could become a possible root-cause for violations seen from the ontology of the relevant GDPR article. For effective privacy management, a good understanding of the difference between the privacy function versus its construction and bridging the gap between them using (security and privacy) architecture is important.
Requirement analysis & synthesis are important instruments to validate the design of technical (privacy) measures against the formulated requirements.

The GDPR describes the **privacy function**, **not** the **construction of that function.**
A (ongoing) translation, (re)design & synthesis and (privacy) architecture is needed to come from the privacy ontology and required functionality to the construction of that required privacy functionality in a particular IT environment.
Violation of the GDPR and possible fines are mainly related to a failing construction of the privacy function (not failing to *know what* we need to do, but *failing to implement/execute it*).

[26] Source: https://www.springer.com/gp/book/9783540291695 (Retrieved at 05.2020)

§ 3.8 GRC: an integrated approach to GDPR related change management

Dealing with different **principals with divergent interests**, **skills and risk viewpoints** (§ 3.3 and § 3.4) requires an integrated approach combining the risk, governance and compliance aspects.
The perceived **GDPR ambiguity** (§ 3.5) mainly lies in the (to the legislator unknown) **organizational data processing context and risks** (§ 3.6), that must be analysed first in an integrated way balancing the organizations risks and risk mitigating activities from the different perspectives of different stakeholders.
Once the organization has clarity and alignment on the privacy and security risks and understands what "the right things to do" are (governance, shaping the privacy function) it must bridge the (resource) barrier to execution, to "do the things right". This requires a translation & synthesis to come from the privacy ontology and required functionality to the construction of that required functionality in a particular IT environment. (§ 3.7).
One helpful instrument to combine and align these different challenges is GRC.

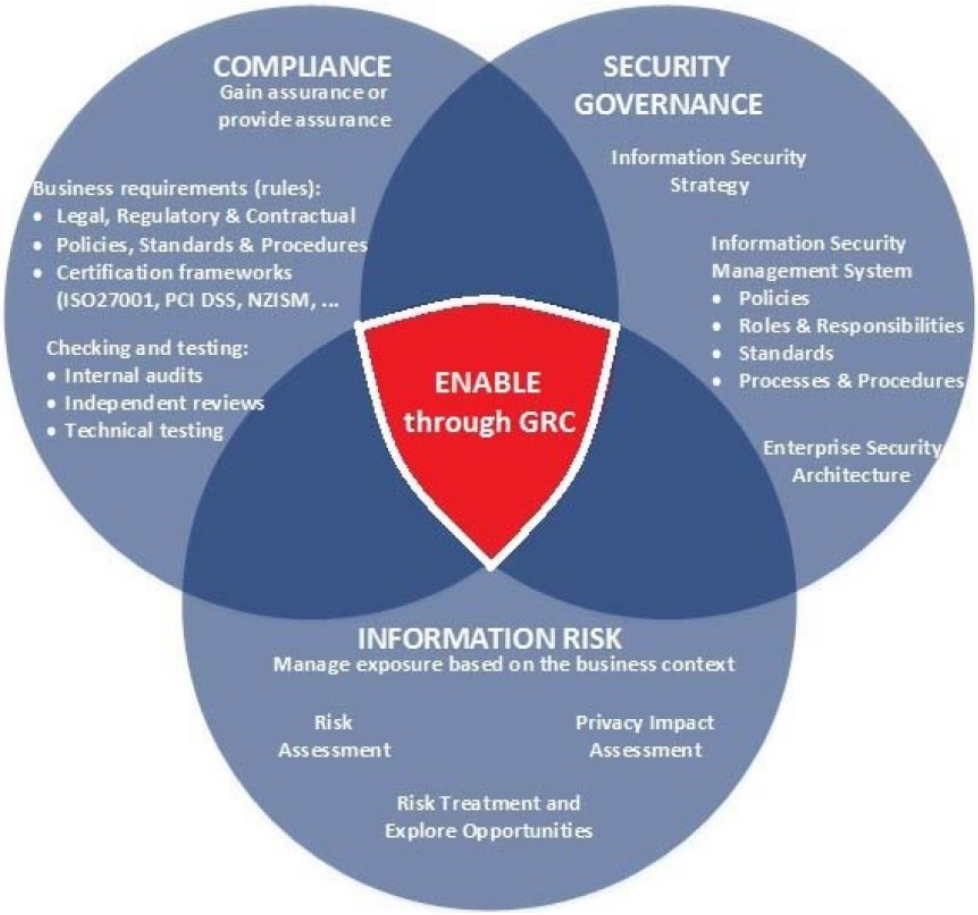


Figure 13: GRC - combining governance, risk and compliance

GRC[27] is a discipline that "aims to synchronize information and activity across governance and compliance in order to operate more efficiently, enable effective information sharing, more effectively report activities and avoid wasteful overlaps.
GRC is an integrated, holistic approach to organisation-wide GRC ensuring that an organisation acts ethically correct and in accordance with its risk appetite, internal policies and external regulations through the alignment of strategy, processes, technology and people, thereby improving efficiency and effectiveness.". Each of the core disciplines – Governance, Risk Management and Compliance – consists of the four basic components: strategy, processes, technology and people. In the next chapter we will look at these aspects (strategy, processes, technology and people) from a COBIT perspective.

[27] Source: https://en.wikipedia.org/wiki/Governance,_risk_management,_and_compliance (Retrieved at 05.2020)

§ 3.9 Chapter summary

Question 1

What are the perceived (data privacy) governance and change management challenges / risks and gaps companies could / are facing?

Summarized findings: To implement a complex change successfully, like in this case complying with the GDPR, there is more needed than a technical plan on how to go from A to B. One change management aspect that complicates data (privacy) governance is the "principle-agent-problem" mentioned e.g. by Dallas (Dallas, 2004). Although the protection of data and digital assets has matured over time and is often covered by 'agents' like the CISO, this agent primarily serves *the company* (as its 'principle') and views data protection from a more internal angle compared to a DPO (Data Privacy Officer).
With the role of the DPO we see a new type of 'agent-principle' relationship occurring, where the *individual,* gains more influence on how companies must handle their digital assets – a much more outward looking view and with a different risk awareness and focus compared to the CISO (focussing on the companies digital assets).
Meyer identified different change barriers (Meyer, 2019) that could also influence the road to compliance with the GDPR. Some of the most important change management gaps are:

***Specificity ambiguity*.** It is unclear what needs to be done, when, how and by whom.
***Consistency ambiguity*.** No clarity regarding (competing) priorities / views of stakeholders
Resource barriers. Lack of tangible resources, e.g. money, and/or intangible resources, e.g. knowledge, skills, relations and mind-set.
***Political resistance*.** Changes may not be in people's perceived interest.
***Cognitive resistance*.** Changes may go against people's views on what should be done. They resist because they believe the proposed changes don't make sense.

Therefore, in shaping effective privacy governance and management practices, it is important to realize that we are dealing with different principal-agent relations having divergent interests, roles, tasks, knowledge and risk orientations that must be "paired" to create consistent and effective data privacy governance and management.

Question 2

What are the possible ambiguities in the legislative text of this GDPR article and how to address them?

Summarized findings: organizations could perceive the GDPR as not been made tangible enough to act upon. It is often unclear what exactly needs to be done, when, how and by whom. In GDPR article 32 we find phrases like "taking into account", "varying likelihood", "severity" "appropriate measures" and "take steps" can be seen as very ambiguous and leave room for interpretation.
It is however unavoidable that parts of the GDPR are formulated in a "technology and context agnostic" way, and as a consequence of that some ambiguity has been introduced.
When we take a closer look at the type of ambiguity we can detect in article 32 we can identify two types: context sensitivity (*meaning* is not clear without a specific context) and under specification (*actions* are not specific due to a lack of context), (Sennet, 2016).
If we want to reduce the perceived ambiguity in the GDPR text, we need to apply the process of disambiguation.
The steps to reduce ambiguity are:

1) perform a (contextual/risk) analysis of data processing activities in your company and
2) formulate concrete steps that addresses the contextual usage of privacy relevant data and the related data processing risks.

The GDPR ontology (Pandit, 2020) discussed in chapter 2 mentions all the contextual (risk) analysis aspects we need to consider. The identified risk and data processing context can be mapped to the relevant risk mitigation activities also mentioned in article 32.
These activities on their turn must be mapped to the technological context and possibilities of the data processing systems we use. **In short:** the perceived ambiguity does not lie in the semantics of the GDPR text. It lies in the (unknown) data processing context and risks that takes place in your organization.
A data processing context and risk assessment will reduce this ambiguity.

Question 3
What could be the possible root-causes for the occurred article 32 violations?

Summarized findings:
In this chapter we answered some of the research sub question using the “mind the gap” model of Meyer (Meyer, 2019). Meyer identified the different change management barriers that could also influence the road to compliance with the GDPR like specificity ambiguity, consistency ambiguity, resource barriers, political and cognitive resistance.

Some of the possible root-causes for failing to comply with the GDPR could be:

Change willingness (political and cognitive resistance)
Data (privacy) governance can be complicated by the "principle-agent-problem".
Divergent interests, roles, tasks and risk orientations of important stakeholders (like a CISO with a focus on the companies digital asset versus the DPO with a focus on the privacy rights if individuals) must be “paired” to create consistent and effective privacy governance.

Specificity ambiguity
Often the change itself (comply with the GDPR) hasn’t been made tangible enough to act upon. It is unclear what (according the GDPR legislative text) exactly needs to be done, when, how and by whom.
This “ambiguity” can be found in the (for the legislator unknown) data processing context and risks that takes place in your organization.
A data processing context and risk assessment will reduce this ambiguity.

Resource barriers and consistency ambiguity
Organizations may lack the necessary tangible resources, e.g. money, and/or intangible resources, e.g. knowledge, skills, relations and mind-set to comply with the GDPR.
Changes may also be inconsistent with the stakeholders’ other priorities.
One important hurdle to translate privacy governance into effective privacy management and operations is the function construction gap – the inability to bridge the gap between “know what to do” (function) to “know how to do this” (construction).

The GDPR describes the privacy function, not the construction of that function.
A (ongoing) translation, (re)design & synthesis is needed to come from the privacy ontology and required functionality to the construction of that required privacy functionality in a particular IT environment.
Violation of the GDPR and possible fines are mainly related to a failing construction of the privacy function (not failing to *know what to do*, but *failing to execute it*.)

One helpful instrument to combing and align these different challenges is GRC (Governance Risk and Compliance). GRC is an integrated, holistic approach to organisation-wide GRC ensuring that an organisation acts ethically correct and in accordance with its risk appetite, internal policies and external regulations through the alignment of strategy, processes, technology and people, thereby improving efficiency and effectiveness.
Each of the core disciplines – Governance, Risk Management and Compliance – consists of the four basic components: strategy, processes, technology and people.

4. Questionnaire: the perceived GDPR activities & risks related to article 32 and value of standards

§ 4.1 Introduction

In this chapter we aim to give an answer to the following research sub questions:

- How are companies perceiving IT related GDPR change management ambiguities, risks & challenges and are (ISO) standards be of added value in that process?

§ 4.2 Insight in the population (country, role, industry, personal data processed)

A questionnaire (see annex for the list of questions) has been send out using different channels (email, social media, etc.) to reach the community involved in data privacy. Professional social networks on LinkedIn involved in privacy are approached, but also work related peers in my personal network and in the network of others are used to get in touch with different type of stakeholders, The collected data can be found in the Annex.

45 responses are received in the period 10-2-2020 -16-3-2020 from respondents located in 13 different countries, with roles and from different industries (see graphical representation).

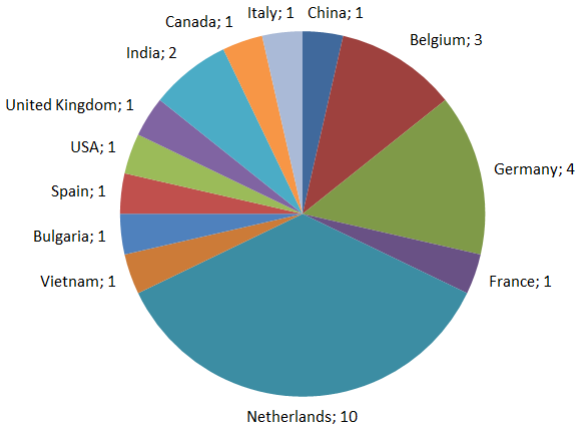


Figure 14: countries of respondents

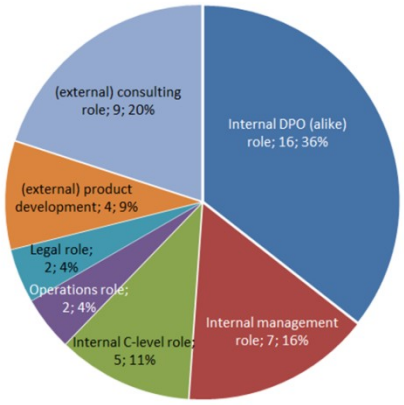


Figure 15: roles of respondents

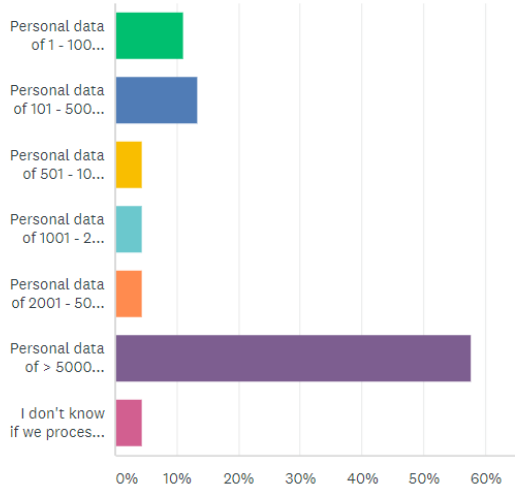


Figure 16: data processing - # of natural persons

ANTWOORDKEUZEN	REACTIES	
Agriculture, Forestry, Fishing	0.00%	0
Utilities	0.00%	0
Manufacturing	4.44%	2
Wholesale	2.22%	1
Retail	2.22%	1
Technical Services	0.00%	0
Transportation and Warehousing	0.00%	0
Telecommunications	0.00%	0
Finance and Insurance	13.33%	6
Software	15.56%	7
Information Services and Data Processing	22.22%	10
Other Information Industry	0.00%	0
Consultancy services	8.89%	4
Real Estate, Rental and Leasing	0.00%	0
Primary, College, University and Adult Education	2.22%	1
Health Care and Social Assistance	2.22%	1
Hotel and Tourism Services	2.22%	1
Entertainment and Recreation	2.22%	1
Legal Services	6.67%	3
Government and Public Administration	11.11%	5
Scientific Services	0.00%	0
Construction	0.00%	0
Other Industry	4.44%	2
TOTAAL		45

Figure 17: industries respondents are working

§ 4.3 Objective and controls of the questionnaire

Objectives. The objective of this questionnaire is to identify what the perceptions of the respondents are regarding:

- The level of (self-explanatory) guidance regarding the fulfilment of the requirements mentioned / found in the legislative text of GDPR article 32
- The (IT) standards used to support compliance with the GDPR
- The identification and handling of relevant RISKS covered by those standards
- The identification and handling of relevant MEASURES covered by those standards
- Open question: the improvements and risks the respondents see regarding compliance with GDPR article 32.

With the collected data we hope to identify the perceived value of IT standards (like delivered by ISO, etc.) regarding privacy governance and management activities like privacy risk assessment and the implementation of privacy relevant measures (scope: GDPR article 32). By requesting some (free text) input from the respondents we hope to collect some additional contextual input on GDPR risks and improvements as well.
We will use that information to verify if these risk and improvement factors are covered in the ISO 27701 standard and to map them against the materialized risks identified by the DPA's.

Questionnaire controls. In order to assure to some extend that the respondents are knowledgeable enough regarding the data privacy subject to answer the questions, we build in some control questions.
In case the respondent answered with NO or I Don't Know to one of the following questions:

Question 2: Is the GDPR relevant for your organization?
Question 3: Are you involved in GDPR related activities?
Question 5: What are the estimated number of natural persons your organization collects and processes personal data from?

, the questionnaire terminates to avoid receiving input from respondents from organizations that don't process personal data or persons that are not involved in privacy related (governance, management or operational) activities.

§ 4.4 Question 6-8: Opinions on the guidance delivered by the GDPR

Question 6-8 are concentrated on the respondent's perception regarding "the level of (self-explanatory) guidance regarding the fulfilment of the requirements mentioned / found in the legislative text of GDPR article 32".
We have collected the answers and summarized this in the table below:

Category	Question	Strongly Disagree	Disagree	∑ (strongly) Disagree	Undecided (Neutral)	Agree	Strongly Agree	∑ (strongly) Agree	N.A. / Don't Know
Opinion on the guidance delivered by the GDPR	Q6. Does the GDPR texts provide in sufficient guidance to identify the "risk(s)" ? Answered: 33 Skipped: 12	0,00% 0	33,33% 11	33,33% 11	15,15% 5	39,39% 13	12,12% 4	51,51% 17	0,00% 0
	Q7.Does the GDPR texts provide in sufficient guidance to assess the "appropriate" level of security related to the identified risk(s)? Answered: 33 Skipped:12	0,00% 0	42,42% 14	42,42% 14	15,15% 5	39,39% 13	3,13% 1	42,42% 14	0,00% 0
	Q8.Does the GDPR texts provide in sufficient guidance to formulate and implement the appropriate technical and organisational measures? Answered:33 Skipped12	9,09% 3	39,39% 13	48,48% 16	15,15% 5	33,33% 11	3,13% 1	36,36% 12	0,00% 0

Table 4: Questionnaire results - the level of guidance found in the legislative text of GDPR article 32.

First conclusion: we see some correlation between the *type of guidance* (general guidance versus practical – actionable guidance) and the level of satisfaction regarding that guidance. The majority of the respondents are satisfied (51,51% (strongly) agree) with the GDPR guidance regarding the *identification of privacy risks,* but less satisfied (36,36% (strongly) disagree) regarding actionable guidance (formulate and implement the appropriate technical and organisational measures) delivered by the legislative text.

A large majority of the respondents are using industry standards as a framework to comply with the GDPR (see Q9 in the table below and annex for details)

COBIT(2019), ENISA, CIS, CSA, ISO (ISO 27001 27002 ISO 29000), NEN (7510, 7512, 7513, 7516), British Standard 10012:12, NIST and the Norea Privacy Control Framework are the mentioned standards or frameworks respondents are using.
The next set(s) of questions are focussed on the identification of the perceived value of these (IT) standards or best practices to comply with the GDPR.

§ 4.5 Question 11-14, Risk identification and handling

Questions 11-14 are concentrated on the respondent's perception regarding the "GDPR RISKS identification and handling - perceived value of (IT) standards or best practices to comply with the GDPR".

Category	Question	Strongly Disagree	Disagree	∑ **(strongly) disagree**	**Undecided (Neutral)**	Agree	Strongly Agree	∑ **(strongly) agree**	N.A. / Don't Know
GDPR Risks identification and handling. Perceived value of (IT) standards or best practices to comply with the GDPR	Q9.Are you using the guidance of particular (IT) standards for defining, controlling and/or executing privacy governance, -management and -operational activities? Answered: 33 Skipped: 12			**NO**: 15,15% 5				**YES**: 84,85% 28	
	Q11.Does this standard, best practice or approach supports you in the process of identifying WHAT the "risks" are? Answered: 32 Skipped: 13	0,00% 0	9,38% 3	9,38% 3	18,75% 6	56,25% 18	12,50% 4	**68,75% 22**	3,13% 1
	Q12.Does this standard, best practice or approach supports you in the process of WHEN the "risks" in your organization could occur?Answered32 Skipped13	0,00% 0	18,75% 6	18,75% 6	15,63% 5	53,13% 17	6,25% 2	59,38% 19	6,25% 2
	Q13.Does this standard, best practice or approach supports you in the process of WHERE and HOW the "risks" of processing privacy rel. data should be identified and addressed? Answered: 32 Skipped: 13	0,00% 0	18,75% 6	18,75% 6	18,75% 6	46,88% 15	9,38% 3	**56,26% 18**	6,25% 2
	Q14.Does this standard, best practice or approach supports you in the process of identifying WHO should BE RESPONSIBLE to identify and handle the "risks"? Answered: 32 Skipped: 13	0,00% 0	21,88% 7	21,88% 7	12,50% 4	37,50% 12	21,88% 7	59,38% 12	6,25% 2

Table 5: Questionnaire results - RISKS identification and handling - perceived value of standards.

First conclusions: the majority of respondents are positive regarding the added value of standards and frameworks in the context of GDPR Risks identification and handling.

1. Risk analysis and identification: what are the risks and **when** can they occur? Compared to risk identification support delivered by the GDPR (Q6, 51,51%) we see that standards and frameworks deliver a (more) positive contribution to the identification on what the data processing risks are (Q11, 68,75% - highest positive score in this section) and when they could occur (Q12, 59,38%).

2. Risk mitigation: where (processing activities) and **how to i**dentify and address them? The lowest score in the table above on the added value of standards and frameworks regarding risk identification are the WHERE and HOW (to's) (Q12, 56,26%) and WHO should be responsible (59,38%, lowest score in the area (strongly) agree)

This indicates a somewhat lower satisfaction regarding the practical risk assessment guidance of some of the standards used.

§ 4.6 Question 15-18, Identification and handling of appropriate measures

Questions 15-18 concentrated on the respondent's perception regarding the "identification and handling of appropriate MEASURES - the perceived value of (IT) standards or best practices".

Category	Question	Strongly Disagree	Disagree	∑ **(strongly) disagree**	**Undecided (Neutral)**	Agree	Strongly Agree	∑ **(strongly) agree**	N.A. / Don't Know
Identification and handling of measures. Perceived value of (IT) standards or best practices to comply with the GDPR	Q15.Does this standard, best practice or approach supports you in the process of identifying WHAT the appropriate technical and organisational measures are? Answered: 32 Skipped: 13	0,00% 0	18,75% 6	18,75% 6	15,63% 5	46,88% 15	12,50% 4	59,38% 19	6,25% 2
	Q16.Does this standard, best practice or approach supports you in the process of WHEN the appropriate technical and organisational measures must be in place/implemented Answered 32 Skipped13	0,00% 0	15,63% 5	15,63% 5	15,63% 5	50,00% 16	12,50% 4	62,50% 20	6,25% 2
	Q17.Does this standard, best practice or approach supports you in the process of WHERE and HOW the appropriate technical and organisational measures of processing privacy relevant data in your organization should be implemented? Answered: 32 Skipped: 13	0,00% 0	25,00% 8	25,00% 8	3,03% 1	53,13% 17	12,50% 4	**65,63% 21**	6,25% 2
	Q18.Does this standard, best practice or approach supports you in the process of identifying WHO should BE RESPONSIBLE to implement the appropriate technical & organisational measures of processing privacy relevant data in your organization? Answered: 32 Skipped: 13	0,00% 0	21,88% 7	21,88% 7	18,75% 6	31,25% 10	21,88% 7	59,38% 12	6,25% 2

Table 6: Questionnaire results - identification and handling of MEASURES - perceived value of standards.

