Universiteit Leiden

ICT in Business

Right of Subject Access

From request to response:

An analysis of process performance

Name: Roger Howard

Student-no: 1315951

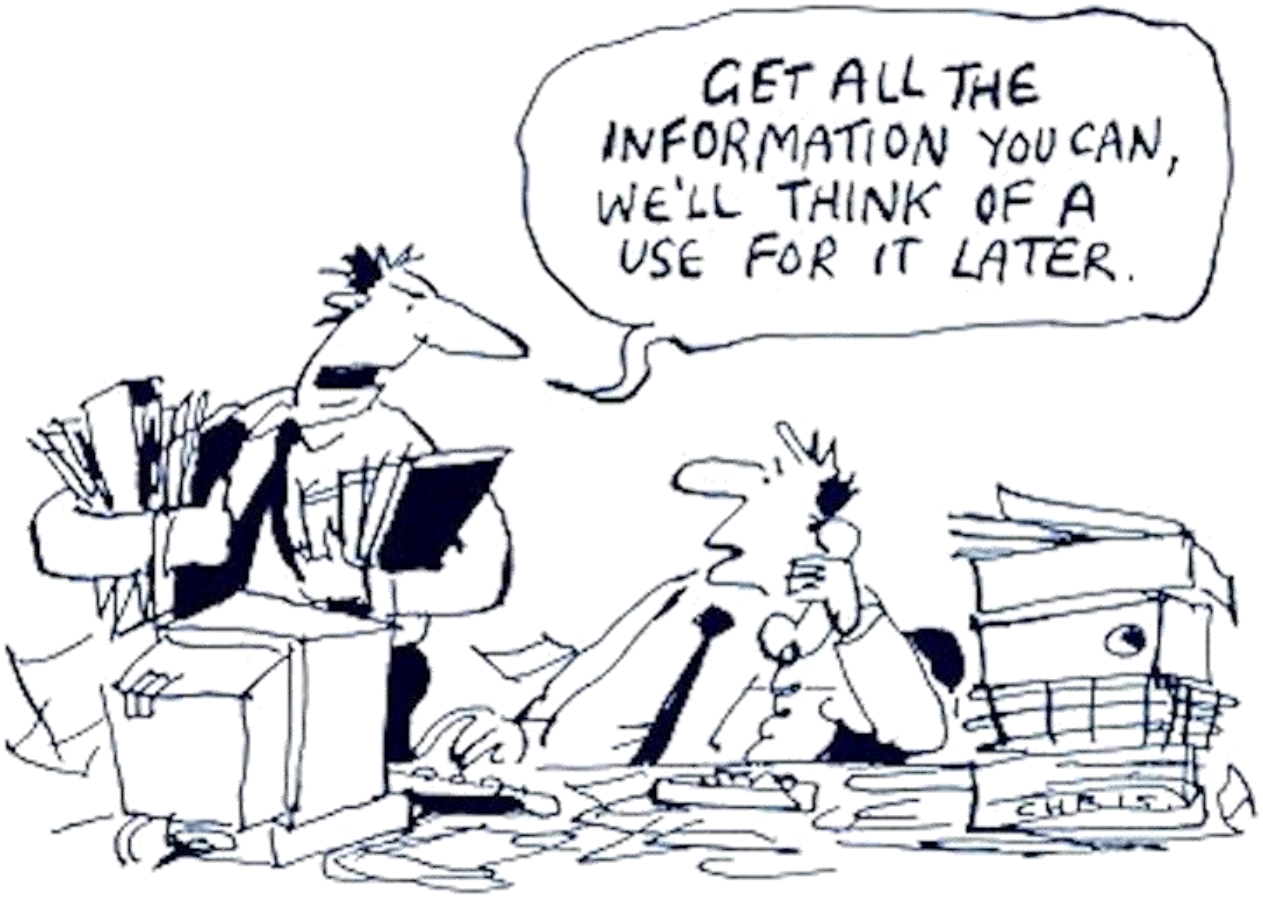
Date: 17/12/2015

1st supervisor: Dr. M. ter Beek

2nd supervisor: Prof. Dr. N. Kok

MASTER'S THESIS

Leiden Institute of Advanced Computer Science (LIACS)
Leiden University
Niels Bohrweg 1
2333 CA Leiden
The Netherlands



Source: Google Images

PREFACE

This thesis marks the successful completion of my Master in ICT in Business at the Leiden Institute of Advanced Computer Science (LIACS) on the alignment of ICT and management. It has been an exciting intellectual journey, in which I learned a lot of new and interesting insights and had to re-learn academic skills that had sunken away in the last 25 years in business, but are ever so important in doing a good job.

The topic for the thesis was chosen for the interest in the preservation of privacy in a digitally accelerating world where business survival depends on being a master of data, but also in being transparent about it. An important business process to implement for transparency is the right of Subject Access. The goal of this thesis is to help achieve a better understanding and appreciation for the importance of the process for companies and government to provide insight why Personally Identifiable Information is collected and stored and to prevent future consumer/patient/student/citizen friction over it, as they grow in understanding the value and risks of personal data in the digital age.

