DEPARTMENT OF
APPLIED IT

PRIVACY MATURITY IN SWEDISH MUNICIPALITIES:

A Quantitative Survey Based on a Privacy Maturity Framework

Marcus Broman

Johan Andersson von Geijer

Thesis:	30 hp
Program:	IT Management – TIA019
Level:	Master Thesis
Year:	2019
Supervisor:	Juho Lindman
Examiner:	Fredrik Svahn
Report nr:	2019:009

Abstract

Municipalities of Sweden are facing challenges complying with the GDPR. New and changed management processes need to be implemented. We used an inductive quantitative approach applying a privacy maturity framework in a survey in May 2019 where 454 controllers in Swedish municipalities answered. Twenty-three measurable criteria are adopted from the technology-neutral international best-practice standard Generally accepted privacy principles (GAPP) and objective descriptions in the Privacy maturity model (PMM). The results are maturity estimates from level 1 to 5 on the 23 criteria, which we grouped in six attributes. Of the controllers, 52 percent are on level 1, 44 percent on level 2, and only 4 percent are above level 3. The survey also includes four significant findings: (1) Controllers in medium-large municipalities are estimating maturity higher than others. (2) Less than a third of the controllers have defined roles and responsibilities for privacy, except for the data protection officer (DPO). DPOs are estimating maturity even lower. (3) There is a risk for not detecting privacy breaches, due to lack of protection, monitoring and testing of safeguards, lack of controls on third-parties security practices, and treating privacy matters as IT-security queries. Controllers working with sensitive data are rating maturity higher in these areas. (4) Municipalities have prioritised visible processes like a privacy notice, meeting requests from registered and retention practices. There are two strategies found – one ambitious and one cautious. Several of these findings imply further research.

Keywords

Information privacy, Privacy, Maturity model, GDPR, Sweden, Municipalities, Benchmarking, GAPP

Table of contents

List of figures

List of tables

1 Introduction

The new legislation General Data Protection Regulation (GDPR) set demands for an increased focus on privacy for the public sector. In Sweden's 290 municipalities, the preparedness is supposed to be adequate, since previous laws had similar privacy requirements. However, the Swedish Data Protection Authority (DPA) believes municipalities have bigger challenges and works less systematically than other parts of the society, with a risk to impede the potential of digitalisation for public welfare, in a recent national report (Datainspektionen, 2019b). It is crucial to gain more understanding in which fields challenges are for the Swedish municipalities.

The research term implied in this thesis is *information privacy*. The term differs from physical privacy. Information and physical privacy are subsets of privacy in general, but for simplicity, we hereafter refer to information privacy as just *privacy*.

The research area of privacy is multi-disciplinary and for information system research it is highly relevant because the continued growth of digitalisation leads to increased concern for invasive use of personal information (Bélanger & Crossler, 2011). In a literary review in MIS Quarterly conducted by Bélanger and Crossler (2011), the main finding is that most studies on privacy have focused on explaining and predicting theoretical contributions. They also find that most literature regarding privacy practices is focused on privacy policies on websites in the US (Bélanger & Crossler, 2011). In another literary review on privacy in the same issue by Smith, Dinev, and Xu (2011), the researchers conclude that many theoretical constructs have not been addressed in empirical research on privacy. Also, most studies that have been conducted are on an individual level and privacy research foresee other areas as groups, organisational and societal levels (Smith et al., 2011). A conclusion is that empirical studies on privacy practices on an organisational and a societal level are under-researched.

Implementing privacy practices requires an understanding of both the regulatory framework and a capability to translate general best practices into organisational processes and practices (Niemimaa & Niemimaa, 2017). The GDPR requires self-regulation, meaning every organisation needs to adapt processes on how to prepare, implement and monitor management process for privacy (Kamara, 2017). A study with a process-oriented approach to examine how far organisations have adapted to handle privacy concerns will gain insights for both practitioners and into areas for further research. This leads to the research question:

What is the level of privacy maturity in municipal organisations in Sweden?

This thesis contributes by investigating the state of maturity in Swedish municipalities in a web survey. We present the maturity levels of the municipalities of Sweden, based on a best-practice framework with objective criteria as a basis for measurement. The framework contains several important aspects of privacy management. A practitioner can use the framework to gain insight on which areas need improved processes and to compare their maturity over time and with others.

We describe the following chapters of this thesis as follows. Chapter 2 defines privacy and frameworks, looks into best practice standards, describes maturity models and the current state of privacy from earlier research. Chapter 3 describes the framework for measuring privacy maturity. Chapter 4 covers the application of the framework with methodological aspects. Chapter 5 holds the results of the survey. Chapter 6 discusses the state of privacy maturity in a general sense for municipalities in Sweden, reflections on the survey, practical implications and proposes further research. Chapter 7 concludes the thesis.

2 Theories and earlier research

2.1 Privacy definitions

The first definition of privacy as "the right to be let alone" was done by two lawyers almost 130 year ago in a concept of "right to privacy" (Warren & Brandeis, 1890). They were concerned that the large-scale distribution of photography and newspapers could intrude into the personal sphere, with severe consequences from publication of photographs, if let unregulated. However, the concept was not clearly established and too vague for law-making (Solove, 2002).

Defining privacy is very difficult. There are several categories of definitions which partly overlap, but still are conceptually very different, according to Daniel J. Solove (2006), and they serve different purposes and separate perspectives. This reasoning fits in with Wittgenstein's family resemblance concept where: something which could be considered to be connected by one essential common characteristic may be connected by a series of overlapping similarities, where no one characteristic is common to all of the elements (Wittgenstein, 1953). We will briefly describe four paths that follow on defining privacy from a philosophical standpoint.

Firstly, Alan F Westin coined the modern definition of information privacy as "the claim of individuals...to determine for themselves when, how and to what extent information about them is communicated" (Westin, 1967). He claims an individual's anonymity is a desired state in the public sphere as well as being reserved–while in a large group having the ability to maintain a psychological distance by avoiding communication. We can make parallels with current privacy laws from this perspective to give the individual control via a choice, a consent, on how personal information is to be processed.

Secondly, Solove understands privacy as an umbrella term for activities and mechanisms that violate the individual's private sphere (Solove, 2006). He proposes a taxonomy for privacy-threatening activities which can be used to determine effects when implementing new services. These activities include, for example, surveillance, interrogation, information disclosure, appropriation, secondary use, distortion etc. Not all of them are technological activities, but rather the result of actions by humans, especially by people in organizations and governments (Solove, 2006).

Thirdly, Helen Nissenbaum use the term contextual integrity, instead of privacy[1], with "norms of information" to govern collection, use and dissemination of information, and that individuals own expectations are specific to different kinds of situations (Nissenbaum, 2004). She insists that one must pay attention to details and view privacy in a context-related perspective and the flow of information. Norms vary across different cultures, time-periods, geographical locations and so do perspectives on violation of privacy. From a practitioner's perspective, this raises a challenge to identify and harmonize with, sometimes conflicting, norms when introducing new technology.

Lastly, Calo (2011) introduces the concept of privacy harm from the perception of the kind of harm inflicted upon the individual. Objective harm is direct, measurable and can be observed. Subjective harm is a potential violation, is indirect and unmeasurable. The subjective harm can occur even if no action is taken by the one intruding on privacy. Both subjective and objective harm can have the same negative impact on an individual. To avoid negative perception of harm, one must build trust-worthy and transparent communication of information processing practices.

One conclusion can be made from these four viewpoints on privacy definitions: Privacy is a complex concept, and perhaps it is not even possible to reach a consensus on a definition. Solove (2006) declares that "Privacy is a concept in disarray. Nobody can articulate what it means…". Privacy fits into the description of an *essentially contested concept*, where endless disputes can take place on the meaning of the concept, without reaching consensus, for example, "art", "democracy", "social justice" and so on (Gallie, 1955). The difficulty to grasp the concept of privacy implies the transformation of privacy concerns into regulations or management practices is a complicated task. Therefore, the four theories above can be seen as the starting point, rather than providing direct detailed prescriptions and instruments grounded in one universal definition.

Also, the four perspectives above address privacy for the individual. Policies and regulations classically address privacy from the perspective of the individual and with a conception of privacy as an individual human right (Bennett & Raab, 2018). To understand the individual conceptions link to practices, there is a need to understand the privacy concerns, risks and vulnerabilities for the individuals (Karwatzki, Trenz, Tuunainen, & Veit, 2017), and address privacy risks as links in a system chain of "technologies–policies–processes–people–society–economy–legislature" (Lowry, Dinev, & Willison, 2017). The scope for this thesis includes

[1] Branting (2016) reflects on that the translation of privacy to Swedish as *personlig integritet* is different from what Nissenbaum uses with contextual integrity and suggests that the term refers to something more like *a contextual personal sphere*. The word integrity is in the USA not used as a synonym for privacy.

addressing privacy risk by researching practical aspects of the policy and processes.

2.2 Privacy risk

Mason (1986) predicted rightly, among other things, that information technology will increase threats for privacy, as an ethical issue in the new information age. The world today is quite different from the 1980s, and these concerns are becoming a focal point. Lowry et al. (2017) claim privacy should now be regarded as being at the centre of IS research, due to the ever-increasing privacy concerns regarding online platforms, the internet of things and big data.

Privacy risks have abstract definitions in privacy research, as either opportunistic behaviour with loss of control of personal information or substantial adverse outcomes for the individual with the release of personal data, according to (Karwatzki et al., 2017). In general risk literature, a more differentiated understanding is found, where risk is perceived as the adverse consequences of negative outcomes of a situation, and the likelihood of their occurrence (Karwatzki et al., 2017).

Since a violation of privacy can be subjective (Calo, 2011), the concerns of threats and risk must be seen on the potential harm that can occur (Solove, 2008). For organisations to address individuals concerns for privacy risks, mitigation mechanisms such as adapting and changing organisational practices are needed (Karwatzki et al., 2017). This necessity would imply transparency and preventive mechanisms to ease the concern of the individuals. However, organisations primary privacy concerns reflect the information the organisation possesses and how to implement management practices best to comply with both regulations and maximise business priorities (Bélanger & Crossler, 2011). The link between the individual and the organisation would be weak without the laws.

Next section describes the general privacy frameworks and principles for privacy concepts introduced in laws and practices.

2.3 Privacy frameworks

Privacy frameworks are expressions used for various processes-oriented templates, tools, laws and standards. A definition of privacy framework, used by the International Association of Privacy Professionals (IAPP), is:

”An implementation roadmap that provides the structure or checklists (documented privacy procedures and processes) to guide the privacy professional through privacy management and prompts them for the details to determine all privacy-relevant decisions for the organization.” (Densmore, 2016).

Information security practices are related to privacy (Lowry et al., 2017), but the theoretical relationship is diverted into which perspective is a part of which. (Krumay & Oetzel, 2011). The concept of privacy frameworks is less comprehensive and far less specific than information security concepts. Privacy frameworks are lacking a common body of knowledge for implementation (Krumay & Oetzel, 2011). Information security, with its triad of confidentiality, integrity and availability (CIA), have for example long-time, well-established standards like the ISO/IEC 27000-series with pre-defined general requirements to implement controls and govern implementation (ISO/IEC, 2013). Still, efforts have emerged for supporting implementation in managing privacy since the 1970s.

Legal privacy frameworks typically answer the question: "What must be done?". There are several significant international laws and regulations, but here we mention some Swedish examples in a European context. Examples of laws in Sweden are: The first-ever national privacy law, the Swedish Datalag (1973:289); the national law Personuppgiftslagen (1998:204), based on Data Protection Directive[2] (European Parliament, 1995); and the far-reaching GDPR (European Parliament, 2016), with increased obligations for organizations and hefty fines for non-compliance.

Other regulatory frameworks with principles for privacy include, for example; the Fair Information Practices (FIPs) with origins in the early 1970s from the US Department of Health & Human Services (1973) and later updated by the Privacy Privacy Protection Study Commission (1977) with a basic set of principles and have generated several modern privacy legislation. The most widely accepted privacy principles are from the 1980s, the *OECD Guidelines on the protection of privacy and transborder flows of personal data* together with the Council of Europe's *Convention 108*, which both are a basis for both the Data Protection Directive and the GDPR (Ustaran, 2017).

To sum up, privacy frameworks are yet to evolve, but a stem of both practice and laws have emerged. Several laws and also other regulations are setting requirements to answer the what-question. The regulators give organisations guidance on what principles are needed to implement, but not how, and then remain in the background to enforce sanctions if laws are breached (Bennett & Raab, 2018). For practical use of how organisations need to address compliance, one must look into privacy standard frameworks.

GDPR is technology-neutral and laws do not change as fast as technology. GDPR also holds an accountability principle. Organisations need to use privacy management to facilitate accountability and standards to provide the means for implementing processes for the use of personal data in technology (Kamara, 2017).

[2] The term *Data Protection* is introduced by the EU and translates to Swedish by the word by "Dataskydd". Both are synonymous with privacy.

As technology changes, so must the internal processes support improvement to continue to be compliant to the law.

2.4 Privacy standards

Privacy research from the business practices perspective is a new area (Kauffman, Lee, Prosch, & Steinbart, 2011). Standards for how to implement privacy principles are hard to find to comply with the GDPR. The OECD Guidelines form a basis for common understanding and are implemented in several laws, but are of less practical value for management since the articles within are high-level aims and principles (Ustaran, 2017)

In 2015, the European Commission issued the first standardisation request to the European Standardization Organisations to develop privacy management standards (Kamara, 2017). One emerging standardisation effort is the ISO/IEC-29000-series of privacy frameworks (ISO/IEC, 2011, 2015). However, these frameworks are not yet a complete standard. An International standard organisation (ISO) technical committee is currently working on a standard called ISO/IEC 27550 (ISO/IEC, 2019; van Dijk, Tanas, Rommetveit, & Raab, 2018). The outcome from European standardisation efforts is not ready to use.

On the other side of the Atlantic, a new standard is being created by the National Institute of Standards and Technology (NIST). They are creating a framework for specifically privacy to help organisations to identify better, assesses, manage, and communicate about privacy risks, which is expected to roll out under 2019 (NIST, 2019). An earlier framework by NIST is SP 500-83 Revision 4, which address both cybersecurity and privacy risks for US federal information systems and organisations (NIST, 2013), where 26 controls for privacy have the scope to comply with the 1974 US Privacy Act. It is fair to assume the both the SP 500-83 Revision 4 and the new NIST Privacy framework are far from the current European legislation.

Privacy-by-Design (PbD) is another example standard framework. PbD contains seven principles and was created by Ann Cavoukian (2009) to help organisations to design-in protections at every stage in developing products and services. To comply with PbD is a legal requirement in the GDPR. Though PbD is an excellent approach to adopt privacy-thinking into service engineering practices early, it is a strategic manifesto of privacy principles, rather than criteria for a how-to implementation. It is also would require further adaption and creation of measurable criteria, before using it in a research survey.

Generally Accepted Privacy Principles (GAPP) is a framework standard that is addressing privacy practices in particular. A task force developed it from the American Institute of Certified Public Accountants (AICPA) and the Canadian

Institute of Chartered Accountants (AICPA/CICA, 2011a). GAPP is not a law but can be regarded as a best-practice standard for compliance with several privacy laws, even though compliance is not mentioned (Govender, 2015). The GAPP standard framework was created as a joint effort to interweave several major international privacy laws and best practices. It a solid benchmark for good privacy practices (Govender, 2015), and have also been used as a framework for analysing literature and research regarding privacy (Kauffman et al., 2011).

GAPP consists of ten principles, with 73 objective and measurable criteria for each principle. The 73 criteria cover how internal policies and communications should be implemented, as well as descriptive criteria for procedures and controls. GAPP is technology-neutral (Gable, 2014). The ten GAPP-principles are shown in Table 1. The framework is built from a business perspective and operationalizes requirements and is meant to guide organizations on how to develop, implement and manage privacy programs to address privacy obligations, risks, and business opportunities (AICPA/CICA, 2011a). It is partly based on the ISO-27002 standard controls for information security. (Gable, 2014). Schroeder and Cohen (2011) express GAPP is a scalable tool for addressing privacy risks, and the main application is that personal information is collected, used, retained and disclosed in accordance with an organization's privacy policy. The privacy functions also need to be well-aligned with the overall information governance framework within an organization to enable successful compliance, risk-reduction, and efficiency and GAPP is a vehicle to support that (Goodman, 2018).

Table 1
The 10 generally accepted privacy principles (AICPA/CICA, 2011a)

Principle	
1. Management	The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures
2. Notice	The entity provides notice about its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained, and disclosed.
3. Choice and consent	The entity describes the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use, and disclosure of personal information.
4. Collection	The entity collects personal information only for the purposes identified in the notice.
5. Use, retention, and disposal	The entity limits the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent. The entity retains personal information for only as long as necessary to fulfill the stated purposes or as required by law or regulations and thereafter appropriately disposes of such information.
6. Access	The entity provides individuals with access to their personal information for review and update.
7. Disclosure to third parties	The entity discloses personal information to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual.
8. Security for privacy	The entity protects personal information against unauthorized access (both physical and logical).
9. Quality	The entity maintains accurate, complete, and relevant personal information for the purposes identified in the notice.
10. Monitoring and enforcement	The entity monitors compliance with its privacy policies and procedures and has procedures to address privacy related complaints and disputes.

Dennedy, Fox, and Finneran (2014) claim GAPP is the most comprehensive privacy framework available and can be aligned with other different standards and other legal privacy frameworks on key principles. See a comparison in Table 2 aligning the GAPP, the OECD Guidelines, the EU Data Protection Directive (European Parliament, 1995), the Federal Trade Commission's version of the Fair Information Privacy Principles (FIPPs) which is a later version of the (FIPs), the ISO 27002 security controls, and the GDPR.

Table 2

Alignment of privacy frameworks, standards and law. Adapted from Dennedy et al. (2014).

GAPP	OECD Guidelines	FTC FIPPS	EU Directive	ISO 27002	[GDPR][3]
1. Management				Operations Management	Responsibilities of controllers and processors, Records of processing activities, Personal data breaches
2. Notice	Specification of Purpose		Transparency		Information, communication obligations
3. Choice/Consent	Individual Participation	Choice/Consent		Asset Management	Consent
4. Collection	Collection Limitation		Proportionality	Information Acquisition	Principles for processing. Processing of special categories
5. Use, Retention, Disposal	Use Limitation		Legitimate Purpose	Asset Management	Purpose limitations, Data minimisation, Storage limitations
6. Access	Openness	Access/Participation		Access Control	Rights of the data subject
7. Disclosure to Third Parties			Transfer of personal data to third parties		Transfer of personal data to third parties, third countries or international organisations
8. Security for Privacy	Security Safeguards	Integrity/Security		Security	Integrity and confidentiality, Security of processing
9. Quality	Data Quality	Notice/Awareness			Accuracy
10. Monitoring and Enforcement	Accountability	Enforcement/Redress	Supervisory authority	Compliance	Supervisory authorities, Data protection impact assessment, Accountability

[3] GDPR is added by the authors, since the alignment table is out-dated regarding EU-legislation.

To the best of our knowledge, a complete non-proprietary privacy standard framework, to measure the level of implementation of privacy management of organisations, is the GAPP framework. It is technology-neutral, scalable and a solid base for benchmarking. It contains 73 measurable objective privacy criteria which are covering the requirements of the GDPR. Moreover, a privacy maturity model is created based on GAPP, to measure privacy maturity in organisations. Next section elaborates the concept of maturity models.

2.5 Maturity models

The concept of maturity models has sprung from the idea that organisational improvement is best developed in different stages – a step-by-step approach. Nolan (1973) first described a stage-theory model for the planning and controlling of computer resources in an organization, which is widely adopted (Pöppelbuß & Röglinger, 2011). In the late 1980s Humphrey *et al* (1987) created the first version of the capability maturity model (CMM) for the use of improving software engineering in an organisation. In the 1990s the CMM was updated to a 1.1 version (Paulk, Curtis, Chrissis, & Weber, 1993) which is the foundation for a plenitude of maturity models.

The CMM 1.1 have a good description of *immature* versus *mature* organisations. (Paulk et al., 1993) states that: "The immature software organisation is reactionary and often solving crises (better known as firefighting). Schedules and budget are routinely exceeded because they are not based on realistic estimations… [and] has no objective way to judge quality."; and that "A mature organisation possesses an organization-wide ability to manage development and maintenance… and work activities are carried out according to planned processes." The CMM 1.1 have five levels on an ordinal scale, 1 to 5, to measure process maturity and evaluate capacity, see *Figure 1*.

- Level 1, Initial, is the starting point, where success depends on individuals and cannot be repeated without the competence and heroic ad hoc co-workers.
- Level 2, Repeatable, is stable since process is disciplined with better planning; and successes can be repeated.
- Level 3, Defined, is consistent and a standard is set. Roles and responsibilities are clear and common processes are shared organization-wide.
- Level 4, Managed, is predictable and quantifiable, since processes are measured. Problems are identified and corrective actions are taken.
- Level 5, Optimized, is a state of continuous improvements by incremental and innovative improvements in a planned way.

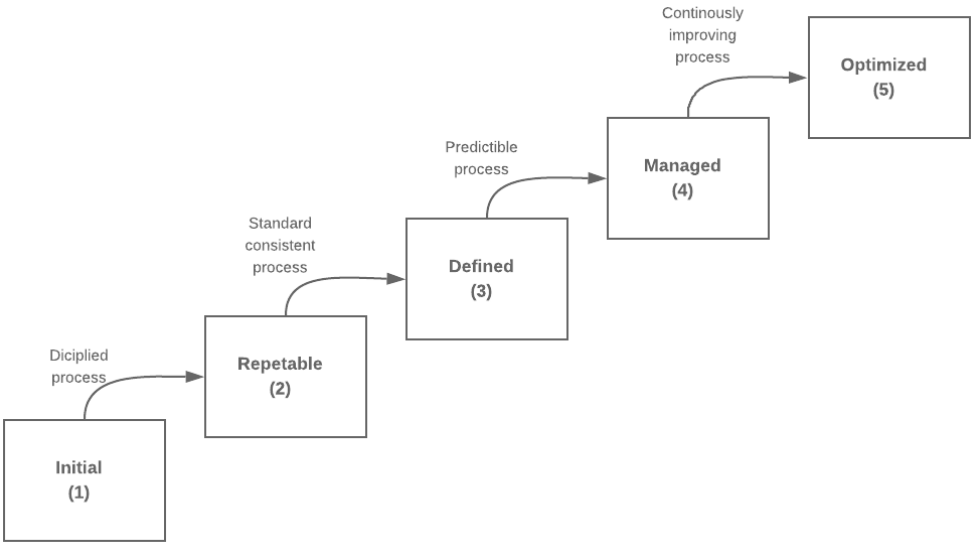

Figure 1 Maturity framework CMM 1.1 with five levels (Paulk et al., 1993)

Closely related to privacy are maturity models for Information security. Several Information Security Maturity models (ISMM) exist; Karokola, Kowalski, and Yngström (2011) analyse eight ISMM and create a proposal a model for secure e-government, which is tested in Tanzania; Ricardo dos Santos, Becker Westphall, Alencar Rigon, and Merkle Westphall (2014) create an ISMM with six stages and an evaluation model based on the 133 controls in ISO/IEC 27002 standard (ISO/IEC, 2013); The Open Group (2011) have created a ISMM called Open Information Security Management Maturity Model (O-ISM3) with five levels based on several standards, with main focus to serve strategic and broad process improvement, rather than risk and security (Karokola et al., 2011); Control Objectives for Information and Related Technology (CobiT) have a six stage scale, which have been tested in an self-administrated survey on 970 individuals in Malaysian Public Service organizations, with the result of almost 2/3 are on level 3 (Dzazali, Sulaiman, & Zolait, 2009). However, these maturity models are not covering the all the specific aspects of privacy, which are not security-related.

The Privacy maturity model (PMM) has a five-level scale similar to the CMM 1.1 (AICPA/CICA, 2011b). The PMM is based on GAPP's 10 principles and 73 criteria. Thus, multiplied by five maturity levels, this makes a total of 365 level descriptions that objectively and concretely define what should be done to match each level. The criteria and level descriptions are based on best practices provided by AICPA and CICA professionals. Similarly, the 133 controls of ISO/IEC 27002 are also best practice-oriented (Ricardo dos Santos et al., 2014). In this thesis the survey measurement basis is supported by criteria and level descriptions of the PMM. Also, the PMM is base for the framework used in the survey.

2.6 Critique of maturity models

Maturity models in their different forms are subject for criticism. Benbasat, Dexter, Drury, and Goldstein (1984) criticise the stage-theory model for its lack of evidence of robustness and reliability. They also claim that different criteria for maturity do not consistently progress together and also could transgress in opposite directions. In other words, maturity does not evolve stage by stage.

Other criticism expressed by King and Kraemer (1984) suggests that the assumptions of the model are too simplistic to come to real use and that the model cannot be used for making predictions as intended. Furthermore, they question the empirical foundation of evidence for the model. Note, that this was written in the 1980s, and since then a lot of empirical evaluation has been provided.

Teo and King (1997) point out that the possibility of moving backwards through stages or progressing through the stages in an alternative order is not included in the stage-theory model.

As for criticism of the CMM, Pfeffer and Sutton (1999) complain that although this model might be useful indicating when something needs to be done, the maturity model does not very often advise how to take action to progress through the model.

Critique regarding the insufficiency of reflection on maturity is brought forth by Wendler (2012) who also criticises the uncritical use of influences from the industry and the absence of validation.

Since the intentions were to create a framework that in some way involves maturity, this criticism needs to be considered. Firstly, the scope of this thesis is limited to the domain of maturity of privacy. It is a limited domain constrained by external environmental factors such as laws. If the laws change and invalidate the fundamentals of the model, usefulness of the assessments of maturity will be gone. In that sense, maturity may be seen as a static state. Secondly, the research question includes a comparative aspect on a national level. To make a purposeful comparative maturity model, it includes objective criteria for internal and external benchmarking (Pöppelbuß & Röglinger, 2011).

2.7 Current state of privacy readiness

Internationally, several privacy surveys have been performed on a large scale in companies, mostly by large consultant firms, whose interest is mainly in progress towards compliance with the GDPR and the usage of tools, recourses, and global challenges. In a worldwide study by the IAPP, called the Privacy Governance Report 2018, respondents were asked to self-evaluate the maturity of their privacy programs in early, mid or mature stages and the results showed that in organisations under 5000 employees, 29 percent were perceiving themselves as

early; and in large organisations, with over 75000 employees, 57 percent were mature (IAPP-EY, 2018). Another study by the Ponemon institute where more than 1000 companies in EU and USA are represented shows that 69 percent is working ad hoc or have no governance data program; of the 31 percent that do have a program running, only 15 percent say they are at a mature stage, where "…activities are deployed, maintained and/or refined across the enterprise" (Ponemon, 2018).

A Swedish Government parliamentary committee outlined IT-related risks for breaches of privacy in the society and concluded that the individual's privacy is diminishing in several areas (Integritetskommittén, 2016). The committee has classified risks in three levels; some risk, obvious risk and serious risk. Risks concerning large quantities of sensitive personal data in municipalities are found in schools, working life, social services, health care and E-government, and there are also serious risks related to municipalities and big data, cloud services and biometry (Integritetskommittén, 2016). A summary of privacy risks associated to municipalities can be found in *Appendix 4 – Privacy risks areas in the municipalities.*

Privacy and information security (IS) are related topics and studies can be elaborated from this field into the privacy area. The Swedish Civil Contingencies Agency (MSB) made a study on information security in 2015, where 270 of 290 municipalities participated. The results are: 40 percent of the municipalities do not have a responsible person for IS; 25 percent have less than a 10 percent full-time employee working with IS; 68 percent are not working systematically with IS; and 55 percent have no process for management and reporting of IS-incidents (MSB, 2015, 2016). Regarding privacy capabilities for municipalities, one may expect a similar state of affairs.

A recent national survey by the Swedish DPA show municipalities is facing challenges (Datainspektionen, 2019b). The target group of study was Data Protection Offices (DPOs) for both private and public sectors. DPOs are a legal obligation for all public sector authorities with their administration bodies (hereafter named controllers). 396 of 1687 DPOs from municipalities or regions answered the survey. 92 percent of these 396 came from municipalities. Counting only DPOs from municipalities, this means that 363 answered the survey. Some illustrating differences with lower assessment from municipal and regional DPOs than the rest are; (1) the organisation is not working systematically; (2) the employees of the controllers have less knowledge of the GDPR; and (3) the management is less aware of privacy and is giving this a lower priority.

3 A privacy maturity framework

This chapter focuses on the development of a framework, used to measure privacy maturity in municipalities. The application of the framework is to systematically categorise how well municipal organisation use best-practice privacy management processes by using a self-administered questionnaire. The maturity level should not be regarded as an audit of legal compliance of the municipalities. Instead, then it should be considered as a systematic attempt to collect a self-evaluation of the management approach and process maturity for privacy.

We created the framework in an iterative approach. See *Figure 2* for an overview of creating the Privacy maturity framework.