First conclusions: the majority of respondents are positive regarding the added value of standards and frameworks in the context of the identification and implementation of the appropriate technical & organizational measures.

1. Measures: *what* are the appropriate technical & organizational measures?
Compared to support delivered by the GDPR in this context (Q8, 36,36%) we see that standards and frameworks deliver a (much) more positive contribution to the identification on WHAT the appropriate technical and organisational measures are (Q11, 59,38%) and when they should be implemented (Q12, 62,50%).

2. Measures: *how* the appropriate measures must be implemented
The highest score in the table above on the added value of standards and frameworks regarding appropriate technical and organisational measures can be found in the WHERE and HOW (to's) (Q17, 65,63%, highest score in the area (strongly) agree).
This indicates a relative high satisfaction regarding the practical implementation guidance of some of the standards used.

§ 4.7 Open questions Q19-20: Improvements & risks (activities view)

The participants were asked to reply to two open questions regarding two specific aspects: the **improvements** and **risks** they see regarding the realization of privacy governance, management and operations. (see the Annex for details)
Thirty respondents replied to this and their wording has been analysed and classified (using the COBIT governance and management activity classification) in order to understand the type of activities (management or governance) they see possible data privacy improvements and risks. (See annex for the detailed answers and the applied COBIT activity classification)

Classification of (type of) governance and management activities according COBIT		Mentioned "**improvement** regarding the realization of privacy governance, management and operations" in the open answers can be related to COBIT activity	Mentioned "**risk** regarding the realization of privacy governance, management and operations" in the open answers can be related to COBIT activity
Governance activities (COBIT view)	[MONITOR]	7	1
	[EVALUATE]	14	10
	[DIRECT]	18	16
Management activities (COBIT view)	[PLAN]	4	4
	[BUILD]	6	3
	[RUN]	8	4
	[MONITOR]	9	6

Table 7: Questionnaire results - mentioned risks & improvements mapped against COBIT activities

First conclusion:

1. Dominant area of improvements & risks are: [GOVERNANCE DIRECT | EVALUATE]
In the wordings used by the 30 respondents we see that COBIT governance activity DIRECT (*setting direction* through *prioritisation* and *decision making* according COBIT) can be identified as the dominant area that needs to be improved (18) or is perceived as a risk area (16) for compliance with the GDPR.
The privacy governance activity [EVALUATE] also scores high as improvement- (14) or risk area (10) for compliance with the GDPR.

2. Privacy management [PLAN, BUILD, RUN, MONITOR] seems to be under control
The low number of wordings used by the respondents that could refer to issues related to [PLAN, BUILD, RUN, MONITOR] management activities seems to indicate that privacy management activities are perceived as less subjected to improvements or risks compared to privacy governance related issues.

3. Consistency check open questions against liquor scale based answers

a) **Privacy management.** The liquor scale based answers to questions 11-14 ("GDPR RISKS identification and handling) and questions 15-18 ("identification and handling of appropriate MEASURES) shows that the majority of the respondents satisfied with practical management and operational guidance of the standards (COBIT, ENISA, CIS, CSA, NEN/ISO, etc.) they applied. This is consistent with the low number of management and operational improvements and risks mentioned in the answers to the open questions.
b) **Privacy governance.** The liquor scale based answers to questions 11-14 ("GDPR RISKS identification and hand and questions 15-18 ("identification and handling of appropriate MEASURES) shows that the majority of the respondents are satisfied with governance guidance of the standards they use.
However, the high number of mentioned improvements & risks in the area GOVERNANCE (EVALUATE, DIRECT) suggest that this guidance seems to be less effective in practice. Since activity DIRECT (setting direction through prioritisation and decision making) must be turned into tangible actions to operationalize it, it is possible that the respondents feel that the privacy governance function is not well developed or not given priority to (lead) possibly leading to failing to operationalize it (lag). Since management activity PLAN and BUILD is not mentioned very frequently, this could indicate a gap between governance and management.

§ 4.8 Chapter summary

In this chapter we answered the following research sub question:

Question 1
How are companies perceiving IT related GDPR change management ambiguities, risks & challenges and are standards be of added value in that process?

Summarized findings:

1. Opinions on the practical guidance delivered by the GDPR

The majority of the respondents are satisfied (51,51% (strongly) agree) with the GDPR guidance regarding the identification of privacy risks, but the majority was not satisfied (39,39% (strongly) disagree) regarding actionable guidance (formulate and implement the appropriate technical and organisational measures) delivered by the legislative text.

2. The value of standards regarding the GDPR RISKS identification and handling.
The majority of respondents are positive regarding the added value of standards and frameworks in the context of the risk identification and handling. 68,75% is the highest score (in the area (strongly) agree) regarding the practical RISK guidance of some of the standards used.

3. The value of standards and best practices regarding the identification and handling of appropriate organizational and technical MEASURES.

The majority of respondents are positive regarding the added value of standards and frameworks in the context of the identification and implementation of the appropriate technical & organizational measures. The high score of 65,63% in the area (strongly) agree) regarding the practical implementation guidance of some of the standards used shows the perceived added value of standards in this area.

4. Open question: the **improvements** and **risks** regarding the realization of privacy governance, management and operations.
In the wordings used by the 30 respondents we see that COBIT governance activity DIRECT (*setting direction* through *prioritisation* and *decision making)* can be identified as the dominant area that needs to be improved (18) or is perceived as a risk area (16) for compliance with the GDPR. The privacy governance activity [EVALUATE] also scores high as improvement- (14) or risk area (10) for compliance with the GDPR.
Since activity DIRECT (setting direction through prioritisation and decision making) must be turned into tangible actions to operationalize it, it is possible that the respondents feel that the privacy governance function is not well developed or not given priority to (lead) possibly leading to failing to operationalize it (lag).
See also chapter 3 – resource barrier, function-construction gap.

5. Synthesis: consolidation of chapter 2-4

§ 5.1 Introduction

In chapter 5 we will formulate and consolidate the outcome of the literature research (text/ ambiguity analysis), the registered GDPR violations (actual violations/risks) and the results of the questionnaires (perceived activities/risks).

- In this chapter we aim to summarize the results of the findings so far and use that as input for chapter 6, the fit-gap analysis of ISO 27701:2019 (new privacy extension to ISO27001 published in October 2019)

In chapter 2-4 we directly or indirectly touched many of the aspects that, from the viewpoint of COBIT, are important to consider in order shape an effective (privacy) governance and management system (see figure below): COBIT defines the components to build and sustain a governance system: processes, organizational structures, policies and procedures, information flows, culture and behaviours, skills, and infrastructure (with these seven components previously termed “enablers” in COBIT 5). In this chapter we refer to the different COBIT components we touched (in)directly in the previous chapters.

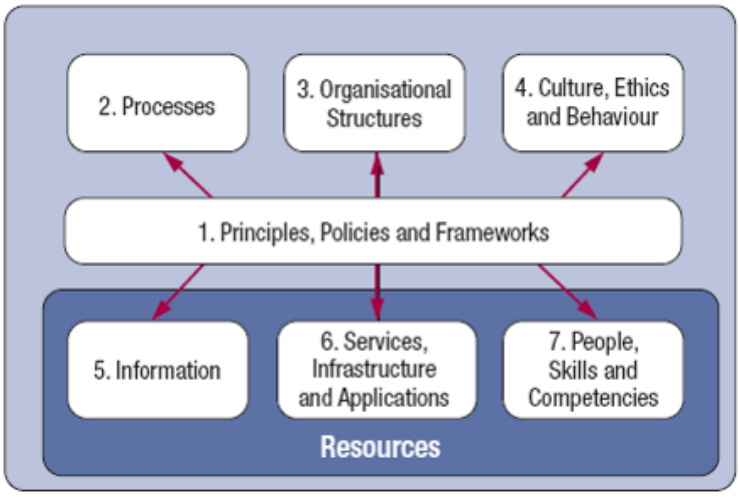


Figure 18: COBIT 2019 components needed for a proper functioning governance system

§ 5.2 Identify common GDPR risks & violations using the C|M|S violation database

Complying with the GDPR requires in many cases a risk assessment regarding the way organizations are processing privacy relevant data and possible areas of non-compliancy. The difficulty with risk assessments in general is often determining the possible rate of the (risk) occurrence and (financial) impact of a materialized risk since statistical information is not always available on past incidents.

Fortunately we had at the moment this paper has been written, +/- 21 months after May 2018 when the GDPR can into force, useful statistical information available on how the Data Privacy Authorities (DPA) judged/fined non-compliance with specific GDPR articles so far. We used the GDPR violation database published by (Law firm C|M|S, 2020) to identify the materialized GDPR violations.

The type of GDPR violation that occurred the *most frequently* up to 03.2020 seems to be “insufficient legal basis for data processing” (article 6), however the type of GDPR violation that has the highest sum of (publically published) fines imposed to companies since enforcement of the GDPR in up to 03.2020 seems to be “insufficient technical and organizational measures to ensure information security” (article 32).
In order to limit the scope of this research (relevance of the study) we focus mainly on the analysis of the context around **GDPR article 32** (information security) since violation of this GDPR article 32 has led to the highest cumulated fine of € 332.000.000+ (01.03.2020). This makes a better understanding of the requirements / context of article 32 very relevant.

§ 5.3 Article 32: the ontology and violation hotspots

Component 1: "principles, policies and frameworks". (see § 2.6 - § 2.7, § 2.9)

Just reading the legislative text of GDPR article 32 and the related recitals 75-79 and 83 will not always be sufficient for policy makers and management to actually *understand what is required*, what the *risks* are and how to *enforce and control the legislative requirements*.
One way to represent information regarding a specific subject schematically is the use of the **domain ontology** (to express privacy principles in a framework). The **GDPRtEXT ontology,** developed by Pandit (Pandit, 2020) has been used and enriched to identify the specific article 32 violation aspects (or hotspots). Based on the 53 case rulings describing the context of the article 32 violation more in detail (see annex), we have isolated the top 3 of most occurring violation aspects (hotspots). These are:

1. Failing ongoing **confidentiality** of processing: 43 violations
2. Failing ongoing **integrity** of data processing: 14 violation
3. Failing ongoing **resilience of systems / services**: 8 violation

In the **ontological scheme** of article 32 in § 2.6 you will find these "violation hotspots".

We clearly see that the DPA's mainly fines the **visible symptoms** of GDPR non-compliancy rather than fining and describing the underlying root cause of those symptoms.

§ 5.4 Article 32: the (COBIT) governance and management activities

Component: "organizational structures" and "processes". (see §2.7 - §2.8, §2.10, §3,8)
COBIT clearly separates (privacy) governance from management activities and the way they are organized.

(Privacy) governance: *ensures* that enterprise objectives are achieved by *evaluating* stakeholder needs, conditions and options, *setting direction* through *prioritisation* and *decision making*, and *monitoring* performance, compliance, and progress against plans.
(Privacy) management: *plans, builds, runs and monitors activities* in alignment with the direction set by the governance body to achieve the enterprise objectives.

Looking at the *type of activities* (according the categorization governance or management activities as used by COBIT (ISACA, 2020)) we see that the violations are mainly concentrated around (failing or ineffective) **privacy management** and violation aspects activities like PLAN-BUILD-RUN-MONITOR.
In order to identify the possible root-causes, we identified the possible different (cascaded or chained) leading & lagging indicators that possibly have led to the (operational) violation.

Component: "Culture, ethics and behaviour". (see § 2.10 - § 3.2, § 3,8)

§ 5.5 Article 32: change management aspects & risks

Change management in general is an important factor for successfully change the organization, thus also in to the context of GDPR. We used the "mind the gap" model (Meyer, 2019) to have a look at the following change management aspects:

Specificity ambiguity.
Often the change itself (comply with the GDPR) hasn't been made tangible enough to act upon. It is unclear what needs to be done, when, how and by whom.

Consistency ambiguity.
Changes may also be inconsistent with the stakeholders' other priorities.
This can lead to un-clarity as to what (competing) objectives should be given priority to.

Resource barriers.
Organizations may lack the necessary tangible resources, e.g. money, and/or intangible resources, e.g. knowledge, skills, relations and mind-set.

Political resistance.
Going along with the changes may not be in people's perceived interest.
Their resistance is then a rational and calculated response to a potential loss.

Cognitive resistance. Going along with the changes may go against people's views on what should be done. They resist because they believe the proposed changes don't make sense.

§ 5.6 Article 32: (con)textual ambiguities

Change willingness (political and cognitive resistance). (see § 3.3 - § 3.4, §3,8)
Data (privacy) governance can be complicated by the "principle-agent-problem".
Divergent interests, roles, tasks and risk orientations of important stakeholders (like a CISO with a focus on the companies digital asset versus the DPO with a focus on the privacy rights if individuals) must be “paired” to create consistent and effective privacy governance.

Specificity ambiguity.
Some article 32 phrases[28] like “taking into account”, “varying likelihood”, “severity” “appropriate measures” and “take steps” can be seen as very ambiguous and leave room for interpretation. One could ask: what does the legislator means exactly with these phrases and how can companies comply with these “requirements” that can be interpreted in different ways?
One reason is that the speed of technological change and innovation, including new ways to use privacy relevant data, makes it difficult to be *prescriptive in detail* about data protection (implementation) activities, since that could become outdated as soon new technologies or ways to use personal data are introduced. This specificity “ambiguity” can be found in the (for the legislator unknown) data processing context and risks that takes place in your organization. A data processing context and risk assessment will reduce this ambiguity.

Component: “resources” including people, skills and competencies. (see § 3.7)

Resource barriers.
Organizations may lack the necessary tangible resources, e.g. money, and/or intangible resources, e.g. knowledge, skills, relations and mind-set to comply with the GDPR.

§ 5.7 Article 32: the privacy function-construction gap

One important hurdle to translate privacy governance into effective privacy management and operations is the function construction gap – the inability to bridge the gap between “know what to do” (function) to “know how to do this” (construction).
The GDPR describes the privacy function, not the construction of that function.
A (ongoing) translation, (re)design & synthesis is needed to come from the privacy ontology and required functionality to the construction of that required privacy functionality in a particular IT environment. Violation of the GDPR and possible fines are mainly related to a failing construction of the privacy function (not failing to *know what to do*, but *failing to execute it*.)

§ 5.8 Article 32: questionnaire findings (perceived risks, gaps, activities)

Opinions on the practical guidance delivered by the GDPR. (see § 4.7 - § 4.8)
The majority of the respondents are satisfied with the GDPR guidance regarding the identification of privacy risks, but not satisfied regarding actionable guidance (formulate and implement the appropriate technical and organisational measures) delivered by the legislative text.

The value of standards
The majority of respondents are positive regarding the added value of standards and frameworks in the context of the risk identification and handling and the implementation of the appropriate technical & organizational measures. Standards provide in more practical guidance compared to the directions given in the GDPR legislative text.

The respondents also identified that governance activity DIRECT (*setting direction* through *prioritisation* and *decision making)* and EVALUATE can be identified as the dominant area that needs to be improved or is perceived as a risk area for compliance with the GDPR.

[28] See article 32 text: https://gdpr-info.eu/art-32-gdpr/ (Retrieved at 05.2020)

§ 5.9 Synthesis of the findings

Based on the outcome of chapter 2-4 we can conclude the following:

1. The **Data Privacy Authorities** (DPA) primarily fined the visible symptoms of GDPR non-compliancy and refers to missing or failing privacy management or -operations in their case descriptions. [MANAGEMENT- PLAN-BUILD-RUN-MONITOR].

2. The **questionnaire respondents** identified privacy improvements and risks mainly on governance level, especially in the area of EVALUATE and DIRECT.

Classification of (type of) governance and management activities according COBIT		**The organizations view (questionnaire):** perceived GDPR governance and management risks / improvements (lead)		**The regulators view:** Published GDPR violations (lag)
		Mentioned "improvements regarding the realization of privacy governance, management and operations"	Mentioned "risks regarding the realization of privacy governance, management and operations"	Missing/failing types of activities linked to the violation case(s).
Governance (COBIT view)	[MONITOR]	4	2	4
	[EVALUATE]	15	14	
	[DIRECT]	19	17	
Management (COBIT view)	[PLAN]	0	2	50
	[BUILD]	3	2	
	[RUN]	3	2	
	[MONITOR]	2	3	

Table 8: Privacy governance & management improvements/risks/measured violations:
The perspective of the regulator versus the organization (orange = risk & activity focus)

3. The **literature study** shows (and this bridges the above findings) that:

a) **Change management gaps** and aspects are important to consider in order to successfully implement a change (**mind the gap model change management model**)

b) **A privacy governance system** should cover the components (and carefully alignment of) processes, organizational structures, policies and procedures, information flows, culture and behaviours, skills, and infrastructure. (**COBIT 2019 components**)

c) **Privacy architecture** is needed to address the function construction gap – the inability to bridge the gap between "know what to do" (function) to "know how to do this" (construction). The GDPR describes the privacy function, not the construction of that function.
A (ongoing) translation, (re)design & synthesis is needed to come from the privacy ontology and required functionality to the construction of that required privacy functionality in a particular IT environment (DIETZ, Design process and architecture).

6. Are the identified privacy activities, risks and gaps effectively addressed and mitigated in ISO 27701:2019?

§ 6.1 Introduction

In the previous chapter 5 we analysed and consolidated the outcome of the literature research, the registered GDPR violations and the results of the questionnaires

In this chapter we aim to map the consolidated outcome of chapter 5 to the guidance provided by ISO 27701:2019 in order to identify if this ISO standard addresses the identified activities, (change management) risks and ambiguities'.
In this chapter we aim to give an answer to the following research sub question:

- Are the identified non-compliancy risks and perceived GDPR governance and management activities, ambiguities' and risks effectively addressed and mitigated in the ISO 27701:2019[29] (new privacy extension to ISO27001 published in October 2019)?

§ 6.2 Security standards ISO27001 & 27002

One of the most widely adopted security standards in the world are ISO 27001 and ISO27002. These standards were also used by many companies to cover the obligations mentioned in GDPR article 32 and its predecessor the EU privacy directive.
The final control in ISO 27001 annex 1 for example requires that security professionals are knowledgeable of all relevant legal requirements (including the GDPR).
Security professionals should also incorporate privacy requirements into security plans, so that ISO 27001 based policies and procedures reflect the requirements of e.g. the GDPR.
Although ISO 27001 and 27002 are good frameworks for establishing and operating an ISMS (Information Security Management System) through the PDCA cycle, it turned out that ISO 27001 and 27002 didn't covered many GDPR articles and aspects[30].

§ 6.3 The new standard for privacy management: ISO 27701:2019

In August 2019, ISO/IEC released a new privacy standard set to become the benchmark for helping organisations to comply with international privacy frameworks and laws.
ISO/IEC 27701:2019 serves as a **privacy extension** to the internationally recognised management standard for information security ISO/IEC 27001.

§ 6.4 Requirements for implementing ISO 27701 as privacy management system

If an organisation has implemented ISO 27001, it can use ISO 27701 to extend its security efforts to cover privacy requirements. Organisations that have not implemented an ISMS can implement ISO 27001 and ISO 27701 together as a single implementation project, but ISO 27701 cannot be implemented as a standalone standard. Only combined with ISO 27001, ISO 27701 can help organisations to compliance with key privacy laws like the GDPR.
The reason for this is that an ISO 27001-conforming ISMS is the kernel onto which the ISO 27701 additions accommodate data privacy (see table below).

Table F.1 — Mapping of the extension of the term information security by privacy

ISO/IEC 27001	This document (extension)
information security	information security and privacy
information security policy	information security and privacy policy
information security management	information security and privacy information management
information security management system (ISMS)	privacy information management system (PIMS)
information security objectives	information security and privacy objectives
Information security performance	information security and privacy performance
Information security requirements	information security and privacy requirements
information security risk	information security and privacy risk
information security risk assessment	information security and privacy risk assessment
information security risk treatment	information security and privacy risk treatment

Table 9: ISO 27701:2019 as **privacy extension** to information security standard ISO/IEC 27001

[29] See: https://www.iso.org/obp/ui/#iso:std:iso-iec:27701:ed-1:v1:en (Retrieved at 05.2020)

[30] Podcast Fieldfischer: https://soundcloud.com/fieldfishersiliconvalley/episode-7-iso-27001-and-the-gdpr (Retrieved at 05.2020)

The full name of this ISO standard is: ISO/IEC 27701 **security techniques** – extension to ISO 27001 and 27002 for privacy information management.
This context raises an interesting question: are the activities, controls, the risk context & -identification etc. conforming to an information **security** management system (ISMS) standard compatible and exchangeable with what we can expect from a PIMS (Privacy Information Management System) like ISO 27701?
Security is not equal to privacy, and privacy covers much more than data security!

§ 6.5 Privacy and security are different qualities with different stakeholders

We addressed the risk of having different agents, principles and cognitive views in chapter 2. The agent (like a CISO) using the ISO 27001:2013 standard primarily serves the company (as its 'principle') and views data protection from a more internal angle compared to a DPO (Data Privacy Officer).
With the role of the DPO we see a new type of 'agent-principle' relationship occurring, where the individual, as a new type of principle, gains more influence on how companies must handle their digital assets – a much more outward looking view and with a different risk awareness and focus compared to the CISO (focussing on the companies' digital assets).

Therefore, in shaping (data) governance, it is important to realize that we are dealing with different principal-agent relations having divergent interests, roles, tasks and risk orientations (possible political and cognitive resistance according Meyer (Meyer, 2019)) that must be "paired" to create consistent and effective (data security AND privacy) governance.