SUMMARY

The Dutch data protection law requires from organisations that any personal data that is collected at all times is clearly defined, clearly described and justifiable. Leading in the law is the principle of transparency.

Research problem

Organisations have difficulty to comply with Privacy regulations and be as transparent as they can be. This can be derived from the fact that organisations show poor performance in responding to right of subject access requests. This prompts to search what disruptive factors within organisations diminish the ability to respond properly and what can be done to eliminate and/or mitigate them.

Main results

The four researched financial and government organisations, three of them with millions of customers, serve but not actively promote Subject Access (SA) as a means of transparency. An active promotion is considered, directly or indirectly, as to taxing for an organisation. Subject Access is kept as 'little' as possible and therefore is not in the picture for continuous improvement and enhancement. The 'little' that is done is managed in such a way that the organisational ripples of it do notrock the boat. Not one of the investigated cases evaluates its SA maturity level substandard and in need of improvement. For this research the proof was in eating the pudding and three of the four organisations showed a substantial difference between the perceived SA maturity and the SA response that was received. The financial organisations even showed the worst responses and because of this the hypothesis that financial organisations would prove to be the better 'organisers' to provide the best possible responses had to be rejected.

Conclusion

This case study shows that to improve the right of SA process, it is important to:

- Centralize request receipt;
- Standardize the SA response on the basis of the legal requirements. Build a Response template and use that as the basis for a reverse process design;
- Build and maintain an Application register for all systems handling personal data and get a good overall view of 'the Wood';
- Develop a 'Meta data application' to be able to discover and find in which applications someone is registered ('Know the trees in the wood');
- Audit regularly and keep the 'privacy spirit' of business managers and employees alive;
- Appointment of a Chief Privacy Officer, to be a motivator of appointed 'privacy advocates' (super-users) throughout the organisation who are his liaisons to business managers.

Discussion

Data privacy is getting a place at the compliance table and as the youngest kid on the block it is not always taken as serious as it should be. Every week new data privacy incidents show that serious harm can be done to the reputation of an organisation. Customers slowly, but steadily, start realizing that their personal data not only can be of help but also become a burden when it gets in the wrong hands. The time has come for both organisations and customers to actively keep track of it. To make this happen the first has to be transparent, the latter aware and critical about the response received.

ACKNOWLEDGEMENT

The author thanks Dr. Maurice ter Beek for his support and input during his visiting year to LIACS and later for seeing it to an end after he returned to the National Research Council (CNR) of Italy in Pisa.

Furthermore, I also extend my gratitude to Professor Joost Kok who has played an important role in making 'things' possible and happen.

However, I am and always will be grateful to the support and patience of my lovely wife Helene. She has been a good listener and on many occasion pointed me in the right direction when I was wandering too far off. And our three wonderful children that had to put up with a father who spent a lot of his time reading and studying and less of the normal 'dad stuff'.

I also want to thank all the wonderful people I met because of my academic journey and with whom I had interesting discussions and shared many 'aha-erlebnissen'.

TABLE OF CONTENTS

ABBREVIATIONS

AC-PMM	AICPA/CICA Privacy Maturity Model
AFM	The Netherlands Authority for the Financial Markets
AICPA	American Institute of Certified Public Accountants
Awb	Algemene wet bestuursrecht (General Administrative law)
BPM	Business Process Management
CbD	Compliance by design
CBP	Dutch Data Protection Authority
CICA	Canadian Institute of Chartered Accountants
CMM	Capability Maturity Model
DPO	Data Protection Officer
ECHR	European Convention on Human Rights
ECJ	European Union Court of Justice
EU	European Union
FG	Functionaris voor de Gegevensbescherming (Dutch DPO)
GAPP	Generally Accepted Privacy Principles
LFO	Large Financial Organisation
LGO	Large Governmental Organisation
OECD	Organisation for Economic Cooperation and Development
P3P	Platform for Privacy Preferences
PbD	Privacy by Design
PET	Privacy Enhancing Technologies
PIA	Privacy Impact Analysis
PII	Personally Identifiable Information
PMM	Privacy Maturity Model
SA	Subject Access
SAM	SA-Maturity
SAR	SA-Response
Wbp	Wet bescherming persoonsgegevens

1 Introduction

1.1 Background

"when something online is free, you're not the consumer, you're the product." (Szilvasi, 2012)

More and more Personal data is getting mined intensively, constantly processed and refined in search of the best personal profiles that can best predict the outcome of (non-)commercial actions towards its owners.

Although privacy has no price tag and it seems hugely discounted, people, customer or patient, student or citizen, are slowly growing to be aware of what is happening and are starting to value their privacy in its own right. Like with fresh air and water, which also has no price tag on it, it is of great value. Once it has been depleted, there is no getting it back. So, like a growing group of concerned consumers expect from organisations to produce in an environmentally conscious way, it is also becoming standard that organisations are expected to take care and treat personal data in the same conscious way.

Organisations need to be transparent about what personal data they have gathered and what objectives they have with it, so that people have the possibility to inquire what is done with their personal data. As the amount of data generated from internet, mobile, social media and smart TV's is exploding, wrong assumptions on the basis of data, leading to wrong decisions will inevitably become a part of living in a highly digitized society. When this happens it is of utmost importance for individuals to be able to set things (data!) right.