First, we made a conceptual analysis and decomposition of the level descriptions in the PMM. Second, we created a questionnaire covering the complete PMM with 134 questions. A description of the question construction is found in the second section. Third, we tested the questionnaire in a pilot study with practitioners in one municipality. Forth, based on feedback from the pilot, we analysed the questionnaire, resulting in a reduction of questions (and criteria). Fifth, we created six grouping attributes as a result of further analysis and from the feedback, and then we created a new second questionnaire with some control questions and questions for correlation. Sixth, we performed a second pilot on the reduced questionnaire, with the same group of practitioners as in the first pilot and also added some respondents from other municipalities. The second pilot received a positive response in feedback from testers. Seventh, we adjusted some questions, and then we created an analysis template with the final scoring of the questions. Last, we deployed the final questionnaire in a web survey, described in chapter 4 with research settings, sample, and other methodological aspects.

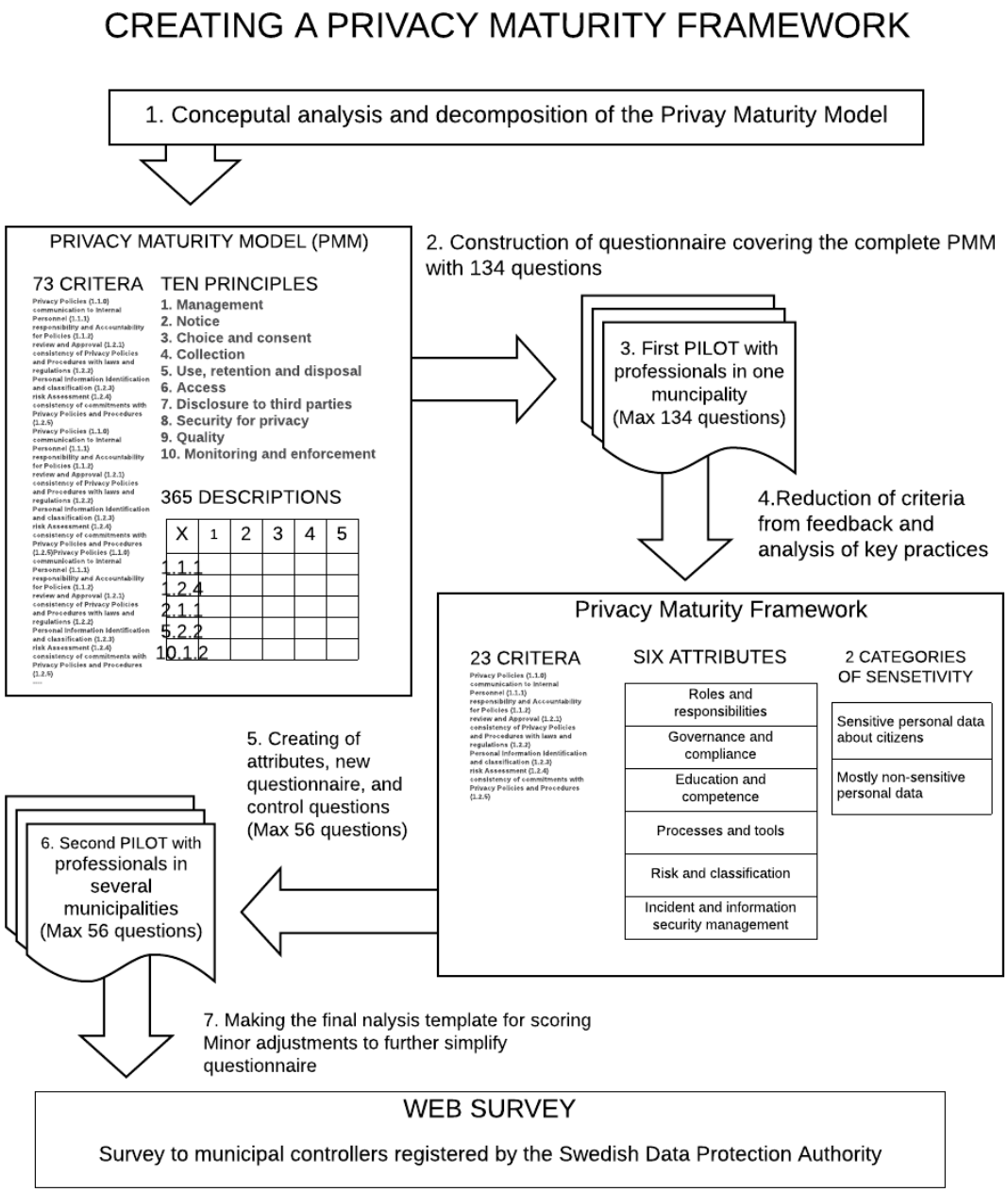

Figure 2 Development of the framework

3.1 Conceptual analysis

The outset of the framework is the PMM (AICPA/CICA, 2011b), based on GAPP (AICPA/CICA, 2011a). The PMM provides 10 principles, 73 criteria and 365 level descriptions. Each of the level descriptions for the criteria in PMM is quite similar, but with different concrete descriptions for what is required to reach each level. See the example of the level descriptions in *Figure 3*. The first three levels in each criterion offer exclusive different degrees of process maturity, from ad hoc (level

1), then repeatable (level 2) and to a defined process (level 3). The two top-levels include added descriptions for managed (level 4) and optimized (level 5). Level 3 is in the PMM regarded as a mature state (AICPA/CICA, 2011b) and the same reasoning applies of maturity applies on organisations in the CMM (Paulk et al., 1993).

		AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
Privacy Policies (1.1.0)	**The entity defines and documents its privacy policies with respect to notice; choice and consent; collection; use, retention and disposal; access; disclosure to third parties; security for privacy; quality; and mon- itoring and enforcement .**	Some aspects of privacy policies exist informally.	Privacy policies exist but may not be comlplete, and are not fully documented.	Policies are defined for: notice, choice and consent; collection; use, retention and disposal; access; disclosure; security for privacy; quality; and monitoring and enforcement.	Compliance with privacy policies is monitored and the results of such monitoring are used to reinforce key privacy messages.	Management monitors compliance with policies and procedures concerning personal information. Issues of non-compliance are identified and remedial action taken to ensure compliance in a timely fashion.

Figure 3 Example of a privacy maturity model criteria (AICPA/CICA, 2011b)

The different criteria in GAPP are grouped into aspects of either "*Policies and Communications"* or "*Procedures and Controls"*. Ten of the criteria deal with policies within each of the principles and there is a similar situation with criteria for Communication. This similarity means that 20 criteria are almost identical in the level descriptions of the PMM. See *Appendix 1 – GAPP principles and criteria* for a complete list of for all principles, criteria and aspects.

The principles are a way of sorting the criteria with headers and the grouping into aspects does not contain any information other than forming a structure. The distribution of criteria for the principles is found in Table 3. A lot of useful basis for measurement is found within the first principle, the Management principle, where several criteria can guide procedures to test in practice (Kauffman et al., 2011). For example, 1.1.0 Privacy policies can be used to measure the scope of internal policies; 1.1.2 Responsibility and accountability for policies can determine the sheer existents of a privacy function and how extensive it is; 1.2.4 Risk assessment can be used to measure the risk-based approach of the organisation; 1.2.7 Incident and breach management can be used for measuring the procedures and preparedness for personal data breaches and mitigation strategies; 1.2.8 Supporting personal can give a measuring for the seniority of privacy personnel; and 1.2.10 Privacy awareness and training can be used to measure the strategy of training and awareness for personnel in general. All of these crucial principles to determine practices in key aspects of privacy management are concentrated in one principle. The point is, there is an uneven balance between the different principles. Possibly, there could be other ways of grouping the criteria into something else than the principles. One way would be to use the principles found in different legislations on which GAPP is based on could be one possible way of grouping the criteria. Another way of grouping the criteria could be on the functional aspects of an organisation. The criteria purposefully hold meaningful granular information to

describe how processes should be performed and this can be grouped in several ways, without losing the relevance found the criteria.

Table 3
Distribution of GAPP criteria grouped in the different principles

Principle	Criteria
1. Management	14
2. Notice	5
3. Choice and consent	7
4. Collection	7
5. Use, retention, and disposal	5
6. Access	8
7. Disclosure to third parties	7
8. Security for privacy	9
9. Quality	4
10. Monitoring and enforcement	7
Total	**73**

Some of the criteria descriptions and the level descriptions are quite wordy. A comprehensive approach would be to try to catch all content in the descriptions and create an extensive questionnaire. However, it would not be feasible to accomplish and use for our research question, including a nation-wide aspect of the "…privacy maturity in municipal organisations in Sweden". Respondents would not likely give answers to such a far-reaching approach. The question designer should have a respondent perspective and not burden the respondents more than necessary (Persson, Fjelkegård, Hartwig, & Sundström, 2016). With this in mind, there is a need to simplify the wordy descriptions used in PMM, when constructing questions and answers. The trade-off between the comprehensive and the minimalistic approaches is that the exactness with detailed information is lost, but there is still general information identified pointing towards the privacy maturity. Next section explains how we used a paradigm to systematically create the minimalistic approach for handling the detailed and wordy criteria level descriptions.

3.2 Questionnaire construction

The questionnaire was created using the Goal-Question-Metric (GQM) paradigm, which has its origin in software engineering (Basili, 1989; Van Solingen, Basili, Caldiera, & Rombach, 2002). GQM has been used to erect metrics in a variety of different research contexts. For example in maturity model for documentation process (Visconti & Cook, 1998), accountability for could services (Nuñez, Fernández-Gago, & Luna, 2016) process assessments for IT service management (Shrestha, Cater-Steel, Toleman, & Tan, 2014). GQM offers a structured approach with a three levels top-down decomposition, from a conceptual level with the goal

to suit the needs, through an operational level where questions are created and to a quantitative level where the resulting metrics are scored (Basili, 1989; Van Solingen et al., 2002). See *Figure 4*. The point is to link measurement to overall goals because a set of measurements can be more successful with the goals in mind (Visconti & Cook, 1998).

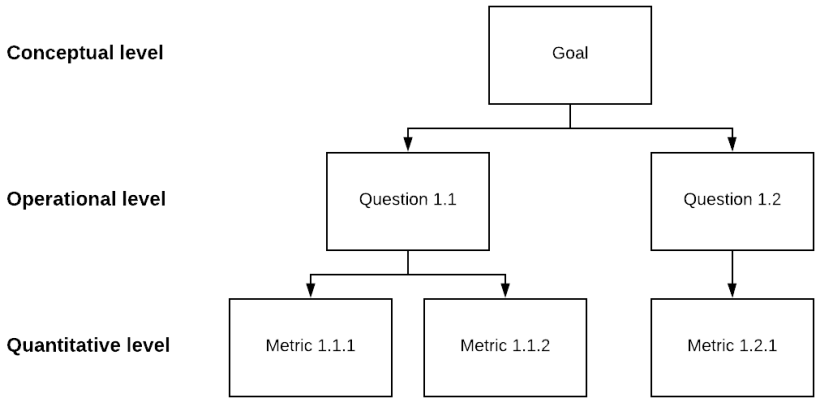

Figure 4 The Goal-Question-Metric paradigm (Nuñez et al., 2016).

In developing the framework, the primary goal is linking the assessment on a level of granularity for each area on the criteria level. The criteria description and level descriptions (policies, artefacts or practices) become the goal on a conceptual level. These are broken down to concrete questions with response options to match the level descriptions (operational level). The responses to the question are then used to score the maturity level within each criterion (quantitative level). See *Figure 5*

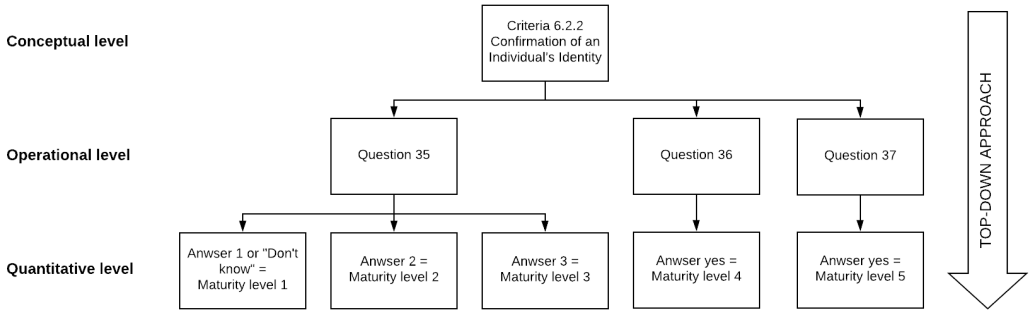

Figure 5 The GQM paradigm applied on the framework for question creation.

The construction of the full survey in Swedish contains a minimum of 71 and a maximum of 134 questions, depending on which path through the questionnaire the respondent will take. The response options are in general closed single-choice filter questions for the level 1-3 and multiple-choice questions for the supplementary questions. In general, ratings are given on a sequence of questions starting with a filter question, and then one or two follow up questions, as in the example above. The number of questions for each criterion depended on whether if the level

descriptions in the PMM contained mutually exclusive descriptions. As an example, we use the case of the criterion 6.2.2, where the levels 1-3 are mutually exclusive to the different degrees of process maturity; one question addressed this. The two follow-up questions require that the respondent answered response 3. The levels 4-5 if scored if answered "yes". In the case for question 37, also the answer "partially" were considered and resulted in maturity level 4, since the maturity is between level 4 and 5. See the questions (translated to English) in the example and how it connects with the wordy level descriptions in *Figure 6*.

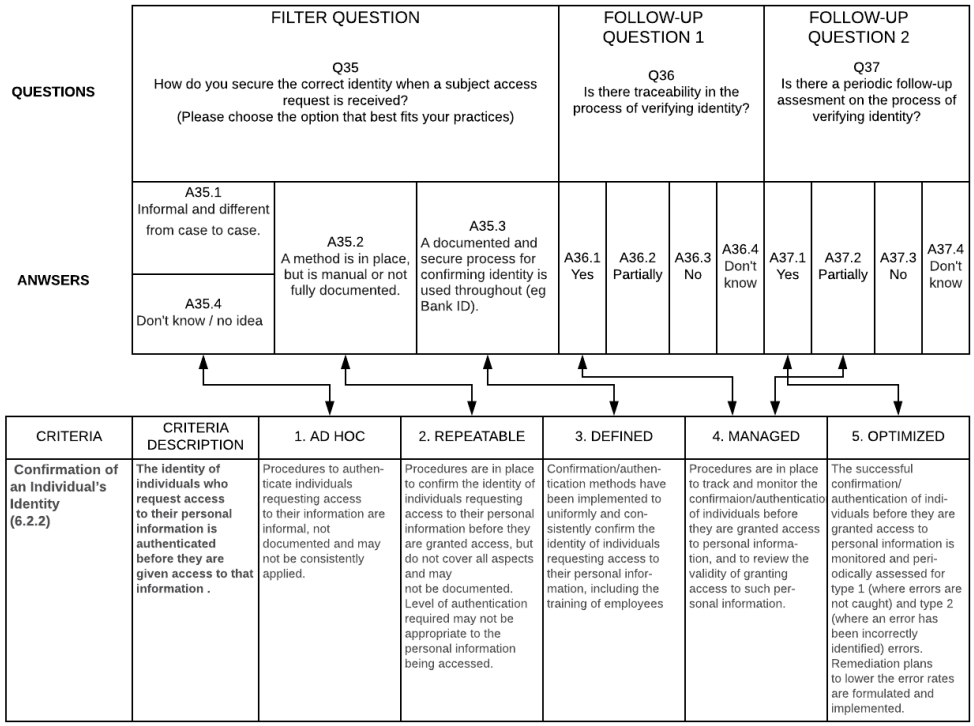

Figure 6 Example of questions and their link to level descriptions in the PMM

In some cases, all five maturity levels are achievable in a one question answer, which is the case in questions 21 and 29. We also use different ways for ratings of these questions. In question 21, it is sufficient to select either one of the levels 1-4 answers to get the score of maturity 1 to 4. The highest possible answer gives the maturity level. Only level 5 also requires the level 4 answer. In question 29, all lower levels are needed to gain a higher level, and it is harder to obtain a high rating based on these conditions.

Some questions do not rate maturity at all, since there are no corresponding maturity in the PMM or there are no description available to determine maturity objectively. For example, question 11 "How often do you carry out and update assessments in your risk management?", does not say much about the quality of the risk assessments or process-oriented maturity. Rather this is included as a control question and for finding possible correlations.

Since the target group of the survey is controllers in Swedish municipalities, the survey is written in Swedish and a familiar vocabulary for the municipalities of Sweden is used[4].

More, we added some questions and answers which do point to a level of maturity but are not part of the GAPP framework Aforementioned, most of the GAPP criteria are technology neutral, as are most privacy laws, especially the GDPR. By adding more of concrete and technical descriptions as options for answers, it would possibly become easier for respondents to answer, since current technology is easier to relate to, than abstract descriptions. These answers may be objective and can be linked to maturity, but the answers are not technology neutral. An example is in question 12 "An IT tool is used for handling and documentation of risks (Not excel or equivalent)". Moreover, we have included the possibility to add comments to multiple choice questions. This gives input to more descriptions, which can be added in the future as a sign of maturity level.

As mentioned in the analysis above, this means that 20 criteria are almost identical in the level descriptions of the PMM. Regarding questions on *Policies and Communications,* we only use one criterion each. This approach is the first version of the questionnaire directly covering 53 criteria, with its 134 questions.

3.3 Pilot on the first questionnaire

A group of eight practitioners within one municipality did a first pilot test on the first version, covering the full range of criteria in GAPP, with a minimum of 71 and a maximum of 134 questions. Each of the respondents has professional skills in privacy issues within different areas in the municipality, and they are well-known by one of the authors. The respondents had six days to complete the questionnaire between April 3rd and 8th 2019. Only one person out of eight answered the pilot survey, and it took around 45 minutes. Another person had started but dropped out. The respondents gave feedback at a meeting, and there we had a sum-up discussion with them. The common conclusion at the meeting was that the questionnaire was too long to be feasible for a wide-spread national survey. Lengthy and tiresome sessions for the respondents are known to increase the risk of respondents attrition, especially fielding new studies that have not been previously tested or validated (Hochheimer et al., 2016). We also had a workshop with the one who answered the complete survey. To walk through all the answers took almost three hours.

[4] For example, the word "dokumenthanteringsplan" is used as a term in the concept of "Use, retention and disposal".

3.4 Scope reduction

A scope reduction was used to adapt the framework into the field of study of a municipality context. Therefore, we considered common privacy practices and risks in a municipality as a basis to contextualise the framework and reduce the questionnaire. We conducted an analysis of the questionnaire based on the feedback from the pilot. The analysis was done on the question level to find key practices among the answers and to find the most relevant criteria to use for assessment. The review process was a bottom-up approach to handle the GQM paradigm in reverse. See the example below in *Figure 7*. As input, we used three guiding principles from the feedback of the pilot and literature.

First, we used a risk-based approach with key practices found in literature, and the criteria covering those key practices are prioritised. A risk-based approach is central and propagated by the GDPR legislation, stating in Article 32 that the "…the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk" (European Parliament, 2016). As explained above mature practices is found in the level 3 descriptions of the criteria in the PMM, which is considered a mature state (AICPA/CICA, 2011b). See Table 4 below for the key practices identified in the first questionnaire.

Second, we filtered out the questions that could be redundant. Another requirement for calculating the completeness of a maturity levels is that all levels need to be possible to reach in each criterion. In some cases, questions are needed to get a complete set of maturity from 1-5. In other cases, we deemed it possible to get the score for levels 4-5 in another question, so then these were set as redundant too.

Third, with the feedback from the pilot, we removed questions not common in a municipality context. To sum up, in the analysis we have given the following *prioritisation score* to questions that are:

1 for questions we consider as a key practice or are needed for completeness.
2 for redundant questions, where the key practice is already mentioned, or answers are covered by another questions.
3 for practices that is not considered common in a municipality context.

Only criteria with prioritisation score 1 are used in the creation of the new second questionnaire.

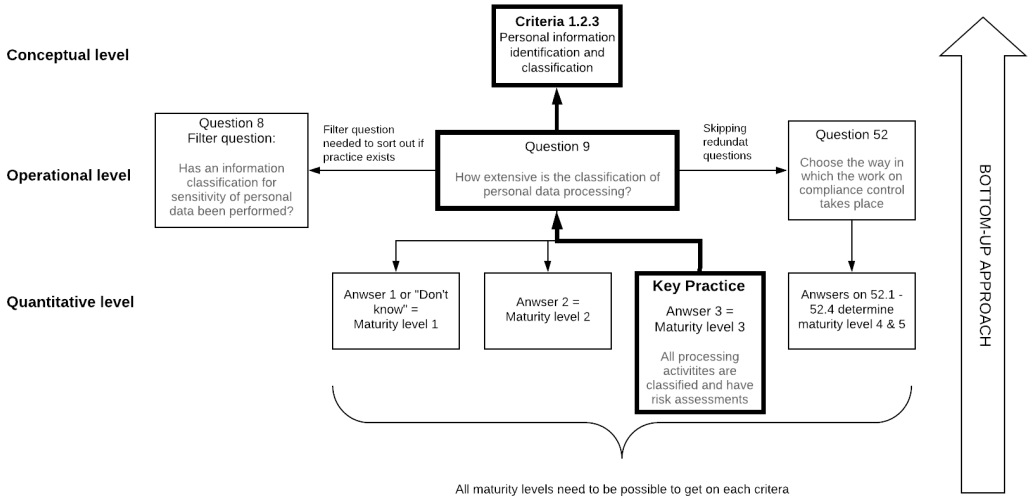

Figure 7 Example reversed GQM paradigm as a bottom-up approach

As seen in the example above in for criteria 1.2.3, the key practice is found in the level 3 answer. The choice lead to give question 9 a prioritisation score of one, and we keep the filter question 8 since it is needed to sort out whether practice exists. We categorise two other questions as redundant, and to meet the completeness requirement we use question 52 to score levels 4-5. The full list of questions in the first questionnaire, the prioritisation score used in the analysis for the reverse GQM-process, and the selected criteria is found in *Appendix 2 – Scope reduction and key practices analysis.*

Table 4
Key practices found in the questionnaire with link to criteria

Key Practices	→	**Criteria**	**Reference**
Has internal regulations (policy)	→	1.1.0	(Bélanger & Crossler, 2011; Krumay & Oetzel, 2011)
Defined roles and responsibilities exist	→	1.1.2	(Kauffman et al., 2011)
Regulations are reviewed to ensure that they comply with legislation	→	1.2.2	(Schroeder & Cohen, 2011)
All processing activities are classified and have risk assessments	→	1.2.3	(Govender, 2015; Nuñez et al., 2016)
Risk process exists and is used	→	1.2.4	(Govender, 2015; Kauffman et al., 2011; Schroeder & Cohen, 2011)
Review agreements for personal information	→	1.2.5	(Kauffman et al., 2011; Schroeder & Cohen, 2011)
Data protection impact assessments are performed	→	1.2.6	(Kauffman et al., 2011; Krumay & Oetzel, 2011)
Incident process established	→	1.2.7	(Kauffman et al., 2011; Nuñez et al., 2016; Schroeder & Cohen, 2011)
Available resources among staff	→	1.2.8	(Kauffman et al., 2011)

Formal requirements for internal staff are available	→	1.2.9	(Nuñez et al., 2016)
Education in privacy takes place	→	1.2.10	(Govender, 2015; Kauffman et al., 2011; Schroeder & Cohen, 2011)
Information to registered persons is done	→	2.2.1	(Kauffman et al., 2011)
Document management plan exists and works	→	5.2.2	(Cavoukian, 2009)
Process for registry extracts is available	→	6.2.1	(Nuñez et al., 2016)
Identity verification process	→	6.2.2	(Nuñez et al., 2016)
Process for personal data agreement	→	7.2.2	Requirement by the GDPR: (European Parliament, 2016)
Has information security programs	→	8.2.1	(Govender, 2015; Kauffman et al., 2011)
Information security is handled as a part of privacy	→	8.2.1	(Govender, 2015; Kauffman et al., 2011)
External audits of information security take place	→	8.2.1	(Govender, 2015; Kauffman et al., 2011)
Basic protection for logical access is available	→	8.2.2	(Kauffman et al., 2011)
Protection for mobile devices is available	→	8.2.6	(Kauffman et al., 2011)
Information security audits are performed and is defined	→	8.2.7	(Kauffman et al., 2011)
Analysis of root cause	→	8.2.7	(Checkland, 1989; Kauffman et al., 2011)
Compliance Control defined	→	10.2.3	(Hertzberg, 2018)
Deviation handling defined	→	10.2.4	(Kauffman et al., 2011)
Monitoring effectiveness of controls	→	10.2.5	(Dennedy et al., 2014; Kauffman et al., 2011)

A consequence of the reduction of criteria is that it is not possible to produce a report based on the ten grouping principles. Also, there can be missing measures for maturity. The measure of maturity is, after the reduction, not a complete assessment of privacy maturity, according to PMM. However, we find it not feasible to go along with the complete PMM and still be able to do a nation-wide survey. The aim of this thesis is for the results to be generalisable. Too low response rate impedes that.

3.5 Creation of a new questionnaire and attributes

The new second questionnaire is based on the reduced scope of the framework. The common denominator between the PMM and the Privacy maturity framework is

the criteria level. The new questionnaire consists of 23 of the total 73 criteria. The number of questions is a minimum of 30 and maximum 56 questions depending on how a respondent answer. Since it would not make sense to use the grouping of the principles, as mentioned above, we use another method.

The grouping structure of GAPP has a legal perspective with the of the ten principles compiled of several legislations. There is a difference in whether to implement practises from a legal or a technical viewpoint. Adequate protection for privacy cannot be thought of only in terms of compliance with legal frameworks, but it also has technological and practical aspects (Rachovitsa, 2016). Instead of the legal perspective, the grouping is done with an IT-management perspective, from a practical point of view. We continued on the bottom-up analysis from the reversed GQM paradigm to select questions and criteria with key practices. Each criterion was examined and evaluated for similarities with each other. Here we have grouped the criteria in six attributes, where each attribute can be seen as a subject or managerial and practical aspects of process maturity, related to business problems rather than to regulations. See *Figure 8*. Wahlgren, Fedotova, Musaeva, and Kowalski (2016); Wahlgren and Kowalski (2016) conducted a similar approach of using attributes in the creation of a maturity model for measuring escalation capability of IT-related security incidents in Sweden. Nuñez et al. (2016) use attributes to group aspects of accountability.

The six attributes are built from groups of criteria:

1. **Roles and responsibilities** deal with management involvement, accountability and ownership; supporting resources; and ongoing monitoring. In this attribute one can determine whether management gives privacy issues sufficient resourses and mandate, excluding the Data Protection Officer.
2. **Governance and compliance** are concerned with privacy policy; consistency of commitments; regulatory aspects and governance, compliance review; and noncompliance. This attribute is concerned with the existence of, how the process of rules is governed, how they are made purposeful and updated.
3. **Education and competence** are addressing privacy education and awareness of employees; and establishes qualifications for personnel responsible for protecting personal data.
4. **Processes and tools** cover communication to individuals such as provision of notice; automation; third party audits; data processing amendments; subject access requests; and retention of personal information.
5. **Risk and classification** cover risk assessment; personal information identification and classification; and Data Protection Impact Assessments

(DPIA)[5]. This attribute is addressing the proactiveness of the organisation's privacy processes to determine what to prioritise and which protective measures are appropriate for personal data.

6. **Incident and information security management** is concerned with incident and breach management; Information security program; Logical Access Controls; Portable Media; and testing security safeguards. Security for privacy and especially information security can cover a lot more, but these are a selection, where the sheer existence of an information security program is covered and testing the efficiency of the program. The control of logical access to information is included as well, since this will uncover potential incidents. Unauthorised access accounts for 23 percent of the type of personal data breaches reported to the Swedish Data Protection Authority (DPA) (Datainspektionen, 2019a). Also, portable devises are in scope here, since lost devices (portable computers, tablets and mobile phones) are included in the cause behind 14 percent of the personal data breaches reported to the Swedish DPA (Datainspektionen, 2019a).

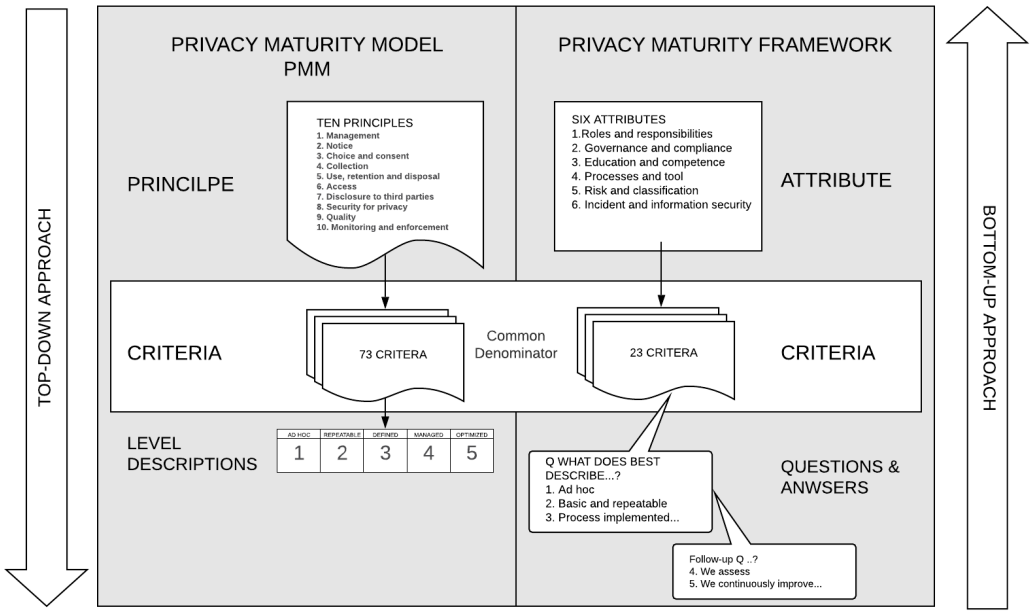

Figure 8 Comparison between the PMM and the Privacy maturity framework.