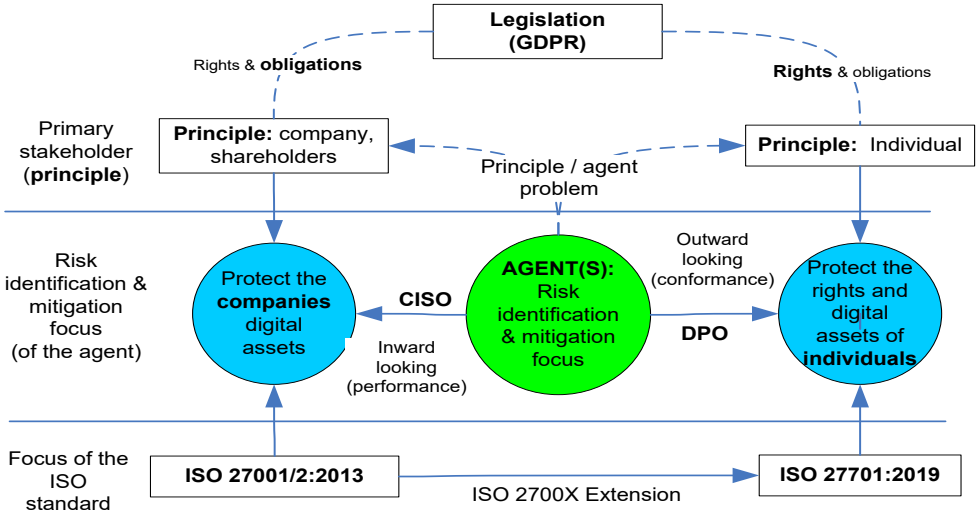


Figure 19: principles of different ISO standards – protect the organization versus individual's assets

ISO indeed recognizes that privacy and security are different properties & qualities (see annex 5.4.1.2 and .3 where we can read that the "relationship between information security and PII protection is appropriately managed" (ISO, 2019)

Critical note: in theory a PIMS that *refers* to a ISMS could work, and indeed security and privacy are at least partly interdependent and intertwined.
However, we clearly see that ISO 27701 for at least 60-70% refers to and relies on ISO standards and guidelines (ISO 27001:2013) that are shaped and published at least 5 years *before* the GDPR became active as law in Europe. In other words: many data *security* guidelines in ISO 27001:2013 were not designed with *privacy* in mind. Simply adding "and privacy.." to the table of data security activities (see table 9 - ISO 27701:2019 as privacy extension to information security standard ISO/IEC 27701 may be too simplistic.

The focus of ISO 27701 is data *security*…but its less focussed on strong guidance related to data *privacy* (governance and management) aspects mentioned in the GDPR like the rights of the data subjects, etc. These topics are only briefly "touched" in ISO 27701 (see table 11).
For effective privacy governance & management, most likely more is needed than extending the existing data security activities – privacy asks for different skills, knowledge & mind-sets.

§ 6.6 Article 32 ontology, violation hotspots and activities mapped to ISO 27701

In this section we used the previously identified GDPR ontology of article 32 and identified violation hotspots (see § 2.9) and mapped that to the coverage in ISO27701 based on the ISO27701 - GDPR mapping table in the annex and the relevant ISO article text.
Please note that this is done based on the personal judgement of the ISO27701 text.

GDPR article	**GDPR activities** (high level)	**GDPR aspects** (contextual details regarding aspects to be considered when executing the activities)	**ISO 27701** (article 32 view) ISO 27701 article according the **ISO 27701 - GDPR mapping table** (see annex)	**COBIT activity type view on ISO 27701:** What **type of activities**?						
				Governance			**Management**			
				Monitor	**Evaluate**	**Direct**	**Plan**	**Build**	**Run**	**Monitor**
Article 32:1, 2 Recital 83 Recital 75-79	**(Governance)** **[MONITOR EVALUATE]** **Identify / assess** data processing **risks** related to the following aspects:	**Cost of risk mitigation** (32:1)	< not found in mapping table> Risk addressed in 5.4.1.2 & 3							
		State of the art of data processing (32:1)	< not found in mapping table> Risk addressed 5.4.1.2, 7.2.X							
		Nature of data processing (32:1)	< not found in mapping table> Risk addressed 5.4.1.2, 7.2.X							
		Scope of data processing (32:1)	< not found in mapping table> Risk addressed 5.4.1.2, 7.2.X							
		Context of data processing (32:1)	< not found in mapping table> Risk addressed 5.4.1.2, 7.2.X							
		Purpose of data processing (32:1)	< not found in mapping table> Risk addressed 5.4.1.2, 7.2.X							
		varying **likelihood and severity** for (violating) the rights of persons	< not found in mapping table> Risk addressed 5.4.1.2,7.2.X							
		Accidental or unlawful **destruction** (32:2)	5.2.3&4 | 5.4.1.2&3 | 6.15.2.1&3, etc.							
		Loss of data (32:2)	5.2.3&4 | 5.4.1.2&3 | 6.15.2.1&3, etc.							
		Alteration of data (32:2)	5.2.3&4 | 5.4.1.2&3 | 6.15.2.1&3, etc.							
		Unauthorised **disclosure** (32:2)	5.2.3&4 | 5.4.1.2&3 | 6.15.2.1&3, etc.							
		Access to personal data transmitted, stored, etc. (32:2)	5.2.3&4 | 5.4.1.2&3 | 6.15.2.1&3, etc.							
Article 32:1a-c Recital 83 Recital 75-79	**(Management & operations)** **[PLAN,BUILD, RUN, MONITOR]** **Implement** appropriate **technical** measures, like:	Pseudonymisation, anonymization/encryption (32:1a)	6.5.3.1&3 | 6.7.1.1 | 6.11.1.2							
		Ongoing **confidentiality** of processing (43 violations) (32:1b)	5.4.1.2&3 | 6.11.1.2 | 6.15.1.1							
		Ongoing **integrity** of data processing (14 violations) (32:1b)	5.4.1.2&3 | 6.11.1.2 | 6.15.1.1							
		Availability of data (32:1b)	5.4.1.2&3 | 6.11.1.2 | 6.15.1.1							
		Ongoing **resilience** of systems / services (8 violations) (32:1b)	5.4.1.2&3 | 6.11.1.2 | 6.15.1.1							
		The **ability to restore** the **availability and access** to personal data after an incident,(32:1c)	6.9.3.1							
Article 32:1d Recital 75-79	**(Governance)** **[MONITOR, EVALUATE]** **Implement** appropriate **organizational** measures	**Testing** the **effectiveness** of technical & org. measures (32:1d)	6.15.2.1 & 3							
		Assessing the **effectiveness** of technical & org. measures (32:1d)	6.15.2.1 & 3							
		Evaluating the **effectiveness** of technical & org. measures (32:1d)	6.15.2.1 & 3							
Article 32:3		**Demonstrate compliance** with the GDPR requirements (32:3)	5.2.1							
Article 32:4 Recital 75-79	**(Governance)** **[DIRECT, MONITOR]** Provide in data processing instructions and oversight	Data controller **instructs (in writing)** the processor on **how to process the data** (32:4)	< not found in mapping table> Addressed in 7.2.6.							
		Data controller must **ensure** that **processor processes the data according instructions** (32:4)	< not found in mapping table> Addressed in 7.2.6.							

Table 10: The ontology of article 32 mapped to ISO27701 articles and COBIT activities

Black marked = (medium-strong) coverage in ISO27701 article.. **Grey marked** = some/weak coverage of activity
Orange marked = Article 32 violation hotspots (high number of violation occurrences)

First findings: looking at table 10 (previous page) we see that most of the ontological aspects of GDPR article 32 are covered in ISO27701 however most of the ISO activities are not directly helpful from an operational and execution point of view (activities BUILD & RUN). The quality of *operational* privacy controls in ISO27701:2019 are weak or even absent. When controls are mentioned they can be seen as security – not privacy control *objectives* rather than operational privacy controls with their related concrete metrics.

§ 6.7 Is the article 32 ontology mapped to ISO 27701:2019 articles?

Regarding the coverage of in § 2.9 mentioned ontological aspects of article 32 and its sub articles we can say that all of the article 32 aspects can be mapped against ISO27701 articles, although the GDPR - ISO27701 index does not refer to all the article 32 aspects. However, after careful analysis we could find sufficient guidance for all the aspects (see table 10).

§ 6.8 Are the article 32 violation hotspots addressed in ISO 27701:2019?

Yes, the identified GDPR violation hotspots (failed to implement ongoing confidentiality of processing, integrity of data processing and resilience of systems / services) are covered according the GDPR - ISO27701 index in the annex by ISO27701 articles 5.4.1.2&3, 6.11.1.2 and 6.15.1.1.
However, the in ISO27701 delivered guidance is very high level and mainly concentrated around privacy *governance* activities (like risk assessments and treatment, identification of relevant legislation and contractual requirements). Some practical guidance is given regarding network security (6.11.1.2), but practical operational guidance is limited.

Looking at the proposed mitigation options on one of the biggest privacy violation hotspot (confidentiality of processing - 43 violations), we see that ISO27701 e.g. refers to article 6.6 (access control). The guidance of article 6.6 and its sub articles are too high level and referring to other ISO 27002:2013 articles (9.X) for more detailed guidance. This is not substantial enough.
The combined ISO 27002:2013 and ISO27701:2019 guidance is not sufficient in addressing the GDPR violation hotspots. They are too generic and less data privacy aware or focussed to effectively address and control the operational privacy issues described by the DPO in the violation cases. It gives merely a direction.

§ 6.9 Are the governance and management activities & controls addressed?

Yes, the different types of governance and management activities (COBIT view) that can be found in GDPR article 32 are addressed, however only from a limited perspective. ISO27701:2019 seems more focused on privacy *security* governance [MONITOR – EVALUATE – DIRECT] and less specific regarding management and operations [PLAN, BUILD, RUN, MONOTOR].
The table below from the ISO documentation shows that there are mostly no additional information *privacy* management system (PIMS) specific requirements and controls formulated for governance activities like leadership, performance evaluation or (continue) improvements or management activities like operations and support.
How to be in control of privacy if there are very limited (PIMS specific) controls?

Table 1 — Location of PIMS-specific requirements and other information for implementing controls in ISO/IEC 27001:2013

Clause in ISO/IEC 27001:2013	Title	Subclause in this document	Remarks
4	Context of the organization	5.2	Additional requirements
5	Leadership	5.3	No PIMS-specific requirements
6	Planning	5.4	Additional requirements
7	Support	5.5	No PIMS-specific requirements
8	Operation	5.6	No PIMS-specific requirements
9	Performance evaluation	5.7	No PIMS-specific requirements
10	Improvement	5.8	No PIMS-specific requirements

Table 11: Privacy (PIMS) governance and management requirements and controls in ISO 27701 (ISO document)

From that perspective we can conclude that ISO27701:2019 in the context of the GDPR and article 32 has a strong focus on the privacy ***security*** function and related governance objectives and less focussed on ***privacy*** governance, operations and the construction & control of the privacy solution.

§ 6.10 Are the change management *risks* addressed in ISO 27701:2019?

Meyer identified the different change management barriers that could also influence the road to compliance with the GDPR like specificity ambiguity, consistency ambiguity, resource barriers, political and cognitive resistance.

ISO27701:2019 has not a strong focus on (privacy) change management aspects.
One example is the fact that data (privacy and security) governance can be complicated by the "principle-agent-problem". The divergent interests, roles, tasks and risk orientations of e.g. the CISO (focus on the companies' digital assets) versus the DPO with a focus on the privacy rights of individuals are mentioned but not clearly addressed ("paired") in ISO27701:2019 to create consistent and effective privacy governance and management.

§ 6.11 Are the contextual *ambiguities'* addressed in ISO 27701:2019?

Often it is unclear what (ambiguity in the GDPR legislative text) exactly needs to be done, when, how and by whom. This "ambiguity" can be found in the (for the legislator unknown) data processing context and risks that takes place in your organization.
A data processing context and risk assessment will reduce this ambiguity.
These activities are clearly mentioned in ISO27701:2019 but there is a lack of practical guidance available, especially regarding the privacy aspect. Risks guidance is more focussed on data security and less "privacy" aware.

§ 6.12 Are the function – construction gaps addressed in ISO 27701:2019?

For effective privacy management, understanding the difference between privacy function versus construction is needed. The inability to bridge the gap between "know what to do" (function) to "know how to do this" (construction) will lead to ineffective privacy management or even violations of the GDPR.
ISO27701:2019 mainly describes the privacy function, not the construction of that function.
The (re)design & synthesis needed to come from the required functionality to the construction of that required privacy functionality in a particular IT environment is hardly addressed.

> **Note:** Maybe it is not fair to expect detailed operational guidance from ISO27701:2019. The question we can ask: are ISO standards designed to provide in detailed guidance on how a privacy function should be constructed in a particular IT system? Not likely.

According Complianceforge.com we cannot expect that ISO standards will deliver robust detailed (tactical) guidance. In figure 21 and 22 we see that ISO standards are positioned to deliver operational guidance with a moderate (practical and project specific) coverage.

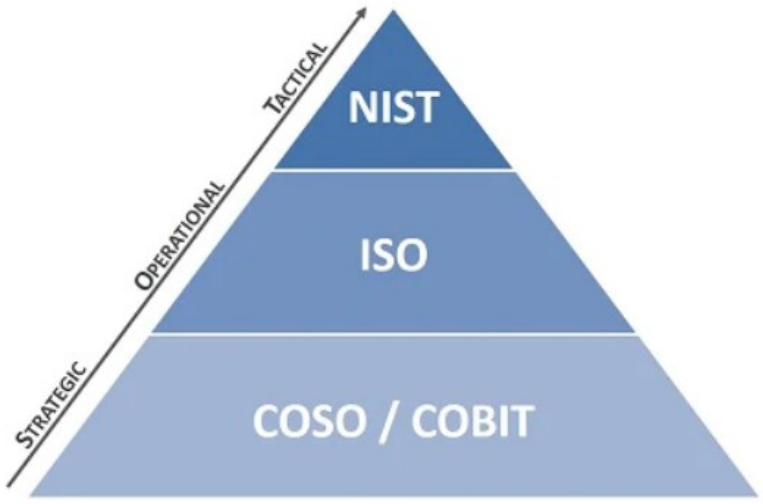


Figure 20: frameworks positioned in a strategic, operational and tactical context
Source: https://www.complianceforge.com/product/cybersecurity-risk-management-program-rmp/ (Retrieved at 05.2020)

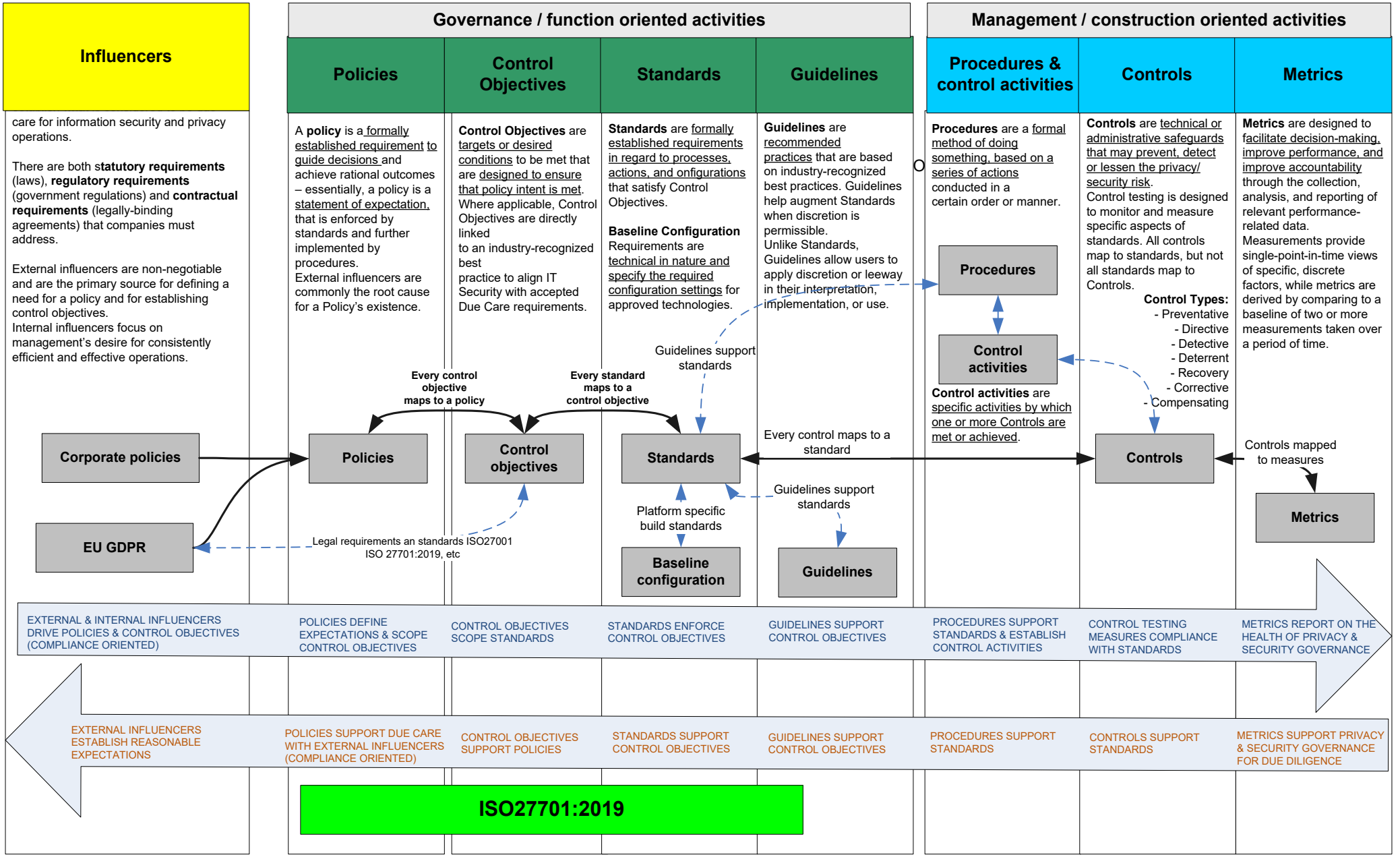
Complianceforge positions the different frameworks like this:

- COSO / COBIT – Strategic (Enterprise-Level Approach to Risk Management)
- ISO – Operational (Initiative / Program-Level Approach to Risk Management)
- NIST – Tactical (Asset / Project-Level Approach to Risk Management)

Figure 21: Operational (risk mitigating) value of different frameworks (information security)
Source: https://www.complianceforge.com (Retrieved at 05.2020)

From that perspective we can position ISO27701:2019 as a standard that delivers useful *data security* guidance on program-level with moderate coverage on the level of detailed tactical guidance.

Other standards, like e.g. NIST are probably more suited to deliver guidance regarding the construction, practical procedures and activities, operational controls and related metrics as displayed on the next page.



Scheme above: Adapted scheme – Original: Compliance Forge (Copyright © 2020 by ComplianceForge, LLC)
Source: https://www.complianceforge.com/word-crimes/policy-vs-standard-vs-control-vs-procedure

§ 6.13 Formulated ISO27701:2019 fit/gap findings

We have raised the question: Are the identified non-compliancy risks and perceived GDPR governance and management activities, ambiguities' and risks effectively addressed and mitigated in the ISO 27701:2019[31]?

In the table below we summarize the different aspects of our findings:

Fit / Gap assessment aspect(s)		Fit – Gap assessment	
		Fit or gap as PIMS?	**Comment**
The **foundation** of ISO 27701:2019		Medium fit as overall PIMS covering *all* the GDPR aspects. ISO 27701 has a very strong security focus, less focussed and detailed on other privacy aspects	ISO27701 as PIMS (Privacy Information Management System) is dependent on an existing ISMS (Information Security Management System) see § 6.4. The majority of the activities in the document are based on ISO27001 & 2:2013 (security & security extensions)
The **focus/core** of ISO 27701:2019			The full description of this ISO standard is: ISO/IEC 27701 **security techniques** – extension to ISO 27001 and 27002 for privacy information management. Security is not equal to privacy and privacy covers much more than data security! Privacy specific aspects are mentioned, but only a general direction is given, implementation specific guidance is lacking. (see § 6.5)
GDPR **article 32 aspects** mentioned?		Good fit	Most article 32 aspects are mentioned (see § 6.6)
Are the **article 32 violation hotspots (risks)** effectively addressed in ISO 27701:2019?		Weak - Medium fit	Yes, the risks related to the article 32 violation hotspots (§ 2.9) are mentioned however mainly on governance level. The DPA identified and fined the ineffective privacy *operations and operational controls*. ISO 27701:2019 has a limited focus on privacy, more on security. Operational guidance, -controls and metrics are weaker or absent in some cases (§ 6.8 and § 6.9)
Quality of controls in ISO 27701:2019?		Weak – medium fit	§ 6.9 shows that there are weak (or no) controls on the level of data *privacy* governance and management (PIMS), but much stronger control objectives regarding data security (ISMS). How to be in control of privacy if there are very limited (PIMS specific) controls?
Coverage of the GDPR requirements **as PIMS** including continues privacy improvement cycle?		Weak fit	ISO 27701 is focussed on *security* techniques as the extension to ISO 27001 and 27002. The *privacy* governance and management focus including controls and an improvement cycle are underdeveloped (§ 6.9) ISO 27701 cannot be seen as a strong PIMS, rather a privacy enhancement on top of an ISMS.
Privacy governance (COBIT view, see § 6.6 & 6.9)	[MONITOR]	Good fit	Good fit from an ISMS view (less from PIMS viewpoint)
	[EVALUATE]	Good fit	Good fit from an ISMS view (less from PIMS viewpoint)
	[DIRECT]	Good fit	Good fit from an ISMS view (less from PIMS viewpoint)
Privacy management (COBIT view, see § 6.6 & 6.9)	[PLAN]	Medium fit	Medium fit from an ISMS view (less from PIMS viewpoint)
	[BUILD]	Some/weak fit	Some/weak fit from an ISMS view (absent in PIMS view)
	[RUN]	Some/weak fit	Some/weak fit from an ISMS view (absent in PIMS view)
	[MONITOR]	Medium fit	Medium fit from an ISMS view (less from PIMS viewpoint)
Are contextual ambiguities addressed in ISO 27701:2019?		Medium fit	Privacy risk assessments performed in the context of data processing activities will reduce ambiguity (see § 3.6, § 6.11) The assessment aspects of article 32 § 6.11) are mentioned in section 7.2 of ISO 27701 (there is some guidance) but not very extensive (only high level).
Are (privacy) change management aspects addressed in ISO 27701:2019?		Weak fit	The aspects related to the successful implementation of a change (§ 3.2) are hardly addressed in ISO 27701.
Are the **privacy function – construction gaps** addressed in ISO 27701:2019?		Weak fit	ISO 27701 is focussed on the security & privacy *function* not its construction (see § 6.12 & 6.9), so implementation & execution specific guidance cannot be expected.

Table 12: Fit-gap assessment: are GDPR governance and (change) management activities, ambiguities' and risks effectively addressed and mitigated in ISO 27701:2019?

[31] See: https://www.iso.org/obp/ui/#iso:std:iso-iec:27701:ed-1:v1:en (Retrieved at 05.2020)

Findings summarized.
ISO 27701:2019 has been introduced as "guidance for establishing, implementing, maintaining and continually improving a Privacy Information Management System (PIMS)".
We have seen that ISO27701 has a strong focus on data security and this aspect is even dominant in the naming of the standard: ISO/IEC 27701 **security techniques** – extension to ISO 27001 and 27002 for privacy information management.
From a privacy governance and management point of view, data security is indeed a very important aspect, and ISO27701 addresses many privacy risks we identified as violation hotspots. However data security covers only one of the seven privacy principles mentioned in GDPR.
It is possible to have a very secure system that does not respect the privacy of the user.