The Dutch data protection law requires from organisations that any personal data that is collected at all times is clearly defined, clearly described and justifiable. Leading in the law is the principle of transparency. Meaning that to anybody whose personal data is kept and inquires why this is done, it must be made clear what happens with it and why. The purpose of collecting personal data must be made transparent. This is called the right of subject access. Commonly referred to as subject access (SA).

Everybody in the Netherlands can exercise his SA on a regular base, within reason. From what is learned from a SA can result in exercising another right: The right of revision. The revision means improve, add, delete, conceal or in other ways make sure that erroneous data is not used any longer.

At the beginning of 2012 a journalist from a Dutch IT website tested 25 organisations for which he could exercise his SA. From the 25 only two were able to provide him an answer in accordance with the instructions set in the Dutch law (Wet bescherming persoonsgegevens: Wbp) (Vermeer, 2012). The majority was not able to give a response within the legal term and when he received the information it stated only the personal information that was collected but not what was done with it and why. When he inquired at the organisations why they failed to comply he was mostly told that papers of the request had gone from department to department, with nobody having a clear notion what had to be done. Also the request had a tendency to get lost in the response process, which maybe endemic when there are no obvious procedures what to do in such a case.

It seems that organisations are getting increasingly efficient in the collection and subsequent processing of personal data but not in keeping track of the purpose of the modus operandi and in informing the persons themselves.

The problem statement for this thesis is:

Organisations have difficulty to comply with Privacy regulation. This can be derived from the fact that organisations show poor performance in responding to right of subject access requests. This prompts to search what disruptive factors within organisations diminish the ability to respond properly and what can be done to eliminate and/or mitigate them.

1.2 Research scope

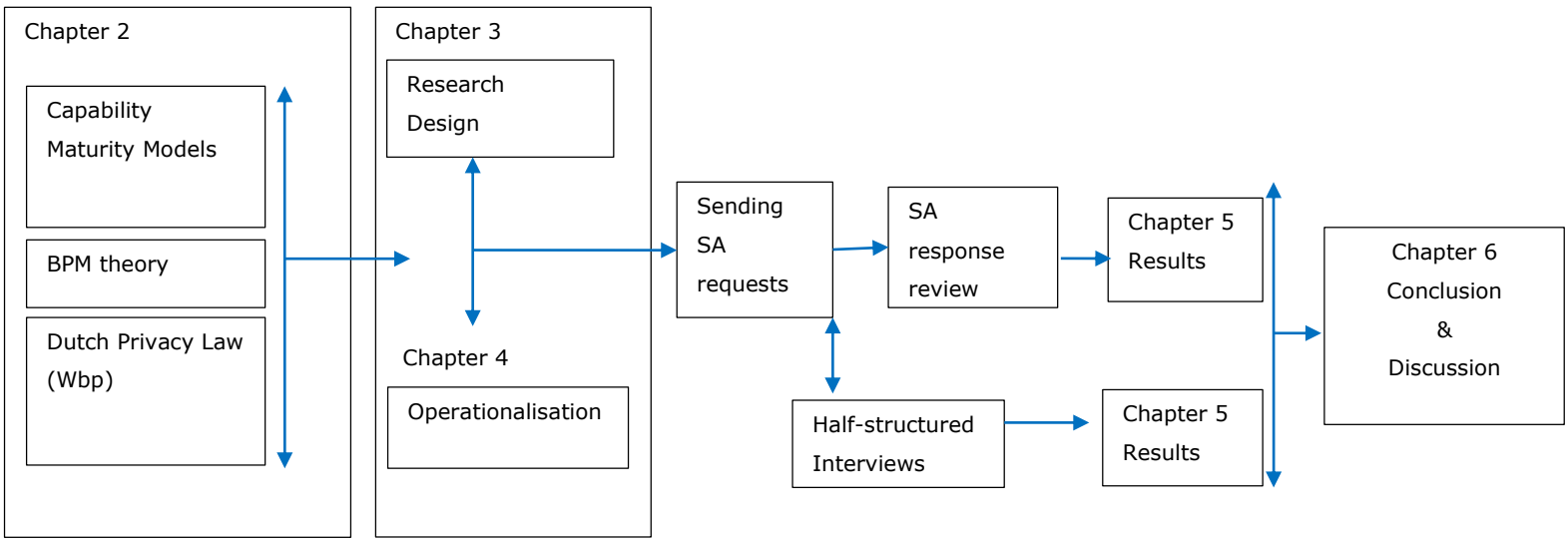
1.2.1 Objective

The objective of this research is to come to recommendations for the improvement of the Right of subject access obligation of organisations by obtaining insight in and understanding of the process performance of composing a response for a request.

The assumption is that organisations that are more process oriented have less difficulty responding to right of subject access requests than organisations with a lesser orientation.

1.2.2 Research model

Prior to formulating the research question a research model was composed, as advocated by Verschuren en Doorewaard (2010). This model schematically depicts what steps will be made to accomplish the objective of the research. In the diagram below the steps are shown by the rectangles.