A comparison between the PMM and the Privacy maturity framework is in order. The former is comprehensive and include a lot more than needed in a municipal context. It would most likely also not be possible to use for a nation-wide survey of maturity, because attrition would make a lot of respondents drop out. The latter is more simplistic, and details are lost, but these details are outside the municipality context. Still, it is a framework to find out if key practices are present or not; and point towards a state of privacy practices maturity in a municipality context. If the

[5] *Konsekvensbedömning*

PMM can be used to determine an exhaustive representation of privacy maturity generally, then the Privacy maturity framework can be used to exhibit a perception of privacy maturity and point in the right direction in a municipality context.

In the new questionnaire, two questions are added as independent variables; (1) the size of the municipality; (2) and in which public sector area they represent.

1. The size of the municipality used a simplification of the Swedish Association of Local Authorities and Regions (SKL) classification of municipalities (SKL, 2017). It is the standard way to define municipalities in public statistics. However, the classification designates three groups of municipalities, including nine types. The classification includes five types of municipalities that not defined by size but instead defines them as a municipality with commuting distance from a city, medium-sized town or small town. We only used numerical values for both inhabitants in the municipality and inhabitants in the largest urban area[6]:
   - At least 200000 inhabitants and at least 200000 inhabitants in the urban centre
   - At least 50000 inhabitants and at least 40000 inhabitants in the urban centre
   - At least 15000 inhabitants and at least 15000 inhabitants in the urban centre
   - Less than 15000 inhabitants in the urban centre

2. We have also added a multiple-choice question to determine in which public-sector area the controllers work: *In which public sector areas do you work?* An analysis was done to determine if their area contains sensitive personal data. The result of the analysis is presented in *Table 5.* Some areas within a municipality contain a large number of sensitive personal data about citizens, for example social welfare and education (Integritetskommittén, 2016).

   We used two categories for the public-sector areas:
   - Sensitive personal data about citizens
   - Mostly non-sensitive data

[6] We regard it would possibly be too complicated for the respondents to give a correct answer if we would use all nine types of municipalities. However, if we were to identity the municipalities instead of anonymous answers, this question would not be needed. Then again, without anonymity, we would perhaps not get true responses, since some questions could possibly be interpreted as breaking the law.

Table 5
In which public sector areas do you work? (Multiple-choice question)

Response options	Likeliness of sensitive personal data
Management, law, finance, central service and administration	Mostly non-sensitive personal data
Labour market issues	Sensitive personal data about citizens
Childcare and preschool activities	Sensitive personal data about citizens
Municipal company	Mostly non-sensitive personal data
Culture and leisure	Mostly non-sensitive personal data
Environmental and health protection	Mostly non-sensitive personal data
Order and security	Mostly non-sensitive personal data
Building and construction issues	Mostly non-sensitive personal data
Cleaning and waste management	Mostly non-sensitive personal data
Emergency services	Mostly non-sensitive personal data
City and environmental planning	Mostly non-sensitive personal data
Social services	Sensitive personal data about citizens
Education for children and youth	Sensitive personal data about citizens
Water supply and drainage	Mostly non-sensitive personal data
Adult education	Sensitive personal data about citizens
Health care and care of the elderly and the disabled	Sensitive personal data about citizens

3.6 Pilot on the second questionnaire

We performed a second pilot on the reduced questionnaire, where the number of questions was a minimum of 30 and maximum of 56. We extended the test into two groups. The first group was the same eight practitioners as in the first pilot from one municipality. In addition, we included seven Data protection officers (DPOs) from other municipalities and one DPO from a municipal company. The questionnaire was open for one week between April 23rd and 30th 2019. In total, 16 testers yielded 11 completed survey responses.

During a meeting, we held a feedback-session with the practitioners from one municipality. They gave a positive response in feedback to the second questionnaire and said it was easy to understand and answer the questions. The group of DPOs sent their input via e-mail and on comments in the survey. Our intention was not to use the framework for examining the maturity of the DPO, but rather their counterpart, the controllers. The questions are not formulated to address the DPO. There were some comments. One example of this is: “Based on the role of DPO, many of the questions are difficult to answer.”. The feedback from both groups group led to minor adjustments to the questionnaire. Questions were shortened further and simplified.

3.7 Analysis template

We created an analysis template with the final scoring of the assessment questions. The complete set of questions and the analysis template is provided in *Appendix 3 – Questions, responses and analysis template.* The template is used to score the answers into maturity ratings following the answers in a submitted questionnaire top-down. The score is rated on the criteria level. Initially, on each criterion, the value in the maturity column estimates a score from the selected answer. If a respondent has answered a follow-up question, the level can be raised further, as described below. A rating cannot be lowered. Each of the 23 GAPP-criteria in the framework has a representation of all levels 1–5, as described above. The scoring analysis template holds the documentation for all scores. The logic in the template includes one normal case and four special cases

The way of scoring in the normal case:

- One filter question contains a possibility to score levels 1-3
- A follow up question contains a possibility to score level 4
- A second follow-up question contains a possibility to score level 5

  See the example of the normal case in the 6.2.2 criterion above in *Figure 6* in the section *Questionnaire construction*.

The way of scoring in four special cases:

1. *Redundancy cases*. The case is that follow up questions are missing. Then either level 4 and 5 or only level 5 are scored on another question. This affects 9 criteria. An example of this case is shown in *Figure 7* above in the section *Scope reduction.*

2. *Multiple answers needed cases*. This is the case in some follow-up questions for level 4 and 5, where the PMM required several practices in a level description. The answers in the follow-up question reflect this and is a multiple-select. This affects 7 criteria.
   Question 27 is an example of *Multiple answers needed* (criterion 1.2.10 for rating levels 4-5):

Question:	Select the descriptions that best match the education program regarding data protection and privacy issues:
Answers (multiple select):	❑ E-training is used for new employees and at least annually for all employees. ❑ The courses that the employees have undergone are documented and can occur in performance reviews ❑ The education program is periodically evaluated to cover changes in regulations and legislation.

- ❑ A strong culture of data protection exists. When incidents occur, renewed training and information campaigns take place.
- ❑ Other, please specify: _____

In this case, both first and second answer are checked this scores level 4 and if also third and fourth answers are checked this scores level 5. The answer "Other, please specify:" does not affect the score.

Another variant of *Multiple answers needed* is that two of three answers are needed, to get a level score or that all answers are needed to level score. This reflects that some level descriptions were similar in both the level 4 and 5 of the PMM. Then an answer could be interpreted as both 4 and 5. To solve this we added the scoring cases *2 of 3, 3 of 3 and 10 of 10,* This affects 3 criteria.

Question 32 is an example of the variant of *Multiple answers needed* (criterion 5.2.2 for rating levels 4-5):

Question:	Choose from the descriptions about verifying the retention of personal data in a correct way:
Answers (multiple select):	❑ Verification that the retention is in accordance with the document management plan takes place automatically. ❑ Personal data retention is regularly reviewed in a suitability assessment. ❑ Changes or deviations are monitored, and the process is updated as a result. ❑ Other, please specify: _____

In this case, if *2 of 3* answers are checked these scores level 4 and if *3 of 3* answers are checked these scores level 5. The answer "Other, please specify:" does not affect the score.

3. *All levels in one question cases*. In two criteria either four (level 2-5) or all five levels (levels 1-5) are represented within one question. This is described above in *Questionnaire construction* regarding question 21 (criterion 1.2.8) and 29 (Criterion 2.2.1). The latter is also an example of special case 2, *Multiple answers needed.*

4. *Control questions*. There are two control questions which is not giving a score at all. Also, the first three questions (1-3) on independent variable do not rate score.

The maturity level does not explain whether the municipalities are following legal requirements. If this was the case, possibly many respondents would not answer truthfully. No one wants to admit they are breaking the law. Even if a respondent answers negatively to a question or the actual process is, in reality, is non-existent. The lowest level is still level 1, *ad hoc* or *at the starting point*. One might argue that a "don't know" answer is not valid for setting a maturity score of ad hoc,

because someone else in the same municipality has a piece of better knowledge. But then the potential practice cannot be common knowledge within that municipality and can then be interpreted as a sign of low maturity. Also, for reasons of completeness, all 23 criteria need a score. Otherwise, the comparison between categories would have different samples. The logical way is to purpose, if they don't know, they are at the starting point, so then they get the lowest score.

The consequences for some criteria not having "full" coverage in one single criterion for levels 4-5, is that the maturity assessments can differ from what the PMM has prescribed in the level descriptions. This, in turn, could suggest that the measuring of maturity is incomplete. However, the creation of the analysis template and scoring method in the special cases was interpreted with a lens of the general levels' descriptions in GAPP and CMM, see *Figure 1* framework CMM 1.1 with five levels (Paulk et al., 1993) described in chapter 2, section *2.5 Maturity models.* This included the detail estimation on responses available of how we could use a special case (or combination of cases) for scoring, if we consider the general description for levels 4-5.

AICPA/CICA (2011b) describes the maturity levels 4 and 5 in general as:

4. Managed – reviews are conducted to assess the effectiveness of the controls in place.

5. Optimized – regular review and feedback are used to ensure continuous improvement towards optimization of the given process.

4 Application of the privacy maturity framework

In the study, an inductive approach is used with a starting point in a search for a pattern or empirically based conclusions (Patel & Davidson, 2011). Our reasoning for studying municipalities' privacy maturity with a framework, which is based on an adapted best-practice standard, is to be useful in a quantitative study for nation-wide comparison and generalisation. The approach is open-ended, bottom-up and subjective, but at the same time descriptive and with an exploratory data analysis. We use both theory, research on the current state, prerequisites such as laws and standards involved; and data collection of empirical evidence in a search for new knowledge. Case studies and using semi-structured open-end questions could be useful for using an inductive approach, but they are prone to being ungeneralizable (Bryman, 2016). A statistics-based generalisation of the results is possible with a quantitative method (Patel & Davidson, 2011). Therefore, we use a quantitative survey using a questionnaire to the target population of municipal data protection controllers.

4.1 Research context

The units of interest for this study are the municipalities in Sweden. Data protection responsibility within the municipalities lies on the municipal councils as legal entities. In each municipality, there are several councils, in some large cities, even 10-50 councils. A council consists of politicians, but the concept of the controller encompasses, in reality, the organisation. For example, the social welfare board as a controller in a municipality includes administrative staff at the administration offices. Politicians might not have a detailed knowledge of the management processes required to answer the questionnaire. Consequently, there was a need to address the administrative staff at the administration offices that could answer for the account of the personal data controller.

GDPR requires public authorities to designate a data protection officer (DPO) and report to the data protection authority (DPA) (European Parliament, 2016). The role of the DPO is to monitor the organisation's compliance with the GDPR. The DPO is an independent function to audit, educate and advise controllers, similar to public auditors. However, the DPOs are not responsible for how controllers in municipalities are handling the issue of privacy management. DPOs regards controllers as the counterpart (Brezniceanu, 2017). A DPO can be an external part. Also, as a group of controllers from different public authorities can share one DPO.

The DPOs are not the target for the survey since DPOs do not possess detailed knowledge with the management practices of the controller. The controllers are the target of the study.

4.2 Data collection

Since the interest is in controllers, we contacted the Swedish DPA (Datainspektionen) and requested them to disclose the contact information, including names and e-mail addresses to the controllers within municipalities and their DPOs. Datainspektionen sent us a complete list, extracted on February 15th, 2019, of all notifications of data protection officers from controllers in Sweden. The list we received was in printed format and contained controllers with their DPOs. After OCR-scanning and then filtering the respondent list based on e-mail address validation, the database consisted of a list of 1987 controllers in municipalities, which made out the respondents of the survey.

The list of respondents contains some oddities that were not detected when the list was being processed. These problems were not discovered until after the invitations of the survey had been sent out. Since the list was expected to contain only the current DPOs and controllers, there was no suspicion of the existence of duplicates, which is the reason why no duplication check was performed. However, the list from Datainspektionen do not contain only the current registered DPOs and controllers, but also contact data for former DPOs. We identified 131 duplicates. We also noted that eight of the recipients are councils shared by a group of two to four municipalities, which is no result of an error, but it might be worth noting.

In order to use the answer to a specific question for drawing general conclusions about the state in the population from which the sample is selected, a certain confidence level is needed. For example, a confidence level of 95 percent would mean that, if the survey would be repeated 100 times, it is expected that in 95 of the cases the unknown true value would be within the limits of the confidence interval. Also, in 5 of the cases, the true value would be expected not to be within the confidence interval (Körner, 1996). The confidence level and confidence interval are normally be calculated per variable after the completion of a survey. However, to get an idea of how many respondents would be needed in order to possibly obtain a specific confidence level, Cochran (1977) provides methods to calculate the needed sample size to reach the desired confidence level and a desired margin of error. As an example, to obtain a confidence level of 95 percent and a margin of error of 5 percent for a dichotomous variable and assuming the population to be 1987 in total, a sample of 323 respondents is needed. However, taking into account the 131 duplicates and assuming the population to be 1856, the minimal number of respondents would instead be 319 respondents, which is only four respondents less. Consequently, this uncertainty of the exact population size will only to a limited extent change the number of respondents needed to have confidence in the results.

Finally, it is worth repeating that this calculations was done only to estimate the number of respondents needed, and that it was done for an example variable just to get an idea of the needed sample size and that each variable would have its own confidence level and margin of error, after the completion of the survey.

4.3 Web survey

The tool selected to collect the data is a web questionnaire tool. One of the reasons for the choice is the control it gives over the respondent's flow through the survey (Persson et al., 2016). For example, the questions that do not apply to a respondent may be hidden with the usage of filter questions. That is, when a certain question is answered in a specific way it opens up for an additional question that is only relevant if the first question is answered in a specific way. Another reason for why a web tool it useful is the expected easiness in which it could export data directly in digital format which would facilitate further processing.

Survey tools may offer a way to develop and maintain the questions within the survey platform. However, a decision was made to manage the questions and response alternatives outside the survey platform to gain control over the access to the material, which for instance, would facilitate the creation of question handouts to interested parties after the survey.

4.4 Deploy survey

The survey was conducted between May 2nd and 13th 2019. First, it was planned to be open for ten days. A reminder was sent out after five days. In order to make it possible for the respondents to have an extra chance to answer the survey after the weekend, the closure was postponed until May 13th, and a second message was sent out as a reminder.

When the survey was deployed, a total of 1987 respondents were invited with an email containing a unique and individual link to the survey. A setting in the survey platform allowed us to not connect the respondents with the corresponding submitted answers, so the respondents are anonymous for us. The final number of submitted completed surveys is 454. Additionally, 274 respondents have completed a part of the survey. The response rate is 22,85 percent for the submitted surveys. With an actual number of 454 respondents, the earlier estimated minimum number of 323 respondents is reached with a margin of 131 respondents.

4.5 Analysis

The survey tool provides functionality for exporting data files for both submitted survey forms and unsubmitted surveys. However, we decided not to use the data from the partly-answered surveys in the data analysis. Using not completed surveys will possibly create a low maturity on questions not answered and thereby contribute to a misleading result for these respondents and also would have an impact on the overall results of the survey.

A small number of the 454 respondents that submitted the survey, skipped some questions. In total, out of the 52 questions used for calculating maturity, 20 questions do not have any partial dropout at all. For the single selection questions, mostly rating levels 1-3, nine questions have 1 dropout, four questions have 2, eight questions have 4, two questions have 5, and 1 question have 8 dropouts. Six multiple-choice scoring mostly levels 4-5 questions have 5, 6, 11, 12, 13 and 14 dropouts respectively. In total, we conclude that the partial dropouts are irregular and of a minimal amount, compared to the total answers. A common reason is that the respondent clicked on and missed the question (Persson et al., 2016). Given the fact that these respondents continued with the other questions and finally submitted the survey, it does not seem likely that the partial dropout was caused by attrition. We decided to interpret the non-responses as an irregularity and used imputation to substitute the value for the missing data (Little & Rubin, 1987). In the cases where this occurred for an initial filter question, the level is interpreted as level 1, ad hoc. A skipped question does not add to the possibility of advancing maturity. Therefore, a respondent does not gain any extra level but keep the achieved maturity level for a skipped question.

After the closure of the survey, the data of the submitted surveys were exported from the online survey tool in a semi-colon separated text file. This data file was formatted with the questions in the first row as a header line, with the answers from one respondent per subsequent row. Statistical Package for the Social Sciences (SPSS) is a software tool to analyse statistical data. However, we estimated the amount of work was too high to get SPSS to calculate the maturity levels based on the answers from several questions. Instead, there was a need for either manual coding of the results into maturity levels or the use of a separate tool for the calculation of the maturity levels. Also, the complexity of the calculation of maturity levels based on the respondents' alternative paths determined by their answers to filter questions and supplementary questions, required us to use a separate tool.

Therefore, a Python script was developed for the purposes of calculating maturity levels and formatting the data to easier fit into SPSS. For example, to make the analysis tool accept multiple selection answers, the selected alternatives has to be extracted from one field and spread out to a separate field for every possible

alternative. The script works through the semicolon separated file, a row per row, as each row contained the answers of one respondent. For every criterion, the data fields containing the answers to the questions belonging to that criterion are analysed in order. For each question, the given answer is compared with the known set of alternatives and given a level according to the assessment rules of the framework. The level is then recorded by the script into a new variable containing the achieved level for that criterion. After the maturity of all criteria is calculated and stored in separate variables, one for each criterion, mean values for the attributes are calculated based on the criteria values of each attribute. Also, a mean value is calculated based on all criteria and stored in a separate variable. The script stores existing variables into a new semi-colon separated file, enriched with variables of calculated maturity levels.

The work with the script was an iterative process. One of the authors took the role as a programmer and the other as a tester. The tester selected samples of the responses and then used the analysis template manually to score maturity[7]. Acceptance sampling was chosen randomly from the 454 submitted questionnaires. We then compared the results of the manual control with the results of the script. The programmer made corrections to the script into a new version. The work lasted several iterations, during which feedback was exchanged to improve the code. After the final iteration, the Python script contained around 1200 lines of code.

After the pre-processing step, the data set contained maturity levels for all the 23 criteria, mean values for the criteria within each of the attributes, a mean value for all criteria, as well as responses from the respondents. The data set was imported into SPSS, where the variables of the categorical level intended as independent variables within the data analysis were completed with labels. In SPSS it is possible to assign labels to the variable names and variable values in order to make the output from analysis more comprehensible. Variables treated like so are the grouping variables for municipality size, DPO/non-DPO and the variable for Category of sensitive data.

Stevens (1946) presents four different scale levels of data: nominal, ordinal, interval and ratio, where a variable having a ratio scale permits the full set of statistical analysis methods while a variable with a nominal scale permits a minimal set of statistical methods. Kremelberg (2011) and other text books for statistic method might refer to nominal scale as categorical variables and interval or ratio as continuous variables. Variants of the nomenclature obviously also exist in statistical software as SPSS.

The criteria variables have an ordinal scale from 1 to 5 with the corresponding names *Initial, Repeatable, Defined, Managed and Optimized*. In an ordinal scale,

[7] See *Appendix 3 – Questions, responses and analysis template*

one value must be assigned to one category, but for a group of values, it makes sense to use means and variance to compare the result with other groups. Thus, a group value can be in-between two levels. A median value, which is the prescribed alternative to mean values for use with ordinal data, would not indicate a group of values being in-between. Stevens (1946) point out that in its strictest use, arithmetic calculations, such as means, variance and standard deviations should not be used based on ordinal data. Though, it is not forbidden and furthermore he states that *"…On the other hand, for this 'illegal' statisticizing there can be invoked a kind of pragmatic sanction: In numerous instances it leads to fruitful results"* (Stevens, 1946). Briand, Emam, and Morasca (1996) presents a pragmatic approach in the application of measurement theory, brought forward by the debate about the restrictive use of measurement theory after Stevens article (Briand et al., 1996). For the past 30 years the use of mean-based statistics to categorize actual measurements in a useful way is not controversial, but rather a choice (Zumbo & Kroc, 2019). Consequently, a pragmatic approach towards the level of data was applied and mean values of the criteria variables' values were calculated in accordance with that pragmatism.

Analysis of variance (ANOVA), is a statistical method that is using the means of a dependent variable to compare differences between two groups or more in an independent variable. It is used for finding out whether statistical significance exists in the differences between these groups. The independent variable, containing the groups is a categoric variable, while the depending variable is a continuous variable (Kremelberg, 2011). Gaito (1980) however, states that in contrary to what is suggested in many statistic text books, statistical procedures do not require specific scales in order to be used. He also explicitly points out that the assumptions of ANOVA don't include assumptions about a specific scale and that the choice of scale has little impact on the significances found with ANOVA-tests. Norman (2010) also argues that ordinal scale variables could be used and that in fact, the risk of coming to a wrong conclusion is very small for robust parametric methods, such as ANOVA. Also, the robustness of ANOVA makes it forgiving regarding violations of assumptions about sample size, normal distribution. Briand et al. (1996) debate against a dogmatic selection of analysis methods based on variable scales. In fact, they indicate that measurement scales should not be used to proscribe statistical methods, but instead, common sense and a pragmatic approach should be used (Briand et al., 1996). Considering these arguments, ANOVA is estimated as suitable for analysing the differences between the grouping variables for *municipality size*, *DPO/non-DPO* and the variable for *Category of sensitive data*. In other word, three analyses are performed with ANOVA. In the first set of ANOVA-tests, attribute mean values are compared between multiple categories of municipalities with different sizes. In the second set of ANOVA-test each criterion is compared between the two groups of DPOs and non-DPOs. Finally, in the third

set of ANOVA-tests, each criterion is compared between the two groups of respondents from areas with high volume of sensitive data, and other respondents.

When there are more than two groups in an ANOVA test, the test can only reveal significances in the general difference between the groups. An additional test is therefore needed to compare every group with all the other groups after the execution of the first test in order to find out whether there are significances between the specific groups. Such tests are called post hoc test, of which there are some to choose from. However, the Games-Howell test might be used even though the variances in the groups do not equal (Kremelberg, 2011). Consequently, Games-Howell post hoc tests were used for the comparison of maturity levels between categories of different sizes of municipalities.

A specific notation is used to describe the results of an ANOVA test. An example of this notation might be: $F(1, 452) = 5{,}177$, $p<0{,}05$. In this notation, the "*F"* represents the *F* statistic or *F*-test, which is used in ANOVA to decide whether there is a significance in the results. Within parenthesis is the degrees of range, based on the number of compared groups and the sample size. Finally, the "*p"* indicates the probability level of the found significance. (Kremelberg, 2011)

Apart from the statistical analysis, extraction of descriptive statistics, such as confidence intervals, cross reference tables, and frequencies was also performed in SPSS.

5 Results of the survey

In total 454 out of 1987 respondents completed and submitted the survey. The confidence level is at 95%. The response rate is 22,85 percent for the submitted surveys. The results are shown as tables and diagrams showing the criteria grouped into the six attributes. The diagrams are shown with the value of maturity based on the analysis. The aggregated general mean is 2,013 on a scale from 1 to 5. Almost at level 2 of maturity indicates that the controllers are in a defined and repeatable state. Routines and processes exist. However, these are not fully implemented. Most of the controllers score in the area round level 2 and only a few have reached above level 3, see Table 6 and Figure *9*. Only two controllers are above level 4.

Table 6
Swedish municipal controllers in privacy maturity levels by criteria

Controllers	Number	Percentage (n = 454)
Below level 2	238	52%
Between 2-3	198	44%
Above level 3	18	4%

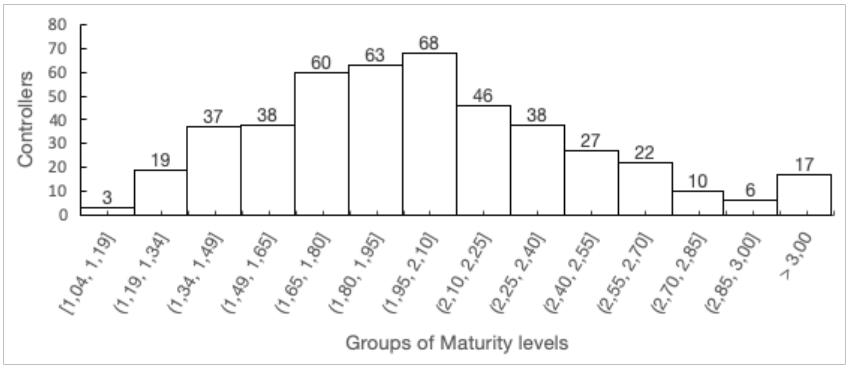

Figure 9 Histogram with the number of controllers by maturity levels

Breaking down the results, still on a general level, into the attribute-level and then the criteria level, reveals the maturity level for the six attributes and more detailed into each criterion. See the combined general results of the attributes and criteria in Table *7*. and a comparison of how many controllers are rated at each maturity level, sorted by level 1 in *Figure 10*.

Table 7
Privacy maturity in Swedish municipalities by attributes and by criteria

Attributes and criteria (n = 454)		Mean	SD[9]	SE[10]	95% Confidence interval[8] Lower bound	95% Confidence interval[8] Upper bound
Roles and responsibilities		**1,993**	**0,670**	**0,031**	**1,932**	**2,055**
1.1.2	Responsibility and accountability for policies	2,256	0,801	0,038	2,182	2,329
1.2.8	Supporting resources	2,441	1,252	0,059	2,325	2,556
10.2.5	Ongoing monitoring	1,284	0,617	0,029	1,227	1,341
Governance and compliance		**1,920**	**0,627**	**0,029**	**1,862**	**1,978**
1.1.0	Privacy policies	2,782	0,958	0,045	2,694	2,870
1.2.2	Consistency of privacy policies and procedures with laws and regulations	1,795	1,005	0,047	1,702	1,888
1.2.5	Consistency of commitments with privacy policies and procedures	1,681	0,632	0,030	1,622	1,739
10.2.3	Compliance review	1,632	0,994	0,047	1,540	1,724
10.2.4	Instances of noncompliance	1,709	1,089	0,051	1,609	1,810
Education and competence		**1,796**	**0,776**	**0,036**	**1,725**	**1,868**
1.2.9	Qualifications of internal personnel	1,888	1,039	0,049	1,792	1,984
1.2.10	Privacy awareness and training	1,705	0,936	0,044	1,619	1,791
Processes and tools		**2,378**	**0,671**	**0,032**	**2,316**	**2,440**
2.2.1	Provision of notice	2,119	0,709	0,033	2,054	2,184
5.2.2	Retention of personal information	2,725	1,180	0,055	2,616	2,833
6.2.1	Access by individuals to their personal information	2,304	1,218	0,057	2,192	2,416
6.2.2	Confirmation of an Individual's Identity	2,339	1,209	0,057	2,228	2,451
7.2.2	Protection of personal information	2,403	1,193	0,056	2,293	2,513
Risk and classification		**1,941**	**0,711**	**0,033**	**1,875**	**2,006**
1.2.3	Personal information identification and classification	1,731	0,736	0,035	1,663	1,799
1.2.4	Risk assessment	2,218	1,237	0,058	2,104	2,332
1.2.6	Infrastructure and systems management	1,872	0,897	0,042	1,790	1,955
Incident and information security management		**1,881**	**0,543**	**0,025**	**1,831**	**1,932**
1.2.7	Privacy incident and breach management	2,110	0,986	0,046	2,019	2,201
8.2.1	Information security program	2,531	0,893	0,042	2,448	2,613
8.2.2	Logical access controls	1,535	0,750	0,035	1,466	1,604
8.2.6	Personal information on portable media	1,872	1,082	0,051	1,772	1,972
8.2.7	Testing Security Safeguards	1,359	0,833	0,039	1,282	1,436
Average by criteria		**2,013**	**0,491**	**0,023**	**1,967**	**2,058**

[8] A 95 % confidence that the true mean value for the population would be found within the interval spanning from the lower bound to the upper bound.
[9] Standard Deviation
[10] Standard Error is measuring the accuracy with which the sample represents the population. Here it is expressed as a decimal value, e.g. 0,023, but it can also be shown as a percentage, e.g. 2,3%.