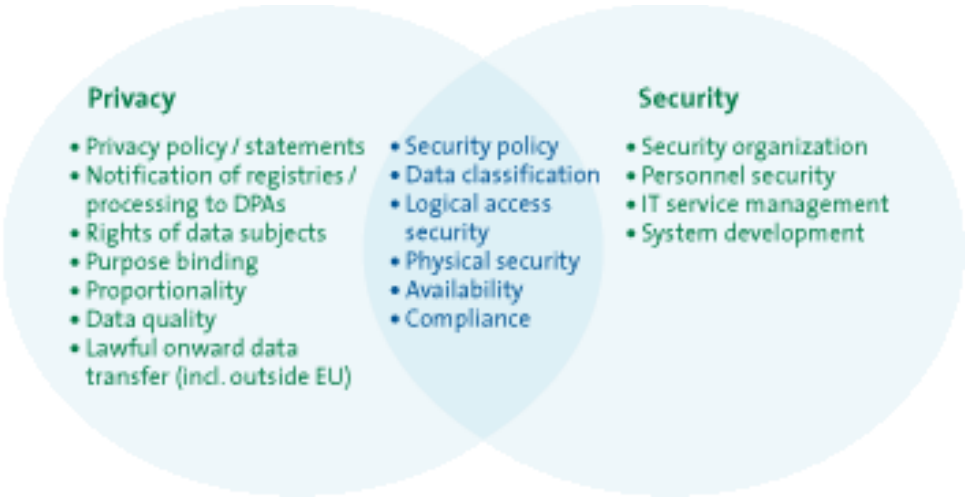


Figure 23: Similarities and differences between security and privacy [32]

The challenge is applying privacy enhancing technologies that do more than just improve data security measures. Security and privacy require different approaches: security still focuses predominantly on building walls around large personal information databases.
In contrast, privacy protection is aimed at minimizing the personal data collected and processed, while ensuring that this data is handled carefully through its lifecycle, wherever it flows or resides.

§ 6.14 Formulated ISO27701:2019 improvements

- Privacy and security (governance, management and operations) must be balanced (more) in order to fulfil the GDPR requirements. This balance can be improved in the ISO 27701 standard in order to qualify as a PIMS that covers both security and privacy.

- The full functional description of the PIMS is "scattered" over different standards: ISO 27001, ISO 27002 and ISO 27701. This is not very practical.

- Many data security guidelines in ISO 27001 and ISO 27002 were not designed in 2013 with privacy in mind, at least not with the GDPR in mind since the GDPR became law in 2018. ISO 27701 as a privacy extension to the ISO security standards is usable however simply adding "and privacy..." (see table 9) to an existing security standard may be too simplistic to cover the privacy principles and aspects mentioned in the GDPR.
  For effective privacy governance & management, most likely more is needed than adding privacy aspects to existing data security activities – data privacy asks for different skills, knowledge & mind-sets. A GRC (process) approach, merging the different security, privacy, risk and compliance disciplines might be a good instrument to mention.

[32] Picture reused from:
https://www.compact.nl/articles/privacy-by-design-from-privacy-policy-to-privacy-enhancing-technologies/
(Retrieved at 05.2020)

- The different change management barriers that could also influence the road to compliance with the GDPR like specificity ambiguity, consistency ambiguity, resource barriers, political and cognitive resistance are not really covered but relevant for effective privacy governance and management programs.

- The inability to bridge the gap between “know what to do” (function) to “know how to do this” (construction) will lead to ineffective privacy management or even violations of the GDPR. ISO27701 mainly describes the privacy function, not the construction of that function.

  Although ISO27701 can be seen as a standard that delivers useful guidance on program-level with moderate coverage on the level of detailed tactical guidance, it might be useful to refer to other standards for detailed governance guidance (like COBIT) or tactical guidance (like e.g. NIST, etc.).
  Standards, like e.g. NIST are probably more suited to deliver guidance regarding the construction, practical procedures and activities, operational controls and related metrics of the privacy function.

§ 6.15 Expert review on the research findings

The findings of chapter 2 – 6 are also reviewed by two experts active in the field of data privacy. Dr. Sandro Lovisa is leading the development of privacy governance software (SPG) at SAP in Waldorf, Germany. Dr. Anderson Santana de Oliveira is certified as GDPR privacy specialist (CIPP/E). I asked them to review the findings and conclusions of this research.

Review of Anderson Santana de Oliveira

“Translation of GDPR article 32 into effective privacy governance and management practices. A view on GDPR ambiguity, non-compliancy risks and effectiveness of ISO 27701:2019 as Privacy Management System”.

Author: Ing. J W (Nico) Kuijper MSc

The thesis makes a systematic analysis of enforcement actions undertaken in the first two years since the EU GDPR has come into effect. It tries to identify ambiguities in the guidance provided in the regulation itself and related security/privacy governance standards, such as COBIT and ISO 27701, which may result in faulty implementations of technical and organizational measures to comply with Article 32.

The EU GDPR, as a number of other regulations, contains legal terms and language that leave room for interpretation and legal debate. Principles such as data minimization and proportionality can be interpreted in different contexts in several ways, allowing data controllers to justify their processing activities. Albeit the existing ambiguity in Article 32, it has an inescapable non-compliance proof: when data breaches happen, which combined with Article 33, forces companies to recognize non-compliant practices, regarding data security, which is confirmed by the findings.

The work unveils the lack of a consistent and comprehensive standards conciliating privacy and security objectives. The survey conducted with privacy professionals revealed the need to bridge governance to technical privacy architecture in systems and processes - possibly resulting in an overarching privacy by design approach.

This thesis is timely and much welcome. Perhaps it can influence the next generation of privacy standards, where hopefully accountability will be in their core, reducing the "thick the box" behaviour induced by most standards today.”

Review of Sandro Lovisa

“Translation of GDPR article 32 into effective privacy governance and management practices. A view on GDPR ambiguity, non-compliancy risks and effectiveness of ISO 27701:2019 as Privacy Management System”.

Author: Ing. J W (Nico) Kuijper MSc

The presented work of Nico JW Kuijper provides an interesting research approach on possible root causes of GDPR compliance breaches, where legal ambiguity is evaluated as one. The gained findings of compliance obstacles, especially in the context of GDPR Art. 32, are then mapped in a second step against existing ISO 27701 to evaluate if the standard may address these.

The used adoption of change management aspects is a fresh way to detect potential challenges in the context of implementing new regulatory frameworks. Following this approach, the analysis delivers tangible results like the presented function-construction gap.

In order to comply with privacy requirements, the needed alignment of different disciplines, as policy defining (legal/DPO) and compliance enabling (information technology/CISO), is deducted very comprehensively from the research findings.

This aspect finds explicit support in the relevance of the identified new types of principle-agent relationships, giving the individual more influence on how organizations handle their data, as also on enhancing the formerly security focused principle-agent relationship by a new privacy angle. As outlined, resulting in a new and very different risk concept as in the classical IRM discipline.

Nico JW Kuijper defines this in a wider sense as privacy architecture and proposes correctly the usage of GRC as a corporate function and methodology to potentially solve the structural and conceptual problem. In this context future research could also be extended to the respective line of business as the actual data controller, completing the various resources affected by privacy requirements in an organization (e.g. an explicit three lines of defence privacy concept).

The potential ambiguity of legal texts may find its justification in the discipline of law itself, or as outlined in the necessity of technological neutrality, so the importance of rather hard coded guidance like ISO standards are an essential aid to translate the law into practical controls for the various strategic, operational or tactical levels.

The conducted analysis of ISO 27701 demonstrates that the standard does not provide tangible guidance on all levels of detail. Further it is argued, that its content is still too much deducted from a pure security perspective, neglecting the necessary privacy risk point of view.

This finding is a good starting point for further work on concrete examples for privacy controls to enhance the existing guidance. However, an additional analysis of other standards like NIST may also add to the research and may help to better understand if missing guidance within ISO is due to the outlined difference between strategic, operational and tactical standards. In this context the conducted fit/gap analysis within chapter 6 points out concrete missing privacy controls as major weakness and gaps to be closed.

Last but not least, the chosen methodical approach of exploratory case study makes much sense under the actual circumstance of missing extensive research on this specific subject.

A strength of this thesis is its accuracy on outlining logically reproducible findings.

All in all, this thesis unfolds its relevance to the field of privacy research from a corporate risk perspective and is a very good starting point for additional work.

Sandro Lovisa, 8th May 2020

7. Conclusions and recommendations

§ 7.1 Introduction

In this chapter we discuss the findings and conclusion of the research and some further research recommendations are formulated.

§ 7.2 Main research question, findings

Our main research question we aimed to answer has been formulated as follows:

> What are the most violated GDPR articles/aspects in combination with the highest fines? What are the (perceived) risks, ambiguities, the required governance and (change) management activities of this most violated article and are these effectively addressed in ISO 27701 as Privacy Information Management System?

The summarized answers to the (sub) questions are:

1. What are the most violated GDPR articles in combination with the highest financial fines? (Chapter 2).

- The most violated **article** is article *32* (secure data processing). It is linked to the highest cumulative fines and is the 2nd most violated GDPR article (period 04.2018 – 03.2020).
- **Violation hotspots** according the article 32 ontological domain classifications, combined with the analysis of the DPA rulings, are: failing to realize ongoing confidentiality and integrity of data processing, failing to realize resilience of systems / services.

2. What are the (perceived) risks, ambiguities, the required governance and (change) management activities of this article? (Chapter 3 and 4)

- **Privacy activities.** The ontology of article 32 reveals the COBIT activities: data privacy risk analysis & instructions (governance) and risk mitigation/monitoring (management).
- **Violation risks area's:** the authorities mainly fined the article 32 violation symptoms; failing or ineffective privacy management activities like PLAN-BUILD-RUN-MONITOR (COBIT view) without clarifying the possible underlying root causes.
- **Perceived risks:** the questionnaire respondents identified the privacy improvements and risks mainly on governance level (COBIT activities EVALUATE and DIRECT).
- **Change management risks** identified on privacy governance & management level are:
  - Change clarity – the ambiguity (reduction) of the GDPR requires a contextual analysis
  - Change ability – security & privacy requires different skills, knowledge and frameworks
  - Change willingness - expect resistance (divergent interests, roles and cognitive views)
- **A (privacy) governance system** (GRC) should cover the complex and ongoing alignment of processes, organizational structures, policies and procedures, information flows, culture and behaviours, skills, and infrastructure. (COBIT 2019 components).
- **(Privacy) architecture** addresses the function construction gap – the inability to bridge the gap between "know what to do" (function) to "know how to do this" (construction). Both the GDPR & ISO 27701 describe the function, not the construction of that function.

3. Are the required governance and (change) management activities, ambiguity and violation risks of article 32 effectively addressed in ISO 27701? (Chapter 6)

- ISO 27701:2019 has a predominant focus on data security, however data security covers only one of the seven privacy principles mentioned in GDPR.
- Most of the ontological aspects of article 32 are covered in ISO27701 however these are not directly helpful from an operational and execution point of view (BUILD & RUN).
- The quality of *operational* privacy controls in ISO27701:2019 are weak or even absent. When controls are discussed they can be seen as (security – not privacy) control objectives rather than operational privacy controls with concrete metrics.
- Privacy and security (governance, management and operations) must be balanced (more) in order to fulfil the GDPR requirements. This balance can be improved in the ISO 27701 standard in order to qualify as a PIMS that covers both security and privacy.
- The full functional description of the PIMS is "scattered" over different standards: ISO 27001, ISO 27002 and ISO 27701. This is not very practical.

- Adding "privacy" (see table 9) to an existing security standard may be too simplistic to cover the privacy principles and aspects mentioned in the GDPR.
  For effective privacy governance & management, most likely more is needed than adding privacy aspects to existing data security activities – data privacy asks for different skills, knowledge & mind-sets. A GRC (process) approach, merging the different security, privacy, risk and compliance disciplines might be a good instrument to mention.
- The different change management barriers that could also influence the road to compliance with the GDPR like specificity ambiguity, consistency ambiguity, resource barriers, political and cognitive resistance are not really covered but relevant for effective privacy governance and management programs.
- The inability to bridge the gap between "know what to do" (function) to "know how to do this" (construction) will lead to ineffective privacy management or even violations of the GDPR. ISO27701 mainly describes the privacy function, not the construction of that function.
- Although ISO27701 can be seen as a standard that delivers useful guidance on program-level with moderate coverage on the level of detailed tactical guidance, it might be useful to refer to other standards for detailed governance guidance (like COBIT) or tactical guidance (like e.g. NIST, etc.).

Summarized: ISO27701:2019 is a strong standard regarding the improvement of data security and taking into account different privacy aspects. However, it does not cover all the privacy governance and management requirements, aspects and risks sufficiently and in a well-structured way (as elaborated by the GDPR) to see the standard as a mature and solid Privacy Information Management System (PIMS).

§ 7.3 Recommendation in the context of privacy challenges related to COVID-19 applications

This research addressed many different privacy aspects and gaps and highlighted the need for a holistic and systematic approach of (privacy) governance and management based on e.g. COBIT 2019 components, pairing the different viewpoints, risks and aspects of both privacy and security in a structured way.
Current affairs and the news make sometimes painfully visible what the consequences are when this holistic and systematic approach on (privacy) governance and management is not embraced.

One example: in April 2020, the Dutch government organized an "appathon"[33] for the development of a privacy proof COVID19 mobile app to track, trace and inform people that came near a Corona / COVID19 infected person. 750 companies responded to this request to deliver a design for a "smart digital solution" in this context. After three days, only seven companies were selected and put on the shortlist. The role of the society in reviewing the (privacy) design of the solution is also remarkable: the Dutch government made the source code of the applications public for review. This highlights the increased influence of the individual and society as "principle" regarding privacy related topics (see § 3.3).

After a review of the seven solutions, the ruling was that *none of these solutions* fulfilled the requirements of the GDPR. This is interesting since the ICO for example published [34] some guidelines regarding the processing of privacy relevant data in the context of COVID19.
In the evaluation by experts[35] on what went wrong in this process, we can recognize some aspects we addressed in this research, like e.g.
- Incomplete formulation of requirements and privacy by design aspects.
- Failing change management (due to time pressure).
- A clear gap between the privacy function and its construction (privacy architecture).

This emphasizes the complexity and the need for a holistic and systematic approach of (privacy) governance and management.

[33] Source: https://www.nrc.nl/nieuws/2020/04/19/ministerie-kleunt-mis-met-appathon-a3997235 (Retrieved at 05.2020)

[34] Source: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/04/combatting-covid-19-through-data-some-considerations-for-privacy (Retrieved at 05.2020)

[35] Source: (Retrieved at 05.2020)
https://www.security.nl/posting/653173/Privacyanalyse%3A+contactonderzoekapps+voldoen+niet+aan+alle+eisen+AVG

§ 7.4 Conclusions

Standards, like ISO 27701, fulfil a useful role in compliance with the GDPR, but standards are only a part of the solution.
Data privacy is a complex and ever evolving topic that asks for careful contextual judgement and alignment of governance and management activities.
A more holistic and systematic approach of (privacy) based on e.g. COBIT 2019 or GRC components, pairing the different viewpoints, risks and aspects of both privacy and security in a structured way will contribute to more mature data privacy concepts.
The focus of the authorities, that at the end will determine if you comply with the GDPR, is how effective your privacy governance and management practices at the end are.
The inability to construct and operate the privacy function you have designed is the most significant risk, and that the type of risk the authorities will focus on!

§ 7.5 Reflection

In this second master (of IT Governance, Risk and Assurance) that I attended at the AMS, the corporate governance aspect and the translation of governance into effective management including all the relevant controls has been highlighted.
The course at the University of Maastricht on GRC has a strong financial and operational risk audit and governance focus and is less IT driven. Nevertheless many of the aspects I have learned can be applied to other (IT related) topics like privacy governance and management. That inspired me to apply the knowledge learned in this master to this particular work field of data privacy. It was interesting to see how human behaviour plays an important role in governance and management, and I was in particular inspired by the “mind the gap” model of AMS Prof. Ron Meyer. It helped me to focus (more) on the many complex factors and hurdles are that we will face with every major change we try to implement in an organization.

§ 7.6 Contribution and limitations

This research aimed at the identification of materialized GDPR violation risks, the related privacy activities and violation risks area’s identified in article 32.
It also identified the type of (COBIT) privacy governance and management activities that could be linked to the GDPR violations and the possible violation root causes and the risk mitigating value of ISO 27701 as Privacy Information Management System (PIMS).
These topics were not yet researched since the GDPR is a relatively new legislation as well as the ISO standard reviewed and this hopefully contributes to new knowledge in this area.
This contributed to a certain level of rigour, although practitioners as well bring a lot of value and relevance into this research. It must however being mentioned that the number of respondents in the survey are a limitation in the research.
Nevertheless this paper could bring some contribution to science by bringing information from different theoretical models together and combining this with the perception of practitioners in this ever and quickly evolving field of data privacy.

§ 7.7 Recommendations and further research

I hope this paper can contribute to an improved and more structured way to approach data privacy governance and management – beneficial to both organisations as individuals.
This exploratory case study contributed to the identification of relevant privacy governance and management aspects that can influence the road to GDPR compliance. It demonstrated that standards are just one, sometimes limited, instrument in the road to GDPR compliance.

The research also leaves questions unanswered regarding e.g. the *actual* (measurable) root causes of the GDPR violations, like:
Are the current Article 32 DPA rulings the result of ambiguities in the legislative text?
Or due to poor PIMS implementations? Or caused by gaps in standards? Or due to poor governance? Or a poor translation of the privacy function to the technical construction of that privacy function? Or failing change management?

More research is therefore needed to further explore this complex and ever evolving topic, and I hope these questions will be addressed in future research.

Bibliography and references

§ 8.1 Bibliography

Dallas, G. (2004). *Governance and Risk: An Analytical Handbook for Investors, Managers, Directors, and Stakeholders.* MCGRAW-HILL Professional .

Dietz, J. (2006). *Enterprise Ontology, Theory and Methodology.* Springer.

Dietz, J., & Mulder, H. (2020). *Enterprise Ontology, A Human-Centric Approach to Understanding the Essence of Organisation.* Springer.

European Union. (2018, 04). *European Union Regulation 2016/679, General Data Protection Regulation (GDPR).* Retrieved from GDPR: http://eur- lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

Fieldfischer Silicon Valey. (2020). *Episode 7 - ISO 27001 and the GDPR*. Retrieved from https://soundcloud.com/ (Podcasts): https://soundcloud.com/fieldfishersiliconvalley/episode-7-iso-27001-and-the-gdpr

Friedman, A., & Darrell , M. (2010). Privacy and Security in Cloud Computing. *Issues in Technology Innovation*, http://ent.cs.nccu.edu.tw/drupal/files/privacySecurityInCloudComputing(Brookings).pdf.

Hoogervorst. (2009). Enterprise Governance and enterprise engineering. In Hoogervorst, *Enterprise Governance and enterprise engineering* (p. 294). Springer.

ISACA. (2020). *Cobit resources.* Retrieved from ISACA: https://www.isaca.org/resources/cobit

ISO. (2019). *ISO/IEC 27701:2019*. Retrieved from ISO.ORG: https://www.iso.org/obp/ui/#iso:std:iso-iec:27701:ed-1:v1:en

Law firm C|M|S. (2020, 03). *Fine statistics*. Retrieved from GDPR Enforcement tracker: https://www.enforcementtracker.com

Lokin, M. (2018). *Wendbaar wetgeven.* Retrieved from Publications - Research output: https://research.vu.nl/en/publications/wendbaar-wetgeven

Massey , A. (2014). Identifying and classifying ambiguity for regulatory requirements. *https://ieeexplore.ieee.org/abstract/document/6912250* (pp. 83-92). Karlskrona: IEEE 22nd International Requirements Engineering Conference, https://ieeexplore.ieee.o.

Meyer, R. (2019). *Mind the gap Changemanagement model*. Retrieved from blog.antwerpmanagementschool.be: https://blog.antwerpmanagementschool.be/en/ron-meyer-episode-1-mind-the-gap

Pandit, H. (2020, 03 31). *GDPRtEXT*. Retrieved from GDPR Ontology specification: https://openscience.adaptcentre.ie/ontologies/GDPRtEXT/deliverables/docs/ontology#DataSecurity

Poel, K. v. (2012). *Lagging and leading indicators*. Retrieved from KPI Library: https://kpilibrary.com/topics/lagging-and-leading-indicators

Recker, J. (2013). Scientific Research in Information Systems A Beginner's Guide. In J. Recker, *Scientific Research in Information Systems A Beginner's Guide [Book]. pp. 95-97) : Springer, 2013* (pp. 95-97). Springer.

Sennet, A. (2016). *Ambiguity*. Retrieved from Stanford Encyclopedia of Philosophy: https://plato.stanford.edu/archives/spr2016/entries/ambiguity/

§ 8.2 List of Tables

§ 8.3 List of Figures

§ 8.4 Abbreviations used

AMS	Antwerp Management School
CISO	Chief Information Security Officer
COBIT	Control Objectives for Information and related Technology
DPA	Data Privacy Authorities
DPO	Data Privacy Officer
EGIT	Enterprise Governance of IT
GDPR	General Data Protection Regulation
ISO	International Standardization Organization
IT	Information Technology
ICO	Information Commissioners Office (UK)
ICT	Information and communication technology
ISACA	Information Systems Audit and Control Association
ISMS	Information Security Management System
KPI	Key Performance Indicator
PIMS	Privacy Information Management System

§ 8.5 Document versions

Version	Date	Distributed to	Description of changes
0.1	27.11.2019	Hans Mulder	Initial draft version of the research question and research plan
0.2	16.1.2020	Hans Mulder	Discussed questionnaire approach, etc.
0.3	30.3.2020	Hans Mulder	Requested to review chapter 2 - 3
0.4	21.4.2020	Hans Mulder	Requested to review chapter 2 - 6
0.5	27.4.2020	Hans Mulder	Requested to review chapter 2 - 8
0.6	2.5.2020	Sandro Lovisa, Anderson Santana de Oliveira	Requested Dr. Sandro Lovisa, Dr. Anderson Santana de Oliveira to review the findings
0.7	9.5.2020	Hans Mulder	Processed last corrections, added expert review to chapter 6, Requested final review
1.0	11.5.2020	AMS	Final version

Annexes

GDPR Article 32, recital 82

GDPR Article 32 - Security of processing

1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:
(a) the pseudonymisation and encryption of personal data;
(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

3. Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.

4. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.

Recital (83)
In order to maintain security and to prevent processing in infringement of this Regulation, the controller or processor should evaluate the risks inherent in the processing and implement measures to mitigate those risks, such as encryption. Those measures should ensure an appropriate level of security, including confidentiality, taking into account the state of the art and the costs of implementation in relation to the risks and the nature of the personal data to be protected. In assessing data security risk, consideration should be given to the risks that are presented by personal data processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed which may in particular lead to physical, material or non-material damage.

C|M|S GDPR Compliancy tracker - Article 32 violations up to 03.2020

Source: https://www.enforcementtracker.com/
Filter applied: article 32 violations.