1.2.3 Research questions

On the basis of the problem statement, the objective derived of it and bifurcation of the research model, the following main research question and sub questions are defined:

Main research question:

> **How can the right of subject access process within organisations be improved to deliver timely and adequate responses?**

Sub questions*:*

> **1. What circumstances and bottlenecks surrounding the response process can be identified within an organisation?**

We do this by interviewing employees who manage and contribute to responses and to learn about the response process and their view on the preparedness and professionalism of their organisation in the matter. The interviews will result in a privacy maturity level. The level of privacy maturity of an organisation is expected to determine the quality of a response. This leads us to the second research question:

> **2. What is the quality of a response to a right of subject access request in accordance with the legal requirements?**

The privacy maturity results will be compared with the performance on the response review criteria. This leads us to the third research question:

> **3. What can be learned from the comparison of the analysis of the findings on privacy maturity and response quality to come to recommendations for an effective process around right of subject access?**

1.3 Structure of the thesis

This master thesis has the following chapters, the main contribution of a chapter and the relation between them.

Chapter 1: Introduction
In this chapter the reason for this research is explained and what the goal and scope of the thesis is.

Chapter 2: Review of related literature
Responding to Right of subject access requests depends on an organisation' intention to comply and to comply with privacy laws it has to implement certain processes. Related literature on Data protection, Compliance (by design), Business Process Management and Privacy by Design (PbD) is reviewed in relation to Privacy law in general and Right of subject access in particular.

Chapter 3: Research design
This chapter describes available methods, what is appropriate and feasible for this research.

Chapter 4: Operationalisation
In this chapter the choices are made how the variables, determining the quality of the right of Subject Access, are defined into measurable factors. As the measurements are of ordinal nature and as such are fairly arbitrary, it is here where the rigour of the research is determined.

Chapter 5: Findings, Analysis & Results
The analysis of results of the research. The results of the process of analysis followed is by answering the research questions.

Chapter 6: Conclusion & Discussion
Conclusions, or better directions, on the basis of the research results. In the discussion an analogy is made with a different and former 'impossible' situation to emphasise that also for Subject Access a higher level of ambition is possible.

2 Review of related literature

2.1 Privacy under siege

2.1.1 Personal data dragnet

The term privacy is an umbrella term, with many different meanings for many different people. Looking at information privacy "…new technologies have given rise to a panoply of new privacy harms." (Solove, 2006). The focus in this research is on the collection and processing of information relating to an individual's identity and an individual's right to control his/her personal information/data through exercising his/her right of subject access.

From PCs, tablets and smartphones to web portals, social media sites and smart meters, everybody is, knowingly or unknowingly, 'contributing' to an ever growing mountain of data collected by all sorts of organisations; public and commercial. Everybody pays contribution by leaving their trails of data behind through communicating, browsing, buying, sharing and searching. Trails of the alternate roles everybody plays in life, as a customer, patient, student, citizen, et cetera. And the lure of new technological advancements are widening the digital trails left behind. For instance Google Now and Apple's Siri, aptly marketed as virtual assistants, only get better the more data they collect of a person.

The latest disclosures of Edward Snowden and the Guardian on top-secret U.S. data surveillance and all sorts of collection and intrusion programs in the war against terrorism, is regarded by many as the pinnacle of privacy intrusion. The need for information privacy is becoming increasingly constitutional for the information age.

2.1.2 Data maximisation concerns

With 6 billion mobile telephone subscriptions (International Telecommunication Union, 2012), and counting, in the world, and the phones getting smarter and smarter through the apps installed on them, it is more the rule than exception to track the location of everybody, as well as their social connections and transactions. To learn more about customers is to offer them desirable applications.

The expansion of access to abundant data and the diminishing prices of IT technology to mine it ('Big Data'), are enabling organisations to increasingly predict and respond to individuals behaviour and excel in 'one-to-one marketing', which is called by critics a euphemism for surveillance. The personalisation of interactions is generally considered to foster greater customer loyalty.

Data maximisation is growing in importance as a business objective and gradually becoming synonymous with profit maximisation. According to the Boston Consulting Group (BCG), the financial value that companies derived from personal data in Europe was $72 billion in 2011. But BCG states in her report that "personal data has become a new form of currency", and that not only organisations will gain from the 'spending' of personal data, reaching an annual economic benefit of € 330 billion by 2020, but consumers even more: € 670 billion a year by 2020 (Boston Consultancy Group, 2012).