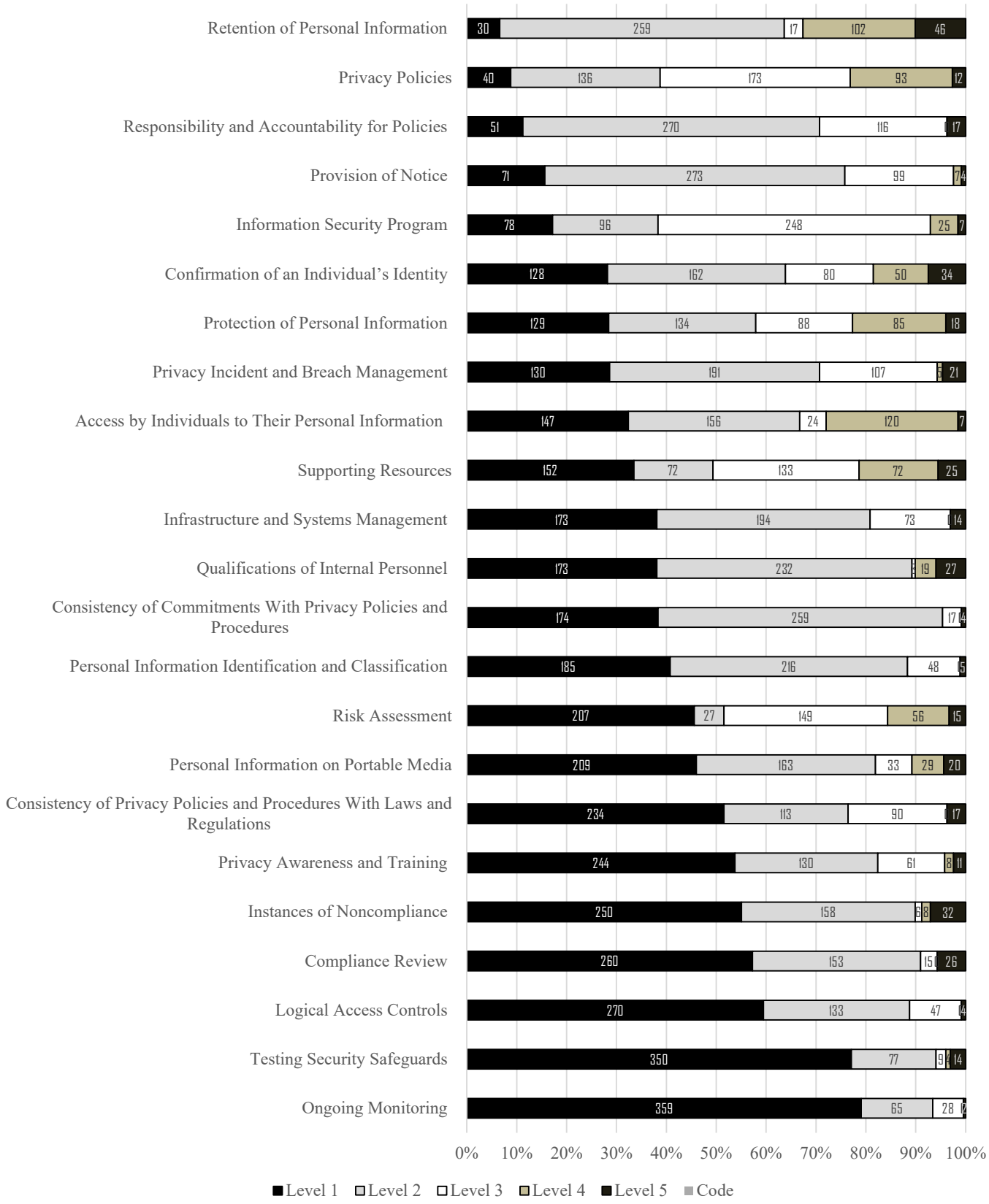

Figure 10 Number of controllers by criteria and sorted by level 1 (n = 454).

Size of municipality is used for comparison between the different categories of municipality size. See the maturity result by size in Table 8.

Table 8
Privacy maturity in Swedish municipalities by size and attributes

Attribute	< 15000 [11]	15000-49999 [12]	50000-199999 [13]	≥ 200000 [14]
Roles and responsibilities	1,869	2,024	2,151	2,032
Governance and compliance	1,835	1,894	2,075	1,987
Education and competence	1,699	1,790	1,967	1,758
Processes and tools	2,141	2,500	2,728	2,090
Risk and classification	1,772	1,989	2,116	2,065
Incident and information security management	1,807	1,827	2,081	1,832

Within the roles and responsibilities attribute, there is significance for a general difference in maturity between municipalities of different sizes, $F(4, 448) = 3{,}234$, $p < 0{,}05$. And specifically, the large municipalities (50 000-199 000 inhabitants) have higher maturity than the smallest municipalities (< 15 000 inhabitants), $p < 0{,}01$.

Within the governance and compliance, there is also a significance in the difference generally between municipalities of different sizes, $F(4, 448) = 2{,}655$, $p < 0{,}05$, and the large municipalities have higher maturity than the smallest, $p < 0{,}05$.

Within the education and competence, there is no significance in maturity generally between the groups of municipalities of different size. However, the Games-Howell post hoc test shows significance in the specific difference in maturity levels between large municipalities which have higher maturity levels than the smallest municipalities, $p < 0{,}05$.

For the processes and classification attribute, the significance in the general difference in maturity between different municipality sizes is $F(4, 448) = 17{,}599$, $p < 0{,}01$. Here, the large municipalities have higher maturity levels than the smallest municipalities, $p < 0{,}001$, and also higher than the largest municipalities (≥200 000 inhabitants) $p < 0{,}05$. Also, the small municipalities (15 000-49 999 inhabitants) have a higher maturity than the smallest, $p < 0{,}001$, as well as the largest, $p < 0{,}001$.

[11] Less than 15000 inhabitants in the urban center
[12] At least 15000 inhabitants and with at least 15000 inhabitants in the urban center
[13] At least 50000 inhabitants and with at least 40000 inhabitants in the urban center
[14] At least 200000 inhabitants and with at least 200000 inhabitants in the urban center

There is also a significance for the general difference between different municipality sizes within Risk and classification, $F(4, 448) = 5{,}148$, $p < 0{,}01$. Also, there is a significance in that large municipalities have higher maturity than the smallest municipalities, $p < 0{,}01$.

Finally, within the attribute Incident and information security management, there is a general difference in maturity levels between municipalities of different size, $F(4, 448) = 5{,}081$, $p < 0{,}01$. And specifically, there is a significance in that large municipalities have a higher maturity level than the small, $p < 0{,}01$, and smallest municipalities, $p < 0{,}01$.

Controllers working with sensitive data reveals the following: The category with controllers working with sensitive personal data answer they are more mature than the rest working with mostly non-sensitive personal data. The result of controllers grouped into the categories is shown in Table 9. A correlation is made between these two categories and various criteria and attributes to find significance with maturity levels. Results are presented within the six attributes in *Figure 11*.

Table 9
Controllers with sensitive data based on public service activity

Category of sensitive data	Controllers	Percent (n=454)
Sensitive personal data	161	35%
Mostly non-sensitive personal data	293	65%
Total		100%

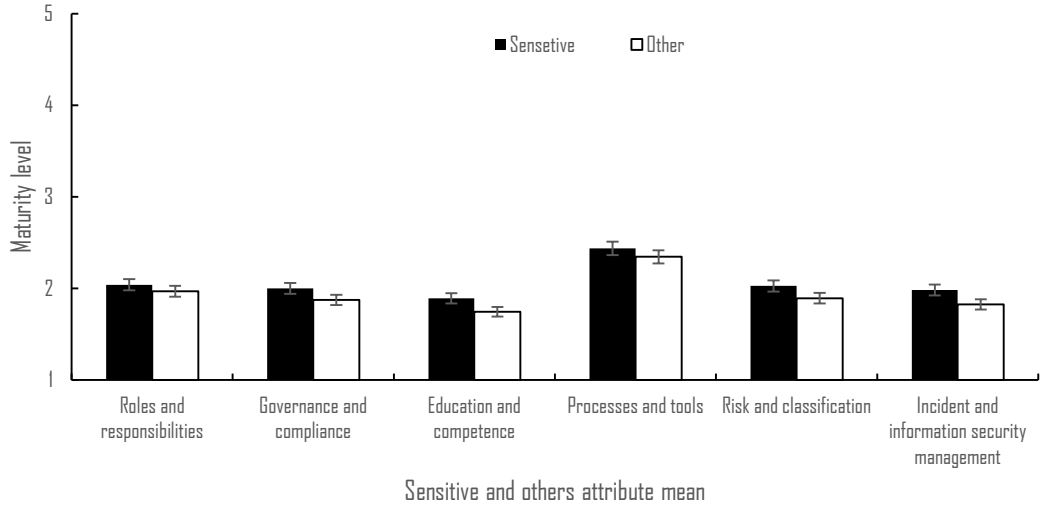

Figure 11 Comparison controllers with sensitive data and others by attribute.

Data protection officers also answered the survey even though the survey was sent to controllers' representatives and not to the DPO. The survey includes an obligatory question: *Are you a Data protection officer?* with just yes/no/other

response options. The results of both the *No* and the *Other*-option are grouped. 25 percent answered *Yes* to the DPO-question, see *Figure 12*. Generally, a functional e-mail address within the administration of the municipality, is the address of the controllers. Some invitations must have been forwarded to the DPOs. This can be seen as a sign of low maturity. However, there is no maturity level based on the DPO-question in the survey. The question is intended for correlation, to find out if DPOs are estimating that their counterpart, the controllers, have higher or lower privacy maturity.

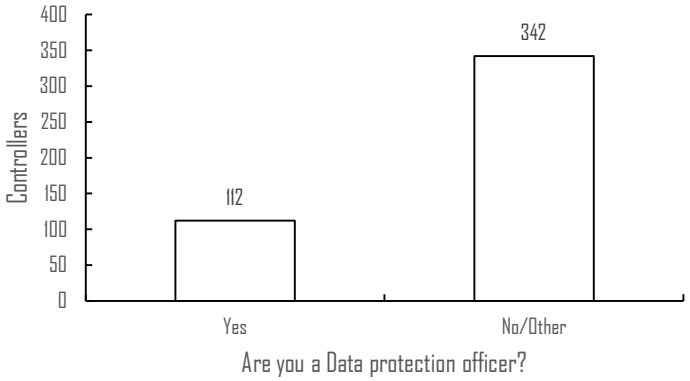

Figure 12 Number of DPOs answering the survey.

DPOs are rating the maturity lower on all attributes, except Education and competence. See

Figure *13*. One possible explanation to the higher rating in the Education and competence attribute is that the DPOs is responsible for privacy training. The differences shown on the attribute level are within the margin of error.

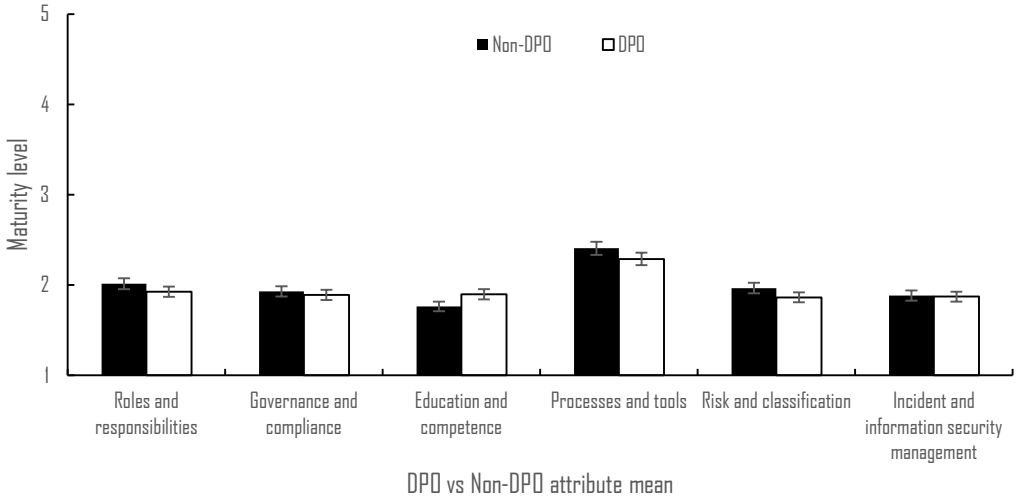

Figure 13 Comparison with DPO and other respondents by attribute.

5.1 Roles and responsibilities

Roles and responsibilities deal with management involvement, accountability and ownership; supporting resources; and ongoing monitoring. The average maturity in the attribute and the criteria within is shown in *Figure 14*.

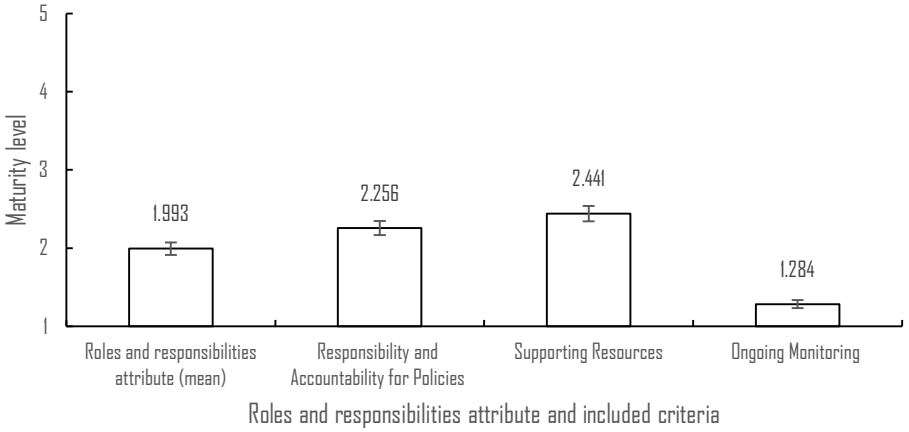

Figure 14 Maturity levels of roles and responsibilities attribute and criteria.

Responsibility and accountability for policies (criterion 1.1.2) point out if there is an appointed responsible and if this person has authority and recourses. 11 percent say they do not have a responsible person or group, except for the DPO; or they answer, "do not know" (Level 1); 59 percent have a responsible person or group, with limited resources and mandate. (level 2); 26 percent say that clearly defined roles and responsibilities exist and a documented process is used to evolve internal regulations (level 3); 0 percent furthermore periodically monitor the compliance (level 4); and top 4 percent above all else, also periodically assess the process to ensure continuous improvements (level 5). An ANOVA-test shows a significance between DPOs and non-DPOs in criterion 1.1.2 Responsibility and accountability for policies, $F(1, 452) = 6{,}486$, $p<0{,}05$ (Mean DPOs: 2,089, standard error: 0,076, Mean non-DPOs: 2,310, standard error: 0,043). DPOs rate the maturity lower than the rest of the respondents.

Supporting resources (criterion 1.2.8) cover the topic of how resources are allocated by the management to implement and support the privacy policies of the organisation, except for the DPO. 35 percent of respondents claim resources are provided on an "as needed" basis to deal with privacy issues (level 1); 16 percent say resources are available, but the work is not supported by privacy specialists (level 2); 29 percent answer that resources are available and empowered with appropriate authority and funding (level 3); 16 percent claim management ensures that adequately qualified resources are available throughout the organisation for

different aspects of privacy (level 4); and finally 6 percent states that management performs yearly a review of the performance of resources (level 5).

Ongoing monitoring (criteria 10.2.5) shows how the organisation is working on improving where necessary, related to an effective risk assessment and is also an accountability issue of taking long-term responsibility. 30 percent of the respondents answer that ongoing monitoring is informal, incomplete and inconsistently applied (level 1); 49 percent say they do not know (also level 1) which makes a total of 79 percent; 14 percent claims measuring is done, but does not cover all aspects (level 2); and 6 percent states they do have implemented documented process for monitored privacy controls, based on a risk assessment (level 3); 0 percent updates policies as a consequence of risk treatment, and perform both internal and external privacy risk reviews. (level 4); 0,4 percent additionally both has a formal evaluation of the efficiency of the risk process and has risk management adapted to various purposes. (level 5).

5.2 Governance and compliance

Governance and compliance are concerned with privacy policy; consistency of commitments; regulatory aspects and governance, compliance review; and noncompliance. The average maturity in the governance and compliance attribute and the criteria within is shown in *Figure 15*

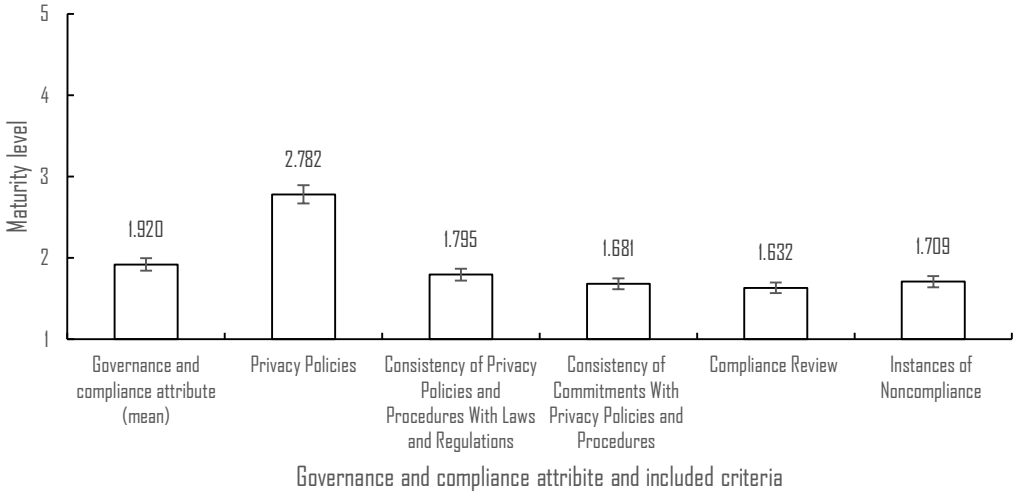

Figure 15 Maturity levels of governance and compliance attribute and criteria.

Several questions cover privacy policies (criterion 1.1.0), and a key filter question is asking if there is an internal regulation covering integrity and data protection, like a privacy policy or other internal governing rules. 9 percent say they do not have an internal regulation covering integrity and data protection, or they do not know (Level 1); 30 percent answer they do have one partly. (level 2); 38 percent answer yes, they do have one (level 3); 21 percent also mark that all 10 GAPP

principles were included in the internal regulation (level 4), and 3 percent also periodically assess the policy creating process to ensure continuous improvement (level 5). The following significance was found: Controllers with sensitive data, estimated higher maturity than other respondents. $F(1, 452) = 5{,}177$, $p<0{,}05$. The mean of maturity of the sensitive data group was 2,919 standard error was 0,069 while the mean of the others was 2.706 and standard error was 0,058.

Consistency of privacy policies and procedures with laws and regulations (criterion 1.2.2) is concerned with aspects of how comparison of internal regulation and the law is made. 52 percent say comparisons are done partly, but may be inconsistent, or do not know (level 1); 25 percent claim they do compare, but no documented guidance is provided (level 2); 20 percent answer a process has been implemented for regular law review and comparisons (level 3); 0 percent furthermore periodically monitor the compliance (level 4); and 4 percent also periodically assess the process to ensure continuous improvements (level 5).

The consistency of commitments with privacy policies and procedures (criterion 1.2.5) are covering review of agreements where data processing agreements are needed. 38 percent state that reviews of contracts for data processing agreements are incomplete, inconsistent or they do not know (level 1); 57 percent answer that a process exists to review contracts and other commitments (level 2); Only 4 percent say they have an established process covering all aspects and do reviews regularly (level 3); in addition, 0 percent periodically monitor the compliance (level 4); and 1 percent also periodically assess the process to ensure continuous improvements (level 5).

Compliance Review (criteria 10.2.3) is central for answering how an organisation works with compliance. How it is addressing long-term maturity and if commitments are managed systematically. 57 percent answer that compliance review is sporadic, informal or they do not know (level 1); 34 percent say compliance review is performed regularly but may not cover all aspects and are not fully documented (level 2); 9 percent have an established process covering all aspects and do reviews regularly (level 3). The follow-up question is used to set levels 4 and 5. It reached by only 0,9 percent of the respondents, and the responses to this question are also used for level 4 and 5 maturity ratings for several other questions. Of the total responses (n=454) 0 percent periodically monitor the compliance (level 4), and including all else, 6 percent also periodically assess the process to ensure continuous improvements (level 5).

Instances of Noncompliance (criteria 10.2.4) deal with deviations of the privacy policies. 55 percent answer that handling of deviations is sporadic, informal or they do not know (level 1); 35 percent say handling of deviations is systematic and regularly occurring but may not be fully documented (level 2); Only 1 percent have an established process covering all aspects, all deviations are fully documented,

including disciplinary actions (level 3); 7 percent periodically assess the process to improve and avoid future instances of noncompliance partly (level 4); and moreover, 1 percent do this completely (level 5).

On the questions 5,7 and 52 in the survey within the Governance and compliance attribute, there are also responses to open questions, which can be added to the attribute in a future version. The comments are in Swedish and here is a translation presented. Some examples from question 5 in criteria 1.1.0 for adding to the list of content of the privacy policy, which now is the list of GAPP-principles, are incident management; e-mail policy; procurement; protected identity; and DPIA. Question 7 is a follow-up question that is shown when someone has a no or do not know to the key filter question in 1.1.0. Here some reasons are given why there are no internal rules, and some example of responses: “We hired a person, starting in September to address this work”; “A management system is under construction.”; and “We don’t have our own rules, but are following the existing regulation”. From question 52, an example is “We follow up the previous work we did before the GDPR”.

5.3 Education and competence

The Education and competence attribute are addressing privacy education and awareness of employees; and establishes qualifications for personnel responsible for protecting personal data. The average maturity in the education and competence attribute and the criteria within is shown in *Figure 16*

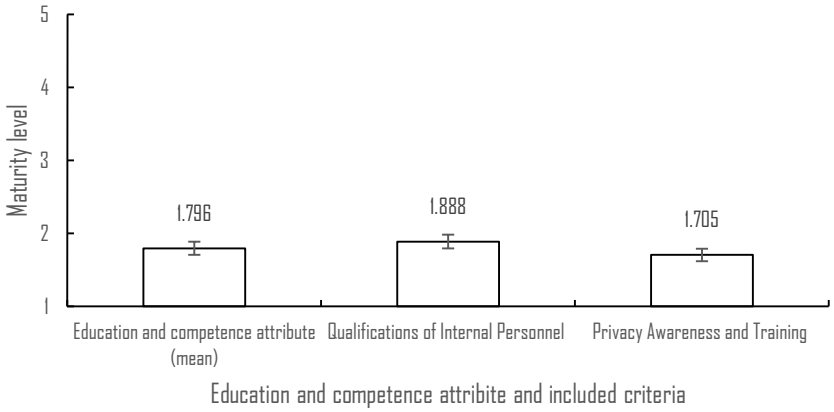

Figure 16 Maturity levels of education and competence attribute and criteria

Qualifications of internal personnel (criterion 1.2.9) are covered in three questions. 39 percent state there are no formal qualifications for personnel or they do not know (level 1); 51 percent say the organisation has some established qualifications for personnel but no documented guidelines (level 2); and 0,7 percent have formal requirements for personnel, have received appropriate training and have the necessary knowledge (level 3); 4 percent state there are specialists of privacy

among the internal personnel (level 4); and 6 percent are providing competence development including privacy certifications (level 5). An interesting significance, $F(1, 452) = 5{,}665$, $p<0{,}05$, is found here, where controllers working in areas with sensitive data say they are more mature for the criteria (with a mean of 2,043; standard error of 0,090) than others within the total group of respondents (with a mean of 1,802; standard error of 0,057).

Privacy Awareness and Training (criterion 1.2.10) deal with awareness and specific training for personnel in general and is covered in three questions. 54 percent state they have never had any privacy training, or they do not know if they had one (level 1); 29 percent say awareness campaigns are done, but sporadic, inconsistent and a training plan is missing (level 2); 14 percent claim a formal training plan exists, is consistent, and meets applicable laws (level 3). 2 percent say learning for new employees with yearly updates and training are used in performance reviews with employees (level 4); and 2 percent have a strong privacy culture and launch an awareness campaign with training after an incident; and training is periodically evaluated to cover changes in both internal regulations as well as legislation (level 5).

5.4 Processes and tools

Processes and tools cover communication to individuals such as provision of notice; automation; third party audits; data processing amendments; subject access requests; and retention of personal information. The average maturity in the processes and tools attribute and the criteria within is shown in *Figure 17*.

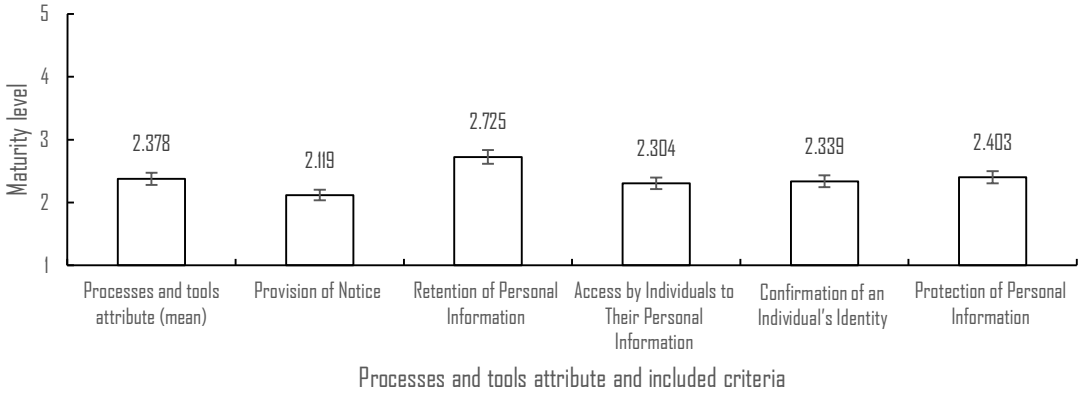

Figure 17 Maturity levels of processes and tools attribute and criteria.

Provision of notice (criterion 2.2.1) deals with how information about the processing of personal data is given to the individual by the organisation. 16 percent answer the notice is not available, only given sporadic or they do not know (level 1); 60 percent say there is a general notice provided on the web or by another means (level 2); 22 percent also inform in a timely fashion for any changes or new

purposes (level 3); 2 percent furthermore trace the communication and know, at any given time, what information was given (level 4). On top of all other options, 1 percent have integrated the information into services, in line with the Privacy by Design framework, and have an established process for improvements (level 5).

Retention of personal information (criterion 5.2.2) reflects on how data is retained by the organisation, focussing on the use limitation principle in GDPR (European Parliament, 2016), requiring that data is not retained longer than necessary to fulfil the purposes unless a law or regulation specifically requires otherwise. In Swedish municipalities, a retention plan is referred to as a document management plan. 7 percent answer a valid document management plan is not available, is used sporadic or they do not know (level 1); 57 percent say a document management plan exists but is not entirely implemented (level 2); 4 percent answer additionally that there is a document management plan that covers processes and routines and that it is in accordance with how it works in practice (level 3); 22 percent furthermore periodically review the plan and implement changes when needed (level 4); and 10 percent also have a verification process for retention periods, monitoring deviations and make suitability assessments (level 5). Within this criterion there is significance in the difference in the maturity levels between the respondents from areas with high volume of sensitive data with a mean of 2,882, a standard error of 0,094, and other respondents with a mean value of 2,638, standard error of 0,068. $F(1, 452) = 4{,}469$, $p<0{,}05$.

Access by individuals to their personal information (criterion 6.2.1) covers the management procedures for subject access requests, how they are handled as well as procedures for searching and gathering the personal data. 32 percent answer there is no specific procedure, it is sporadic, or they do not know (level 1); 34 percent say there is a manual process, for example with a simple web form or document (level 2); 5 percent have a documented process covering all aspects of a subject access request, for example via a digital service (level 3); 26 percent furthermore report a process to search and compile personal data is implemented (level 4) 2 percent additionally deliver an automated self-service technical system handling subject access requests (level 5).

Confirmation of an individual's identity (criterion 6.2.3) focuses on how the organisation have designed procedures for verifying the identity of individuals sending in subject access requests. 28 percent answer the identification is informal, sporadic or they do not know (level 1); 35 percent claim a method is in place, but not wholly documented (level 2); 18 percent report they consistently use a secure identification process (level 3); 11 percent of furthermore have traceability of the identification verification process (level 4); and on top 7 percent also monitor and periodically assess the process (level 5).

Protection of personal information (criterion 7.2.2) covers the combined topic of instructions (in the data processing agreement) to third-party and monitoring compliance with the instructions. 28 percent answer the handling is ad hoc, with no specific routines to evaluate the effectiveness of third-party controls to protect personal data, or they do not know (level 1); 30 percent say routines exist to ensure correct agreement with a reasonable assessment of the third-party protection, but processes are not fully implemented. (level 2); 19 percent say there is a documented process for managing the data processing agreement that includes specific instructions and requirements (level 3); 19 percent furthermore periodically monitor and assess the process (level 4); and, over and above, 4 percent also monitor and evaluate the third-party environment to ensure continuous requirement compliance (level 5). There is significance in the results indicating that DPOs give answers that lead to lower maturity level compared to non-DPOs, of the criterion 7.2.2, Protection of personal information, $F(1, 452) = 7{,}165$, $p<0{,}01$. The mean of the DPOs is 2.143 and the standard error is 0,112, whereas the mean of the other group is 2.488 and standard error is 0,064.