Authority (DPA)	Case number	Date	Fine [€] x 1000	Data controller / Processor	Violation Quoted GDPR Art.	Violation Type category	Violation summary	Source
Spanish Data Protection Authority (aepd)	1	3-3-2020	42	Vodafone España, S.A.U.	Art. 5 (1) f) GDPR, Art. 32 GDPR	Insufficient technical and organisational measures to ensure information security	According to the AEPD, the company had not been able to demonstrate adequate measures to ensure information security, leading to unauthorized access to personal data of a client. [PLAN,BUILD, RUN, MONITOR]	link
Spanish Data Protection Authority (aepd)	2	28-2-2020	48	Vodafone ONO, S.A.U.	Art. 32 GDPR	Insufficient technical and organisational measures to ensure information security	The decision was taken due to several deficiencies in information security. For example, two people were given the same security access key. [PLAN,BUILD, RUN, MONITOR]	link
Spanish Data Protection Authority (aepd)	3	14-2-2020	2,5	Grupo Valsor Y Losan, S.L.	Art. 5 (1) f) GDPR , Art. 32 GDPR	Insufficient technical and organisational measures to ensure information security	The controller had disclosed personal data to a third party in a property purchase agreement (breach of principles of integrity and confidentiality of personal data) [RUN]	link
Spanish Data Protection Authority (aepd)	4	14-2-2020	42	Vodafone España, S.A.U.	Art. 5 (1) f) GDPR, Art. 32 GDPR	Insufficient technical and organisational measures to ensure information security	The complainant had access to third party data in his personal Vodafone profile. [PLAN,BUILD, RUN, MONITOR]	link
Spanish Data Protection Authority (aepd)	5	14-2-2020	30	Xfera Moviles S.A.	Art. 5 (1) f) GDPR, Art. 32 GDPR	Insufficient technical and organisational measures to ensure information security	The AEPD found that a third party had access to the name, telephone number and address of another customer. [PLAN,BUILD, RUN, MONITOR]	link
Italian Data Protection Authority (Garante)	6	23-1-2020	30	Azienda Ospedaliero Universitaria Integrata di Verona (Hospital)	Art. 5 (1) f) GDPR, Art. 32 GDPR	Insufficient technical and organisational measures to ensure information security	The fine was preceded by access to health data by unauthorised persons, allowing a trainee and a radiologist to gain access to the health data of their colleagues. The investigations revealed that the technical and organisational measures taken by the hospital to protect health data had proved to be insufficient to ensure adequate protection of patients' personal data, resulting in unlawful data processing. According to the data protection authority, the breach could have been avoided if the hospital had simply followed the guidelines for health records issued by the data protection authority in 2015, which stipulate that access to health records must be restricted only to health personnel involved in patient care. [PLAN,BUILD, RUN, MONITOR]	link
Italian Data Protection Authority (Garante)	7	23-1-2020	30	Sapienza Università di Roma	Art. 5 (1) f) GDPR, Art. 32 GDPR	Insufficient technical and organisational measures to ensure information security	The fine is based on the fact that, according to the data protection authority, the Sapienza Università made available online identification data of two people who had reported possible illegal behaviour to the university. This was due to the lack of adequate technical access control measures within the whisleblowing management system, which had not limited access to such data to authorized personnel only. [PLAN,BUILD, RUN, MONITOR]	link

Authority (DPA)	Case number	Date	Fine [€] x 1000	Data controller / Processor	Violation - Quoted Art.	Violation Type	Violation summary	Source
Cyprian Data Protection Commissioner	8	13-1-2020	9	Social Insurance Services of the Ministry of Labor, Welfare and Social Insurance	Art. 32 GDPR	Insufficient technical and organisational measures to ensure information security	Granting the police access to personal data and failing to take adequate measures to secure the data, despite the warnings of the Supervisor, constituted a breach of Article 32 of the GPPR. [PLAN,BUILD, RUN, MONITOR]	link
Hellenic Data Protection Authority (HDPA)	9	19-12-2019	150	Aegean Marine Petroleum Network Inc.	Art. 5 GDPR, Art. 6 GDPR, Art. 32 GDPR	Insufficient technical and organisational measures to ensure information security	Companies outside the Aegean Marine Petroleum Group had access to its servers containing personal data and copied the contents of the servers, since Aegean Marine Petroleum failed to take the necessary technical measures to secure the processing of large amounts of data and to keep the relevant software separate from the personal data stored on the servers. Furthermore, Aegean Marine Petroleum had not informed the data subjects of the processing of their personal data stored on the servers. [PLAN,BUILD, RUN, MONITOR]	link
Romanian National Supervisory Authority for Personal Data Processing (ANSPDCP)	10	18-12-2019	2	Telekom Romania Mobile Communications SA	Art. 32 GDPR	Insufficient technical and organisational measures to ensure information security	The company has failed to ensure the accuracy of the processing of personal data which resulted in a disclosure of a clients personal data to another client. [PLAN,BUILD, RUN, MONITOR]	link
Information Commissioner (ICO)	11	17-12-2019	320	Doorstep Dispensaree Ltd. (Pharmacy)	Art. 32 GDPR	Insufficient technical and organisational measures to ensure information security	The company had stored some 500,000 documents containing names, addresses, dates of birth, NHS numbers and medical information and prescriptions in unsealed containers at the back of the building and failed to protect these documents from the elements, resulting in water damage to the documents. [PLAN,BUILD, RUN, MONITOR]	link
Spanish Data Protection Authority (aepd)	12	10-12-2019	5	Shop Macoyn, S.L.	Art. 32 GDPR	Insufficient technical and organisational measures to ensure information security	The company has sent advertising e-mails to several recipients where the e-mail addresses of all other recipients were visible to all recipients, because the recipient addresses were inserted as CC and not as BCC. [PLAN,BUILD, RUN, MONITOR]	link

Authority (DPA)	Case number	Date	Fine [€] x 1000	Data controller / Processor	Violation - Quoted Art.	ViolationType	Violation summary	Source
Romanian National Supervisory Authority for Personal Data Processing (ANSPDCP)	13	10-12-2019	14	Hora Credit IFN SA	Art. 5 GDPR, Art. 25 GDPR, Art. 32 GDPR, Art. 33 GDPR	Insufficient technical and organisational measures to ensure information security	The sanctions were applied as a result of a complaint alleging that Hora Credit IFN SA transmitted documents containing personal data of another person to a wrong e-mail address. Following the investigation it was found that Hora Credit IFN SA processed the data without providing effective mechanisms for verifying and validating the accuracy of the data collected processed according to the principles set out in art. 5 of the GDPR. It was also found that the operator did not take sufficient security measures for personal data, according to art. 25 and 32 of the GDPR, so as to avoid unauthorized and accessible disclosure of personal data to third parties. At the same time, Hora Credit IFN SA did not notify the Supervisory Authority of the security incident that was brought to its notice, according to art. 33 of the GDPR, within 72 hours from the date it became aware of it. The fine consists of three partial fines of EUR 3000, EUR 10000 and EUR 1000. [PLAN,BUILD, RUN, MONITOR]	link
The Federal Commissioner for Data Protection and Freedom of Information (BfDI)	14	9-12-2019	9,550,000	Telecoms provider (1&1 Telecom GmbH)	Art. 32 GDPR	Insufficient technical and organisational measures to ensure information security	The Controller is a company offering telecommunication services. A caller could obtain extensive information on personal customer data from the company's customer service department simply by entering a customer's name and date of birth. In this authentication procedure, the BfDI aws a violation of Article 32 GDPR, according to which a company is obliged to take appropriate technical and organisational measures to systematically protect the processing of personal data. Due to the company's cooperation with the data protection authority, the fine imposed was at the lower end of the scale. [PLAN,BUILD, RUN, MONITOR]	link
Romanian National Supervisory Authority for Personal Data Processing (ANSPDCP)	15	4-12-2019	20	S CNTAR TAROM SA (Airline)	Art. 32 GDPR	Insufficient technical and organisational measures to ensure information security	The Romanian data protection authority imposed a sanction on an airline because it has not taken appropriate measures to ensure that any natural person acting under its supervision processes personal data in accordance with its instructions (Article 32(4) of the GDPR). This resulted in an employee having unauthorized access to the booking application and being able to photograph a list with the personal data of 22 passengers/customers to disclose this list on the Internet. [PLAN,BUILD, RUN, MONITOR]	link

Romanian National Supervisory Authority for Personal Data Processing (ANSPDCP)	16	29-11-2019	500	Homeowners Association	Art. 32 GDPR	Insufficient technical and organisational measures to ensure information security	The association used video surveillance systems without proper information according to Art. 13 GDPR and without adequate security measures regarding the persons having access to the system. [PLAN,BUILD, RUN, MONITOR]	link
Authority (DPA)	**Case number**	**Date**	**Fine [€] x 1000**	**Data controller / Processor**	**Violation - Quoted Art.**	**ViolationType**	**Violation summary**	**Source**
Romanian National Supervisory Authority for Personal Data Processing (ANSPDCP)	17	28-11-2019	80	ING Bank N.V.	Art. 32 GDPR	Insufficient technical and organisational measures to ensure information security	ING Bank has not taken appropriate technical and organisational measures for an automated data processing system during the settlement process of card transactions affecting 225,525 customers, resulting in double transactions being executed between 8 and 10 October. [PLAN,BUILD, RUN, MONITOR]	link
Romanian National Supervisory Authority for Personal Data Processing (ANSPDCP)	18	25-11-2019	11	Courier Services Company	Art. 32 GDPR	Insufficient technical and organisational measures to ensure information security	The fine was imposed because the controller failed to take appropriate technical and organisational measures leading to the loss and unauthorised access to personal data (name, bank card number, CVV code, cardholder's address, personal identification number, serial and identity card number, bank account number, authorised credit limit) of approximately 1,100 data subjects. [PLAN,BUILD, RUN, MONITOR]	link
Spanish Data Protection Authority (aepd)	19	19-11-2019	60	Corporación radiotelevisión espanola	Art. 32 GDPR	Insufficient technical and organisational measures to ensure information security	CORPORACIÓN RADIOTELEVISIÓN ESPAÑOLA and the trade union have reported a security breach to the AEPD after six unencrypted USB sticks containing personal data were lost. The violation affected about 11,000 people, including identification data, employment data, data about criminal convictions and health data. [PLAN,BUILD, RUN, MONITOR]	link
Spanish Data Protection Authority (aepd)	20	19-11-2019	60	Xfera Moviles S.A.	Art. 32 GDPR	Insufficient technical and organisational measures to ensure information security	An individual complainant had received an SMS from Xfera Móviles which was to be addressed to a third party and which allowed him to access the account and personal data of this third party on the Xfera Móviles website via the telephone number and password received by SMS. [PLAN,BUILD, RUN, MONITOR]	link
Dutch Supervisory Authority for Data Protection (AP)	21	31-10-2019	900	UWV (Dutch employee insurance service provider)	Art. 32 GDPR	Insufficient technical and organisational measures to ensure information security	As the UWV (the Dutch employee insurance service provider - "Uitvoeringsinstituut Werknemersverzekeringen") did not use multi-factor authentication when accessing the online employer portal, security was inadequate. Employers and health and safety services were able to collect and display health data from employees in an absence system. [PLAN,BUILD, RUN, MONITOR]	link

Data Protection Authority of Baden-Wuerttemberg	22	24-10-2019	100	Food company	Art. 5 GDPR, Art. 32 GDPR	Insufficient technical and organisational measures to ensure information security	The company had set up an applicant portal on its website where interested parties could submit their application documents online. However, the company did not offer an encrypted transmission of the data, nor did it store the applicant data in an encrypted or password-protected manner. In addition, the unsecured applicant data was linked to Google, so that anyone searching for the respective applicant names on Google could find their application documents and retrieve them without access restrictions. [PLAN,BUILD, RUN, MONITOR]	link
Romanian National Supervisory Authority for Personal Data Processing (ANSPDCP)	23	9-10-2019	150	Raiffeisen Bank SA	Art. 32 GDPR	Insufficient technical and organisational measures to ensure information security	Raiffeisen Bank Romania carried out scoring assessments on the basis of personal data of individuals registered on the Vreau Credit platform provided by the platform's staff via WhatsApp and then returned the result to Vreau Credit using the same means of communication [PLAN,BUILD, RUN, MONITOR].	link
Romanian National Supervisory Authority for Personal Data Processing (ANSPDCP)	24	9-10-2019	20	Vreau Credit SRL	Art. 32 GDPR, Art. 33 GDPR	Insufficient technical and organisational measures to ensure information security	Raiffeisen Bank Romania carried out scoring assessments on the basis of personal data of individuals registered on the Vreau Credit platform provided by the platform's staff via WhatsApp and then returned the result to Vreau Credit using the same means of communication. [PLAN,BUILD, RUN, MONITOR]	link
Polish National Personal Data Protection Office (UODO)	25	10-9-2019	645	Morele.net	Art. 32 GDPR	Insufficient technical and organisational measures to ensure information security	The Polish data protection authority imposed a fine of over PLN 2.8 million (approx. €644,780) on Morele.net for insufficient organisational and technical safeguards, which led to unauthorised access to the personal data of 2.2 million people. [PLAN,BUILD, RUN, MONITOR]	link
Data Protection Commision of Bulgaria (KZLD)	26	28-8-2019	2,600,000	National Revenue Agency	Art. 32 GDPR	Insufficient technical and organisational measures to ensure information security	Leakage of personal data in a hacking attack due to inadequate technical and organisational measures to ensure the protection of information security. It was found that personal data concerning about 6 million persons was illegally accessible. [PLAN,BUILD, RUN, MONITOR]	link
Data Protection Commision of Bulgaria (KZLD)	27	28-8-2019	511	DSK Bank	Art. 32 GDPR	Insufficient technical and organisational measures to ensure information security	Leakage of personal data due to inadequate technical and organisational measures to ensure the protection of information security. Third parties had access to over 23000 credit records relating to over 33000 bank customers including personal data such as names, citizenships, identification numbers, adresses, copies of identity cards and biometric data. [PLAN,BUILD, RUN, MONITOR]	link

French Data Protection Authority (CNIL)	28	25-7-2019	180	ACTIVE ASSURANCES (car insurer)	Art. 32 GDPR	Insufficient technical and organisational measures to ensure information security	Large amount of customer accounts, clients' documents (including copies of driver's licences, vehicle registration, bank statements and documents to determine whether a person had been the subject of a licence withdrawal) and data were easily accessible online. The CNIL, between others, criticised the password management (unauthorized access was possible without any authentication). [PLAN,BUILD, RUN, MONITOR]	link
Information Commissioner (ICO)	29	9-7-2019	110,390, 200	Marriott International, Inc	Art. 32 GDPR	Insufficient technical and organisational measures to ensure information security	Please note: This fine is not final but will be decided on when the company and other involved supervisory authorities of other member states have made their representations. The ICO issued a notice of its intention to fine Marriott International Inc which relates to a cyber incident which was notified to the ICO by Marriott in November 2018.GDPR infringements are likely to involve a breach of Art. 32 GDPR. A variety of personal data contained in approximately 339 million guest records globally were exposed by the incident, of which around 30 million related to residents of 31 countries in the European Economic Area (EEA). Seven million related to UK residents. It is believed the vulnerability began when the systems of the Starwood hotels group were compromised in 2014. Marriott subsequently acquired Starwood in 2016, but the exposure of customer information was not discovered until 2018. The ICO's investigation found that Marriott failed to undertake sufficient due diligence when it bought Starwood and should also have done more to secure its systems. [EVALUATE, DIRECT - PLAN,BUILD, RUN, MONITOR]	link
Information Commissioner (ICO)	30	8-7-2019	204,600, 000	British Airways	Art. 32 GDPR	Insufficient technical and organisational measures to ensure information security	Please note: This fine is not final but will be decided on when the company and other involved supervisory authorities of other member states have made their representations. The ICO issued a notice of its intention to fine British Airways £183.39M for GDPR infringements which likely involve a breach of Art. 32 GDPR. The proposed fine relates to a cyber incident notified to the ICO by British Airways in September 2018. This incident in part involved user traffic to the British Airways website being diverted to a fraudulent site. Through this false site, customer details were harvested by the attackers. Personal data of approximately 500,000 customers were compromised in this incident, which is believed to have begun in June 2018. The ICO's investigation has found that a variety of information was compromised by poor security arrangements at the company, including log in, payment card, and travel booking details as well name and address information. [MONITOR]	link

Authority (DPA)	Case number	Date	Fine [€] x 1000	Data controller / Processor	Violation - Quoted Art.	ViolationType	Violation summary	Source
Romanian National Supervisory Authority for Personal Data Processing (ANSPDCP)	31	5-7-2019	3	LEGAL COMPANY & TAX HUB SRL	Art. 32 GDPR	Insufficient technical and organisational measures to ensure information security	The fine was imposed because adequate technical and organizational measures to ensure a level of security appropriate to the risk of processing were not implemented. This has led to unauthorized disclosure and unauthorized access to the personal data of people who have made transactions received by the avocatoo.ro website (name, surname, mailing address, email, phone, job, details of transactions made), due to publicly accessible documents between 10th of December 2018 and 1st of February 2019. The National Supervisory Authority applied the sanction following a notification dated 12th of October 2018 indicating that a set of files regarding the details of the transactions received by the avocatoo.ro website which contained the name, surname, address correspondence, email, telephone, job and details of transactions made, was publicly accessible through two links. [PLAN,BUILD, RUN, MONITOR]	link
Romanian National Supervisory Authority for Personal Data Processing (ANSPDCP)	32	2-7-2019	15	WORLD TRADE CENTER BUCHAREST SA	Art. 32 GDPR	Insufficient technical and organisational measures to ensure information security	The breach of data security was that a printed paper list used to check breakfast customers and containing personal data of 46 clients who stayed at the hotel's WORLD TRADE CENTER BUCHAREST SA was photographed by unauthorized people outside the company, which led to the disclosure of the personal data of some clients through online publication. The operator of WORLD TRADE CENTER BUCHAREST SA has been sanctioned because it has not taken steps to ensure that data is not disclosed to unauthorized parties. [PLAN,BUILD, RUN, MONITOR]	link
Romanian National Supervisory Authority for Personal Data Processing (ANSPDCP)	33	27-6-2019	130	UNICREDIT BANK SA	Art. 25 (1) GDPR, Art. 5 (1) c) GDPR	Insufficient technical and organisational measures to ensure information security	The fine was issued as a result of the failure to implement appropriate technical and organisational measures (related to (1) the determination of the processing means/operations, and (2) the integration the necessary safeguards) resulting in the online-disclosure of IDs and addresses (interla/external transactions) of 337,042 data subjects to their respective beneficiary (between 25.05.2018 -10.12.2018). [PLAN,BUILD, RUN, MONITOR]	link

Authority (DPA)	Case number	Date	Fine [€] x 1000	Data controller / Processor	Violation - Quoted Art.	ViolationType	Violation summary	Source
Dutch Supervisory Authority for Data Protection (AP)	34	18-6-2019	460	Haga Hospital	Art. 32 GDPR	Insufficient technical and organisational measures to ensure information security	The Haga Hospital does not have a proper internal security of patient records in place. This is the conclusion of an investigation by the Dutch Data Protection Authority. This investigation followed when it appeared that dozens of hospital staff had unnecessarily checked the medical records of a well-known Dutch person. To force the hospital to improve the security of patient records, the AP simultaneously imposes an order subject to a penalty. If the Haga Hospital has not improved security before 2nd of October 2019, the hospital must pay 100,000 EUR every two weeks, with a maximum of 300,000 EUR. The Haga Hospital has meanwhile indicated to take measures. [PLAN,BUILD, RUN, MONITOR]	link
French Data Protection Authority (CNIL)	35	28-5-2019	400	SERGIC (Real Estate)	Art. 32 GDPR	Insufficient technical and organisational measures to ensure information security	The CNIL based the penalty on two grounds: Lack of basic security measures and excessive data storage. As to the first, sensitive user documents uploaded by rental candidates (including ID cards, health cards, tax notices, certificates issued by the family allowance fund, divorce judgments, account statements) were accessible online without any authentication procedure in place. Although the vulnerability was known to the company since March 2018, it was not finally resolved until September 2018. In addition, the company stored the documentation provided by candidates for longer than necessary. The CNIL took into account i.a. the seriousness of the breach (lack of due care in addressing vulnerability and the fact that the documents revealed very intimate aspects of users' lives), the size of the company and its financial standing. [PLAN,BUILD, RUN, MONITOR]	link
Norwegian Supervisory Authority (Datatilsynet)	36	29-4-2019	120	Oslo Municipal Education Department	Art. 32 GDPR	Insufficient technical and organisational measures to ensure information security	Fine for security vulnerabilities in a mobile messaging app developed for use in an Oslo school. The app allows parents and students to send messages to school staff. Due to insufficient technical and organizational measures to protect information security, unauthorized persons were able to log in as authorized users and gain access to personal data about students, legal representatives and employees. The fine has meanwhile been reduced to EUR 120.000, see link [PLAN,BUILD, RUN, MONITOR]	link
Italian Data Protection Authority (Garante)	37	17-4-2019	50	Italian political party Movimento 5 Stelle	Art. 32 GDPR	Insufficient technical and organisational measures to ensure information security	A number of websites affiliated to the Italian political party Movimento 5 Stelle are run, by means of a data processor, through the platform named Rousseau. The platform had suffered a data breach during the summer 2017 that led the Italian data protection authority, the Garante, to require the implementation of a number of security measures, in addition to the obligation to	link

							update the privacy information notice in order to give additional transparency to the data processing activities performed.While the update of the privacy information notice was timely completed, the Italian data protection authority, raised its concerns as to the lack of implementation on the Rousseau platform of some of GDPR related security measures. It is worth it to mention that the proceeding initiated before May 2018, but the Italian data protection authority issued a fine under the GDPR since the Rousseau platform had not adopted security measures required by means of an order issued after the 25th of May 2018. Interestingly, the fine was not issued against the Movimento 5 Stelle that is the data controller of the platform, but against the Rousseau association that is the data processor. [PLAN,BUILD, RUN, MONITOR]	
Data Protection Authority of Baden-Wuerttemberg	38	12-4-2019	80	Company in the financial sector	Art. 5 GDPR, Art. 32 GDPR	Insufficient technical and organisational measures to ensure information security	In an administrative decision dated 12 April 2019, the authority imposed a fine of 80,000 euros on a medium-sized financial services company. This company had failed to take the necessary care to preserve the integrity and confidentiality of information within the meaning of Art. 5 para. 1 lit. f GDPR when disposing of documents containing personal data of two customers. Thus, without prior anonymisation, the papers were disposed of in the general waste paper recycling system, where the documents were found by a neighbour. [PLAN,BUILD, RUN, MONITOR]	link
Norwegian Supervisory Authority (Datatilsynet)	39	2019-03	170	Bergen Municipality	Art. 5 (1) f) GDPR, Art. 32 GDPR	Insufficient technical and organisational measures to ensure information security	The incident relates to computer files with usernames and passwords to over 35000 user accounts in the municipality's computer system. The user accounts related to both pupils in the municipality's primary schools, and to the employees of the same schools. Due to insufficient security measures, these files have been unprotected and openly accessible. The lack of security measures in the system made it possible for anyone to log in to the school's various information systems, and thereby to access various categories of personal data relating to the pupils and employees of the schools. The fact that the security breach encompasses personal data to over 35 000 individuals, and that the majority of these are children, were considered to be aggravating factors. The municipality had also been warned several times, both by the authority and an internal whistleblower, that the data security was inadequate. [PLAN,BUILD, RUN, MONITOR]	link