On the flipside seventy percent of Europeans are concerned that their personal data held by companies may be used for a purpose other than that for which it initially was collected. For a growing flood of people Big Data is becoming synonymous with privacy intrusion and concerns are growing (McKinsey Global Institute, 2011; Arnbak & Van den Berg, 2011; Attitudes on data protection and electronic identity in the European Union, 2011; Bloem, Van Doorn, Duivestein, Van Manen, & Van Ommeren, Privacy, technologie en de wet. Big Data voor iedereen door goed design, 2013). The growing numbers of security breaches and the loss of millions of records contribute to these concerns. Breaches involving personal data are hazardous to both individuals (e.g. identity theft) and organisations (e.g. loss of public trust, legal liability)

In Smith et al., four dimensions of privacy concerns about organizational information privacy practices have been identified. These are (1) the collection and storage of large amounts of personal information data, (2) the unauthorised secondary use of personal data, (3) the errors in collected data, and (4) the improper access to personal data due to managerial negligence (Smith, Milberg, & Burke, 1996). The addressing of these privacy concerns is not just a matter of compliance by adhering to privacy and data protection laws or implementation of technological measures but a matter of close alignment of both aspects to give clear answers to questions as why data is collected, why it is shared with other parties, why it has been enriched, how it can be checked and changed if necessary. Yet for many organisations giving clear answers, when called upon, is not 'business as usual'.

Governments and organisations need to work closely together to eliminate the gnawing fear of people that the end of privacy is near and they will become prey to the perils of data profiling in the name of efficiency, productivity and profit (Garfinkel, 2000; Tokmetzis, 2012; Bloem, Van Doorn, Duivestein, Van Manen, & Van Ommeren, Big Social. Predicting behavior with Big Data, 2012). The new EU Regulation for data protection and the recently proposed "Right to Know" bill in California are necessary democratic evolutions to establish the trust of the public through a new system of supervision for organisations processing personal information, and at the same time making it possible to reap the macro-economic benefits of it.

2.2 Information protection and control

2.2.1 Privacy

Privacy laws are considered in the context of an individual's privacy rights or reasonable expectation of privacy. All the member states of the European Union are signatories of the European Convention on Human Rights (ECHR), which entered into force on 3 September 1953. Article 8 of the ECHR provides a right to respect for one's "private and family life, his home and his correspondence," subject to certain restrictions. Thus privacy as a broad concept. Solove (2006) notes that privacy is a difficult concept to grasp and that "privacy problems are frequently misconstrued or inconsistently recognized in the law" (p.481). Article 8 therefore has been, and still is, subject of very broad interpretation.

Privacy is frequently defined in terms of control over information about ourselves. So Information privacy "the ability (i.e., capacity) of the individual to control personally (vis-à-vis other individuals, groups, organisations, etc.) information about one's self." (Stone, Gardner, Gueutal, & McClure, 1983, p.2), also called data privacy, is seen as an important issue because, "Information Technology (IT) continues to increase in capability and to decline in cost, allowing information to be used in ways that were previously impossible or economically impractical." (Culnan & Armstrong, 1999). The collection and processing of information relating to an individual's identity, or 'personal data' is defined by the European Data

Protection Directive, through 'Opinion 4/2007 on the concept of personal data', as follows (Article 29 Data Protection Working Party, 2007):

"Personal data shall mean any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity".

The ultimate purpose of the rules contained in the Directive is to protect individual' rights with regard to the processing of personal data. The processing of personal data is a comprehensive concept and is described as follows in the Dutch Data protection law (Wbp):

Processing refers to any operation or set of operations which is performed upon personal data including anyway the collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure, transmission, dissemination or otherwise making available, assembling, interrelating and the blocking, erasure or destruction of data. (Sauerwein, L.B.; Linneman, J.J., 2002, p13)

Any party who asks for personal data has to state in advance for what reason(s) and objectives it is done (purpose specification). And only to collect 'precisely' the personal data that is needed for the objective. After storing it in a structured way, either in a rolodex sort of way or with computers, one becomes responsible for it. Only under strict conditions data collected can be used for other purposes than those for which they were originally collected (purpose limitation). This requires that measures have to be taken to monitor the processing of personal data to be able to track and report afterwards that everything done with it was necessary and with good reason.

As can be inferred from the above it is quite clear that the protection of personal data is by no means an easy task to organise. The measures that need to be taken, necessary to keep track of personal data, in terms of organisation, processes and IT can be quite extensive and therefore costly. And even more so when doing business in different countries. This feeds on the inclination of a lot of organisations to postpone necessary steps and take their chances getting caught.

The growing number of media reports on information privacy violations, bad decisions on the basis of wrong profiles, indicates that prudence with regards to data collection and processing should be the way to go for organisations. Even so since empirical evidence shows that organisations can even gain a competitive advantage by behaving ethically and when concerns about privacy are addressed by fair procedures (Culnan & Armstrong, 1999).

Ethical organisational behaviour that would come from understanding concepts like the 'right to be forgotten', already mentioned, which originates from Professor Mayer-Schönberger of the Oxford Internet Institute, makes a point that humans needing to make decisions about the present and the future also need to forget, which enables us to think in the present. But digital memories will only remind us of the failures of our past, so that we have no ability to forget or reconstruct our past. Grasping such concepts will make organisations understand that deleting personal data in time, is just as necessary as collecting it (Mayer-Schönberger, 2011; Druschel, Backes, & Tirtea, 2011). The recent ruling (may 2014) by the Luxembourg-based European Union Court of Justice (ECJ) that people can request Google to delete sensitive information

from its Internet search results, could be seen as an endorsement for the supporters of privacy rights, who pursue the possibility for people to be able to remove their digital traces from the Internet. The dollar per gigabyte storage ratio should not be the only consideration to hold on to personal data that can affect someone's life.