To the questions, 29,32 and 40 in the survey within the processes and tools attribute there are also responses as open questions, which can be added to the attribute in a future version. The comments are in Swedish and here is a translation presented. Some examples are on retention (5.2.2): “No regular control is done, but we actively handle deviations when they appear.” and “It is done when updating the archive, or when a co-worker have opinions on how it is done”. Both of these comments are reactive approaches. Also, on the concept of instructions (7.2.2) a DPO is commenting “The authorities usually send me, as a DPO, agreements. Intolerable! This is an area for improvement. The controller must create their own process for this”. Another typical comment is: “Data processing agreements are sent to concerned parties in time, but not everyone has signed them yet”.

5.5 Risk and classification

Risk and classification cover risk assessment; personal information identification and classification; and Data Protection Impact Assessments (DPIA). The average

maturity in the risk and classification attribute and the criteria within are shown in *Figure 18*.

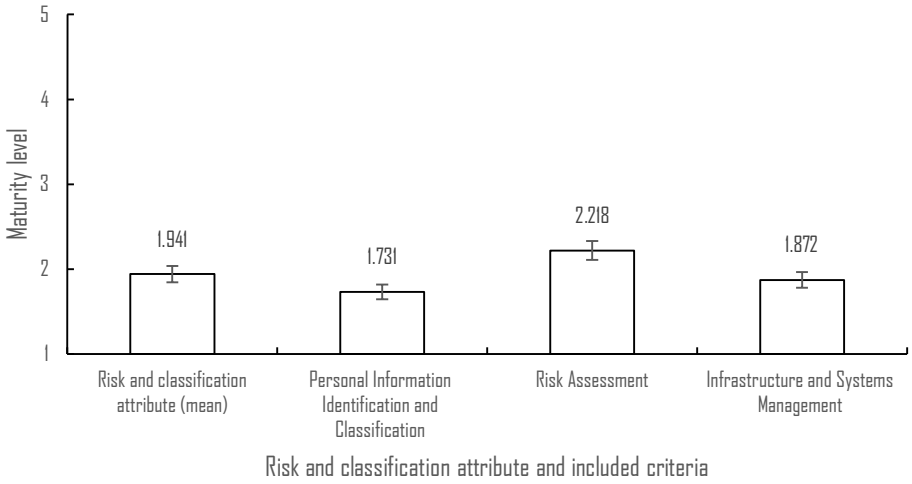

Figure 18 Maturity levels of risk and classification attribute and criteria.

Personal information identification and classification (criterion 1.2.3) focus on management of classifying types of personal information and sensitive personal information at different levels of urgency. 41 percent have not classified the information, the classification is outdated, parts are missing or the do not know (Level 1); 48 percent say a basic classification is done, but with missing risk assessments (level 2); 11 percent report that all processing activities are classified, with risk assessments (level 3); 0 percent furthermore periodically monitor compliance, both internally and with third-parties (level 4); and top 1 percent above all else, also periodically assess the process to ensure continuous improvements (level 5).

Risk assessment (criterion 1.2.4) covers the processes used to identify, assess, and respond to risks regarding personal data. 46 percent do not have a complete process for risk assessment regarding personal information handled by the organisation or the do not know (Level 1); 6 percent state they do have a risk process and that employees are generally aware of privacy risks (level 2); 33 percent report that a formal framework is used and documented, including risk identification, risk assessment and reporting (level 3); 12 percent also update policies as a consequence of risk treatment, and perform both internal and external privacy risk reviews. (level 4); 3 percent additionally say they have both a formal evaluation of the efficiency of the risk process and risk management adapted to various purposes (level 5).

Infrastructure and systems management (criterion 1.2.6) deals with management of DPIA and potential privacy consequences when new or changed services are implemented. The DPIA is a special kind of risk assessment. Article 35 requires it

is compulsory to perform a DPIA if the processing may result in a high risk for the individual (European Parliament, 2016). 38 percent answer DPIA are performed sporadically for new business processes, new systems or they do not know (Level 1); 48 percent preform DPIA for new systems or change to existing systems, but processes are informal and not fully documented (level 2); 16 percent report that formal DPIAs are done in a process, covering both implementation or changes to products, services, businesses and infrastructure. (level 3); 0 percent furthermore periodically monitor the process, both internally and potentially with third-parties (level 4); and top 3 percent above all else, also periodically assess the process to ensure continuous improvements (level 5). A significance is found: Respondents working in areas with sensitive data has higher maturity levels for this criterion compared to all other respondents, $F(1, 452) = 8{,}582$, $p<0{,}05$. 2,037 is the mean maturity level of the sensitive data group (standard error is 0,070) while the mean of the complementary group is 1,782 with a standard error of 0,052.

To the questions 11, 12 and 13 (all criterion 1.2.4) regarding risk assessment in the survey within the *risk and classification* attribute there is also a possibility to add comments and other descriptions, which can be included in future versions of this survey. The comments are in Swedish and here is a translation presented. 55 comments come from question 11 *How often do you use and update risk assessments?* Here are some examples: “For all new processing, one DPIA is done according to GDPR, previously only for systems”; “A huge work is in progress to find the processing activities”; “This is being done in a project right now. When the project ends it will be handed over to operations.”; “not decided yet”; “it’s a future task together with the information management plan”; “ a work is being done to asses risks for the first time”; “We are just about to start using KLASSA[15].”

5.6 Incident and information security management

Incident and information security management is mainly concerned with incident and breach management; information security program; logical access controls; portable media; and the testing of security safeguards. The average maturity in the

[15] KLASSA is a web application to support Swedish municipalities and regions with information classification. https://klassa-info.skl.se

incident and information security management attribute and the criteria within is shown in *Figure 19*.

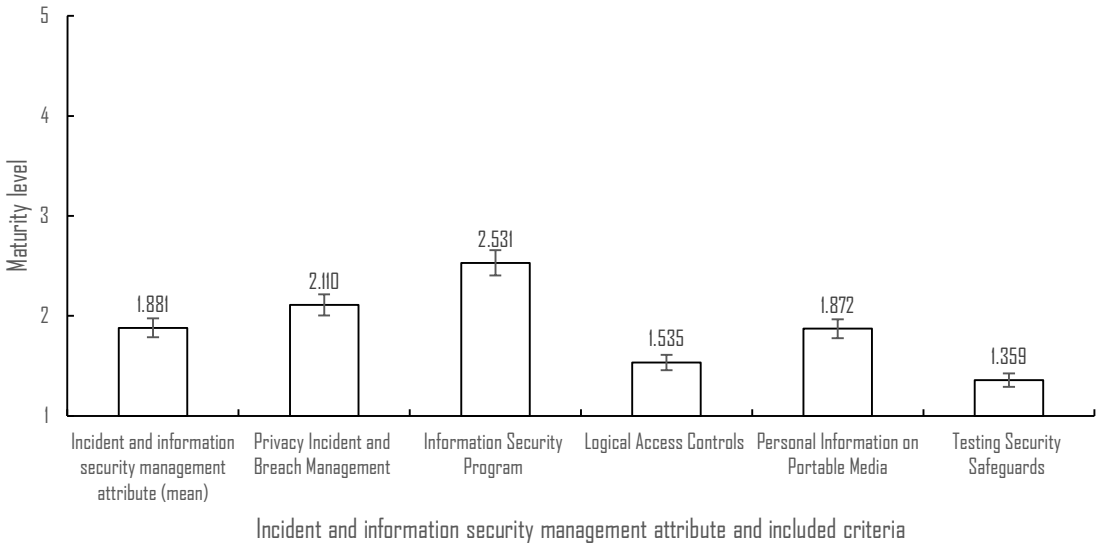

Figure 19 Maturity levels of the incident and information security management attribute and criteria.

Privacy Incident and Breach Management (criterion 1.2.7) focus on the existence of incident and breach management routines and processes. 29 percent confirm routines exist to identify privacy incidents, but not fully documented, and management practices are ad hoc, or the answer is they do not know (Level 1); 42 percent say a process has been developed on incidents, but not enough training has been provided (level 2); 24 percent report a process is implemented, including accountability, identification, risk assessment and response, containment, communications and monitoring (level 3); 1 percent furthermore is testing the breach management process (level 4); 5 percent say they also do both periodical and post-breach management assessment on the process to ensure improvements, and they have an *Incident response team* (IRT) ready to be summoned quickly (level 5). The following significance is found: Respondents within areas with sensitive data have higher maturity levels for this criterion compared to all other respondents, $F(1, 452) = 9{,}233$, $p<0{,}05$. The mean maturity level of the sensitive data group is 2,298 with a standard error of 0,087 and the mean maturity level of other respondents is 2,007 with a standard error of 0,053.

Information Security Program (criterion 8.2.1) covers how security for privacy is related to the work on information security and whether a function exists and if it is evaluated. Here one could add a further deepening discourse with a systematic perspective on Information security with various approaches. However, it is out of scope for this thesis, due to limited time. 17 percent either relate to privacy as a

subtask of information security, they do not have a security function, unit or program working systematically or they do not know (Level 1); 21 percent say they partly have a security function, unit or program (level 2); 54 percent report that a security function, unit or program is in place working systematically with privacy-related security, or they claim that work related to information security is part of the organisation-wide protection for privacy(level 3); 6 percent are additionally using external audits to review the program (level 4); and top 1 percent, also periodically assess the process to ensure continuous improvements (level 5).

Logical Access Controls (criterion 8.2.2) deals with mechanisms to restrict access to information and control how privileges are used. 59 percent have either not been able to answer this, due to that they do not work systematically with information security, or they answer "do not know" (Level 1); 29 percent do one of two things, they review log files regularly for signs of intrusion or unauthorised access; or they have implemented technical systems for intrusion detection and monitoring (level 2); 10 percent have both in level 2 (level 3); 0 percent furthermore periodically monitor compliance, both internally and with third-parties (level 4); and top 0,9 percent also periodically assess the process to ensure continuous improvements (level 5). Within the criterion Logical Access Controls, there is a significance in the difference in maturity level between respondents from the areas with high sensitive data in contrast to the rest of the respondents, $F(1, 452) = 14{,}638$, $p<0{,}01$. The sensitive data group has a mean of 1,714 with a standard error of 0,067, whereas the group with the rest of the respondents has a mean of 1,437 with a standard error of 0,039. The mean of all the respondents is 1,535 with a standard error of 0,035.

Personal Information on Portable Media (criterion 8.2.6) reflects on how the organisation is managing protection for data on portable media or devices from unauthorised access. 46 percent say routines and processes for management protection of portable devices are missing or inconsistent, or they “do not know“ (Level 1); 36 percent have a basic but limited protection and may have technical safeguards implemented, for example mobile devise management. (level 2); 7 percent report that processes, routines and protection for portable devises are in place, including monitoring, testing and reviews (level 3); 6 percent additionally require an acknowledgement of responsibilities before a devise is issued to an employee, or there is a protection mechanism (encryption) for devices during transfer and physical transport (level 4); and 4 percent have both and are continuously implementing improvements (level 5).

Testing Security Safeguards (criterion 8.2.7) covers the overall testing of efficiency of organisational, technical and physical security. 77 percent say tests are sporadic and inconsistent, or they answer, “do not know” (Level 1); 17 percent have a regular tests of security safeguards of different functions, with varied scope. (level 2); 2 percent say tests of security safeguards in all significant areas are done yearly, documented by qualified personnel (level 3); 0,9 percent partly analyse test to find

root cause to improve the overall security of the organisation (level 4); and 3 percent are either doing full root cause analysis to improve the overall security of the organisation, or make periodical assessments for the process to ensure continuous improvements (level 5).

6 Discussion

In this chapter, we further analyse the findings on the state of privacy maturity in Swedish municipalities. First, we present some general significances on the results. Second, we discuss the findings on the different attributes and included criteria in six sections. We sum up the discussion with reflections on the municipal controllers' inclination to perform visible practices and neglecting other privacy matters. Third, we suggest topics for further research. Fourth, we consider practical implications. The chapter ends with some self-critically discussions on the limitations of the study.

6.1 Privacy maturity in Swedish municipalities

We found a significance by the size of the municipality and the different attributes, especially the process and tools attribute. The medium-large municipalities scores higher in average to other groups, both smaller and larger, see Table 8. Perhaps, theory on organisational innovation and potential determinants could be used to explain, such as specialisation, functional differentiation, professionalism, centralisation, managerial attitude toward change, technical knowledge resources, administrative intensity, slack resources, and external and internal communication (Damanpour, 1991). Too small municipalities lack resources for specialisation and professionalisation, and the large cities are too centralised, formalised and hindered by vertical differentiation. This size-related topic is an area for further research.

In the survey, there were several instances of significance between the group working in areas with the likeliness of large quantities of sensitive personal data having higher maturity scores, than others. A possible explanation for this is that already existing rules and processes are being used, which is not a far-reaching conclusion, e.g. in the student health in schools. Likewise, practitioners in social-work also work with sensitive information and have a long tradition of working with confidentiality and ethical issues (Millstein, 2000). Unfortunately, some areas pose significant risks. The municipal healthcare system has extensive regulations regarding how sensitive information should be handled, but at the same time, they have several actors nationally, regionally and locally. Lots of risks have been identified due to shortcomings in management, compliance, coordination, complexity, interoperability, information security, information sharing; and there is a severe risk with spreading personal information. (Integritetskommittén, 2016).

DPOs are rating the maturity lower than the rest. The differences are not proven statistically significant in the attributes, but there is still an indication of a possible

difference. Since the role of the DPO is new, specific theories have not been found in the literature to explain this. One possible way to explain is that the DPO is supposed to criticise and be realistic. The DPO-role is required to be independent, and DPOs must show firmness towards the controller and not be obedient (Brezniceanu, 2017). With this line of thinking, more research would be needed into the role of the DPO. Not only that, the legal requirement for public authorities is only a year old yet. Much more can be learned about the view of privacy of DPOs and their counterparts, the controllers, by investigating further.

6.1.1 Roles and responsibilities

For the organisation of privacy work in municipalities, the results show that less than a third of the controllers have defined roles and responsibilities, except for the Data Protection Officers (level 3, criterion 1.1.2). Among the DPOs, the rating is even lower for the criterion 1.1.2. This low rating indicates that understanding the role of the DPO as an independent auditor is perhaps not understood, or prioritised, by the leaders. Perhaps the municipalities leaders think it is enough to have a DPO. Even though roles and responsibilities are not defined, about half of the controller's state that there are resources available empowered with appropriate authority and funding (level 3, criterion 1.2.8). Monitoring of the effectiveness of controls for long-term responsibility and accountability is almost neglected completely. Only a few are addressing the responsibility to implement a documented process for monitored privacy controls, based on a risk assessment (level 3, criterion 10.2.5).

The low maturity regarding roles and responsibilities could also be seen as a confirmation of the survey by the Swedish DPA that management in municipalities is less aware of privacy and is not giving this a priority, compared with other sectors. (Datainspektionen, 2019b).

6.1.2 Governance and compliance

The point of departure for a systematic approach to govern privacy in an organisation is the existence of an internal regulation – a privacy policy (Densmore, 2016). A majority of the municipal controllers state they do have internal regulation covering privacy and data protection (level 3 and above, criterion 1.1.0). An internal privacy policy's function is to govern the organisation and can be treated as a checklist for legal compliance (Krumay & Oetzel, 2011). It will be difficult to show evidence to the regulator of how the laws are implemented for self-regulatory accountability if there is no internal policy or governance framework (Bennett & Raab, 2018).

Only a quarter of the controllers in municipalities say regulations are reviewed to ensure that they are consistent with legislation (level 3 and above, criterion 1.2.2). However, very few checks that their commitments are consistent with these regulations. Only 5 percent state they have a process in place covering all aspects to review contracts and other commitments (level 3 and above, criterion 1.2.5). The

two consistency criteria (1.2.2 and 1.2.4) together with the risk assessment criterion 1.2.4 (discussed below), are essential for the process of creating a scalable risk management framework in an organisation, according to Schroeder and Cohen (2011).

Very few controllers state they have defined compliance controls, only one in ten, to review that compliance is performed regularly covering all aspects and are fully documented (level 3 and above, criterion 10.2.3). A compliance review is one of the tasks of the DPO but could also be done by an internal audit function (Hertzberg, 2018). Also, very few claims having a documented process for noncompliance deviations, including disciplinary actions, covering all aspects (level 3 and above, criterion 10.2.4). If processes for reviewing compliance do not exist, there is no way of proving the policies are used purposefully.

6.1.3 Education and competence

The awareness cannot be sufficient since half of the controllers in municipalities say they never performed any training in privacy. Some controllers have had some training, bot sporadic, most likely during the GDPR implementation projects. However, only a fifth say they do have a consistent formal training plan, or awareness program, and do regular training for internal personnel, in general as well as for persons working directly with privacy (level 3 and above, criterion 1.2.10). This division indicates that some become more aware of privacy, while others do not know much. Adequate and efficient training is necessary to create and improve user awareness and behaviour, and even though the topic of privacy and security seem boring to some people, motivation can be raised with training in small groups on an individual level, and with an increased organisational knowledge as a result (Albrechtsen & Hovden, 2010).

Regarding formal requirements for internal personnel working with sensitive information, only one in ten say they have reached the level of doing appropriate training and with the necessary knowledge, (level 3 and above, criterion 1.2.9) but half of the controllers show at least some requirements (level 2, criterion 1.2.9). This criterion also uncovers the existence of privacy specialists, except for the DPO, but a scarce one. There is a significance for persons working with sensitive information to show higher maturity. This reality is not surprising since laws are requiring particular qualifications for persons working in specific jobs within municipalities. For example, when applying for a job working with children, an applicant needs to show a police record of his or her criminal history. Also, within healthcare and social services, there are a lot of sensitive data, but regulations and practices exist and apply (Integritetskommittén, 2016).

6.1.4 Processes and tools

Most controllers show the provision of notice as a web page and refer to this page when communicating to individuals. The existence of public notice (some prefer to

call this the policy) is crucial and one of the first steps an organisation can do to show the public how they are complying with the GDPR privacy requirements. To be mature, it is not enough to have a notice on a web page, but also to inform in a timely fashion for any changes or new purposes (level 3 and above, criterion 2.2.1). To publicly explain how an individual's personal information is collected, stored, used, retained and shared is one thing that can be done to gain trust. Proper communication with individuals is a display of the organisation's transparency and should meet the expectations from individuals to avoid adverse consequences (Karwatzki et al., 2017), even for subjective harm (Calo, 2011).

Almost all controllers in municipalities say they have a document management plan in place (level 2 and above, criterion 5.2.2) and about two of five say it is accurate with how it works in practice (level 3 and above, criterion 5.2.2). For municipalities, the existence of laws for how authorities should retain information is not a new thing.

Another visible area is how the municipalities are dealing with the right to subject access requests (SAR) to individuals. GDPR requires that a registered receives an extract of the records in one month, under normal circumstances. To see how municipalities addresses this is very interesting. There are two strategies revealed in the results – one ambitious and one cautious. The ambitious strategy aims for a digital solution of at least the requesting of a SAR and the identification. One third claim to have a documented process covering all aspects of a subject access request, and using, for example, a digital service (level 3 and above, criterion 6.2.1) and also, one third consistently use a secure identification process, via for example a digital citizen identification solution, such as BankID (level 3 and above, criterion 6.2.2). The other strategy is cautious and not investing in automation and are instead using no specific method or using a standard form for the request process (level 2 and below, criterion 6.2.1) and a manual method for verification of identity (level 2 and below, criterion 6.2.2). Likely, considerable investments have been made by the ones with the ambitious strategy. This effort is also a display of trying to meet the expectations of the individuals, regarding transparency.

Another area where efforts have been made is to create processes for handling personal data agreement with third-parties and make assessments of third-parties. To have a personal data agreement is a requirement by the GDPR (European Parliament, 2016). Two of five have a documented process for managing the data processing agreement that includes specific instructions and requirements (level 3 and above, criterion 7.2.2). DPO rates the maturity significantly lower for criterion 7.2.2. One assumption is that many DPOs have been responsible for not only review but also to produce the agreements. Some evidence for this is found in the comments of the results. Third-parties are often cloud providers, and the use of cloud services lead to a loss of transparency and control, which are areas of serious privacy risk due to incorrect assumptions about the service provider's security

activities, according to Integritetskommittén (2016). External parties can handle sensitive personal data and municipalities often have deficiencies in competence for assessing this accurately (see criterion 1.2.9) above under *Education and competence.*

6.1.5 Risk and classification

Half of the controllers say they have a formal risk framework that is used, at least once a year, with documented, including risk identification, risk assessment and reporting (level 3 and above, criterion 1.2.4), but only one in eight have classified the processing activities, with risk assessments (level 3 and above, criterion 1.2.3). A particular form of risk analysis is the Data Protection Impact Assessments (DPIA), required by the GDPR when there is high risk for individuals (European Parliament, 2016). One-fifth of the controllers in municipalities claim they use formal DPIAs in a process, covering both implementation or changes to products, services, businesses and infrastructure level 3 and above, criterion 1.2.6).

A lot of different comments were added by controllers in the results, showing an awakening in the use of risk assessments, DPIAs and classification. An assumption is that a lot is going on at the moment. Risk assessments are the foundation for addressing privacy management and measure proactiveness of the organisation's privacy processes to determine what to prioritise and which protective measures are appropriate (Govender, 2015; Kauffman et al., 2011; Schroeder & Cohen, 2011). The question that follows is how much should a controller invest in mitigating risks in security and privacy protection. Kauffman et al. (2011) suggest and refer a stream of value-at-risk theory from financial economics, to use as an approach for investing in privacy protection, based on risk estimations, to find suitable thresholds, similar to stop-loss mechanisms. There should be an interval of a best and a worst possible consequence if risks are realised. This reasoning is consistent with the idea of a balance between how-to comply both with regulations and maximises at the same time business priorities (Bélanger & Crossler, 2011).

6.1.6 Incident and information security management

Almost a third of the controllers are prepared for potential breaches and have a comprehensive personal data breach process established (level 3 and above, criterion 1.2.7). So, the rest claim routines exist, but they lack training, or it is not documented. Also, controllers working with sensitive data claim they have a higher maturity. Only one in ten of controllers say they have basic protection for logical access available, where they review log files for signs of intrusion or unauthorised access; and have implemented technical systems for intrusion detection and monitoring (level 3 and above, criterion 8.2.2). One in six, claim they have adequate protection for mobile devices available (level 3 and above, criterion 8.2.6) and a quarter claim that limited information security audits are done (level 2 and

above, criterion 8.2.7) and only a few actually say they have defined processes for this practised on regular basis (level 3 and above, criterion 8.2.7).

The requirement from the law is that controllers must report within 72 hours to the Swedish DPA if a personal data breach occurs if there will include risk for individuals (European Parliament, 2016). Breaches reported from the start of GDPR, from May 25th, 2018 and until April 2019 to the Swedish DPA consisted of a majority of incidents, where emails were sent to wrong recipients and errors by granting access to wrong persons. Both these types of error can be seen as minor issues, with possible limited consequences for registered individuals; this could be a sign of over-reporting to the DPA. However, since maturity of many controllers' knowledge of third-parties security practises are low (criterion 7.2.2); classification with risks assessments are only done by a few (criterion 1.2.3); and only a few have necessary protection for logical access (criterion 8.2.2): extremely few are testing security in a comprehensive regularly way (criterion 8.2.7); this could also be a sign of controllers not knowing of incidents, and there may be under-reporting on incidents where there are severe consequences for individuals. Controllers may simply do not know whether they had a breach.

Two-thirds of the controllers in municipalities have an information security program or a person responsible for information security, or they claim the information security is part of the privacy protection function (8.2.1). This lack of security function is similar to the study from MSB in 2015; 2 of 5 of the municipalities did not have a responsible person for information security (MSB, 2015, 2016). To consider information security as a part of privacy is by PMM regarded as a mature practice (AICPA/CICA, 2011b). Security is more visible than privacy (Krumay & Oetzel, 2011), but privacy is also broader than security covering aspects of, e.g. transparency and lawfulness. Many of the activities suggested in Solove (2008) that many privacy invasive actions like for example interrogation, surveillance, secondary use, exclusion, explosion are not issues that can be solved by improved technical controls. These are not information security issues. We infer that sorting privacy practices in a municipality under an IT-security umbrella is an immature practice since a lot of essential aspects of privacy cannot be addressed purely from an IT-perspective. Still, we see examples of this in the results.

6.2 Transparency is prioritised, risks are neglected

The CMM defines mature and immature organisations, stating the former are more proactive than the latter (Paulk et al., 1993). Where should the limit be drawn of what maturity is enough? This boundary is a question, which must be answered by each organisation. With the results at hand, one could suggest that the state of privacy maturity uncovered for Swedish municipals is not a satisfying one, and

there is room for improvement. Especially on the protection and meeting risks that are less visible.

Privacy risks are emerging with the rise of new technologies and are putting pressure to meet the individual's concern for adverse consequences (Karwatzki et al., 2017). Laws have been created to answer the individual's concerns of privacy. Laws, which are instruments for policy (Bennett & Raab, 2018). The results in this survey reveal significant problems in municipalities with having working processes to meet the regulations. If laws are not obeyed this will indirectly affect the individual's concerns of privacy in the chain of "technologies–policies–processes–people–society–economy–legislature" (Lowry et al., 2017). Technology, by itself, is not offensive (Nissenbaum, 2004). It depends on the norms and the expectations of the individual in the current context. One clear line is that municipalities have prioritised concerns of transparency, which are needed to avoid negative perception, as stated by (Calo, 2011). The results show more effort is put into visible artefacts, like information and privacy notices and handling subject access requests. However, the other parts of privacy practices are less visible to persons outside the organisation – if nothing happens. When a breach occurs, or an inspection by the Swedish DPA, deficiencies in practices will become a focal point if neglected. How much a bad privacy practice becoming visible will affect the trust of the organisation, depends on where, when and how it occurs. A suggestion for a sufficient level of privacy maturity would be to be able to avoid and handle the consequences of all privacy risks, even the less visible.

6.3 Future research

Further research could also be done by applying the privacy maturity framework in other areas. For example, cross-national, public companies, regions, government authorities, non-governmental organisations or the private sector. The questions need to be adjusted in some cases, but also a slightly different set of criteria could be included, which would, of course, make comparisons harder. Some of the added criteria could be used without modification, and this would then be the common ground for comparison. There are also some notes in some areas for research in the conclusion below.

6.4 Practical implications

Here is a practical use to benchmark for practitioners who participated in the survey. When the questionnaire was completed, there was a possibility given to download the answers. There are two options to find out the score. One is to use the analysis model in *Appendix 3 – Questions, responses and analysis template* to set a maturity score manually. The other is to send the time-stamp on when the survey was submitted, which can be found on the PDF with the answers. We can

then reply with the maturity score on the attributes and the criteria. The email address to use for this is gusbroma@student.gu.se.

6.5 Limitations of the study

Below are some reflections and limitations of the Privacy maturity framework, an evaluation of the work, possible effects on the result and potential improvement possibilities.

The privacy maturity framework is created with a starting point in the PMM to be used in a quantitative study. The use of a maturity model is too simplistic for making predictions, according to King and Kraemer (1984). However, we are not prescribing, but rather comparing the municipal entities on a national level. For comparisons and benchmark, the privacy maturity framework can be useful, since a maturity score gained by answering the questionnaire now has a baseline for comparison. A controller can compare its own scores with the national levels. Also, a comparison can be made at a later time to reflect on changes.

The risk assessment criteria cover five questions due to the importance of using a risk-based approach to privacy management. It was not possible to change this after sending the questions. The same goes for some criteria, which were only covered by one question. If done again, another method of rating would have been used for some of the criteria. However, the results would not be comparable with the results of this survey.

The concept of consent was left out from the survey since municipalities have few processing activities based on consent. If comparisons to other areas were to be done, consent would probably need to be addressed. Westin (1967) argues that individuals are to determine for themselves about when they choose to participate or not in an activity and to choose anonymity. This determination refers to give a choice to the individual via consent and has been included in GDPR if no other legal grounds are possible. The legal requirements for consent require defined processes, and it would be interesting to research further into this area.

If one were to redo the survey, one way would be to standardise the questionnaire further to handle the level 4-5 scoring. We would also use another way to calculate the highest levels for several questions, to keep the integrity of each criterion as a requirement and to set all levels without referring to another question. The disadvantage in the current survey is that a few respondents may have been given lower maturity score on some questions, since they might have failed to answer the filter question response 3 in question 51 and missed the level 4-5 question 52.

The criterion 8.2.7, Testing Security Safeguards, received very low maturity rating. A few respondents gave comments on this, stating that it would be insecure to give away such information, so they refused to answer. However, all the answers were

anonymous. It is not known whether this has affected the results on this criterion. Still, the results of this criterion should be considered with this in mind.

Privacy by design is not covered in the survey. PbD, is a set of principles on how to design privacy into services (Cavoukian, 2009). Still, PbD is a legal requirement. The application of PbD principles would automate much information and also retention (with automatic archiving and deletion), leading to a whole set of possible descriptive aspect to include in future maturity studies.