Authority (DPA)	Case number	Date	Fine [€] x 1000	Data controller / Processor	Violation - Quoted Art.	ViolationType	Violation summary	Source
Czech Data Protection Auhtority (UOOU)	40	28-2-2019	582	Unknown	Art. 32 GDPR	Insufficient technical and organisational measures to ensure information security	Data was not 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 organisational measures ('integrity and confidentiality'). [PLAN,BUILD, RUN, MONITOR]	link
Data Protection Commissioner of Malta	41	18-2-2019	5	Lands Authority	Art. 5 GDPR, Art. 32 GDPR	Insufficient technical and organisational measures to ensure information security	As a result of the lack of appropriate security measures on the Lands Authority website, over 10 gigabytes of personal data became easily accessible to the public via a simple google search. The majority of the leaked data contained highly-sensitive information and correspondence between individuals and the Authority itself. The Lands Authority chose not to appeal. In Malta, in the case of a breach by a public authority or body, the Data Protection Commissioner may impose an administrative fine of up to €25,000 for each violation and may additionally impose a daily fine of €25 for each day such violation persists. [PLAN,BUILD, RUN, MONITOR]	link
Czech Data Protection Auhtority (UOOU)	42	4-2-2019	1,165	Credit brokerage	Art. 32 GDPR	Insufficient technical and organisational measures to ensure information security	Data was not 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 organisational measures ('integrity and confidentiality'). [PLAN,BUILD, RUN, MONITOR]	link
Data Protection Authority of Baden-Wuerttemberg	43	2019	80	Unknown	Art. 32 GDPR	Insufficient technical and organisational measures to ensure information security	In a digital publication, health data was accidentally published due to inadequate internal control mechanisms. [PLAN,BUILD, RUN, MONITOR]	link
Spanish Data Protection Authority (aepd)	44	2019	48	VODAFONE ONO, S.A.U.	Art. 32 GDPR	Insufficient technical and organisational measures to ensure information security	Customers could access personal data of other customers in the customer area. The initial fine of EUR 60.000 was reduced to EUR 48.000. [PLAN,BUILD, RUN, MONITOR]	link
Spanish Data Protection Authority (aepd)	45	2019	30	Vodafone España, S.A.U.	Art. 5 (1) f) GDPR, Art. 32 GDPR	Insufficient technical and organisational measures to ensure information security	Disclosure of customer personal data (i.a. purchase history) via an SMS to another customer. The initial fine of EUR 50.000 was reduced to EUR 30.000. [PLAN,BUILD, RUN, MONITOR]	link

Data Protection Authority of Baden-Wuerttemberg	46	21-11-2018	20	Knuddels.de	Art. 32 GDPR	Insufficient technical and organisational measures to ensure information security	After a hacker attack in July personal data of approx. 330.000 users, including passwords and email addresses had been revealed. [PLAN,BUILD, RUN, MONITOR]	link
Portuguese Data Protection Authority (CNPD)	47	17-7-2018	400	Public Hospital	Art. 5 (1) f) GDPR, Art. 32 GDPR	Insufficient technical and organisational measures to ensure information security	Investigation revealed that the hospital's staff, psychologists, dietitians and other professionals had access to patient data through false profiles. The profile management system appeared deficient – the hospital had 985 registered doctor profiles while only having 296 doctors. Moreover, doctors had unrestricted access to all patient files, regardless of the doctor's specialty. [PLAN,BUILD, RUN, MONITOR]	link
Slovak Data Protection Office	48	Unknown	Unknown	Unknown	Art. 5 (1) f) GDPR, Art. 32 GDPR	Insufficient technical and organisational measures to ensure information security	Documents containing personal data were disposed of in the area of the municipal garbage dump. [PLAN,BUILD, RUN, MONITOR]	link
Slovak Data Protection Office	49	Unknown	Unknown	Unknown	Art. 5 (1) f) GDPR, Art. 32 GDPR	Insufficient technical and organisational measures to ensure information security	Violation of information security measures (no further information available at the moment) [PLAN,BUILD, RUN, MONITOR]	link
Slovak Data Protection Office	50	Unknown	40	Slovak Telekom	Art. 32 GDPR	Insufficient technical and organisational measures to ensure information security	The controller did not take adequate security measures when processing personal data, thereby breaching the obligation to protect the processed personal data. [PLAN,BUILD, RUN, MONITOR]	link
Spanish Data Protection Authority (aepd)	51	Unknown	12	Madrileña Red de Gas	Art. 32 GDPR	Insufficient technical and organisational measures to ensure information security	The gas company did not have appropriate measures in place to verify the identity of the data subject. The person who filed the complaint alleges that the company e-mailed his information to a third party in response to a request. [PLAN,BUILD, RUN, MONITOR]	link
Slovak Data Protection Office	52	Unknown	50	Social Insurance Agency	Art. 32 GDPR	Insufficient technical and organisational measures to ensure information security	Applications for social benefits from Slovak citizens were sent by post to foreign authorities. These were lost by post, with the result that the whereabouts of these personal data could not be clarified. [PLAN,BUILD, RUN, MONITOR]	link

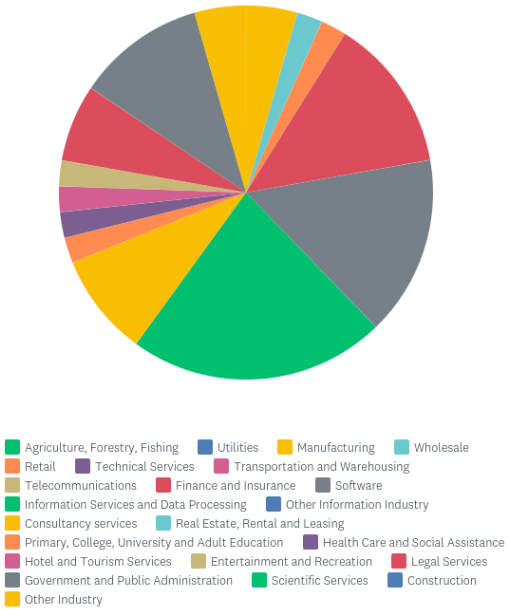
Czech Data Protection Auhtority (UOOU)	53	Unknown	980	Individual entrepreneur - no further details published	Art. 32 GDPR	Insufficient technical and organisational measures to ensure information security	The operator of an online game was exposed to several DDoS attacks which caused the malfunctioning of the servers. The attacker blackmailed the operator stating that the attacks will not stop unless he pays money. As part of the blackmail, the attacker offered the operator that he will create an upgraded and better firewall protection to the servers of the operator. The operator agreed and paid the attacker. The operator implemented the new code from the attacker which proved better than the old one but there was a "backdoor" in the code. The attacker used the backdoor to steal all the data from the server about the players and uploaded these details to his website. The Office for Personal Data Protection concluded that the operator did not take apropriate security measures. [PLAN,BUILD, RUN, MONITOR]	link

Questionnaire – Results questions 1-5

Understanding the industry you are active in and your role related to data privacy

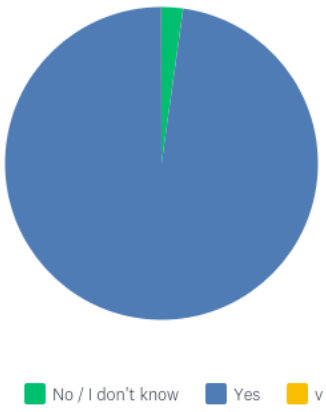
Q1: Which of the following categories best describes the industry you primarily work in (regardless of your actual position)?

(Answered 45 Skipped: 0)



ANTWOORDKEUZEN	REACTIES	
Agriculture, Forestry, Fishing	0.00%	0
Utilities	0.00%	0
Manufacturing	4.44%	2
Wholesale	2.22%	1
Retail	2.22%	1
Technical Services	0.00%	0
Transportation and Warehousing	0.00%	0
Telecommunications	0.00%	0
Finance and Insurance	13.33%	6
Software	15.56%	7
Information Services and Data Processing	22.22%	10
Other Information Industry	0.00%	0
Consultancy services	8.89%	4
Real Estate, Rental and Leasing	0.00%	0
Primary, College, University and Adult Education	2.22%	1
Health Care and Social Assistance	2.22%	1
Hotel and Tourism Services	2.22%	1
Entertainment and Recreation	2.22%	1
Legal Services	6.67%	3
Government and Public Administration	11.11%	5
Scientific Services	0.00%	0
Construction	0.00%	0
Other Industry	4.44%	2
TOTAAL		45

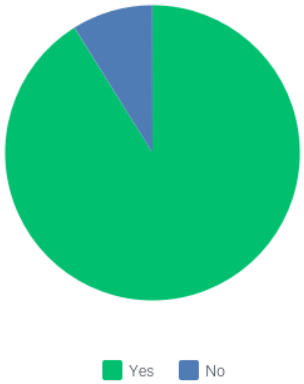
Q2: Is the GDPR relevant for your organization (from a compliance perspective)?
(Answered 45 Skipped: 0)



ANTWOORDKEUZEN	REACTIES	
No / I don't know	2.22%	1
Yes	97.78%	44
v	0.00%	0
TOTAAL		45

Note: if the respondent answered “No / I Don’t Know”, the respondent was forced to exit the questionnaire after question 5 (to avoid low quality replies in the questionnaire)

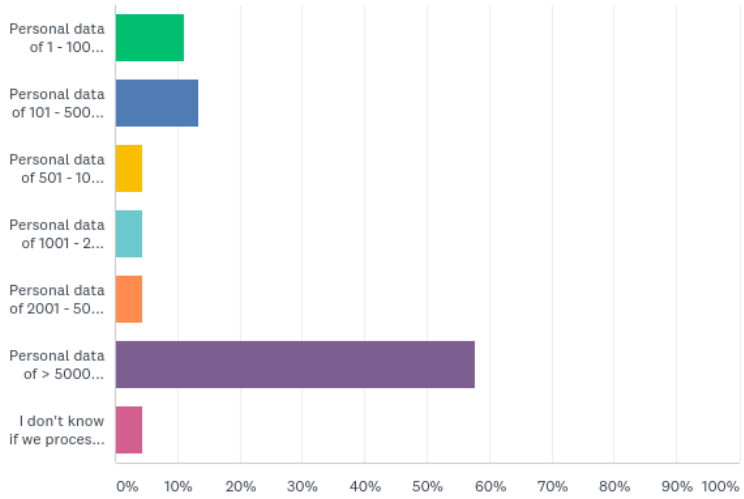
Q3: Are you involved in GDPR related activities? (Answered 45 Skipped: 0)



ANTWOORDKEUZEN	REACTIES	
Yes	91.11%	41
No	8.89%	4
TOTAAL		45

Note: if the respondent answered “No”, the respondent was forced to exit the questionnaire after question 5 (to avoid low quality replies in the questionnaire)

Q5: What are the estimated number of natural persons your organization collects and processes personal data from? Think of e.g. customers, vendors, employees, patients, students, etc., etc. For the definition of personal data and natural person, see https://gdpr-info.eu/art-4-gdpr/ (article 4:1).



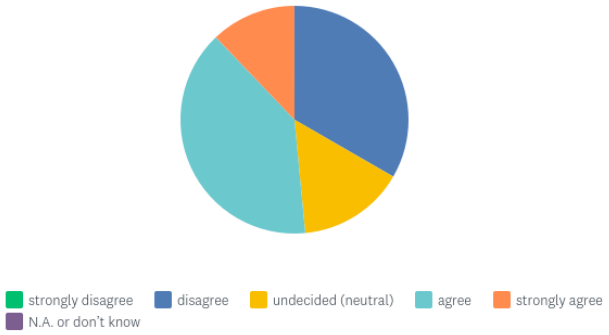
ANTWOORDKEUZEN	REACTIES	
Personal data of 1 - 100 natural persons	11.11%	5
Personal data of 101 - 500 natural persons	13.33%	6
Personal data of 501 - 1000 natural persons	4.44%	2
Personal data of 1001 - 2000 natural persons	4.44%	2
Personal data of 2001 - 5000 natural persons	4.44%	2
Personal data of > 5000 natural persons	57.78%	26
I don't know if we process the privacy relevant data of natural persons in our organization	4.44%	2
Totaal aantal respondenten: 45		

Questionnaire – Results questions 6-8

Topic: Self-explanatory guidance on the fulfilment of the GDPR requirements.

Q6: Context: how to apply the GDPR requirements as outlined in article 32 (see https://gdpr-info.eu/art-32-gdpr/ for details).
Question: Does the GDPR texts provide in **sufficient guidance to identify the "risk(s)"** (violation of privacy rights) of processing privacy relevant data in your organization? (in terms of the "what, when, where, how and who")

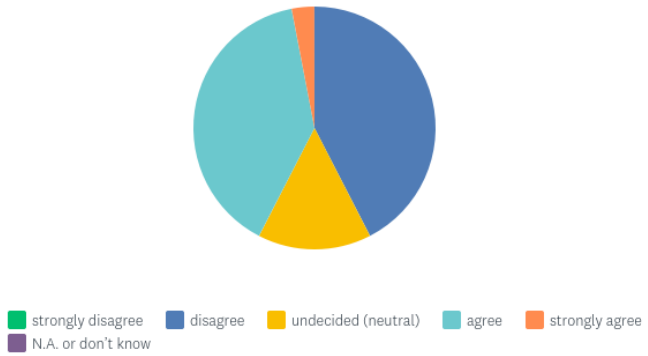
Answered: 33 Skipped: 12



	STRONGLY DISAGREE	DISAGREE	UNDECIDED (NEUTRAL)	AGREE	STRONGLY AGREE	N.A. OR DON'T KNOW	TOTAAL	GEWOGEN GEMIDDELDE
(geen label)	0.00% 0	33.33% 11	15.15% 5	39.39% 13	12.12% 4	0.00% 0	33	3.30

Q7: Context: how to apply the GDPR requirements as outlined in article 32 (see https://gdpr-info.eu/art-32-gdpr/ for details).
Question: Does the GDPR texts provide **in sufficient guidance to assess the "appropriate" level of security related to the identified risk(s)** of processing privacy relevant data in your organization? (in terms of the "what, when, where, how and who")

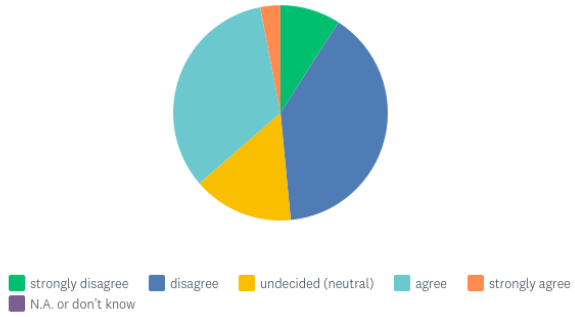
Answered: 33 Skipped: 12



	STRONGLY DISAGREE	DISAGREE	UNDECIDED (NEUTRAL)	AGREE	STRONGLY AGREE	N.A. OR DON'T KNOW	TOTAAL	GEWOGEN GEMIDDELDE
(geen label)	0.00% 0	42.42% 14	15.15% 5	39.39% 13	3.03% 1	0.00% 0	33	3.03

V8: Context: how to apply the GDPR requirements as outlined in article 32 (see https://gdpr-info.eu/art-32-gdpr/ for details).
Question: Does the GDPR texts provide in **sufficient guidance to formulate and implement the appropriate technical and organisational measures** regarding processing privacy relevant data in your organization in a secure way?(in terms of the "what, when, where, how and who")

Answered: 33 Skipped: 12

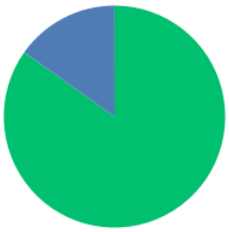


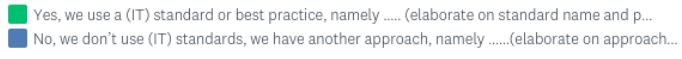
	STRONGLY DISAGREE	DISAGREE	UNDECIDED (NEUTRAL)	AGREE	STRONGLY AGREE	N.A. OR DON'T KNOW	TOTAAL	GEWOGEN GEMIDDELDE
(geen label)	9.09% 3	39.39% 13	15.15% 5	33.33% 11	3.03% 1	0.00% 0	33	2.82

Questionnaire – Results questions 9-10
Topic: perceived value of (IT) standards or best practices, etc. to comply with the GDPR

Q9: Are you **using the guidance of particular (IT) standards** like ISO, COBIT, NIST, etc. or other best practices in the context of defining, controlling and/or executing privacy governance, -management and -operational activities?

Answered: 33 Skipped: 12





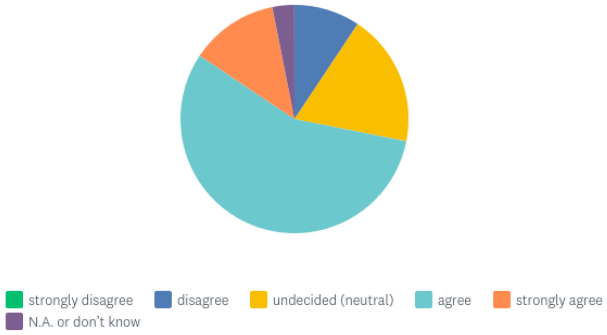
ANTWOORDKEUZEN	REACTIES
Yes, we use a (IT) standard or best practice, namely ..... (elaborate on standard name and perceived effectiveness)	84.85% 28
No, we don't use (IT) standards, we have another approach, namely ..... (elaborate on approach and perceived effectiveness)	15.15% 5
TOTAAL	33

Questionnaire – Results questions 11-14

Topic: the privacy related RISKS - the perceived value of (IT) standards or best practices

Q11: Does this standard, best practice or approach **supports you in the process of identifying WHAT the "risks" are** of processing privacy relevant data are in your organization? (in the context of GDPR article 32 - see https://gdpr-info.eu/art-32-gdpr/ ?

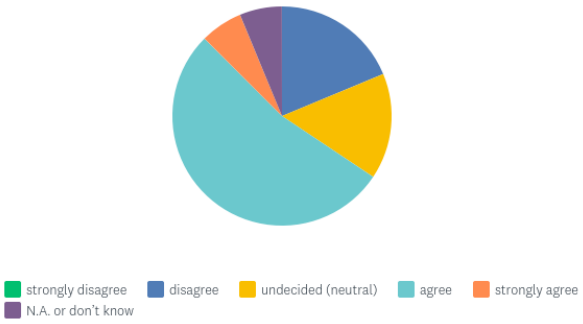
Answered: 32 Skipped: 13



	STRONGLY DISAGREE	DISAGREE	UNDECIDED (NEUTRAL)	AGREE	STRONGLY AGREE	N.A. OR DON'T KNOW	TOTAAL	GEWOGEN GEMIDDELDE
(geen label)	0.00% 0	9.38% 3	18.75% 6	56.25% 18	12.50% 4	3.13% 1	32	3.74

Q12: Does this standard, best practice or approach support you in the process of **identifying WHEN the "risks"** of processing privacy relevant data **in your organization could occur**? (in the context of GDPR article 32 - see https://gdpr-info.eu/art-32-gdpr/)

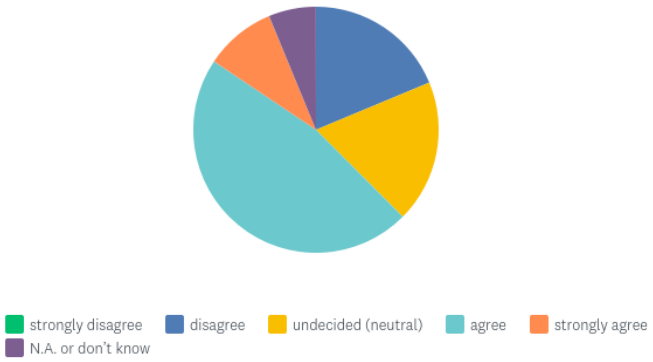
Answered: 32 Skipped: 13



	STRONGLY DISAGREE	DISAGREE	UNDECIDED (NEUTRAL)	AGREE	STRONGLY AGREE	N.A. OR DON'T KNOW	TOTAAL	GEWOGEN GEMIDDELDE
(geen label)	0.00% 0	18.75% 6	15.63% 5	53.13% 17	6.25% 2	6.25% 2	32	3.50

Q13: Does this standard, best practice or approach support you in the process of identifying **WHERE and HOW the "risks"** of processing privacy relevant data in your organization **should be identified and addressed?** (in the context of GDPR article 32 - see https://gdpr-info.eu/art-32-gdpr/)

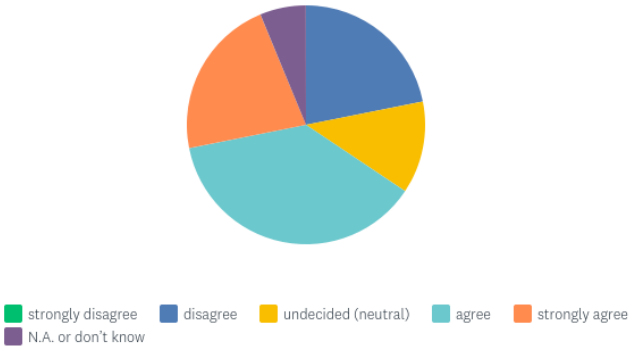
Answered: 32 Skipped: 13



	STRONGLY DISAGREE	DISAGREE	UNDECIDED (NEUTRAL)	AGREE	STRONGLY AGREE	N.A. OR DON'T KNOW	TOTAAL	GEWOGEN GEMIDDELDE
(geen label)	0.00% 0	18.75% 6	18.75% 6	46.88% 15	9.38% 3	6.25% 2	32	3.50

Q14: Does this standard or approach support you in the process of identifying **WHO should BE RESPONSIBLE to identify and handle the "risks"** of processing privacy relevant data in your organization? (in the context of GDPR article 32 - see https://gdpr-info.eu/art-32-gdpr/)