The information privacy struggle can, with some imagination and stretching, be compared to the succession of child labour laws, the so-called Factory Acts, at the start of the industrial revolution two hundred years ago to curb the economic urge to permit child labour. "Children younger than nine were not allowed to work, those aged 9-16 could work 16 hours per day per Cotton Mills Act. In 1856, the law permitted child labour past age 9, for 60 hours per week, night or day. In 1901, the permissible child labour age was raised to 12" (Child Labour, n.d.). Maybe in 25 years from today the information revolution and the start of privacy regulations and concepts as the 'right to be forgotten', will make as much sense as child labour laws do now.

But at the time predominantly economic considerations are the main driver when it comes to business decisions in information matters. Data storage prices keep on dropping, making data hoarding the modus operandi. Also the authorities within the EU countries do not have enough resources to supervise data protection laws comprehensively, the risk of paying a penalty of € 4.500 per incidence for non-compliance within the directive is so little that it does not outweigh in any way the costs for organisations to pursue compliance. Even if they would have to pay € 4.500 per incidence several times, it makes business sense to take the risk. And apparently the risk of the management going to jail for six months (maximum sentence) for non-compliance is either not very known or deemed very unlikely to happen.

Research confirming the lack of enforcement of Data Protection Acts throughout the EU, although specifically for providers (i.e. news portals, web shops, auction platforms and messaging services), point very much in that way (Burghardt, Bohm, Buchmann, Kuhling, & Sivridis, 2010). To move organisations in the right direction apparently more 'stimulation' has to be administered.

Koops (Arnbak & Van Den Berg, 2011) argues that the last fifteen years of ex-ante control of the collection and processing of data have proven not to work and that the focus should be redirected towards ex-post control of the decision processes. Organisations should be transparent on how they have come to decisions on the basis of the data collected. Although the paradigm shift of Koops has its intellectual merits, it is far from practical. Ex-post control of a decision process will also require insight in the collection and processing of data leading to a decision. From a practical standpoint it makes more sense to control the data that goes in a decision process than making sense of what came out.

2.2.2 Data Protection

The invasion of someone's (information) privacy is generally regarded as a serious matter and therefore something that has to be prevented. Data protection is focused on information privacy issues. The focus in this research is on the collection and processing of information relating to an individual's identity, known as 'Personally Identifiable Information' (PII), personal information or personal data, and the protection of it.

In an effort to create a comprehensive data protection system throughout Europe the Organisation for Economic Cooperation and Development (OECD) issued in 1980 the 'Guidelines on the Protection of Privacy and Transborder Flows of Personal Data' (OECD Guidelines on the Protection of Privacy and Transborder

Flows of Personal Data, n.d.). A set of principles for national and international use with regard to information privacy issues.

The seven principles governing the OECD's recommendations for protection of personal data were:

- Notice—data subjects should be given notice when their data is being collected;
- Purpose—data should only be used for the purpose stated and not for any other purposes;
- Consent—data should not be disclosed without the data subject's consent;
- Security—collected data should be kept secure from any potential abuses;
- Disclosure—data subjects should be informed as to who is collecting their data;
- Access—data subjects should be allowed to access their data and make corrections to any inaccurate data; and
- Accountability—data subjects should have a method available to them to hold data collectors accountable for following the above principles.

Article 8 of the ECHR and the OECD principles have played an important role in harmonising national laws and to impel member states to consider privacy protection aspects into national laws. The Data Protection Directive (officially Directive 95/46/EC) from 1995 is a European Union directive which regulates the processing of personal data within the European Union and in many ways mirrors the OECD principles (Zwenne, Privacy and the protection of personal data in Europe, 2012). The Data Protection Directive is nonbinding, and being a directive, intended to guide or influence; therefore data privacy laws vary across European member states.

With the intention only to guide, definitions within the Regulation are prone to varying interpretations, of which some then need to be elaborated upon. In 2007 the Article 29 Working Party, an independent European advisory body on data protection and privacy, set up under Article 29 of Directive 95/46/EC and named after it, had to "come to a common understanding of the concept of personal data, the situations in which national data protection legislation should be applied, and the way it should be applied." (Article 29 Data Protection Working Party, 2007, p3)

The varying breadth and depth of implementations of the directive within EU countries has proven to be a costly administrative burden. Organisations doing business within the EU have to deal with 27 different national data protection laws. Some countries have very strict (Germany, Netherlands) interpretations of the Directive and others less strict (Spain) (Privacy and Data Protection by country, 2013). Alleviating organisations from the administrative burden of different compliance levels, is one of the main drivers for the ongoing 'upgrade' of the Directive, but also to build individuals' trust in e-business. (How will the EU's data protection reform benefit European businesses?)

The new data protection rules will not be a directive any more, but a regulation. The regulation largely repeats the Directive but adds to and varies it, but with the big difference that the regulation is binding in its entirety and each EU member state has to accept the same definitions. The regulation will not allow countries the opportunity to interpret the ruling in different ways, like the current directive. Regulations are directly applicable under EC Law, which means that they automatically become part of National law of the 27 Member States and so nullify all the separate Data Protection Actions. This will be the case in 2015 or 2016, depending on when the Directive is ratified.