The framework to measure privacy maturity have limitations in conception. Conceptually, one can ask: *Can privacy maturity be determined by asking questions in a web survey?* It is a challenge to conduct a study on an organisational level for privacy practices with data collection techniques such as online surveys (Smith et al., 2011). We agree to this finding and infer that, for using a full PMM-scope, it would be tough to uncover with the online survey data collection method. A more qualitative method should be used to get closer to reality since attrition would make the respondent unwilling to answer a more comprehensive questionnaire and likely drop-out of the survey. Perhaps a possible approach would be to the use of the full GAPP framework and the PMM in a series of either focus group or in-depth interviews workshops. These workshops or interviews would take considerably more time, and a comparison would be tough to generalise on a nation-wide level. However, it would provide a deeper understanding of the privacy maturity, specific challenges and suggestions for improvements.

Additionally, respondents understand concepts and questions differently. Therefore, answers and maturity must be seen in the context of diverse knowledge, experience, available time, willingness to participate and other possible limitations. The answers are no absolute truths. What is interesting is the comparison within the group of Swedish municipalities. Also, does the framework represent the real processes? Uncertainties can arise because both parameters in the framework and that calculations are empirically determined and represent multiple processes.

Lastly, this survey may affect the respondents to improve their processes. When doing the study, several mails were received where respondents wanted to use the questionnaire as a basis of discussion. There might be a chance that the survey has affected the respondents to improve their privacy management processes.

7 Conclusion

We have conducted a survey on the municipalities of Sweden with a quantitative approach using framework for measuring privacy maturity. Through an iterative process, we created a Privacy Maturity framework, which consists of 56 questions and is supported by 23 criteria of the GAPP best-practice standard. The approach is to make an inductive and systematic attempt to measure descriptive and comparative maturity in municipalities. A web-survey on 454 municipal controllers in Sweden reveals significant challenges. The level of maturity of Swedish municipals is around two on average on a scale of 1-5. It is not satisfying.

In the results, there are several significant patterns, and there are four most striking findings of the survey:

First, controllers in medium-large municipalities are estimating maturity higher than others. An explanation may be that small municipalities lack resources, and the large cities are too complicated. More research is needed in this area.

Second, less than a third have defined roles and responsibilities for privacy, excluding the DPO. Privacy is perhaps not understood, or prioritised, by leaders in municipalities. DPOs are estimating maturity lower than others. The role of the DPO is an exciting research topic.

Third, there may be under-reporting on incidents and breaches where there are severe consequences for individuals, due to lack of protection, monitoring and testing of safeguards, lack of checks of third-party security practices and treating privacy topics as IT-security problems. Controllers working with a lot of sensitive data are rating maturity higher in these areas. Why this area is under-prioritised is interesting for further studies.

Last, municipalities have prioritised concerns of transparency and communication. Visible processes like communication of privacy notice, meeting requests from registered, and retention practices are the areas with the highest estimated maturity. There are two strategies found – one ambitious and one cautious. The ambitious strategy puts effort into the use of digital services, and the cautious have more or less informal manual practices. Why some are cautious and what motivates the organisations that are ambitious is a topic for further research.

8 References

AICPA/CICA. (2011a). *Generally Accepted Privacy Principles*. American Institute of Certified Public Accountants and Canadian Institute of Chartered Accountants Retrieved from www.cica.ca/privacy

AICPA/CICA. (2011b). *Privacy Maturity Model*. American Institute of Certified Public Accountants and Canadian Institute of Chartered Accountants Retrieved from www.cica.ca/privacy

Albrechtsen, E., & Hovden, J. (2010). Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study. *Computers & Security, 29*(4), 432-445.

Basili, V. R. (1989). *Software development: a paradigm for the future.* Paper presented at the Proceedings of the Thirteenth Annual International Computer Software & Applications Conference, 1989.

Bélanger, F., & Crossler, R. E. (2011). Privacy in the digital age : a review of information privacy research in information systems. *MIS Quarterly, 35*(4), 1017-1041.

Benbasat, I., Dexter, A. S., Drury, D. H., & Goldstein, R. C. (1984). A Critique of the Stage Hypothesis: Theory and Empirical Evidence. *Communications of the ACM, 27*(5), 476-485.

Bennett, C. J., & Raab, C. D. (2018). Revisiting the governance of privacy: Contemporary policy instruments in global perspective. *Regulation and Governance*.

Branting, J. (2016). Ett svenskt perspektiv på contextual integrity. In W. Agrell & T. Petterson (Eds.), *Övervakning och integritet : teknik, skydd och aktörer i det nya kontrollandskapet*: Stockholm : Carlsson.

Brezniceanu, A. (2017). Data Protection Officer - a new profession in public administration? *Revista de Stiinte Politice*(55), 79-88.

Briand, L., Emam, K., & Morasca, S. (1996). On the application of measurement theory in software engineering. *Empirical Software Engineering, 1*(1), 61-88.

Bryman, A. (2016). *Social research methods* (Fifth edition ed.): Oxford : Oxford University Press.

Calo, M. R. (2011). The boundaries of privacy harm. *Indiana Law Journal, 86*(3), 1131-1162.

Cavoukian, A. (2009). Privacy by Design: The 7 Foundational Principles. Retrieved from https://iapp.org/resources/article/privacy-by-design-the-7-foundational-principles/

Checkland, P. B. (1989). Soft Systems Methodology. *Human systems management, 8*, 273-289.

Cochran, W. G. (1977). *Sampling Techniques* (3rd ed.). New York: John Wiley and Sons, Inc.

Damanpour, F. (1991). Organizational innovation: a meta-analysis of effects of determinants and moderators. (includes appendix). *Academy of Management Journal, 34*(3), 555.
Datainspektionen. (2019a). *Anmälda personuppgiftsincidenter 2018*. Retrieved from https://www.datainspektionen.se/globalassets/dokument/rapporter/anmalda-personuppgiftsincidenter-2018.pdf
Datainspektionen. (2019b). *Nationell Integritetsrapport 2019*. Retrieved from https://www.datainspektionen.se/globalassets/dokument/rapporter/nationell-integritetsrapport-2019.pdf
Dennedy, M., Fox, J., & Finneran, T. (2014). *The Privacy Engineer's Manifesto: Getting from Policy to Code to QA to Value*. Berkeley, CA: Apress.
Densmore, R. R. (2016). *Privacy program management : tools for managing privacy within your organization* (2nd edition. ed.). Portsmouth, NH: International Association of Privacy Professionals IAPP.
Dzazali, S., Sulaiman, A., & Zolait, A. H. (2009). Information security landscape and maturity level: Case study of Malaysian Public Service (MPS) organizations. *Government Information Quarterly, 26*(4), 584-593.
European Parliament, Council of the E. (1995). *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*. Retrieved from http://data.europa.eu/eli/dir/1995/46/oj
European Parliament, Council of the E. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)* Retrieved from http://data.europa.eu/eli/reg/2016/679/oj
Gable, J. (2014). Principles for protecting information privacy. *Information Management, 48*(5), 38-40,42,47.
Gaito, J. (1980). Measurement Scales and Statistics: Resurgence of an Old Misconception. *Psychological Bulletin, 87*(3), 564-567.
Gallie, W. B. (1955). Essentially Contested Concepts. *Proceedings of the Aristotelian Society, 56*, 167-198.
Goodman, S. (2018). Aligning Privacy and IM Within the IG Framework. *Information Management, 52*(2), 30-35.
Govender, I. (2015). *Mapping 'Security Safeguard' Requirements in a data privacy legislation to an international privacy framework: A compliance methodology.* Paper presented at the 2015 Information Security for South Africa - Proceedings of the ISSA 2015 Conference.
Hertzberg, J. (2018). GDPR and internal audit: Auditors can help their organization navigate the compliance risks posed by Europe's General Data Protection Regulation.(Risk Watch). *Internal Auditor, 75*(4), 22.
Hochheimer, C. J., Sabo, R. T., Krist, A. H., Day, T., Cyrus, J., & Woolf, S. H. (2016). Methods for Evaluating Respondent Attrition in Web-Based Surveys. *Journal of medical Internet research, 18*(11), e301-e301.
Humphrey, W., Sweet, William., Edwards, R.., LaCroix, G.., Owens, M.., & Schulz, H. (1987). A Method for Assessing the Software Engineering

Capability of Contractors. Retrieved from http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=10345
IAPP-EY. (2018). *Annual Privacy Governance Report 2018*. Retrieved from https://iapp.org/resources/article/iapp-ey-annual-governance-report-2018/
Integritetskommittén. (2016). *Hur står det till med den personliga integriteten? – En kartläggning av Integritetskommittén, delbetänkande*. (SOU 2016:41). Regeringskansliet: Justitiedepartementet Retrieved from http://www.regeringen.se/rattsdokument/statens-offentliga-utredningar/2016/06/sou-201641/
ISO/IEC. (2011). ISO/IEC 29100:2011 Privacy framework. In: International Organization for Standardization.
ISO/IEC. (2013). ISO/IEC 27002:2013 Information technology — Security techniques — Code of practice for information security management. In: International Organization for Standardization (ISO).
ISO/IEC. (2015). ISO/IEC 29190:2015 Privacy capability assessment model. In: International Organization for Standardization.
ISO/IEC. (2019). ISO/IEC PDTR 27550 Information technology -- Security techniques -- Privacy engineering. Retrieved from https://www.iso.org/standard/72024.html
Kamara, I. (2017). Co-regulation in EU personal data protection: the case of technical standards and the privacy by design standardisation 'mandate'. *European Journal of Law and Technology, 8*(1), 1.
Karokola, G., Kowalski, S., & Yngström, L. (2011). *Towards An Information Security Maturity Model for Secure e-Government Services: A Stakeholders View.* Paper presented at the Proceedings Of The 5th International Symposium On Human Aspects Of Information Security & Assurance,.
Karwatzki, S., Trenz, M., Tuunainen, V., & Veit, D. (2017). Adverse consequences of access to individuals' information: an analysis of perceptions and the scope of organisational influence. *European Journal of Information Systems, 26*(6), 688-715.
Kauffman, R. J., Lee, Y. J., Prosch, M., & Steinbart, P. J. (2011). A survey of consumer information privacy from the accounting information systems perspective.(Survey). *Journal of Information Systems, 25*(2), 47.
King, J., & Kraemer, K. (1984). Evolution and organizational information systems: an assessment of Nolan's stage model. *Communications of the ACM, 27*(5), 466-475.
Kremelberg, D. (2011). *Practical Statistics: A Quick and Easy Guide to IBM® SPSS® Statistics, STATA, and Other Statistical Software*. Thousand Oaks: Sage Publications, Inc.
Krumay, B., & Oetzel, M. C. (2011, 22-26 Aug. 2011). *Security and Privacy in Companies: State-of-the-art and Qualitative Analysis.* Paper presented at the 2011 Sixth International Conference on Availability, Reliability and Security.
Körner, S. (1996). *Praktisk statistik* (2nd ed.): Lund : Studentlitteratur.
Little, R., & Rubin, D. (1987). *Statistical analysis with missing data*. New York: New York : Wiley.
Lowry, P., Dinev, T., & Willison, R. (2017). Why security and privacy research lies at the centre of the information systems (IS) artefact: proposing a bold research agenda. *European Journal of Information Systems, 26*(6), 546-563.

Mason, R. O. (1986). Four Ethical Issues of the Information Age. *MIS Quarterly, 10*(1), 5-12.
Millstein, K. (2000). *Confidentiality in Direct Social-Work Practice: Inevitable Challenges and Ethical Dilemmas* (Vol. 81).
MSB. (2015). *En bild av kommunernas informationssäkerhetsarbete 2015*. The Swedish Civil Contingencies Agency (MSB) Retrieved from https://www.msb.se/RibData/Filer/pdf/27967.pdf
MSB. (2016). *Informationssäkerheten i Sveriges kommuner; Analys och rekommendationer utifrån MSB:s kommunenkät 2015*. The Swedish Civil Contingencies Agency (MSB) Retrieved from https://www.msb.se/RibData/Filer/pdf/28222.pdf
Niemimaa, E., & Niemimaa, M. (2017). Information systems security policy implementation in practice: from best practices to situated practices. *European Journal of Information Systems, 26*(1), 1-20.
Nissenbaum, H. (2004). Privacy as contextual integrity.(Symposium: Technology, Values, and the Justice System). *Washington Law Review, 79*(1), 119-157.
NIST. (2013). *Special publication 500-83 Revision 4*. National Institute of Standards and Technology Retrieved from https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final
NIST. (2019). *NIST Privacy Framework*. National Institute of Standards and Technology Retrieved from https://www.nist.gov/privacy-framework
Norman, G. (2010). Likert scales, levels of measurement and the “laws” of statistics. *Advances in Health Sciences Education, 15*(5), 625-632.
Nuñez, D., Fernández-Gago, C., & Luna, J. (2016). Eliciting metrics for accountability of cloud systems. *Computers & Security, 62*(C), 149-164.
Patel, R., & Davidson, B. (2011). *Forskningsmetodikens grunder : att planera, genomföra och rapportera en undersökning* (4., [uppdaterade] uppl. ed.). Lund: Studentlitteratur.
Paulk, M. C., Curtis, B., Chrissis, M. B., & Weber, C. V. (1993). Capability maturity model, version 1.1. *IEEE Software, 10*(4), 18-27.
Persson, A., Fjelkegård, L., Hartwig, P., & Sundström, A. (2016). *Frågor och svar : om frågekonstruktion i enkät- och intervjuundersökningar* (A. Persson Ed.). Stockholm: Statistiska centralbyrån SCB.
Pfeffer, J., & Sutton, R. I. (1999). Knowing "What" to Do Is Not Enough: Turning knowledge into cation. *California Management Review, 42*(1), 83-108.
Ponemon, McDermott W. E. (2018). *The Race to GDPR: A Study of Companies in the United States & Europe*. Retrieved from McDermott Will and Emery LLP: https://iapp.org/media/pdf/resource_center/Ponemon_race-to-gdpr.pdf
Privacy Protection Study Commission. (1977). Personal Privacy in an Information Society. *The Report of The Privacy Protection Study Commission.* Retrieved from https://epic.org/privacy/ppsc1977report/
Pöppelbuß, J., & Röglinger, M. (2011). *What makes a useful maturity model? a framework of general design principles for maturity models and its demonstration in business process management.* Paper presented at the ECIS 2011 Proceedings. Paper 28.
Rachovitsa, A. (2016). Engineering and lawyering privacy by design: understanding online privacy both as a technical and an international human rights issue. *International Journal of Law and Information Technology, 24*(4), 374-399.

Ricardo dos Santos, D., Becker Westphall, C., Alencar Rigon, E., & Merkle Westphall, C. (2014). A cyclical evaluation model of information security maturity. *Information Management & Computer Security, 22*(3), 265-278.
Schroeder, D., & Cohen, N. A. (2011). GAPP targets privacy risks: principles provide a comprehensive, scalable framework for managing compliance and reputation threats.(generally accepted privacy principles). *Journal of Accountancy, 212*(1), 52.
Shrestha, A., Cater-Steel, A., Toleman, M., & Tan, W.-G. (2014, 2014//). *Building a Software Tool for Transparent and Efficient Process Assessments in IT Service Management.* Paper presented at the Advancing the Impact of Design Science: Moving from Theory to Practice, Cham.
SKL, Swedish Association of Local Authorities and R. (2017). Classification of Swedish municipalities 2017. Retrieved from https://skl.se/tjanster/kommunerochregioner/faktakommunerochregioner/kommungruppsindelning.2051.html
Smith, H. J., Dinev, T., & Xu, H. (2011). Information Privacy Research: An Interdisciplinary Review. *MIS Quarterly, 35*(4), 989-1015.
Solove, D. J. (2002). Conceptualizing Privacy. *California Law Review, 90*, 1087-2143.
Solove, D. J. (2006). A taxonomy of privacy. *University of Pennsylvania Law Review, 154*(3), 477.
Solove, D. J. (2008). *Understanding privacy*. Cambridge, Mass.: Cambridge, Mass. : Harvard Univ Press.
Stevens, S. S. (1946). On the Theory of Scales of Measurement. *Science, 103*(2684), 677-680.
Teo, T. S. H., & King, W. R. (1997). Integration between Business Planning and Information Systems Planning: An Evolutionary-Contingency Perspective. *Journal of Management Information Systems, 14*(1), 185-214.
The Open Group. (2011). Open Information Security Management Maturity Model (O-ISM3). In. Zaltbommel: Van Haren Publishing.
US Department of Health & Human Services. (1973). *Records, Computers and the Rights of Citizens*. Assistant Secretary for Planning and Evaluation (ASPE) Retrieved from https://aspe.hhs.gov/report/records-computers-and-rights-citizens
Ustaran, E. (2017). *European data protection : law and practice*. Portsmouth, NH: International Association of Privacy Professionals.
van Dijk, N., Tanas, A., Rommetveit, K., & Raab, C. (2018). Right engineering? The redesign of privacy and personal data protection. *International Review of Law, Computers & Technology, 32*(2-3), 230-256.
Van Solingen, R., Basili, V., Caldiera, G., & Rombach, H. D. (2002). Goal question metric (gqm) approach. *Encyclopedia of software engineering*.
Visconti, M., & Cook, C. (1998). Evolution of a maturity model - critical evaluation and lessons learned. *Software Quality Journal, 7*(3-4), 223-237.
Wahlgren, G., Fedotova, A., Musaeva, A., & Kowalski, S. (2016). *IT Security Incidents Escalation in the Swedish financial sector: A Maturity Model Study.* Paper presented at the Proceedings of the Tenth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2016), Frankfurt, Germany.

Wahlgren, G., & Kowalski, S. (2016). *A Maturity Model for Measuring Organizations Escalation Capability of IT-related Security Incidents in Sweden.* Paper presented at the Workshop on Information Security and Privacy (WISP) 2016: Proceedings, Dublin, Ireland.
Warren, S. D., & Brandeis, L. D. (1890). The Right to Privacy. *Harvard Law Review, 4*(5), 193-220.
Wendler, R. (2012). The maturity of maturity model research: A systematic mapping study. *Information and Software Technology, 54*(12), 1317-1339.
Westin, A. F. (1967). *Privacy and Freedom*. New York: Atheneum.
Wittgenstein, L. (1953). *Philosophical investigations*. Oxford: Blackwell.
Zumbo, B. D., & Kroc, E. (2019). A Measurement Is a Choice and Stevens' Scales of Measurement Do Not Help Make It: A Response to Chalmers. *Educational and Psychological Measurement*.

9 Appendices

Appendix 1 - GAPP principles and criteria

Report nr: 2019:009

GAPP Principles, aspects and criteria headers in English (AICPA/CICA, 2011a) and Swedish translation.

Principle	Aspect	Criteria	English description	Swedish description
1.0			**Management**	**Styrning och förvaltning**
	1.1		*Policies and communications*	*Policy, riktlinjer och kommunikation*
		1.1.0	Privacy policies	Intern personuppgiftspolicy
		1.1.1	Communication to internal personnel	Intern kommunikation
		1.1.2	Responsibility and accountability for policies	Ansvar och skyldigheter
	1.2		*Procedures and controls*	*Rutiner, processer och kontroller*
		1.2.1	Review and approval	Granskning och godkännande
		1.2.2	Consistency of privacy policies and procedures with laws and regulations	Följdriktighet av policy och riktlinjer med lagstiftning
		1.2.3	Personal information identification and classification	Klassning av personuppgifter
		1.2.4	Risk assessment	Riskbedömningar
		1.2.5	Consistency of commitments with privacy policies and procedures	Granskning av följdriktighet av åtaganden med policy och riktlinjer
		1.2.6	Infrastructure and systems management	Infrastruktur och systemförvaltning
		1.2.7	Privacy incident and breach management	Incidenthantering
		1.2.8	Supporting resources	Tillgängliga resurser
		1.2.9	Qualifications of internal personnel	Kvalifikationer på interna resurser
		1.2.10	Privacy awareness and training	Utbildning och medvetenhet
		1.2.11	Changes in regulatory and business requirements	Förändrade kravställningar
2.0			**Notice**	**Integritetsmeddelande**
	2.1		*Policies and communications*	*Policy, riktlinjer och kommunikation*

		2.1.0	Privacy policies	Policy för information till registrerade
		2.1.1	Communication to individuals	Kommunikation till individer
	2.2		*Procedures and controls*	*Rutiner, processer och kontroller*
		2.2.1	Provision of notice	Tillhandahålla integritetsmeddelande
		2.2.2	Entities and activities covered	Omfattning av aktiviteter och enheter
		2.2.3	Clear and conspicuous	Klar- och tydlighet
3.0			**Choice and consent**	**Samtycke och valmöjligheter för individer**
	3.1		*Policies and communications*	*Policy, riktlinjer och kommunikation*
		3.1.0	Privacy policies	Policy för samtycke och valmöjligheter
		3.1.1	Communication to individuals	Kommunikation till individer
		3.1.2	Consequences of denying or withdrawing consent	Konsekvenser för nekande och återkallelse
	3.2		*Procedures and controls*	*Rutiner, processer och kontroller*
		3.2.1	Implicit or explicit consent	Underförstått och uttryckligt samtycke
		3.2.2	Consent for new purposes and uses	Samtycke för nytt ändamål
		3.2.3	Explicit consent for sensitive information	Uttryckligt samtycke för känsliga uppgifter
		3.2.4	Consent for online data transfers to or from an individual's computer or other similar electronic devices	Samtycke för tillgång till och från individers enheter
4.0			**Collection**	**Insamling av data**
	4.1		*Policies and communications*	*Policy, riktlinjer och kommunikation*
		4.1.0	Privacy policies	Policy för insamling av data
		4.1.1	Communication to individuals	Kommunikation till individer
		4.1.2	Types of personal information collected and methods of collection	Insamlingsmetoder och kategorier av personuppgifter
	4.2		*Procedures and controls*	*Rutiner, processer och kontroller*
		4.2.1	Collection limited to identified purpose	Uppgiftsminimering
		4.2.2	Collection by fair and lawful means	Rättvis och laglig insamling
		4.2.3	Collection from third parties	Insamling från tredjeparter
		4.2.4	Information developed about individuals	Profilering av individer
5.0			**Use, retention, and disposal**	**Användning, lagring och radering**
	5.1		*Policies and communications*	*Policy, riktlinjer och kommunikation*
		5.1.0	Privacy policies	Policy om användning, lagring och radering
		5.1.1	Communication to individuals	Kommunikation till individer
	5.2		*Procedures and controls*	*Rutiner, processer och kontroller*
		5.2.1	Use of personal information	Användning av personuppgifter
		5.2.2	Retention of personal information	Lagring av personuppgifter

		5.2.3	Disposal, destruction and redaction of personal information	Rensning, gallring och arkivering av personuppgifter
6.0			**Access**	**Individers åtkomst till sina data**
	6.1		*Policies and communications*	*Policy, riktlinjer och kommunikation*
		6.1.0	Privacy policies	Policy om individers åtkomst till sina data
		6.1.1	Communication to individuals	Kommunikation till individer
	6.2		*Procedures and controls*	*Rutiner, processer och kontroller*
		6.2.1	Access by individuals to their personal information	Registerutdrag och registrerades rättigheter
		6.2.2	Confirmation of an individual's identity	Begriplig information, tidsramar och kostnader
		6.2.3	Understandable personal information, time frame, and cost	Verifiering av identitet
		6.2.4	Denial of access	Nekande av tillgång till personuppgifter
		6.2.5	Updating or correcting personal information	Uppdatering, korrigering, begränsning och invändning av personuppgifter
		6.2.6	Statement of disagreement	Nekande av ändring eller begränsning
7.0			**Disclosure to third parties**	**Utlämnande till tredjeparter**
	7.1		*Policies and communications*	*Policy, riktlinjer och kommunikation*
		7.1.0	Privacy policies	Policy för utlämning till tredjeparter
		7.1.1	Communication to individuals	Kommunikation till individer
		7.1.2	Communication to third parties	Kommunikation till tredjeparter
	7.2		*Procedures and controls*	*Rutiner, processer och kontroller*
		7.2.1	Disclosure of personal information	Utlämning av personuppgifter
		7.2.2	Protection of personal information	Skriftligt avtal som skydd för personuppgifter
		7.2.3	New purposes and uses	Utlämnande för nya ändamål
		7.2.4	Misuse of personal information by a third party	Felaktig användning av personuppgifter av tredjeparter
8.0			**Security for privacy**	**Informationssäkerhet**
	8.1		*Policies and communications*	*Policy, riktlinjer och kommunikation*
		8.1.0	Privacy policies	Informationssäkerhetspolicy
		8.1.1	Communication to individuals	Kommunikation till individer
	8.2		*Procedures and controls*	*Rutiner, processer och kontroller*
		8.2.1	Information security program	Organisation av informationssäkerhetsarbetet
		8.2.2	Logical access controls	Logiska säkerhetskontroller
		8.2.3	Physical access controls	Fysiska säkerhetskontroller

		8.2.4	Environmental safeguards	Miljörelaterad säkerhet
		8.2.5	Transmitted personal information	Säkerhet vid överföring av personuppgifter
		8.2.6	Personal information on portable media	Säkerhet på mobila enheter
		8.2.7	Testing security safeguards	Granskningar av informationssäkerhet
9.0			**Quality**	**Kvalitet**
	9.1		*Policies and communications*	*Policy, riktlinjer och kommunikation*
		9.1.0	Privacy policies	Policy för kvalitet och riktighet
		9.1.1	Communication to individuals	Kommunikation till individer
	9.2		*Procedures and controls*	*Rutiner, processer och kontroller*
		9.2.1	Accuracy and completeness of personal information	Riktighet och fullständighet av personuppgifter
		9.2.2	Relevance of personal information	Relevans av personuppgifter
10.0			**Monitoring and enforcement**	**Övervakning och upprätthållande**
	10.1		*Policies and communications*	*Policy, riktlinjer och kommunikation*
		10.1.0	Privacy policies	Policy för övervakning och upprätthållande
		10.1.1	Communication to individuals	Kommunikation till individer
	10.2		*Procedures and controls*	*Rutiner, processer och kontroller*
		10.2.1	Inquiry, complaint and dispute process	Utredning, klagomål och tvister
		10.2.2	Dispute resolution and recourse	Tvistlösning och tillämpning
		10.2.3	Compliance review	Efterlevnadskontroll
		10.2.4	Instances of noncompliance	Avvikelsehantering
		10.2.5	Ongoing monitoring	Övervakning av effektivitet av kontroller ur ett riskperspektiv

Appendix 2 – Scope reduction and key practices analysis

Report nr: 2019:009

The full list of questions in the first questionnaire, the prioritisation score used in the analysis for the reduction of scope.

In the analysis we gave the following *prioritisation score* to questions that were:

1 for questions we considered as a key practice or are needed for completeness.
2 for redundant questions, where the key practice is already mentioned, or answers are covered by another questions.
3 for practices that is not considered common in a municipality context.