Answered: 32 Skipped: 13

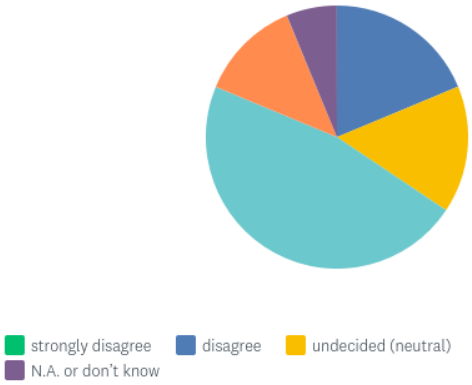


	STRONGLY DISAGREE	DISAGREE	UNDECIDED (NEUTRAL)	AGREE	STRONGLY AGREE	N.A. OR DON'T KNOW	TOTAAL	GEWOGEN GEMIDDELDE
(geen label)	0.00% 0	21.88% 7	12.50% 4	37.50% 12	21.88% 7	6.25% 2	32	3.63

Questionnaire – Results questions 15-18
Topic: the **appropriate measures** - the perceived value of (IT) standards or best practices

---

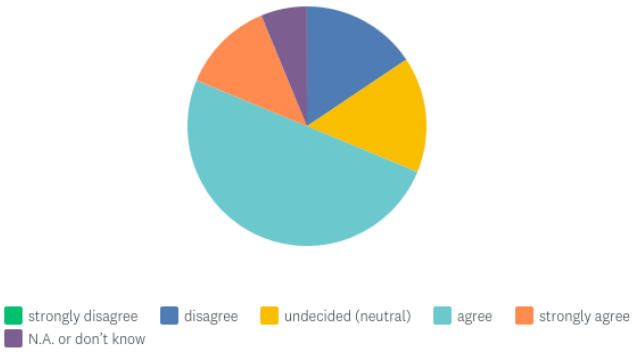
Q15: Does this standard, best practice or approach supports you in the process of identifying **WHAT the appropriate technical and organisational measures are** of processing privacy relevant data are in your organization? (in the context of GDPR article 32 - see https://gdpr-info.eu/art-32-gdpr/)



	STRONGLY DISAGREE	DISAGREE	UNDECIDED (NEUTRAL)	AGREE	STRONGLY AGREE	N.A. OR DON'T KNOW	TOTAAL	GEWOGEN GEMIDDELDE
(geen label)	0.00% 0	18.75% 6	15.63% 5	46.88% 15	12.50% 4	6.25% 2	32	3.57

Q16: Does this standard , best practice or approach supports you in the process of identifying **WHEN the appropriate technical and organisational measures** of processing privacy relevant data in your organization **must be in place/implemented**?
(in the context of GDPR article 32 - see https://gdpr-info.eu/art-32-gdpr/)

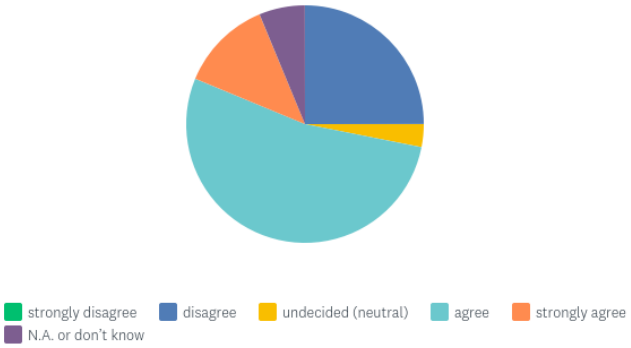
Answered: 32 Skipped: 13



	STRONGLY DISAGREE	DISAGREE	UNDECIDED (NEUTRAL)	AGREE	STRONGLY AGREE	N.A. OR DON'T KNOW	TOTAAL	GEWOGEN GEMIDDELDE
(geen label)	0.00% 0	15.63% 5	15.63% 5	50.00% 16	12.50% 4	6.25% 2	32	3.63

Q17: Does this standard, best practice or approach support you in the process of **identifying WHERE and HOW the appropriate technical and organisational measures** of processing privacy relevant data in your organization **should be implemented**?
(in the context of GDPR article 32 - see https://gdpr-info.eu/art-32-gdpr/)

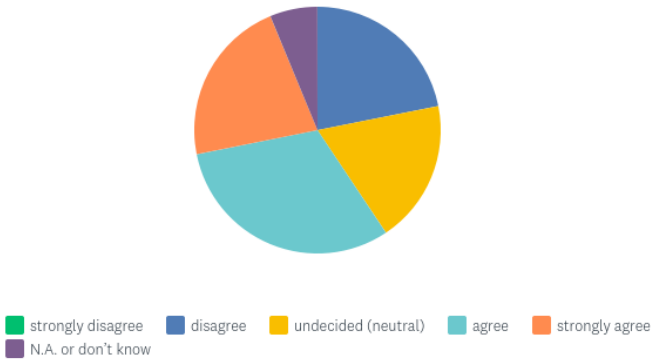
Answered: 32 Skipped: 13



	STRONGLY DISAGREE	DISAGREE	UNDECIDED (NEUTRAL)	AGREE	STRONGLY AGREE	N.A. OR DON'T KNOW	TOTAAL	GEWOGEN GEMIDDELDE
(geen label)	0.00% 0	25.00% 8	3.13% 1	53.13% 17	12.50% 4	6.25% 2	32	3.57

Q18: Does this standard, best practice or approach supports you in the process of **identifying WHO should BE RESPONSIBLE to implement** the appropriate technical and organisational measures of processing privacy relevant data in your organization?
(in the context of GDPR article 32 - see https://gdpr-info.eu/art-32-gdpr/)

Answered: 32 Skipped: 13



	STRONGLY DISAGREE	DISAGREE	UNDECIDED (NEUTRAL)	AGREE	STRONGLY AGREE	N.A. OR DON'T KNOW	TOTAAL	GEWOGEN GEMIDDELDE
(geen label)	0.00% 0	21.88% 7	18.75% 6	31.25% 10	21.88% 7	6.25% 2	32	3.57

Questionnaire – Results questions 4, 10, 19, 20 - **Analysis of open ended questions**

[XXX] = classification of governance and management activities according COBIT

Q4: Please elaborate your role and activities: Open-Ended Response		**Q10:** Please **elaborate on the (IT)standard or (best) practice** your organization applied in order to comply with the GDPR.	**Q19: Most significant improvements:** what are in your view the most significant improvements you see regarding the realization of effective privacy governance, -management and privacy operations?	**Q20: most significant risks factors** - what do you see as the most significant risk factor(s) regarding the realization of effective privacy governance, -management and privacy operations?
Your (privacy) role :	Relevant activities :	Open-Ended Response	Open-Ended Response	Open-Ended Response
Data Protection Officer	Compliance with GDPR and other DP law			
Product Owner	Product Engineering	ISO270001	Better transparency to support proactive decision making **[GOVERNANCE - EVALUATE]**	Reactive process caused by insufficient transparency and continuous monitoring **[MANAGEMENT - MONITOR]**
Domain Architect	Take into account GDPR requirements while designing solutions	ISO and NIST standards are used as general reference, among others, for GDPR matters.	Better cross-border governance of data, in distributed organisation. Not all organisational entities are aligned on the same interpretation of the standards. **[GOVERNANCE - DIRECT]**	Absence of global governance **[GOVERNANCE - DIRECT]**
Manager outsourcing	Besides negotiating contracts and monitoring the compliance advising the board in many areas.			
Cyber Security Manager	Confidentiality, integrity and availability of information; collaboration and alignment with data privacy	ISO 27001, NIST, BSI Grundschutz, CIS Controls, Microsoft Azure best practices, COBIT, also some associations like TeleTrust publish a handbook on the start of the art technology regarding technical measures. Data privacy nowadays is within the DNA of many services, so there is a lot of information available	Transparency over processing activities, identifying the processes for the records of processing activities creates a lot of insight that has not been available before **[MANAGEMENT - MONITOR]**	Especially in large, heterogeneous and complex organisations, it is a constant struggle to identify all processing activities and keep them up to date. **[MANAGEMENT - MONITOR]**
Internal Privacy Compliance Consultant	Advising and Training Software Development teams on GDPR	Our company has several ISO 27K certifications depending on the product/service and business unit. In 2020 we will also focus on NIST.	We improved control on how our services implement support for GDPR compliance requirements. The major risk remain in complexities when special categories of data are involved and on data deletion concerning retention periods. **[MANAGEMENT - RUN]**	Most significant risk is the low frequency of internal audits in big organisations with thousands of different personal data processing activities **[MANAGEMENT - MONITOR]**
Manager	Controlling			
SAP ILM Consultant	SAP ILM Consultant			
legal advisor	advising on issues related to use of personal data in Customs processes and sharing of personal data with other government organisations.	My answer should be interpreted as: I don't know if we use standards, and if so, which standards. I'm not into information security.	Everyone in the organisation is even more aware of responsible processing of personal data. **[GOVERNANCE - DIRECT]**	The GDPR causes a certain 'cramp' in dealing with personal data, especially because of the open norms and the fact that people don't know what is expected from them in processing personal data. **[GOVERNANCE - DIRECT]**
Advisor	Advice	ISO 27001 27002	Non	Awareness management **[GOVERNANCE - DIRECT]**
Project manager	AVG Project IT Department	ISO27000 series	There is clarity in what set of guidelines/requirements are applicable and they can be used in a practical manner. **[GOVERNANCE - DIRECT]**	For the Dutch Government Agencies there are various guidelines / requirements regarding GDPR/AVG. BIR/HIB-BBN, ISO27000, AVG, ... the complexity for us lies in the variety in definitions and therefore the interpretation of these guidelines/requirements. **[GOVERNANCE - EVALUATE]**
Data protection officer	-			
DPO & CISO	GDPR/Security/Privacy advice, training and implementation			
Privacy Product Manager	Develop Privacy Product to be used by organisation to comply with privacy regimes	British Standard 10012:12 Data Protection - Specification for a personal information management system BS EN ISO/IEC 27002:2017 Information technology Security techniques - Code of practice for information	Improvement: Awareness creation for privacy by design principles **[GOVERNANCE - DIRECT]**	Difficulty: Data Categorisation and mapping to purpose, with ongoing evaluation if legal ground for processing is given **[GOVERNANCE - EVALUATE]**

		security controls (ISO/IEC 27002:2013)		
Please elaborate your role:		Please **elaborate on the (IT)standard or (best) practice** your organization applied in order to comply with the GDPR.	**Most significant improvements:** what are in your view the most significant improvements you see regarding the realization of effective privacy governance, -management and privacy operations?	**Most significant risks factors** - what do you see as the most significant risk factor(s) regarding the realization of effective privacy governance, -management and privacy operations?
WMK-toets check	Clarifying de use of data within our organisatieontwikkeling.	We use own standard	Fitst, a good data Governance- and implementation strategy. **[GOVERNANCE – EVALUATE & DIRECT]**	Reputation damage. **[GOVERNANCE – EVALUATE]**
Data Protection Expert	-	Data Protection Management System	-	-
Compliance	Consultant and Review process	ISO 27001, ISO 29000	Examine and evaluate almost processes **[GOVERNANCE – MONITOR, EVALUATE]**	3rd parties/agencies with personal data and permission on apps need to redesign **[MANAGEMENT PLAN, BUILD]**
legal adviser	counsel and implement	ISO	the stronger privacy international standards improve the awareness in a society with significantly lower standards **[GOVERNANCE – MONITOR, EVALUATE - DIRECT]**	Unawareness of the employees, low privacy standards in the local society as whole **[GOVERNANCE – DIRECT]**
privacy advisor	advising on gdpr and other privacy legislation	cobit, NIST, EDPB quidelines, ICO guidelines	continuous improvement **[GOVERNANCE – MONITOR, EVALUATE - DIRECT]**	it must be adjusted to the sensitiveness of personal data processed **[MANAGEMENT - PLAN]**
DPO	DPO	Combining COBIT and ISO27k	Awareness & Processes control **[GOVERNANCE – DIRECT] [MANAGEMENT -MONITOR]**	Lack of commitment at the C level **[GOVERNANCE - EVALUATE, DIRECT]**
IT Risk management	support DPO in technical translation of IT risks (also related to GDPR)			
Management	Consultant for IT security	COBIT and NIST	measurements and metrics. **[MANAGEMENT – MONITOR]**	Inventory of information, risk assessment and measurements /metrics. **[MANAGEMENT – MONITOR, GOVERNANCE – MONITOR EVALUATE]**
Privacy Officer	Customer Rights / implementation & management of GDPR related activities			
DPO	reviewing all privacy DPA	NIST, CIS, CSA, COBIT2019, ENISA	Awareness at executive level Adapting contracts Opening privacy channels internal and external **[GOVERNANCE - EVALUATE, DIRECT]**	People not following the privacy rules within and outside the organisation (employees, contractors, marketing & sales people) **MANAGEMENT – RUN**
Senior System & Network Admin	GDPR/InfoSec Team Member	We combine parts of NIST CSF together with CIS Controls, to try and build a correct policy that can be applied, based on the data classification or business function. As we do not have formalized risk management, nor formalized info-sec, we could debate effectiveness. (As basically the current state of operations can be considered to be partially compliant)		
CEO	General management, IT, marketing	ISO9001-2015	Encrypted data **[MANAGEMENT – BUILD, RUN]**	open data structure, data difusion, mobile data carriers and equipment **[MANAGEMENT – BUILD, RUN]**
CEO	everything	Sales/ Marketing wise GDPR rules are integrated in Hubspot. For clients contracts and employee we used a broad GDPR checklist	It is too complex. Make it simple and make best practices for small companies. **[GOVERNANCE - DIRECT]**	Best practices for small companies including risks. **[GOVERNANCE EVALUATE, DIRECT]**
Data Protection Officer	Data Protection Strategy and Operations	BS 10012, ISO 2700X	Implementation of a Data Protection Management System (DPMS) **[MANAGEMENT BUILD, RUN, MONITOR]**	no or bad organized data protection management **[MANAGEMENT, PLAN]**
Development of a Privacy Solution	Development	not known in detail	Implementing the SAP Privay Governance Solution **[MANAGEMENT: PLAN, BUILD, RUN, MONITOR] [GOVERNANCE – MONITOR, EVALUATE]**	Main risk is that the priority in our organization could too low **[GOVERNANCE EVALUATE, DIRECT]**
Data protection officer	implementing GDPR	In implementing security measures we us iso standards	An clear inventory of risks & clear responsibilities **[GOVERNANCE – MONITOR, EVALUATE]**	No accountability **[GOVERNANCE, DIRECT]**

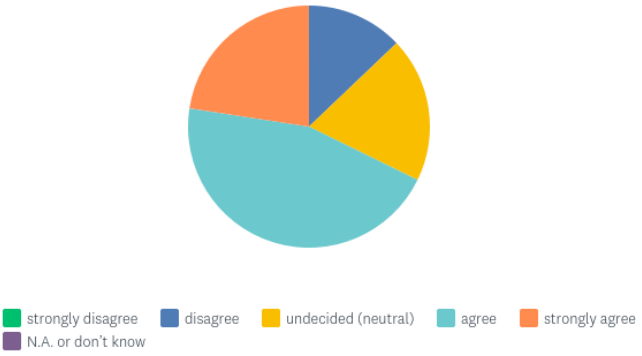
Please elaborate your role:		Please **elaborate on the (IT)standard or (best) practice** your organization applied in order to comply with the GDPR.	**Most significant improvements:** what are in your view the mostsignificant improvements you see regarding the realization of effective privacy governance, -management and privacy operations?	**Most significant risks factors** - what do you see as the most significant risk factor(s) regarding the realization of effective privacy governance, -management and privacy operations?
CIO (internal)	HR	ISO	security by design increasing security awareness within delivered services. **[GOVERNANCE – EVALUATE, DIRECT]**	Unwanted access to customer data by practically oriented employees **[MANAGEMENT RUN, MONITOR]**
DPO	Audit Assignments	ISO27001	guidance on privacy by design **[[GOVERNANCE – EVALUATE, DIRECT]**	focus on technology instead of minimal requirements **[GOVERNANCE – EVALUATE, DIRECT]**
consultant	security culture process	NEN 7510 (7512, 7513, 7516), ISO 27701, Norea Privacy Control Framework, guidance by the DPA	better understanding of risks and necessary controls **[GOVERNANCE – EVALUATE, MONITOR] [MANAGEMENT RUN, MONITOR]**	underestimation of the impact of GDPR **[GOVERNANCE – EVALUATE]**
CEO	responsible	We have an interim manager who helps implementing the processes	Awareness, Procedures for data breaches **[GOVERNANCE – EVALUATE, DIRECT] [MANAGEMENT – PLAN]**	Awareness **[GOVERNANCE – DIRECT]**
Security & Privacy Manager	Introducing ISO 27001, GDPR compliancy	ISO 27xxx family	Establish best practices, readily applicable norms **[GOVERNANCE – DIRECT]**	Leadership **[GOVERNANCE – DIRECT]**
Compliance audit	Compliance And data security audits	We follow various best practices applied (and dependant) by industry . We also use Breech and Attack Simulations to establish, monitor and remedy business processes managing data subject data	Clearly documented processes which are continuously tested and monitored to achieve formal compliance certification **[MANAGEMENT PLAN , BUILD, RUN, MONITOR]**	Lack of international resources and also executive sponsorship and budget to implement and maintain compliance **[GOVERNANCE –DIRECT]**
CIO	gdpr			
Data Protection Officer	according to GDPR role	according to standards but not certified		
Principal Consultant	Data Privacy Consulting	The controls from ISO 27001 are taken as reference for implementing data privacy	Awareness on data privacy risks and ready to take action when there is a disruption **[GOVERNANCE EVALUATE, DIRECT] [MANAGEMENT PLAN , BUILD, RUN, MONITOR]**	Culture of data privacy should be established for effective implementation, which is the biggest challenge **[GOVERNANCE DIRECT] [MANAGEMENT PLAN , BUILD, RUN, MONITOR]**
PMI Director	Integrating newly acquired companies into the group			
Digital Product Counsel	Compliance and risk assessment and counsel for digital products			
DPO	Privacy compliance	NIST PRIVACY+SECURITY	Collaboration between Privacy and Security teams **[GOVERNANCE EVALUATE, DIRECT] [MANAGEMENT PLAN , BUILD, RUN, MONITOR]**	Clear and effective Privacy and Security governance **[GOVERNANCE EVALUATE, DIRECT]**
primarily consulting	handling business sensitive information			
Manager	Controller and processors	As per industry standards	Accountability **[GOVERNANCE - DIRECT]**	Third party n PIA **[[GOVERNANCE - DIRECT]**
Digital governance	Policies' definition	We are adopting a tool of Privacy Management	More customer care, more attention to customer needs **[[GOVERNANCE - DIRECT]**	Minor engagement **[[GOVERNANCE - DIRECT]**

Legend:

Internal DPO/CIS (alike) role	16
Internal management role	7
Internal C-level role	5
Operations role	2
Legal role	2
(external) product development	4
(external) consulting role	9

Q21: Do you believe that existing (IT) standards can contribute to the mitigation or handling of the above defined GDPR risks and improvements?

Answered: 31 Skipped: 14



	STRONGLY DISAGREE	DISAGREE	UNDECIDED (NEUTRAL)	AGREE	STRONGLY AGREE	N.A. OR DON'T KNOW	TOTAAL	GEWOGEN GEMIDDELDE
(geen label)	0.00% 0	12.90% 4	19.35% 6	45.16% 14	22.58% 7	0.00% 0	31	3.77

ISO 27701 – Mapping between GDPR article 32 and ISO 27701 articles

Subclause of this document	GDPR article
5.2.1	(24)(3), (25)(3), (28)(5), (28)(6), (28)(10), (32)(3), (40)(1), (40)(2)(a), (40)(2)(b), (40)(2)(c), (40)(2)(d), (40)(2)(e), (40)(2)(f), (40)(2)(g), (40)(2)(h), (40)(2)(i), (40)(2)(j), (40)(2)(k), (40)(3), (40)(4), (40)(5), (40)(6), (40)(7), (40)(8), (40)(9), (40)(10), (40)(11), (41)(1), (41)(2)(a), (41)(2)(b), (41)(2)(c), (41)(2)(d), (41)(3), (41)(4), (41)(5), (41)(6), (42)(1), (42)(2), (42)(3), (42)(4), (42)(5), (42)(6), (42)(7), (42)(8)
5.2.2	(31), (35)(9), (36)(1), (36)(2), (36)(3)(a), (36)(3)(b), (36)(3)(c), (36)(3)(d), (36)(3)(e), (36)(3)(f), (36)(5)
5.2.3	(32)(2)
5.2.4	(32)(2)
5.4.1.2	(32)(1)(b), (32)(2)
5.4.1.3	(32)(1)(b), (32)(2)
6.2.1.1	(24)(2)
6.3.1.1	(27)(1), (27)(2)(a), (27)(2)(b), (27)(3), (27)(4), (27)(5), (37)(1)(a), (37)(1)(b), (37)(1)(c), (37)(2), (37)(3), (37)(4), (37)(5), (37)(6), (37)(7), (38)(1), (38)(2), (38)(3), (38)(4), (38)(5), (38)(6), (39)(1)(a), (39)(1)(b), (39)(1)(c), (39)(1)(d), (39)(1)(e), (39)(2)
6.3.2.1	(5)(1)(f)
6.4.2.2	(39)(1)(b)
6.5.2.1	(5)(1)(f), (32)(2)
6.5.2.2	(5)(1)(f)
6.5.3.1	(5)(1)(f), (32)(1)(a)
6.5.3.2	(5)(1)(f)
6.5.3.3	(5)(1)(f), (32)(1)(a)
6.6.2.1	(5)(1)(f)
6.6.2.2	(5)(1)(f)
6.6.4.2	(5)(1)(f)
6.7.1.1	(32)(1)(a)
6.8.2.7	(5)(1)(f)
6.8.2.9	(5)(1)(f)
6.9.3.1	(5)(1)(f), (32)(1)(c)
6.9.4.1	(5)(1)(f)
6.9.4.2	(5)(1)(f)
6.10.2.1	(5)(1)(f)