Technological developments and the intertwined boost of globalisation since the inception of the Data Protection Directive in 1995, also make an overhaul due. Under consideration are data portability (article 19), which is of growing importance because of the rapid growth of cloud services. The enhancement with modifications and additional safeguards to the right not to be subject to measures based on profiling (article 20) because of the fast technological advances made in Big Data. And the aforementioned 'right to be forgotten'. For the latter an organisation would have, in addition to deleting personal data, also need to take all reasonable steps and technical measures to inform others using this published content that they are requested by the individual to erase any links to, or copies of, the data. This point is still under discussion and deemed impossible by some, but as EU commissioner Viviane Reding (Justice) aptly noted, compliance to it should not be more cumbersome than what is done for current copyright laws. (Hern, 2014)

Beneficial to comply to the 'right to be forgotten' would also be if the focus would be more on the development of methods and techniques that aim at preventing the unwanted collection and dissemination of information (Druschel, Backes, & Tirtea, 2011). Privacy by Design (PbD) has been pointing in that direction for over twenty years and is gaining support the last few years.

2.3 Privacy by Design

2.3.1 Privacy= de facto standard

On October 29, 2010, Dr. Ann Cavoukian's concept of "Privacy by Design" was unanimously adopted at the 32nd annual International Conference of Data Protection and Privacy Commissioners. This recognition makes it a sort of de facto standard for developing privacy-compliant information systems. The Article 29 Data Protection Working Council positions it actively as an intrinsic "common sense" approach that is "underpinned by the language and logic of regulatory principles" (Davies, 2010, p.6). This viewpoint will undoubtedly have contributed to the requirement in the draft EU Data Protection Regulation to implement "Privacy by Design" rules (article 23).

Cavoukian started 20 years ago by framing privacy as an issue of control, the need to maintain personal control over the collection, use and disclosure of one's personal data. Arguing that good privacy practices are good for business: "Privacy breaches can have profound and long-term adverse consequences, including significant financial impacts and damage to the brand and reputation of organizations" (Cavoukian, 2012, p.5.; Acquisti, Friedman, & Telang, 2006). Unfortunately there seems to be no solid business case (yet?) to be made that can prove that gaining and maintaining trust through investments in PbD leads to competitive advantage (Rubinstein, 2011).

PbD has over those years grown into a mature framework for embedding privacy and data protection throughout the entire life cycle of technologies, from the early design stage to their deployment, use and ultimate disposal. Regulatory focus is slowly shifting toward the design of the systems, not just the policies that govern them (Rubinstein, 2011).

Privacy by Design is all about establishing trust and seven principles are leading in this:
1. Proactive not Reactive; Preventative not Remedial
2. Privacy as the Default
3. Privacy Embedded into Design

4. Full Functionality - Positive-Sum, not Zero-Sum
5. End-to-End Lifecycle Protection
6. Visibility and Transparency
7. Respect for User Privacy
(Cavoukian, 2012; Davies, 2010; Rost & Bock, 2011)

These seven principles must be implemented with a holistic view on the entire organisation' operational practices. "…Building privacy (e.g. data minimization) into technological advances which seek to capture, store, manage, and analyze personal information." (Cavoukian, 2012). Operationalised in (information) systems but also in the work processes, procedures and management structures aligned to it. "PbD is focused on processes rather than a singular focus directing technical outcomes." (Cavoukian, 2013). PbD adds process thinking on top of Privacy Enhancing Technologies (PETs), e.g. anonymous communication (e.g. TOR), data minimisation technologies (blind signatures), privacy policy languages (P3P) and other 'tools'. The approach is based on the principle that that reliable protection in a complex ecosystem can only be achieved through an integrated design approach (Davies, 2010, p.2). But Davies also points out "The drawback is that the approach is in danger of suffering the same shortcomings as a reliance on legal protections" (p.4). A valid point because it is not feasible that principles will succeed where legal protections and enforcement are already proving to fall short.

Fortunately PbD has next to its regulatory stance an engineering side to it. An engineering side that needs an approach for the translation of privacy principles to a functional requirements level that gives direction for the development of PETs. Dix states that "Privacy by Design is no panacea because there is no simple technical fix for complex privacy challenges, but without privacy by design, it will be difficult if not impossible to achieve meaningful privacy protection in the twenty-first century."(2010). Privacy engineers, IT technologists with an appreciation for the interplay of technical, business and legal issues, are a rare breed momentarily but the growing need for them will make it a full blown profession. A rare breed that always is watchful for data minimization possibilities, a foundational PbD principle, and for data creep: The gathering of more PII than necessary.

2.3.2 Web tracking

A cookie is a small text file that a website stores on a computer to help keep track of individual preferences of visitors, like to stay logged into a website; store passwords and forms a user has previously entered, such as a credit card number or an address. With third-party tracking cookies organisations went overboard, compiling long-term records of individuals' browsing histories and sharing it with affiliates and building affiliate networks to learn as much as possible of users every (internet) step. When this grew bigger and bigger with more and more organisations jumping on the band wagon, privacy concerns grew, leading to the EU Cookie law. Some argue that if organisations had adopted PbD and along the way had matured in information ethics this would not have needed to end in legislation. This not being the case, leads to the need of regulation. Regulation that has a hard time keeping up with technological advancements. Already new web tracking mechanisms, like canvas fingerprinting and evercookies, are coming into mainstream and could well fall out of the reach of the cookie law.