Nr	Question	Key Practices	Prio score	Criteria
1	Har ni ett internt regelverk för hantering av integritets- och dataskyddsfrågor (till exempel integritetspolicy, dataskyddspolicy eller motsvarande)?	Has regulations (internal policy)	1	1.1.0 Privacy policies
2	Välj de delar som täcks av ert regelverk:	Scope of regulations (internal policy)	1	
3	Hur gör ni då för att hantera regler internt om integritets- och dataskyddsfrågor?		1	
4	Hur kommunicerar ni med personalen om regler internt gällande integritets- och dataskyddsfrågor?		2	1.1.1 Communication to internal personnel
5	Hur hanterar ledningen ansvar och skyldigheter för integritets- och dataskyddsfrågor?	Defined roles and responsibilities exist	1	1.1.2 Responsibility and accountability for policies
6	Hur hanterar ledningen granskningar och godkännande av regelverk?		2	1.2.1 Review and approval
7	Utförs granskning av regelverk av interna och externa specialister?		2	
8	Genomförs en ledningsgenomgång av regelverk inför granskning och godkännande?		2	
9	Hur säkerställer ni att regelverket stämmer överens med lagstiftningen?	Regulations are reviewed to ensure that	1	1.2.2 Consistency of privacy policies and

Nr	Question	Key Practices	Prio score	Criteria
		they comply with legislation		procedures with laws and regulations
10	Sker en förebyggande bevakning av ny lagstiftning på dataskyddsområdet?		2	
11	Genomförs en ledningsgenomgång av hur förändringar i lagstiftning påverkar det interna regelverket?		2	
12	Har en informationsklassning för känslighet av personuppgifter utförs?	Has classified information sensitivity	1	1.2.3 Personal information identification and classification
13	Hur omfattande är klassningen av behandlingar av personuppgifter? (Välj det alternativ som stämmer bäst)		1	
14	Motsvarar skydd för tjänster och systemnivån av klassningen på personuppgifterna?		2	
15	Finns en dokumenterad process för att uppdatera klassning inklusive riskbedömningar vid förändringar?		2	
16	Har ni en process för riskhantering som omfattar risker för hot mot personuppgifter som er organisation hanterar?	Risk process exists and is used	1	1.2.4 Risk assessment
17	Hur ofta genomför och uppdaterar ni bedömningar i er riskhanteringsprocess?		1	
18	Välj de beskrivningar som bäst stämmer in på er riskhanteringsprocess:		1	
19	Välj de beskrivningar som bäst stämmer in på er riskhanteringsprocess:		1	
20	Hur gör ni då för att identifiera och hantera risker gällande personuppgifter? (Välj det alternativ som stämmer bäst)		1	
21	Gör ni en intern granskning av att avtal innehåller reglering av personuppgifter? (t.ex. personuppgiftsbiträdesavtal, delningsavtal)	Review agreements for personal information	1	1.2.5 Consistency of commitments with privacy policies and procedures
22	Hur omfattande är den interna granskningen av personuppgifter i era avtal? (Välj det alternativ som stämmer bäst)		1	

Nr	Question	Key Practices	Prio score	Criteria
23	Välj de beskrivningar som bäst stämmer in på er process för interna granskningar personuppgifter i era avtal:		2	
24	Gör ni en konsekvensbedömning av risker för hantering av personuppgifter vid införande av nya eller förändringar av befintliga processer? (t.ex. infrastruktur, system, applikationer, tjänster, produkter, databaser, mobil hantering, webbplatser, informationslagring)	Data protection impact assessments are performed	1	1.2.6 Infrastructure and systems management
25	Hur omfattande är konsekvensbedömningar av personuppgifter vid införande av nya eller förändringar av befintliga processer? (Välj det alternativ som stämmer bäst)		1	
26	Välj de beskrivningar som bäst stämmer in på er process för konsekvensbedömningar:		2	
27	Har ni processer och rutiner för att säkerställa att personuppgiftsincidenter identifieras och hanteras på ett effektivt sätt?	Incident process established	1	1.2.7 Privacy incident and breach management
28	Hur omfattande är er process för identifiering och hantering av personuppgiftsincidenter? (Välj det alternativ som stämmer bäst)		1	
29	Välj de beskrivningar som stämmer med er process för identifiering och hantering av personuppgiftsincidenter:		1	
30	Välj de beskrivningar som bäst er organisation gällande resurser för arbete att genomföra och stödja hanteringen av personuppgifter: (Här avses inte dataskyddsombudet, utan andra resurser)	Available resources among staff	1	1.2.8 Supporting resources
31	Välj den beskrivning som bäst stämmer in gällande kvalifikationer på intern personal som hanterar personuppgifter:	Formal requirements for internal staff are available	1	1.2.9 Qualifications of internal personnel
32	Vilka typer av bakgrundskontroller genomförs för anställda som potentiellt har tillgång till konfidentiell information? (Välj en eller flera).			
33	Finns det en kärna av den interna personalen som är specialister på dataskydd och integritetsfrågor?	Data protection specialists are available	1	

Nr	Question	Key Practices	Prio score	Criteria
34	Sker en bedömning av prestationen och kvaliteten sker minst årligen av personalen om hantering av dataskydd och integritetsfrågor?		2	
35	Sker kompetensutveckling av intern personal som innefattar certifieringar inom "privacy" eller relaterade områden?		1	
36	Hur ofta genomförs personalutbildning gällande dataskydd och integritetsfrågor?	Education in privacy takes place	1	1.2.10 Privacy awareness and training
37	Välj den beskrivning som bäst om personalutbildning gällande dataskydd och integritetsfrågor:	Training program exist	1	
38	Välj de beskrivningar som bäst stämmer in om utbildningsprogrammet gällande dataskydd och integritetsfrågor: (Flera svar är möjliga)		1	
39	Välj den beskrivning som bäst stämmer in på hantering av förändringar i kravställningar för dataskydd och integritetsfrågor? Här eftersöks hur hantering sker av förändringar i lagstiftning, kontrakt, SLAer, branschkrav, processförändringar, personalförändringar, roller, ansvar och teknologi		2	1.2.11 Changes in regulatory and business requirements
40	Välj de beskrivningar som bäst stämmer in på förändringshanteringsprocessen gällande dataskydd och integritetsfrågor: (Flera svar är möjliga)		2	
41	Hur lämnas information till registrerade om hur ni hanterar personuppgifter?	Information to registered persons takes place	1	2.2.1 Provision of notice
42	Välj de beskrivningar som bäst stämmer in på informationen till registrerade: (Flera svar är möjliga)		1	
43	Välj bland beskrivningarna om informationen till registrerade omfattar följande: (Flera svar är möjliga)		2	2.2.2 Entities and activities covered
44	Hur sker uppdatering av informationen till registrerade (Välj den beskrivning som bäst stämmer in):		2	

Nr	Question	Key Practices	Prio score	Criteria
45	Hur är informationens tydlighet? (Välj den beskrivning som stämmer in bäst):		2	2.2.3 Clear and conspicuous
46	Hur är följs informationens tydlighet upp?		2	
47	Hur samlar ni in samtycke i de fall det behövs för insamling, användning eller utlämning av personuppgifter?		3	3.2.1 Implicit or explicit consent
48	Skickar ni en fråga om bekräftelse på individens samtycke vid ändringar på tjänsten eller hanteringen?		3	
49	Sker en översyn av processen för insamling av samtycke regelbundet?		3	
50	Hur hanteras nya ändamål som det tidigare samtycket inte täckte. (Välj den beskrivning som bäst stämmer in)?		3	3.2.2 Consent for new purposes and uses
51	Sker en verifiering av tjänster och system för att kontrollera att giltigt samtycke finns		3	
52	Samlar ni in uttryckligt samtycke för känsliga uppgifter, där detta behövs?		3	3.2.3 Explicit consent for sensitive information
53	Välj bland beskrivningarna om uttryckligt samtycke för känsliga uppgifter: (Flera svar är möjliga)		3	
54	Sker en fråga om samtycke för överföringar till eller från en individs dator eller annan enhet? (förutom cookies)		3	3.2.4 Consent for online data transfers to or from an individual's computer or other similar electronic devices
55	Välj bland beskrivningarna om samtycke för överföringar till eller från en individs dator eller annan enhet: (Flera svar är möjliga)		3	
56	Är insamlingen begränsad till att enbart samla in nödvändiga uppgifter som behövs för uppfylla ändamålet?		3	4.2.1 Collection limited to identified purpose
57	Välj bland beskrivningarna om insamling av enbart nödvändiga uppgifter som behövs för uppfylla ändamålet (Flera svar är möjliga)		3	
58	Sker en granskning av att insamling av personuppgifter är laglig och rättvis? (t.ex. av ett dataskyddsombud eller en jurist)		2	4.2.2 Collection by fair and lawful means

Nr	Question	Key Practices	Prio score	Criteria
59	Välj den beskrivning som bäst stämmer in på hur granskning av insamling är laglig och rättvis?		2	
60	Sker en regelbunden uppföljning av processen om granskning av insamling är laglig och rättvis?		2	
61	Hur hanteras klagomål om att insamling skulle ske ojuste eller olagligt? (Flera svar är möjliga)		2	
62	Välj den beskrivning som bäst stämmer om att insamling av uppgifter från annan än den registrerade sker korrekt? (tredje part)		2	4.2.3 Collection from third parties
63	Sker en återkommande kontroll av tredje parters insamlingsmetoder?		2	
64	Sker en uppföljning med att analysera insamlingsmetoder från tredje parter och införa förebyggande förändringar i kravställningar för framtida upphandlingar?		2	
65	Hur informerar ni individer om ni sammanställer uppgifter om dem för att skapa en profil? (Välj den beskrivning som stämmer in bäst):		3	4.2.4 Information developed about individuals
66	Sker en regelbunden uppföljning av processen att informera om profilering?		3	
67	Hur informeras individer om profilering?		3	
68	Hur säkerställer ni att användning av personuppgifter sker på ett korrekt sätt? (Välj den beskrivning som stämmer in bäst)		2	5.2.1 Use of personal information
69	Sker en regelbunden uppföljning av processen att verifiera användning av personuppgifter?		2	
70	Välj bland beskrivningarna om verifiering av användning sker på ett korrekt sätt.(Flera svar är möjliga)		2	
71	Hur säkerställer ni att lagring av personuppgifter sker på ett korrekt sätt? (Välj den beskrivning som stämmer in bäst)	Document management plan exists and works	1	5.2.2 Retention of personal information
72	Sker en regelbunden uppföljning av att dokumenthanteringsplan och verklig lagring överensstämmer?		1	

Nr	Question	Key Practices	Prio score	Criteria
73	Välj bland beskrivningarna om hur verifiering av att lagring av personuppgifter sker på ett korrekt sätt. (Flera svar är möjliga)		1	
74	Hur säkerställer ni att rensning, arkivering och gallring av personuppgifter sker på ett korrekt sätt? (Välj den beskrivning som stämmer in bäst)		2	5.2.3 Disposal, destruction and redaction of personal information
75	Hur hanterar ni begäran om registerutdrag? (Välj den beskrivning som stämmer in bäst)	Process for registry extracts is available	1	6.2.1 Access by individuals to their personal information
76	Hur sker hantering av att söka fram registrerades personuppgifter till ett registerutdrag? (Välj den beskrivning som stämmer in bäst)		1	
77	Sker en regelbunden uppföljning processen av söka fram registrerades personuppgifter till ett registerutdrag?		2	
78	Hur gör ni för att registerutdrag ska vara begripligt, levererat inom rimlig tidsram och till en rimlig kostnad? (Välj den beskrivning som stämmer in bäst)		2	6.2.2 Confirmation of an individual's identity
79	Sker en regelbunden uppföljning processen av söka fram registrerades personuppgifter till ett registerutdrag?		2	
80	Hur ni säkerställer ni rätt identitet vid begäran om registerutdrag från registrerade? (Välj den beskrivning som stämmer in bäst)	Identity verification process	1	6.2.3 Understandable personal information, time frame, and cost
81	Finns det spårbarhet i processen för att verifiera identitet?		1	
82	Sker en regelbunden uppföljning av att processen för verifiera identitet?		1	
83	Välj den beskrivning som stämmer in bäst för att kunna neka tillgång till personuppgifter. (T.ex. att en lag förhindrar det).		3	6.2.4 Denial of access
84	Finns en regelbunden uppföljning av nekanden? (t ex responstid, anledningar för nekande och hur kommunikationen hanterades)		3	
85	Finns det en automatiserad funktion för nekande där så är möjligt?		3	

Nr	Question	Key Practices	Prio score	Criteria
86	Hur hanterar ni begäran om registrerades rättigheter förutom registerutdrag? (Välj den beskrivning som stämmer in bäst)		2	6.2.5 Updating or correcting personal information
87	Finns det spårbarhet i processen för att hantera data och begäran om ändringar?		2	
88	Välj bland beskrivningarna om processen för hantering av registrerades rättigheter.(Flera svar är möjliga)		2	
89	Välj den beskrivning som stämmer in bäst för att neka uppdatering, korrigering, begränsning eller invändning. (T.ex. en lag förhindrar det).		2	6.2.6 Statement of disagreement
90	Finns en regelbunden uppföljning av nekanden? (t ex responstid, anledningar för nekande och hur kommunikationen hanterades)		2	
91	Finns det en automatiserad funktion för nekande där så är möjligt?		2	
92	Välj den beskrivning som stämmer bäst in för att lämna ut personuppgifter till tredje part.		2	7.2.1 Disclosure of personal information
93	Sker det en granskning att processen för att lämna ut personuppgifter till tredje part överensstämmer med det interna regelverket?		2	
94	Välj bland beskrivningarna för att lämna ut personuppgifter till tredje part.(Flera svar är möjliga)		2	
95	Välj den beskrivning som bäst stämmer när det gäller skriftligt avtal som skydd för leverantörers hantering av personuppgifter: (Personuppgiftsbiträdesavtal)	Process for personal data bit agreement exists	1	7.2.2 Protection of personal information
96	Övervakas förändringar på tredje partens tekniska miljö för att säkerställa att de fortsatt lever upp till kravställningarna?		1	
97	Finns en regelbunden bedömning av om processen för att teckna personuppgiftsbiträdesavtal?		1	
98	Hur hanteras utlämnande för nya ändamål? (Välj den beskrivning som bäst stämmer in)?		2	7.2.3 New purposes and uses
99	Övervakas processen för hantering av utlämnande för nya ändamål?		2	

Nr	Question	Key Practices	Prio score	Criteria
100	Välj bland beskrivningarna för att lämna ut personuppgifter till tredje part för nya ändamål.(Flera svar är möjliga)		2	
101	Hur hanteras felaktig användning av personuppgifter av en tredje part? (Välj den beskrivning som bäst stämmer in)?		3	7.2.4 Misuse of personal information by a third party
102	Sker en övervakning av processen för hantering av felaktigheter kan finnas hos en tredje part?		3	
103	Sker en avvikelserapportering för olämplig eller oacceptabel användning av personuppgifter hos en tredje part?		3	
104	Finns en plan för att hantera och avhjälpa olämplig eller oacceptabel användning av personuppgifter hos en tredje part?		3	
105	Har ni en utpekad funktion, enhet eller åtgärdsprogram som systematiskt arbetar med informationssäkerhetsfrågor? (Program för informationssäkerhet)	Has information security programs	1	8.2.1 Information security program
106	Välj de delar som omfattas av ert program för informationssäkerhet. (Flera svar är möjliga)		1	
107	Hur hanteras informationssäkerhet i relation till skydd för personuppgifter? (Välj den beskrivning som bäst stämmer in)	Information security is handled as a part of privacy	1	
108	Välj de delar bland beskrivningarna som stämmer in på ert program för informationssäkerhet.(Flera svar är möjliga)		2	
109	Genomförs årliga externa granskningar av hela programmet för att utvärdera effektiviteten?	External audits of information security takes place	1	
110	Hur hanteras säkerhet för personuppgifter gällande inloggning, behörigheter? (Välj den beskrivning som bäst stämmer in)		2	8.2.2 Logical access controls
111	Hur hanteras annat skydd för logisk access (intrångsförsök och otillåten användning)? (Flera svar är möjliga)	Basic protection for logical access is available	1	
112	Hur hanteras annat skydd för fysisk access? (Välj den beskrivning som bäst stämmer in)		3	8.2.3 Physical access controls
113	Hur övervakas skydd för fysisk access? (Flera svar är möjliga)		3	

Nr	Question	Key Practices	Prio score	Criteria
114	Hur hanteras annat skydd mot naturkatastrofer och miljöfaror? (Välj den beskrivning som bäst stämmer in)		3	8.2.4 Environmental safeguards
115	Hur sker arbetet med kontinuietetsplanen? (Flera svar är möjliga)		3	
116	Hur hanteras skydd vid överföring via nätverk och via fysisk transport? (Välj den beskrivning som bäst stämmer in)		2	8.2.5 Transmitted personal information
117	Hur sker arbetet med skydd vid överföring via nätverk och via fysisk transport? (Flera svar är möjliga)		2	
118	Hur hanteras skydd för mobila enheter (bärbara datorer, surfplattor och smartphones)? (Välj den beskrivning som bäst stämmer in)	Protection for mobile devices is available	1	8.2.6 Personal information on portable media
119	Hur sker arbetet med skydd för mobila enheter, som till exempel bärbara datorer, surfplattor och smartphones? (Flera svar är möjliga)		1	
120	Hur testas effektiviteten av säkerhetsåtgärder för organisatorisk, teknisk och fysisk säkerhet? (Välj den beskrivning som bäst stämmer in)?	Information security audits are performed and is defined	1	8.2.7 Testing security safeguards
121	Leder resultatet av testning till överlämning så att nya åtgärder införs eller att brister blir fixade?		2	
122	Sker en analys av tester för att finna bakomliggande orsaker (root cause) med vidare hantering för förbättringar av hela organisationens säkerhet?	Analysis of underlying causes (root cause)	1	
123	Hur säkerställs kvaliteten på personuppgifter, dess riktighet och fullständighet för ändamålet med behandlingen? (Välj den beskrivning som bäst stämmer in)		2	9.2.1 Accuracy and completeness of personal information
124	Välj på vilket sätt arbetet med att säkerställa kvaliteten på personuppgifter sker. (Flera svar är möjliga)		2	
125	Hur säkerställs relevansen på personuppgifter för ändamålet med behandlingen? (Välj den beskrivning som bäst stämmer in)		2	9.2.2 Relevance of personal information

Nr	Question	Key Practices	Prio score	Criteria
126	Välj på vilket sätt arbetet med att säkerställa att endast personuppgifter som är relevanta behandlas. (Flera svar är möjliga)		2	
127	Hur sker hantering och utredning av klagomål och tvister gällande personuppgiftsbehandling? (Välj den beskrivning som bäst stämmer in)?		3	10.2.1 Inquiry, complaint and dispute process
128	Välj på vilket sätt arbetet utreda och bemöta klagomål och hantera tvister sker. (Flera svar är möjliga)		3	10.2.2 Dispute resolution and recourse
129	Hur sker hantering av kontroll av efterlevnad av regler, lagar samt andra externa och interna krav? (Välj den beskrivning som bäst stämmer in)?	Compliance Control defined	1	10.2.3 Compliance review
130	Välj på vilket sätt arbetet med efterlevnadskontroll sker. (Flera svar är möjliga)		1	
131	Hur sker rapportering av avvikelser i efterlevnad samt korrigeringar? (Välj den beskrivning som bäst stämmer in)	Deviation handling defined	1	10.2.4 Instances of noncompliance
132	Sker en uppföljning av avvikelseprocessen som leder till ett förebyggande arbete för att möta nya avvikelser i framtiden?		1	
133	Hur sker löpande övervakning av att kontroller och riskbedömningar är effektiva ? (Välj den beskrivning som bäst stämmer in)	Monitoring effectiveness of controls exists	1	10.2.5 Ongoing monitoring
134	Välj bland beskrivningarna för hur mätning av kontrollers effektivitet sker .(Flera svar är möjliga)		2	

Appendix 3 – Questions, responses and analysis template

Report nr: 2019:009

Analysis template for scoring privacy maturity on survey question responses

Q	GAPP	A	Req.	Questions	Responses	M	Comment
1	N/A	A0		Är du som svarar Dataskyddsombud?	1.1 Ja	-	N/A
					1.2 Nej	-	N/A
					1.3 Annat, specificera här:	-	N/A
2	N/A	A0		Hur stor är den kommun du verkar för?	2.1 Minst 200 000 invånare och största tätorten har minst 200 000 invånare.	-	N/A
					2.2 Minst 50 000 invånare och största tätorten har minst 40 000 invånare.	-	N/A
					2.3 Minst 15 000 invånare och största tätorten har minst 15 000 invånare.	-	N/A
					2.4 Kommunens största tätort har färre än 15 000 invånare.	-	N/A
					2.5 Vet ej/ingen uppfattning.	-	N/A
3	N/A	A0		Inom vilka verksamhetsområden arbetar du? (Flera svar är möjliga)	3.1 Ledning, juridik, ekonomi, central service- och förvaltning	-	N/A
					3.2 Arbetsmarknadsfrågor	-	N/A
					3.3 Barnomsorg och förskoleverksamhet	-	N/A
					3.4 Kommunalt bolag	-	N/A
					3.5 Kultur och fritid	-	N/A
					3.6 Miljö- och hälsoskydd	-	N/A
					3.7 Ordning och säkerhet	-	N/A
					3.8 Plan- och byggfrågor	-	N/A
					3.9 Renhållning och avfallshantering	-	N/A

Legend:

Q = Question number
GAPP = Corresponding GAPP criteria
A = Attributes
Req. = Requirement for displaying the question
M = Estimated maturity level
N/A = Not applicable

A0 = General questions
A1 = Roles and responsibilities
A2 = Governance and compliance
A3 = Education and competence
A4 = Processes and tools
A5 = Risk and classification
A6 = Incident and information security management

Q	GAPP	A	Req.	Questions	Responses	M	Comment
					3.10 Räddningstjänst	-	N/A
					3.11 Samhällsbyggnad	-	N/A
					3.12 Socialtjänst	-	N/A
					3.13 Utbildning för barn och ungdom	-	N/A
					3.14 Vattenförsörjning och avlopp	-	N/A
					3.15 Vuxenutbildning	-	N/A
					3.16 Vård och omsorg av äldre och funktionshindrade	-	N/A
					3.17 Annat, specificera här:	-	N/A
4	1.1.0	A2		Har ni ett internt regelverk för hantering av integritets- och dataskyddsfrågor?	4.1 Ja	3	
					4.2 Delvis	2	
					4.3 Nej	1	
					4.4 Vet ej	1	
5	1.1.0	A2	If 4.1 or 4.2	Välj de delar som täcks av ert regelverk:	5.1 Förvaltning, ansvar och roller	4 or 5	If all 10 = 4; Level 5 depends on 52.1-52.4
					5.2 Information till registrerade	4 or 5	If all 10 = 4; Level 5 depends on 52.1-52.4
					5.3 Samtycken	4 or 5	If all 10 = 4; Level 5 depends on 52.1-52.4
					5.4 Insamling av data	4 or 5	If all 10 = 4; Level 5 depends on 52.1-52.4
					5.5 Användning, bevarande, gallring och förstöring av data	4 or 5	If all 10 = 4; Level 5 depends on 52.1-52.4
					5.6 Utlämning till tredjeparter	4 or 5	If all 10 = 4; Level 5 depends on 52.1-52.4
					5.7 Informationssäkerhet	4 or 5	If all 10 = 4; Level 5 depends on 52.1-52.4

Legend:
Q = Question number
GAPP = Corresponding GAPP criteria
A = Attributes
Req. = Requirement for displaying the question
M = Estimated maturity level
N/A = Not applicable

A0 = General questions
A1 = Roles and responsibilities
A2 = Governance and compliance
A3 = Education and competence
A4 = Processes and tools
A5 = Risk and classification
A6 = Incident and information security management

Q	GAPP	A	Req.	Questions	Responses		M	Comment
					5.8	Individers åtkomst till sina data	4 or 5	If all 10 = 4; Level 5 depends on 52.1-52.4
					5.9	Kvalitet och riktighet av personuppgifter	4 or 5	If all 10 = 4; Level 5 depends on 52.1-52.4
					5.10	Uppföljning och efterlevnad	4 or 5	If all 10 = 4; Level 5 depends on 52.1-52.4
					5.11	Annat, specificera här:	-	No change
6	1.2.2	A2	If 4.1 or 4.2	Hur säkerställer ni att regelverket stämmer överens med lagstiftningen?	6.1	Jämförelser med lagstiftning sker delvis, men är inte komplett	1	
					6.2	En granskning av överensstämmelse med lagstiftning sker, men utan dokumenterad vägledning	2	
					6.3	En process är införd för att återkommande genomföra jämförelser med lagstiftning.	3	Level 4-5 depends on 52.1-52.4
					6.4	Vet ej/ingen uppfattning	1	
7	1.1.0	A2	If 4.3 or 4.4	Hur gör ni då för att hantera regler internt om integritets- och dataskyddsfrågor?	7.1	Regelverk är under framtagning	1	
					7.2	Regler existerar inte	1	
					7.3	Regler finns, men är inte fullt dokumenterade	1	
					7.4	Annat, specificera här:	-	No change
8	1.2.3	A5		Har en informationsklassning för känslighet av personuppgifter utförs?	8.1	Ja	2	
					8.2	Delvis	1	
					8.3	Nej	1	
					8.4	Vet ej	1	
9	1.2.3	A5	If 8.1 or 8.2	Hur omfattande är klassningen av behandlingar av personuppgifter?	9.1	Ingen fullständig klassning är gjord, den är inaktuell eller det saknas delar	1	

Legend:
Q = Question number
GAPP = Corresponding GAPP criteria
A = Attributes
Req. = Requirement for displaying the question
M = Estimated maturity level
N/A = Not applicable

A0 = General questions
A1 = Roles and responsibilities
A2 = Governance and compliance
A3 = Education and competence
A4 = Processes and tools
A5 = Risk and classification
A6 = Incident and information security management

Q	GAPP	A	Req.	Questions	Responses		M	Comment
					9.2	Grundläggande klassning är gjord, men saknar fullständiga riskbedömningar	2	
					9.3	Alla behandlingar är klassade och har riskbedömningar	3	Level 4-5 depends on 52.1-52.4
					9.4	Vet ej/ingen uppfattning	1	
10	1.2.4	A5		Har ni en process för riskhantering som omfattar risker för hot mot personuppgifter som er organisation hanterar?	10.1	Ja	2	
					10.2	Delvis	1	
					10.3	Nej	1	
					10.4	Vet ej	1	
11	1.2.4	A5	If 10.1 or 10.2	Hur ofta genomför och uppdaterar ni bedömningar i er riskhantering?	11.1	Flera gånger per år	-	No change
					11.2	En gång per år	-	No change
					11.3	Mindre ofta	-	No change
					11.4	Annat, specificera här:	-	No change
12	1.2.4	A5	If 10.1 or 10.2	Välj de beskrivningar som bäst stämmer in på er riskhantering:	12.1	Anställda är överlag medvetna om integritetsrisker	2	
					12.2	Ett formellt fastställt ramverk för identifiering, bedömning och rapportering finns dokumenterad	3	
					12.3	Uppdatering av regelverk och processer sker som en följd av riskbedömningar	3 or 4	12.3 and 12.5 = 4, else 3
					12.4	Ett IT-verktyg används för hantering och dokumentation av risker (Ej Excel eller motsvarande)	-	No change
					12.5	Interna och externa revisioner genomförs som innefattar risker för personuppgifter.	3 or 4	12.3 and 12.5 = 4, else 3
					12.6	Annat, specificera här:	-	No change

Legend:
Q = Question number
GAPP = Corresponding GAPP criteria
A = Attributes
Req. = Requirement for displaying the question
M = Estimated maturity level
N/A = Not applicable

A0 = General questions
A1 = Roles and responsibilities
A2 = Governance and compliance
A3 = Education and competence
A4 = Processes and tools
A5 = Risk and classification
A6 = Incident and information security management

Q	GAPP	A	Req.	Questions	Responses		M	Comment
13	1.2.4	A5	If 12.3, 12.4 or 12.5	Välj de beskrivningar som bäst stämmer in på er riskhanteringsprocess:	13.1	En anpassad riskhantering sker för olika verksamheter	5	13.1 and 13.3 = 5, else no change
					13.2	Ett centralt riskregister finns etablerat med samtliga risker som identifierats.	-	No change
					13.3	En formell bedömning av effektiviteten av riskhanteringen genomförs regelbundet och processförändringar införs	5	13.1 and 13.3 = 5, else no change
					13.4	Annat, specificera här:	-	No change
14	1.2.4	A5	If 10.3 or 10.4	Hur gör ni då för att identifiera och hantera risker gällande personuppgifter?	14.1	Risker identifieras och hanteras sporadiskt	1	
					14.2	Risker identifieras och hanteras, men inte fullt dokumenterat	1	
					14.3	Risker identifieras och hanteras inte	1	
					14.4	Vet ej/ingen uppfattning	1	
					14.5	Annat, specificera här:	-	No change
15	1.2.6	A5		Gör ni en konsekvensbedömning av risker för hantering av personuppgifter vid införande av nya eller förändringar av befintliga processer?	15.1	Ja	2	
					15.2	Delvis	1	
					15.3	Nej	1	
					15.4	Vet ej	1	
16	1.2.6	A5	If 15.1 or 15.2	Hur omfattande är konsekvensbedömningar av personuppgifter vid införande av nya eller förändringar av befintliga processer?	16.1	Konsekvensbedömningar sker sporadiskt för nya verksamhetsprocesser och införande av nya system	1	
					16.2	Konsekvenser bedöms vid införande och vid förändringar av system, men är informella och inte fullt dokumenterade	2	

Legend:
Q = Question number
GAPP = Corresponding GAPP criteria
A = Attributes
Req. = Requirement for displaying the question
M = Estimated maturity level
N/A = Not applicable

A0 = General questions
A1 = Roles and responsibilities
A2 = Governance and compliance
A3 = Education and competence
A4 = Processes and tools
A5 = Risk and classification
A6 = Incident and information security management

Q	GAPP	A	Req.	Questions	Responses		M	Comment
					16.3	Konsekvensbedömningar sker i en formell process, som täcker införande och förändringar i produkter, tjänster, verksamhet och infrastruktur	3	Level 4-5 depends on 52.1-52.4
					16.4	Annat, specificera här:	-	No change
17	1.2.7	A6		Har ni rutiner för att säkerställa att personuppgiftsincidenter identifieras och hanteras på ett effektivt sätt?	17.1	Ja	1	
					17.2	Delvis	1	
					17.3	Nej	1	
					17.4	Vet ej	1	
18	1.2.7	A6	If 17.1 or 17.2	Hur omfattande är er process för identifiering och hantering av personuppgiftsincidenter?	18.1	En rutin finns, men den är inte fullt dokumenterad och hanteringen är ad hoc.	1	
					18.2	En process har utvecklats, men personalen har inte fått tillräcklig utbildning.	2	
					18.3	En dokumenterad process är implementerad som inkluderar ägarskap, identifiering av incidenter, riskbedömningar, skadebegränsning, kommunikation och uppföljning.	3	
					18.4	Vet ej/ingen uppfattning.	1	
19	1.2.7	A6	If 18.3	Välj de beskrivningar som stämmer med er process för identifiering och hantering av personuppgiftsincidenter:	19.1	Incidenthanteringsprocessen testas genom övningar som även inkluderar ledningen.	4	
					19.2	Övervakning sker med tekniska kontroller för att identifiera incidenter.	-	No change
					19.3	Ledningen genomför bedömningar av incidenthanteringsplanen regelbundet eller när en incident skett för att förbättra processen.	5	Req. 19.1 and 2 of 3 of 19.3-19.5 = 5