Subclause of this document	GDPR article
6.10.2.4	(5)(1)(f), (28)(3)(b), (38)(5)
6.11.1.2	(5)(1)(f), (32)(1)(a)
6.11.2.1	(25)(1)
6.11.2.5	(25)(1)
6.11.3.1	(5)(1)(f)
6.12.1.2	(5)(1)(f), (28)(1), (28)(3)(a), (28)(3)(b), (28)(3)(c), (28)(3)(d), (28)(3)(e), (28)(3)(f), (28)(3)(g), (28)(3)(h), (30)(2)(d), (32)(1)(b)
6.13.1.1	(5)(1)(f), (33)(1), (33)(3)(a), (33)(3)(b), (33)(3)(c), (33)(3)(d), (33)(4), (33)(5), (34)(1), (34)(2), (34)(3)(a), (34)(3)(b), (34)(3)(c), (34)(4)
6.13.1.5	(33)(1), (33)(2), (33)(3)(a), (33)(3)(b), (33)(3)(c), (33)(3)(d), (33)(4), (33)(5), (34)(1), (34)(2)
6.15.1.1	(5)(1)(f), (28)(1), (28)(3)(a), (28)(3)(b), (28)(3)(c), (28)(3)(d), (28)(3)(e), (28)(3)(f), (28)(3)(g), (28)(3)(h), (30)(2)(d), (32)(1)(b)
6.15.1.3	(5)(2), (24)(2)
6.15.2.1	(32)(1)(d), (32)(2)
6.15.2.3	(32)(1)(d), (32)(2)
7.2.1	(5)(1)(b), (32)(4)
7.2.2	(10), (5)(1)(a), (6)(1)(a), (6)(1)(b), (6)(1)(c), (6)(1)(d), (6)(1)(e), (6)(1)(f), (6)(2), (6)(3), (6)(4)(a), (6)(4)(b), (6)(4)(c), (6)(4)(d), (6)(4)(e), (8)(3), (9)(1), (9)(2)(b), (9)(2)(c), (9)(2)(d), (9)(2)(e), (9)(2)(f), (9)(2)(g), (9)(2)(h), (9)(2)(i), (9)(2)(j), (9)(3), (9)(4), (17)(3)(a), (17)(3)(b), (17)(3)(c), (17)(3)(d), (17)(3)(e), (18)(2), (22)(2)(a), (22)(2)(b), (22)(2)(c), (22)(4)
7.2.3	(8)(1), (8)(2)
7.2.4	(7)(1), (7)(2), (9)(2)(a)
7.2.5	(35)(1), (35)(2), (35)(3)(a), (35)(3)(b), (35)(3)(c), (35)(4), (35)(5), (35)(7)(a), (35)(7)(b), (35)(7)(c), (35)(7)(d), (35)(8), (35)(9), (35)(10), (35)(11), (36)(1), (36)(3)(a), (36)(3)(b), (36)(3)(c), (36)(3)(d), (36)(3)(e), (36)(3)(f), (36)(5)
7.2.6	(5)(2), (28)(3)(e), (28)(9)
7.2.7	(26)(1), (26)(2), (26)(3)
7.2.8	(5)(2), (24)(1), (30)(1)(a), (30)(1)(b), (30)(1)(c), (30)(1)(d), (30)(1)(f), (30)(1)(g), (30)(3), (30)(4), (30)(5)
7.3.1	(12)(2)
7.3.2	(11)(2), (13)(3), (13)(1)(a), (13)(1)(b), (13)(1)(c), (13)(1)(d), (13)(1)(e), (13)(1)(f), (13)(2)(c), (13)(2)(d), (13)(2)(e), (13)(4), (14)(1)(a), (14)(1)(b), (14)(1)(c), (14)(1)(d), (14)(1)(e), (14)(1)(f), (14)(2)(b), (14)(2)(e), (14)(2)(f), (14)(3)(a), (14)(3)(b), (14)(3)(c), (14)(4), (14)(5)(a), (14)(5)(b), (14)(5)(c), (14)(5)(d), (15)(1)(a), (15)(1)(b), (15)(1)(c), (15)(1)(d), (15)(1)(e), (15)(1)(f), (15)(1)(g), (15)(1)(h), (15)(2), (18)(3), (21)(4)
7.3.3	(11)(2), (12)(1), (12)(7), (13)(3), (21)(4)
7.3.4	(7)(3), (13)(2)(c), (14)(2)(d), (18)(1)(a), (18)(1)(b), (18)(1)(c), (18)(1)(d)
7.3.5	(13)(2)(b), (14)(2)(c), (21)(1), (21)(2), (21)(3), (21)(5), (21)(6)
7.3.6	(5)(1)(d), (13)(2)(b), (14)(2)(c), (16), (17)(1)(a), (17)(1)(b), (17)(1)(c), (17)(1)(d), (17)(1)(e), (17)(1)(f), (17)(2)
7.3.7	(19)
7.3.8	(15)(3), (15)(4), (20)(1), (20)(2), (20)(3), (20)(4)
7.3.9	(15)(1)(a), (15)(1)(b), (15)(1)(c), (15)(1)(d), (15)(1)(e), (15)(1)(f), (15)(1)(g), (15)(1)(h), (12)(3), (12)(4), (12)(5), (12)(6)
7.3.10	(13)(2)(f), (14)(2)(g), (22)(1), (22)(3)
7.4.1	(5)(1)(b), (5)(1)(c)

Table D.1 *(continued)*

Subclause of this document	GDPR article
7.4.2	(25)(2)
7.4.3	(5)(1)(d)
7.4.4	(5)(1)(c), (5)(1)(e)
7.4.5	(5)(1)(c), (5)(1)(e), (6)(4)(e), (11)(1), (32)(1)(a)
7.4.6	(5)(1)(c)
7.4.7	(13)(2)(a), (14)(2)(a)
7.4.8	(5)(1)(f)
7.4.9	(5)(1)(f)
7.5.1	(15)(2), (44), (45)(1), (45)(2)(a), (45)(2)(b), (45)(2)(c), (45)(3), (45)(4), (45)(5), (45)(6), (45)(7), (45)(8), (45)(9), (46)(1), (46)(2)(a), (46)(2)(b), (46)(2)(c), (46)(2)(d), (46)(2)(e), (46)(2)(f), (46)(3)(a), (46)(3)(b), (46)(4), (46)(5), (47)(1)(a), (47)(1)(b), (47)(1)(c), (47)(2)(a), (47)(2)(b), (47)(2)(c), (47)(2)(d), (47)(2)(e), (47)(2)(f), (47)(2)(g), (47)(2)(h), (47)(2)(i), (47)(2)(j), (47)(2)(k), (47)(2)(l), (47)(2)(m), (47)(2)(n), (47)(3), (49)(1)(a), (49)(1)(b), (49)(1)(c), (49)(1)(d), (49)(1)(e), (49)(1)(f), (49)(1)(g), (49)(2), (49)(3), (49)(4), (49)(5), (49)(6), (30)(1)(e), (48)
7.5.2	(15)(2), (30)(1)(e)
7.5.3	(30)(1)(e)
7.5.4	(30)(1)(d)
8.2.1	(28)(3)(f), (28)(3)(e), (28)(9), (35)(1)
8.2.2	(5)(1)(a), (5)(1)(b), (28)(3)(a), (29), (32)(4)
8.2.3	(7)(4)
8.2.4	(28)(3)(h)
8.2.5	(28)(3)(h)
8.2.6	(30)(3), (30)(4), (30)(5), (30)(2)(a), (30)(2)(b)
8.3.1	(15)(3), (17)(2), (28)(3)(e)
8.4.1	(5)(1)(c)
8.4.2	(28)(3)(g), (30)(1)(f)
8.4.3	(5)(1)(f)
8.5.1	(44), (46)(1), (46)(2)(a), (46)(2)(b), (46)(2)(c), (46)(2)(d), (46)(2)(e), (46)(2)(f), (46)(3)(a), (46)(3)(b), (48), (49)(1)(a), (49)(1)(b), (49)(1)(c), (49)(1)(d), (49)(1)(e), (49)(1)(f), (49)(1)(g), (49)(2), (49)(3), (49)(4), (49)(5), (49)(6)
8.5.2	(30)(2)(c)
8.5.3	(30)(1)(d)
8.5.4	(28)(3)(a)
8.5.5	(48)
8.5.6	(28)(2), (28)(4)
8.5.7	(28)(2), (28)(3)(d)

Text of ISO 27701 articles linked to GDPR article 32 (subject to license agreement)

5.2.1 Understanding the organization and its context

A requirement additional to ISO/IEC 27001:2013, 4.1 is:

The organization shall determine its role as a PII controller (including as a joint PII controller) and/or a PII processor.

The organization shall determine external and internal factors that are relevant to its context and that affect its ability to achieve the intended outcome(s) of its PIMS. For example, these can include:

— applicable privacy legislation;

— applicable regulations;

— applicable judicial decisions;

— applicable organizational context, governance, policies and procedures;

— applicable administrative decisions;

— applicable contractual requirements.

Where the organization acts in both roles (e.g. a PII controller and a PII processor), separate roles shall be determined, each of which is the subject of a separate set of controls.

NOTE The role of the organization can be different for each instance of the processing of PII, since it depends on who determines the purposes and means of the processing.

5.2.2 Understanding the needs and expectations of interested parties

A requirement additional to ISO/IEC 27001:2013, 4.2 is:

The organization shall include among its interested parties (see ISO/IEC 27001:2013, 4.2), those parties having interests or responsibilities associated with the processing of PII, including the PII principals.

NOTE 1 Other interested parties can include customers (see 4.4), supervisory authorities, other PII controllers, PII processors and their subcontractors.

NOTE 2 Requirements relevant to the processing of PII can be determined by legal and regulatory requirements, by contractual obligations and by self-imposed organizational objectives. The privacy principles set out in ISO/IEC 29100 provide guidance concerning the processing of PII.

NOTE 3 As an element to demonstrate compliance to the organization's obligations, some interested parties can expect that the organization be in conformity with specific standards, such as the Management System specified in this document, and/or any relevant set of specifications. These parties can call for independently audited compliance to these standards.

5.2.3 Determining the scope of the information security management system

A requirement additional to ISO/IEC 27001:2013, 4.3 is:

When determining the scope of the PIMS, the organization shall include the processing of PII.

NOTE The determination of the scope of the PIMS can require revising the scope of the information security management system, because of the extended interpretation of "information security" according to 5.1.

5.2.4 Information security management system

A requirement additional to ISO/IEC 27001:2013, 4.4 is:

The organization shall establish, implement, maintain and continually improve a PIMS in accordance with the requirements of ISO/IEC 27001:2013 Clauses 4 to 10, extended by the requirements in Clause 5.

5.4.1.2 Information security risk assessment

The requirements stated in ISO/IEC 27001:2013, 6.1.2 apply with the following refinements:

ISO/IEC 27001:2013, 6.1.2 c) 1) is refined as follows:

The organization shall apply the information security risk assessment process to identify risks associated with the loss of confidentiality, integrity and availability, within the scope of the PIMS.

The organization shall apply privacy risk assessment process to identify risks related to the processing of PII, within the scope of the PIMS.

The organization shall ensure throughout the risk assessment processes that the relationship between information security and PII protection is appropriately managed.

NOTE The organization can either apply an integrated information security and privacy risk assessment process or two separate ones for information security and the risks related to the processing of PII.

ISO/IEC 27001:2013, 6.1.2 d) 1) is refined as follows:

The organization shall assess the potential consequences for both the organization and PII principals that would result if the risks identified in ISO/IEC 27001:2013, 6.1.2 c) as refined above, were to materialize.

5.4.1.3 Information security risk treatment

The requirements stated in ISO/IEC 27001:2013, 6.1.3 apply with the following additions:

ISO/IEC 27001:2013, 6.1.3 c) is refined as follows:

The controls determined in ISO/IEC 27001:2013 6.1.3 b) shall be compared with the controls in Annex A and/or Annex B and ISO/IEC 27001:2013, Annex A to verify that no necessary controls have been omitted.

When assessing the applicability of control objectives and controls from ISO/IEC 27001:2013 Annex A for the treatment of risks, the control objectives and controls shall be considered in the context of both risks to information security as well as risks related to the processing of PII, including risks to PII principals.

ISO/IEC 27001:2013, 6.1.3 d) is refined as follows:

Produce a Statement of Applicability that contains:

— the necessary controls [see ISO/IEC 27001:2013, 6.1.3 b) and c)];

— justification for their inclusion;

— whether the necessary controls are implemented or not; and

— the justification for excluding any of the controls in Annex A and/or Annex B and ISO/IEC 27001:2013, Annex A according to the organization's determination of its role (see 5.2.1).

6.5.2.1 Classification of information

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 8.2.1 and the following additional guidance applies:

Additional implementation guidance for 8.2.1, Classification of Information, of ISO/IEC 27002:2013 is:

The organization's information classification system should explicitly consider PII as part of the scheme it implements. Considering PII within the overall classification system is integral to understanding what PII the organization processes (e.g. type, special categories), where such PII is stored and the systems through which it can flow.

6.5.3.1 Management of removable media

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 8.3.1 and the following additional guidance applies:

Additional implementation guidance for 8.3.1, Management of removable media, of ISO/IEC 27002:2013 is:

The organization should document any use of removable media and/or devices for the storage of PII. Wherever feasible, the organization should use removable physical media and/or devices that permit encryption when storing PII. Unencrypted media should only be used where unavoidable, and in instances where unencrypted media and/or devices are used, the organization should implement procedures and compensating controls (e.g. tamper-evident packaging) to mitigate risks to the PII.

Additional other information for 8.3.1, Management of removable media, of ISO/IEC 27002:2013 is:

Removable media which is taken outside the physical confines of the organization is prone to loss, damage and inappropriate access. Encrypting removable media adds a level of protection for PII which reduces security and privacy risks should the removable media be compromised.

6.5.3.3 Physical media transfer

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 8.3.3 and the following additional guidance applies:

Additional implementation guidance for 8.3.3, Physical media transfer, of ISO/IEC 27002:2013 is:

If physical media is used for information transfer, a system should be put in place to record incoming and outgoing physical media containing PII, including the type of physical media, the authorized sender/ recipients, the date and time, and the number of physical media. Where possible, additional measures such as encryption should be implemented to ensure that the data can only be accessed at the point of destination and not in transit.

The organization should subject physical media containing PII before leaving its premises to an authorization procedure and ensure the PII is not accessible to anyone other than authorized personnel.

NOTE One possible measure to ensure PII on physical media leaving the organization's premises is not generally accessible is to encrypt the PII concerned and restrict decryption capabilities to authorized personnel.

6.7.1.1 Policy on the use of cryptographic controls

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 10.1.1 and the following additional guidance applies:

Additional implementation guidance for 10.1.1, Policy on the use of cryptographic controls, of ISO/IEC 27002:2013 is:

Some jurisdictions can require the use of cryptography to protect particular kinds of PII, such as health data, resident registration numbers, passport numbers and driver's licence numbers.

The organization should provide information to the customer regarding the circumstances in which it uses cryptography to protect the PII it processes. The organization should also provide information to the customer about any capabilities it provides that can assist the customer in applying their own cryptographic protection.

6.9.3.1 Information backup

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 12.3.1 and the following additional guidance applies:

Additional implementation guidance for 12.3.1, Information backup, of ISO/IEC 27002:2013 is:

The organization should have a policy which addresses the requirements for backup, recovery and restoration of PII (which can be part of an overall information backup policy) and any further requirements (e.g. contractual and/or legal requirements) for the erasure of PII contained in information held for backup requirements.

PII-specific responsibilities in this respect can depend on the customer. The organization should ensure that the customer has been informed of the limits of the service regarding backup.

Where the organization explicitly provides backup and restore services to customers, the organization should provide them with clear information about their capabilities with respect to backup and restoration of PII.

Some jurisdictions impose specific requirements regarding the frequency of backups of PII, the frequency of reviews and tests of backup, or regarding the recovery procedures for PII. Organizations operating in these jurisdictions should demonstrate compliance with these requirements.

There can be occasions where PII needs to be restored, perhaps due to a system malfunction, attack or disaster. When PII is restored (typically from backup media), processes need to be in place to ensure that the PII is restored into a state where the integrity of PII can be assured, and/or where PII inaccuracy and/or incompleteness is identified and processes put in place to resolve them (which can involve the PII principal).

The organization should have a procedure for, and a log of, PII restoration efforts. At a minimum, the log of the PII restoration efforts should contain:

— the name of the person responsible for the restoration;

— a description of the restored PII.

Some jurisdictions prescribe the content of the logs of PII restoration efforts. Organizations should be able to document compliance with any applicable jurisdiction-specific requirements for restoration log content. The conclusions of such deliberations should be included in documented information.

The use of subcontractors to store replicated or backup copies of PII processed is covered by the controls in this document applying to subcontracted PII processing (see 6.5.3.3, 6.12.1.2). Where physical media transfers take place related to backups and restoration, this is also covered by controls in this document (6.10.2.1).

6.11.1.2 Securing application services on public networks

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 14.1.2 and the following additional guidance applies:

Additional implementation guidance for 14.1.2, Securing application services on public networks, of ISO/IEC 27002:2013 is:

The organization should ensure that PII that is transmitted over untrusted data transmission networks is encrypted for transmission.

Untrusted networks can include the public internet and other facilities outside of the operational control of the organization.

NOTE In some cases (e.g. the exchange of e-mail) the inherent characteristics of untrusted data transmission network systems can require that some header or traffic data be exposed for effective transmission.

6.11.2.1 Secure development policy

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 14.2.1 and the following additional guidance applies.

Additional implementation guidance for 14.2.1, Secure development policy, of ISO/IEC 27002:2013 is:

Policies for system development and design should include guidance for the organization's processing of PII needs, based on obligations to PII principals and/or any applicable legislation and/or regulation and the types of processing performed by the organization. Clauses 7 and 8 provide control considerations for processing of PII, which can be useful in developing policies for privacy in systems design.

Policies that contribute to privacy by design and privacy by default should consider the following aspects:

a) guidance on PII protection and the implementation of the privacy principles (see ISO/IEC 29100) in the software development lifecycle;

b) privacy and PII protection requirements in the design phase, which can be based on the output from a privacy risk assessment and/or a privacy impact assessment (see 7.2.5);

c) PII protection checkpoints within project milestones;

d) required privacy and PII protection knowledge;

e) by default minimize processing of PII.

6.12.1.2 Addressing security within supplier agreements

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 15.1.2 and the following additional guidance applies:

Additional implementation guidance for 15.1.2, Addressing security within supplier agreements, of ISO/IEC 27002:2013 is:

The organization should specify in agreements with suppliers whether PII is processed and the minimum technical and organizational measures that the supplier needs to meet in order for the organization to meet its information security and PII protection obligations (see 7.2.6 and 8.2.1).

Supplier agreements should clearly allocate responsibilities between the organization, its partners, its suppliers and its applicable third parties (customers, suppliers, etc.) taking into account the type of PII processed.

The agreements between the organization and its suppliers should provide a mechanism for ensuring the organization supports and manages compliance with all applicable legislation and/or regulation. The agreements should call for independently audited compliance, acceptable to the customer.

NOTE For such audit purposes, compliance with relevant and applicable security and privacy standards such as ISO/IEC 27001 or this document can be considered.

Implementation guidance for PII processors

The organization should specify in contracts with any suppliers that PII is only processed on its instructions.

6.13.1.1 Responsibilities and procedures

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 16.1.1 and the following additional guidance applies:

Additional implementation guidance for 16.1.1, Responsibilities and procedures, of ISO/IEC 27002:2013 is:

As part of the overall information security incident management process, the organization should establish responsibilities and procedures for the identification and recording of breaches of PII. Additionally, the organization should establish responsibilities and procedures related to notification to required parties of PII breaches (including the timing of such notifications) and the disclosure to authorities, taking into account the applicable legislation and/or regulation.

Some jurisdictions impose specific regulations regarding breach responses, including notification. Organizations operating in these jurisdictions should ensure that they can demonstrate compliance with these regulations.

6.15.1.1 Identification of applicable legislation and contractual requirements

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 18.1.1 and the following additional guidance applies:

Additional other information for 18.1.1, Identification of applicable legislation and contractual requirements, of ISO/IEC 27002:2013 is:

The organization should identify any potential legal sanctions (which can result from some obligations being missed) related to the processing of PII, including substantial fines directly from the local supervisory authority. In some jurisdictions, International Standards such as this document can be used to form the basis for a contract between the organization and the customer, outlining their respective security, privacy and PII protection responsibilities. The terms of the contract can provide a basis for contractual sanctions in the event of a breach of those responsibilities.

6.15.2.1 Independent review of information security

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 18.2.1 and the following additional guidance applies:

Additional implementation guidance for 18.2.1, Independent review of information security, of ISO/IEC 27002:2013 is:

Where an organization is acting as a PII processor, and where individual customer audits are impractical or can increase risks to security, the organization should make available to customers, prior to entering into, and for the duration of, a contract, independent evidence that information security is implemented and operated in accordance with the organization's policies and procedures. A relevant independent audit, as selected by the organization, should normally be an acceptable method for fulfilling the customer's interest in reviewing the organization's processing operations, if it covers the needs of anticipated users and if results are provided in a sufficient transparent manner.

6.15.2.3 Technical compliance review

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 18.2.3 and the following additional guidance applies:

Additional implementation guidance for 18.2.3, Technical compliance review, of ISO/IEC 27002:2013 is:

As part of technical reviews of compliance with security policies and standards, the organization should include methods of reviewing those tools and components related to processing PII. This can include:

— ongoing monitoring to verify that only permitted processing is taking place; and/or

— specific penetration or vulnerability tests (for example, de-identified datasets can be subject to a motivated intruder test to validate that de-identification methods are compliant with organizational requirements).

Text of ISO 27701 articles linked to privacy/processing risks assessment and treatment

5.4.1.2 Information security risk assessment

The requirements stated in ISO/IEC 27001:2013, 6.1.2 apply with the following refinements:

ISO/IEC 27001:2013, 6.1.2 c) 1) is refined as follows:

The organization shall apply the information security risk assessment process to identify risks associated with the loss of confidentiality, integrity and availability, within the scope of the PIMS.

The organization shall apply privacy risk assessment process to identify risks related to the processing of PII, within the scope of the PIMS.

The organization shall ensure throughout the risk assessment processes that the relationship between information security and PII protection is appropriately managed.

NOTE The organization can either apply an integrated information security and privacy risk assessment process or two separate ones for information security and the risks related to the processing of PII.

ISO/IEC 27001:2013, 6.1.2 d) 1) is refined as follows:

The organization shall assess the potential consequences for both the organization and PII principals that would result if the risks identified in ISO/IEC 27001:2013, 6.1.2 c) as refined above, were to materialize.

5.4.1.3 Information security risk treatment

The requirements stated in ISO/IEC 27001:2013, 6.1.3 apply with the following additions:

ISO/IEC 27001:2013, 6.1.3 c) is refined as follows:

The controls determined in ISO/IEC 27001:2013 6.1.3 b) shall be compared with the controls in Annex A and/or Annex B and ISO/IEC 27001:2013, Annex A to verify that no necessary controls have been omitted.

When assessing the applicability of control objectives and controls from ISO/IEC 27001:2013 Annex A for the treatment of risks, the control objectives and controls shall be considered in the context of both risks to information security as well as risks related to the processing of PII, including risks to PII principals.

ISO/IEC 27001:2013, 6.1.3 d) is refined as follows:

Produce a Statement of Applicability that contains:

— the necessary controls [see ISO/IEC 27001:2013, 6.1.3 b) and c)];

— justification for their inclusion;

— whether the necessary controls are implemented or not; and

— the justification for excluding any of the controls in Annex A and/or Annex B and ISO/IEC 27001:2013, Annex A according to the organization's determination of its role (see 5.2.1).

Not all the control objectives and controls listed in the annexes need to be included in a PIMS implementation. Justification for exclusion can include where the controls are not deemed necessary