Legend:
Q = Question number
GAPP = Corresponding GAPP criteria
A = Attributes
Req. = Requirement for displaying the question
M = Estimated maturity level
N/A = Not applicable

A0 = General questions
A1 = Roles and responsibilities
A2 = Governance and compliance
A3 = Education and competence
A4 = Processes and tools
A5 = Risk and classification
A6 = Incident and information security management

Q	GAPP	A	Req.	Questions	Responses		M	Comment
					19.4	Avtal finns med externa resurser för att genomföra exempelvis IT-forensiska undersökningar för att säkra bevis.	5	Req. 19.1 and 2 of 3 of 19.3-19.5 = 5
					19.5	Ett incidentteam är etablerat och har beredskap för att snabbt kunna kallas samman.	5	Req. 19.1 and 2 of 3 of 19.3-19.5 = 5
					19.6	Annat, specificera här:	-	No change
20	1.1.2	A1		Hur hanterar ledningen ansvar och skyldigheter för integritets- och dataskyddsfrågor?	20.1	Ingen ansvarig är utsedd	1	
					20.2	Ansvarig person eller grupp är utsedd, men resurser och mandat är begränsade.	2	
					20.3	Definierade roller och ansvar finns. En dokumenterad process används för att utveckla regelverket.	3	Level 4-5 depends on 52.1-52.4
					20.4	Vet ej/ingen uppfattning	1	
21	1.2.8	A1		Välj de beskrivningar som bäst stämmer gällande resurser för arbete att genomföra och stödja hanteringen av personuppgifter:	21.1	Resurser tilldelas vid behov angående frågor om dataskydd.	1	
					21.2	Rutiner för hur man ska arbeta med har tagits fram, men utan stöd av specialister på dataskydd.	2	
					21.3	Personer finns tillgängliga med mandat och tillgång till resurser och stöd.	3	
					21.4	Ledningen säkerställer att det finns tillgängliga resurser genomgående för att stödja olika arbete med personuppgifter.	4	
					21.5	Ledningen har en årlig översyn av allt arbete och genomför förbättringar på lämplighet, tillgänglighet och prestationer av resurser.	5	Req 21.4
					21.6	Annat, specificera här:	1	

Legend:
Q = Question number
GAPP = Corresponding GAPP criteria
A = Attributes
Req. = Requirement for displaying the question
M = Estimated maturity level
N/A = Not applicable

A0 = General questions
A1 = Roles and responsibilities
A2 = Governance and compliance
A3 = Education and competence
A4 = Processes and tools
A5 = Risk and classification
A6 = Incident and information security management

Q	GAPP	A	Req.	Questions	Responses		M	Comment
22	1.2.9	A3		Välj den beskrivning som bäst stämmer in gällande kvalifikationer på intern personal som hanterar personuppgifter:	22.1	Inga formella kvalifikationer finns specifikt för personal som hanterar personuppgifter.	1	
					22.2	Det finns kvalifikationer för delar av hanteringen av personuppgifter. Det sker en del utbildning som stöd.	2	
					22.3	Det finns formella krav på kvalifikationer för hanteringen av personuppgifter och dokumenterade arbetsbeskrivningar för anställda som har tillgång till konfidentiell och känslig information.	3	
					22.4	Vet ej/ingen uppfattning	1	
23	1.2.9	A3	If 22.3	Finns det en kärna av den interna personalen som är specialister på dataskydd och integritetsfrågor?	23.1	Ja	4	
					23.2	Delvis	4	
					23.3	Nej	3	
					23.4	Vet ej	3	
24	1.2.9	A3	If 23.1 or 23.2	Sker kompetensutveckling av intern personal som innefattar certifieringar inom "privacy" eller relaterade områden?	24.1	Ja	5	
					24.2	Delvis	5	
					24.3	Nej	4	
					24.4	Vet ej	4	
25	1.2.10	A3		Hur ofta genomförs personalutbildning gällande dataskydd och integritetsfrågor?	25.1	Aldrig	1	
					25.2	En gång, vid anställning	1	
					25.3	Vid anställning, och minst en gång per år	2	
					25.4	Vet ej/ingen uppfattning	1	

Legend:
Q = Question number
GAPP = Corresponding GAPP criteria
A = Attributes
Req. = Requirement for displaying the question
M = Estimated maturity level
N/A = Not applicable

A0 = General questions
A1 = Roles and responsibilities
A2 = Governance and compliance
A3 = Education and competence
A4 = Processes and tools
A5 = Risk and classification
A6 = Incident and information security management

Q	GAPP	A	Req.	Questions	Responses		M	Comment
26	1.2.10	A3	If 25.2 or 25.3	Välj den beskrivning som bäst stämmer in om personalutbildning gällande dataskydd och integritetsfrågor:	26.1	Ingen formell utbildning genomförs, utan kunskap sprids via mer kunniga i personalen.	1	
					26.2	Det förekommer kampanjer för att öka medvetenheten, men utbildningen är sporadisk och en sammanhållen utbildningsplan saknas.	2	
					26.3	Ett utbildningsprogram finns för både nya anställda och återkommande utbildning för personalen. Fördjupande utbildningar sker för de som behöver ytterligare kunskap. Utbildningsmaterial är anpassat för organisationen.	3	
					26.4	Vet ej/ingen uppfattning	1	
27	1.2.10	A3	If 26.3	Välj de beskrivningar som bäst stämmer in om utbildningsprogrammet gällande dataskydd och integritetsfrågor:	27.1	E-utbildning sker för nyanställda och minst årligen för alla anställda.	4	req 27.1 and 27.2
					27.2	De utbildningar som de anställda genomgått är dokumenterade och kan förekomma i utvecklingssamtal	4	req 27.1 and 27.2
					27.3	Utbildningsprogrammet utvärderas återkommande för att täcka förändringar i regelverk och lagstiftningar.	5	req 27.3 and 27.4
					27.4	En stark kultur gällande dataskydd finns. När det förekommer incidenter sker förnyad utbildning och informationskampanjer.	5	req 27.3 and 27.4
					27.5	Annat, specificera här:	-	No change

Legend:
Q = Question number
GAPP = Corresponding GAPP criteria
A = Attributes
Req. = Requirement for displaying the question
M = Estimated maturity level
N/A = Not applicable

A0 = General questions
A1 = Roles and responsibilities
A2 = Governance and compliance
A3 = Education and competence
A4 = Processes and tools
A5 = Risk and classification
A6 = Incident and information security management

Q	GAPP	A	Req.	Questions	Responses		M	Comment
28	2.2.1	A4		Hur lämnas information till registrerade om hur ni hanterar personuppgifter?	28.1	Det finns ingen generell information. Vi meddelar från gång till gång när det behövs.	1	
					28.2	Det finns information som beskriver hantering av personuppgifter på vår webbsida eller annan externt tillgänglig plats	2	
					28.3	Vet ej/ingen uppfattning	1	
					28.4	Annat, specificera här:	-	No change
29	2.2.1	A4	If 28.3	Välj de beskrivningar som bäst stämmer in på informationen till registrerade:	29.1	Vi hänvisar till meddelandet på webbsidan.	2	
					29.2	Vi meddelar så snart det är praktiskt möjligt om vi avser använda personuppgifterna för ett annat ändamål.	2	
					29.3	Vi spårar versioner av meddelanden och kommunikation och vet vilken information som givits, vid varje givet tillfälle.	3	req 29.1 - 29.2
					29.4	Vi har integrerat information i tjänsterna och denna är anpassad för den teknologi och plattform som används.	4	req 29.1- 29.3
					29.5	Uppdateringar sker genom en etablerad process som tar hänsyn förändringar i regelverk, processer, som en följd av händelser och nya kravställningar.	5	req 29.1-29-4
					29.6	Annat, specificera här:	-	No change
30	5.2.2	A4		Hur säkerställer ni att lagring av personuppgifter sker på ett korrekt sätt?	30.1	En giltig dokumenthanteringsplan finns inte eller används sporadiskt	1	
					30.2	En dokumenthanteringsplan finns, men är inte fullt ut implementerad.	2	

Legend:
Q = Question number
GAPP = Corresponding GAPP criteria
A = Attributes
Req. = Requirement for displaying the question
M = Estimated maturity level
N/A = Not applicable

A0 = General questions
A1 = Roles and responsibilities
A2 = Governance and compliance
A3 = Education and competence
A4 = Processes and tools
A5 = Risk and classification
A6 = Incident and information security management

Q	GAPP	A	Req.	Questions	Responses		M	Comment
					30.3	En dokumenthanteringsplan finns som täcker in processer och rutiner som stämmer överens med hur det fungerar i praktiken.	3	
					30.4	Vet ej/ingen uppfattning	1	
31	5.2.2	A4	If 30.2	Sker en regelbunden uppföljning av att dokumenthanteringsplan och verklig lagring överensstämmer?	31.1	Ja	4	
					31.2	Delvis	3	
					31.3	Nej	-	No change
					31.4	Vet ej	-	No change
32	5.2.2	A4	If 31.1 or 31.2	Välj bland beskrivningarna om verifiering av lagring av personuppgifter sker på ett korrekt sätt:	32.1	Verifiering av att lagringen stämmer enligt dokumenthanteringsplanen sker automatiskt.	4 or 5	If all 3 = 5, If 2 of 3 =4
					32.2	Lagring av personuppgifter granskas regelbundet i en lämplighetsbedömning.	4 or 5	If all 3 = 5, If 2 of 3 =4
					32.3	Förändringar eller avvikelser övervakas och processen uppdateras som en följd av detta.	4 or 5	If all 3 = 5, If 2 of 3 =4
					32.4	Annat, specificera här:	-	No change
33	6.2.1	A4		Hur hanterar ni begäran om registerutdrag?	33.1	Det finns inget bestämt sätt, utan en begäran kan ske via e-post, telefon eller besök.	1	
					33.2	En process finns, men att skicka in en begäran sker manuellt. (t ex en PDF-fil på en webbsida som skickas per post).	2	
					33.3	En dokumenterad process finns implementerad som täcker alla aspekter av registerutdrag (t.ex. en digital tjänst)	3	
					33.4	Vet ej/ingen uppfattning	1	
34	6.2.1	A4	If 33.3	Hur sker hantering av att söka fram registrerades	34.1	Sökning och sammanställning sker manuellt och sporadiskt	-	No change

Legend:
Q = Question number
GAPP = Corresponding GAPP criteria
A = Attributes
Req. = Requirement for displaying the question
M = Estimated maturity level
N/A = Not applicable

A0 = General questions
A1 = Roles and responsibilities
A2 = Governance and compliance
A3 = Education and competence
A4 = Processes and tools
A5 = Risk and classification
A6 = Incident and information security management

Q	GAPP	A	Req.	Questions	Responses		M	Comment
				personuppgifter till ett registerutdrag?	34.2	Sökning och sammanställning sker manuellt enligt en process som återanvänds och utvecklas.	4	If 33.3 and 34.2 = 4
					34.3	Sökning och sammanställning sker automatiserat och med själv-service i ett tekniskt system	5	If 33.3 and 34.3 = 5
					34.4	Vet ej/ingen uppfattning	-	No change
35	6.2.2	A4		Hur ni säkerställer ni rätt identitet vid begäran om registerutdrag från registrerade?	35.1	Informellt och olika från fall till fall.	1	
					35.2	En metod finns på plats, men är manuell eller inte fullt dokumenterad.	2	
					35.3	En dokumenterad och säker process för att bekräfta identitet används genomgående (t ex Bank-ID).	3	
					35.4	Vet ej/ingen uppfattning	1	
36	6.2.2	A4	If 35.3	Finns det spårbarhet i processen för att verifiera identitet?	36.1	Ja	4	
					36.2	Delvis	3	
					36.3	Nej	-	No change
					36.4	Vet ej	-	No change
37	6.2.2	A4	If 35.3	Sker en regelbunden uppföljning av att processen för att verifiera identitet?	37.1	Ja	5	
					37.2	Delvis	4	
					37.3	Nej	-	No change
					37.4	Vet ej	-	No change
38	1.2.5	A2		Gör ni en intern granskning av att avtal innehåller reglering av personuppgifter?	38.1	Ja	1	
					38.2	Delvis	1	
					38.3	Nej	1	
					38.4	Vet ej	1	

Legend:
Q = Question number
GAPP = Corresponding GAPP criteria
A = Attributes
Req. = Requirement for displaying the question
M = Estimated maturity level
N/A = Not applicable

A0 = General questions
A1 = Roles and responsibilities
A2 = Governance and compliance
A3 = Education and competence
A4 = Processes and tools
A5 = Risk and classification
A6 = Incident and information security management

Q	GAPP	A	Req.	Questions	Responses		M	Comment
39	1.2.5	A2	If 38.1 or 38.2	Hur omfattande är den interna granskningen av personuppgifter i era avtal?	39.1	Ingen fullständig granskning av avtalen sker, granskningar är sporadiska och informella	1	
					39.2	Grundläggande granskning sker och avtal med leverantörer har en reglering (t.ex. personuppgiftsbiträdesavtal)	2	
					39.3	En komplett granskning av avtal utförs i en etablerad process som även inkluderar återkopplande uppföljning	3	Level 4-5 depends on 52.1-52.4
					39.4	Vet ej/ingen uppfattning	1	
40	7.2.2	A4		Välj den beskrivning som bäst stämmer när det gäller skriftligt avtal som skydd för leverantörers hantering av personuppgifter:	40.1	Hantering leverantörer är ad hoc. Rutiner saknas för att utvärdera leverantörens skydd för personuppgifter.	1	
					40.2	Process finns för att säkerställa ett skriftligt avtal finns. Rutiner finns för bedömning om leverantörer har ett rimligt skydd, men är inte generellt infört.	2	
					40.3	En dokumenterad process för hantering av personuppgiftsbiträdesavtal används inklusive specifika instruktioner och kravställningar.	3	
					40.4	Vet ej/ingen uppfattning	1	
					40.5	Annat, specificera här:	-	No change
41	7.2.2	A4	If 40.3	Finns en regelbunden bedömning av processen för att teckna personuppgiftsbiträdesavtal?	41.1	Ja	4	
					41.2	Delvis	3	
					41.3	Nej	-	No change
					41.4	Vet ej	-	No change

Legend:
Q = Question number
GAPP = Corresponding GAPP criteria
A = Attributes
Req. = Requirement for displaying the question
M = Estimated maturity level
N/A = Not applicable

A0 = General questions
A1 = Roles and responsibilities
A2 = Governance and compliance
A3 = Education and competence
A4 = Processes and tools
A5 = Risk and classification
A6 = Incident and information security management

Q	GAPP	A	Req.	Questions	Responses	M	Comment
42	7.2.2	A4	If 40.3	Övervakas förändringar på tredje partens tekniska miljö för att säkerställa att de fortsatt lever upp till kravställningarna?	42.1 Ja	5	
					42.2 Delvis	4	
					42.3 Nej	-	No change
					42.4 Vet ej	-	No change
43	8.2.1	A2		Hur hanteras informationssäkerhet i relation till skydd för personuppgifter?	43.1 Skydd för personuppgifter relateras till och är underordnat arbetet med informationssäkerhet.	1	
					43.2 Skydd för personuppgifter och informationssäkerhet hanteras separat, men en integration är pågående.	2	
					43.3 Arbetet med informationssäkerhet omfattar hela verksamheten och hanteras som en del av skyddet för personuppgifter.	3	
					43.4 Vet ej/ingen uppfattning	1	
44	8.2.1	A6		Har ni en utpekad funktion, enhet eller åtgärdsprogram som systematiskt arbetar med informationssäkerhetsfrågor?	44.1 Ja	3	
					44.2 Delvis	2	
					44.3 Nej	1	
					44.4 Vet ej	1	
45	8.2.1	A6	If 44.1 or 44.2	Genomförs årliga externa granskningar av hela programmet för att utvärdera effektiviteten?	45.1 Ja	4 or 5	Level 5 depends on 52.1-52.4, else = 4
					45.2 Delvis	3	
					45.3 Nej	-	No change
					45.4 Vet ej	-	No change

Legend:
Q = Question number
GAPP = Corresponding GAPP criteria
A = Attributes
Req. = Requirement for displaying the question
M = Estimated maturity level
N/A = Not applicable

A0 = General questions
A1 = Roles and responsibilities
A2 = Governance and compliance
A3 = Education and competence
A4 = Processes and tools
A5 = Risk and classification
A6 = Incident and information security management

Q	GAPP	A	Req.	Questions	Responses		M	Comment
46	8.2.2	A6	If 44.1 or 44.2	Hur hanteras skydd för logisk access (intrångsförsök och otillåten användning)?	46.1	Tekniska system för intrångdetektering och övervakning är implementerade	2 or 3	If 46.1 and 46.2 = 3; if only one = 2; if none = 1; Level 4-5 depends on 52.1 - 52.4
					46.2	Regelbunden granskning av loggfiler för att finna spår av intrångsförsök och otillåten användning	2 or 3	If 46.1 and 46.2 = 3; if only one = 2; if none = 1; Level 4-5 depends on 52.1 - 52.4
					46.3	Vet ej/ingen uppfattning	1	
					46.4	Annat, specificera här:	-	No change
47	8.2.6	A6		Hur hanteras skydd för mobila enheter (bärbara datorer, surfplattor och smartphones)?	47.1	Rutiner och processer för en enhetlig hantering av skydd i mobila enheter saknas eller sker inte konsekvent.	1	
					47.2	Skydd för mobila enheter täcker inte alla delar. Funktioner för begränsningar finns tekniskt implementerade (t.ex. mobile device management).	2	
					47.3	Processer, rutiner och skydd för mobila enheter finns. En granskning av efterlevnaden sker. Dokumenterade tester sker av säkerheten.	3	
					47.4	Vet ej/ingen uppfattning	1	
48	8.2.6	A6	If 47.3	Hur sker arbetet med skydd för mobila enheter, som till exempel bärbara datorer, surfplattor och smartphones?	48.1	Före en enhet lämnas ut till den anställde, krävs ett godkännande av regler.	4	
					48.2	Kontroll av efterlevnaden för skydd vid överföring via nätverk och via fysisk transport.	4	
					48.3	Ett kontinuerligt arbete sker för att ta del av och implementera nya och förbättrade metoder.	5	If 48.1 or 48.2 and 48.3 = 5

Legend:
Q = Question number
GAPP = Corresponding GAPP criteria
A = Attributes
Req. = Requirement for displaying the question
M = Estimated maturity level
N/A = Not applicable

A0 = General questions
A1 = Roles and responsibilities
A2 = Governance and compliance
A3 = Education and competence
A4 = Processes and tools
A5 = Risk and classification
A6 = Incident and information security management

Q	GAPP	A	Req.	Questions	Responses		M	Comment
					48.4	Annat, specificera här:	-	No change
49	8.2.7	A6		Hur testas effektiviteten av säkerhetsåtgärder för organisatorisk, teknisk och fysisk säkerhet?	49.1	Testning av säkerheten sker sporadiskt och oregelbundet.	1	
					49.2	Grundläggande testning sker periodiskt av olika säkerhetsfunktioner. Det kan ske med varierande omfattning.	2	
					49.3	Tester av säkerhetsåtgärder och funktioner sker minst årligen. Tester genomförs enhetligt och dokumenteras av kvalificerad personal för vidare hantering.	3	
					49.4	Vet ej/ingen uppfattning	1	
50	8.2.7	A6	If 49.3	Sker en analys av tester för att finna bakomliggande orsaker (root cause) med vidare hantering för förbättringar av hela organisationens säkerhet?	50.1	Ja	5	
					50.2	Delvis	4	Level 4-5 depends on 52.1-52.4
					50.3	Nej	3	
					50.4	Vet ej	3	
51	10.2.3	A2		Hur sker hantering av kontroll av efterlevnad av regler, lagar samt andra externa och interna krav?	51.1	Efterlevnadskontroll sker sporadiskt och informellt	1	
					51.2	Efterlevnadskontroll sker regelbundet. Omfattningen är inte heltäckande eller helt dokumenterad.	2	
					51.3	Efterlevnadskontroll sker regelbundet enligt en dokumenterad process och täcker alla aspekter för efterlevnad av regler, lagar samt andra externa och interna krav.	3	
					51.4	Vet ej/ingen uppfattning	1	
52	10.2.3	A2	If 51.3	Välj på vilket sätt arbetet med efterlevnadskontroll sker.	52.1	Kvalificerad personal gör efterlevnadskontroll av interna system och tjänster	4	

Legend:
Q = Question number
GAPP = Corresponding GAPP criteria
A = Attributes
Req. = Requirement for displaying the question
M = Estimated maturity level
N/A = Not applicable

A0 = General questions
A1 = Roles and responsibilities
A2 = Governance and compliance
A3 = Education and competence
A4 = Processes and tools
A5 = Risk and classification
A6 = Incident and information security management

Q	GAPP	A	Req.	Questions	Responses		M	Comment
					52.2	Kvalificerad personal gör efterlevnadskontroll av leverantörer	4	
					52.3	Efterlevnadskontroller analyseras och granskas.	5	req 52.1 or 52.2
					52.4	Efterlevnadskontroller leder till förebyggande åtgärder för att säkerställa vidare efterlevnad.	5	req 52.1 or 52.2
					52.5	Annat, specificera här:	-	No change
53	10.2.4	A2		Hur sker rapportering av avvikelser i efterlevnad samt korrigeringar?	53.1	Sporadiskt och informellt.	1	
					53.2	Återkommande och systematiskt. Omfattningen är dock inte heltäckande eller helt dokumenterad.	2	
					53.3	En dokumenterad process och rutiner finns, inklusive eventuella disciplinåtgärder. Alla avvikelser är fullt dokumenterade.	3	
					53.4	Vet ej/ingen uppfattning	1	
54	10.2.4	A2	If 53.3	Sker en uppföljning av avvikelseprocessen som leder till ett förebyggande arbete för att möta nya avvikelser i framtiden?	54.1	Ja	5	
					54.2	Delvis	4	
					54.3	Nej	3	
					54.4	Vet ej	3	
55	10.2.5	A1		Hur sker löpande övervakning av att kontroller och riskbedömningar är effektiva?	55.1	Informellt och inte på ett konsekvent sätt	1	
					55.2	Kontroll av effektiviteten sker genom mätning, men är inte heltäckande	2	
					55.3	En dokumenterad process och rutiner finns för att regelbundet mäta effektiviteten av kontroller. Urvalet av kontroller och hur ofta de sker baseras på riskbedömning.	3	Level 4-5 depends on 13.1-13.3

Legend:
Q = Question number
GAPP = Corresponding GAPP criteria
A = Attributes
Req. = Requirement for displaying the question
M = Estimated maturity level
N/A = Not applicable

A0 = General questions
A1 = Roles and responsibilities
A2 = Governance and compliance
A3 = Education and competence
A4 = Processes and tools
A5 = Risk and classification
A6 = Incident and information security management

Q	GAPP	A	Req.	Questions	Responses	M	Comment
					55.4 Vet ej/ingen uppfattning	1	
56	N/A	A0		Har du några kommentarer eller synpunkter? Beskriv här	56.1		

Legend:
Q = Question number
GAPP = Corresponding GAPP criteria
A = Attributes
Req. = Requirement for displaying the question
M = Estimated maturity level
N/A = Not applicable

A0 = General questions
A1 = Roles and responsibilities
A2 = Governance and compliance
A3 = Education and competence
A4 = Processes and tools
A5 = Risk and classification
A6 = Incident and information security management

Appendix 4 – Privacy risks areas in the municipalities

Report nr: 2019:009

Summary of risks related to Swedish municipalities identified in a report by to the Privacy Committee (SOU 2016:41)

A Swedish Government parliamentary committee outlined IT-related risks of breaches of privacy in society in the report *Hur står det till med den personliga integriteten? – En kartläggning av Integritetskommittén* (Integritetskommittén, 2016) and draws the conclusion that the individual's privacy is diminishing in a number of areas. The committee have classified risks in three levels; some risk, obvious risk and serious risk.

A summary of privacy risks and risk levels relevant to municipalities

Area of concern	**Risk level**			**Comments**
	Some	**Obvious**	**Serious**	
School	Learning analytical methods and working methods gain ground and begin to be used by schools and system suppliers, which gives rise to general risks for "digital tattoos", which characterize and follow students through the education system and later the working life.			
Digital learning platforms and teaching aids			x	Information can be used for entirely new purposes without the possibility of transparency. Free services have personal information and profiling as a business concept — weak privacy protection.
Social media in teaching			x	Unwanted confusion of data by the private and school-related. Difficult for students to abstain.
Student Health	x			Sensitive data, but detailed regulations exist and apply.
Single-sign-on	x			Single-sign-on may entail a risk that sensitive personal information will get more spread than desired, but generally, school federation gives better privacy protection.
Camera surveillance in schools		x		It is regulated in the camera surveillance law and seen as relatively close-knit that cameras capture students' everyday life. Decisions are often made at a lower level; the reason is inadequate and not documented.

Legend:
Q = Question number
GAPP = Corresponding GAPP criteria
A = Attributes
Req. = Requirement for displaying the question
M = Estimated maturity level
N/A = Not applicable

A0 = General questions
A1 = Roles and responsibilities
A2 = Governance and compliance
A3 = Education and competence
A4 = Processes and tools
A5 = Risk and classification
A6 = Incident and information security management

Area of concern	Risk level			Comments
	Some	Obvious	Serious	
Working life	A definite risk is a shifting purpose when employers digitally handle information about employees. Legitimate interests can be applied to employees also for authorities, in their role as employers. The Data protection authority has been historically relatively permissive. Risks of weakening for workers and exclusion from working life.			
Positioning and other monitoring of activities and behaviours			x	Employees have few opportunities to influence because of the employers supervisory right according to the managerial prerogative and employees lack knowledge. It is a risk that the purpose of positioning glides over in other purposes. It is also difficult to control due to the use of external suppliers (cloud services)
Social Media	x			The employer enters a private sphere, but easy for workers to restrict access to statements that may be sensitive or controversial.
Expertise databases and background checks	x			Individual tasks may be sensitive, but dissemination is likely to be limited.
Camera surveillance			x	Many employers misuse protective legislation and use camera surveillance for other purposes.
Healthcare and social services	The healthcare system has many challenges and extensive regulations regarding how sensitive information should be handled and at the same time, amounts with actors nationally, regionally and locally. Several supervisory bodies exist, and it is difficult to give a general assessment.			
Healthcare			x	Quantities of risks have been identified due to shortcomings in management, compliance, coordination, complexity, interoperability, information security, information sharing. Amounts of sensitive information are not properly handled — dangers of spreading personal data.
Welfare technology and digital services within the social services			x	Digitisation such as camera surveillance, GPS transmitters, robots and sensors etc. involves close management. Unclear legislation on how individuals with reduced ability to make decisions can be offered services using welfare technology. Lack of responsibility for how tasks are handled.
E-government	The individual has little influence over authority management. The technical development poses a risk of unwanted dissemination of personal data.			

Area of concern	Risk level			Comments
	Some	Obvious	Serious	
Information management within and between different authorities		x		A risk that sensitive information is not handled correctly in communication between authorities. Personal information can spread to administrators who do not need to take part in these.
Information exchange with individuals	x			Design of e-services can provide inadequate protection. Data can be disseminated following an antagonistic attack (cyber-attack) directed against the authority.
Authorities with information in the cloud and the lack of client expertise			x	External parties can handle a large number of sensitive personal data and general risks are deficiencies in competence, regarding the application of information security, law and requirements.
Authorities in social media and with like buttons on the web	x			A risk that sensitive personal data ends up in third countries without the existence of exact legal mechanisms and that third parties are profiling individuals unlawfully.
PSI legislation		x		Hard to apply and partly unclear legislation, which can lead to incorrect assessments and the risk that personal data will be discharged and also involves an unauthorised shifting of purpose.
Citizen profiling and online controls			x	Difficult to control how authorities use personal data to make predictive analyses (analyse applications with other data and with statistical patterns find potential risks) for preventive control activities.
Information Security (Application)			x	The majority of municipalities do not work systematically with information security, which means that there is a risk that sensitive personal data can be discarded.
Other issues				
Cloud Services			x	Often, there is a lack of a comprehensive risk and vulnerability analysis and incorrect assumptions about the service provider's security activities. Loss of transparency and control involves the risk that you will be handled for the providers own purposes. Free services are often based on the supplier's desire to use personal data for their purposes. Hard to know where data are stored are physically. A risk that data stored in third countries

Area of concern	Risk level			Comments
	Some	Obvious	Serious	
				are being examined by foreign authorities' law enforcement authorities, without the possibility of transparency.
Big data			x	The basic idea of big data is difficult to reconcile with privacy protection. The principle is based on the belief that all data can be useful in the future. The purpose cannot be foreseen, and thus, any consent becomes unclear. Co-processing of large amounts of data means that anonymous data can be re-identified — dissemination of personal data to parties that are not known to the individual. Influence and knowledge are lost.
Biometry		x		Cheaper technology in combination with biometric data (many different biometric techniques) and other data handled digitally, can make identification of individuals easy (for example, facial recognition), making it difficult to remain anonymous. DNA can reveal health, disease or ethnic origin. Identity theft risks. Risk of over-utilisation and shifting purposes.