2.3.3 Appification

PbD might even be more needed with regards to the explosion in mobile application (app) development (Degeling & Loser). Apps give organisations the opportunity to interact directly with consumers. A lot of

apps are for free and the way to earn money is by way of advertising, which is understandable. But many organisations want to gain every advantage possible and track behaviours and preferences, through sensors, messages, contacts and locations in the mobile phones. Most apps request (demand?) access to those features before they will install and can be used. So once installed the 'data dredging' starts. The dredged data is mined (data mining) and personal profiles are constructed that grow more intrusive over time.

The three key perspectives of the PbD concept (regulatory, engineering and managerial) do need to converge and integrate to become a practical framework, or otherwise it risks remaining a theoretical concept. An important part of the protection of privacy will have to be accomplished through organisational measures by means of processes and procedures in operational practices (Blarkom, Borking, & Olk, 2003). A strong theme throughout the pending EU data protection regulation is the expectation of organisations to document each processing operation to demonstrate compliance. At first glance this seems a burden, however new promising techniques like process mining can alleviate this.

2.4 Business Process Management

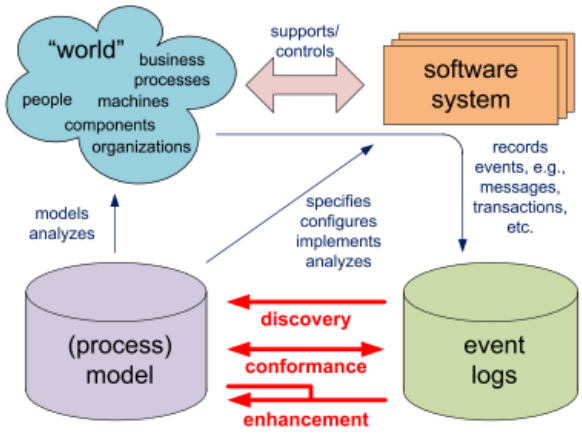
Business Process Management (BPM) has emerged as a comprehensive consolidation of disciplines sharing the belief that a process-centred approach leads to substantial improvements in both performance and compliance of a system. Compliance to legal regulations is an aspect of growing importance within Business Processes Management (Lohmann, 2013). Compliance by design (CbD), like PbD, is based on the principle that systems should be designed right from the start with legislation and rules in mind, in such a way that built in checks for certain thresholds cannot be breached. It is preventative of nature, capitalising on BPM with the potential to include the detective and corrective measures broadly associated with compliance, leading also to a holistic regimen (Governatori & Sadiq, 2009).

A forthcoming requirement of the pending EU data protection regulation is to keep documentation of all processing operations, geared towards establishing transparency and easily accessible policies around personal data to deal with the exercise of data subject rights, being a centrepiece of the regulation. The design of the business processes and information systems in accordance with a regulation like the EU data protection act is a balancing act between performance and conformance: "To evaluate what has happened in the past, to understand what is happening at the moment, or to develop an understanding of what might happen in the future" (Muhlen & Shapiro, 2010). The enhancing of both performance (business objectives) and conformance (control objectives) is also the "win-win" principle that PbD is striving for: Performance and compliance does not need to be a zero-sum game.

The Dutch data protection law is a complex and principles-based regulation, with quite strict rules about what companies can and cannot do in terms of collecting, using, disclosing and storing personal data. But how the principles-based regulations are to be implemented is left to an organisation to interpret and decide (College Bescherming Persoonsgegevens, 2014). Effectuating regulations is in most cases a knowledge-intensive process: processes that primarily revolve around the collection of data, combining the data, reasoning with the insights and ultimately coming to decisions (Hulstijn, 2012).

Process mining, a research discipline between data mining and process modelling, offers a way to both check for compliance and at the same time learn how to improve business processes on the basis of event logs commonly available in today's information systems (Process Mining Manifesto, 2012). Event logs can

be used to conduct the three types of process mining in all phases of the BPM lifecycle: discovery, conformance and enhancement. Conformance checking is especially of importance for business rules/policies and laws.



From (Process Mining Manifesto, 2012, p.6)

Van der Aalst, a driving force within the process mining research community, has just started a government funded research project 'Privacy and Compliance Enforcement' (PriCE) to develop a novel approach that empowers users to control their data and enables organisations to comply with user policies and legal requirements. One of the objectives is to develop methods for infringement identification and management. (Van der Aalst, 2013) With these sort of techniques the improvement of faulty business processes does not have to wait until a laborious audit has been done, but can checked in a continuous manner. Another important objective is the need of a language for policy specification. Legal requirements have a declarative perspective of the objective of processes, what needs to be done and business processes are mainly prescriptive detailing how things should be done. Because of this difference they are treated separately and the checking of compliance is done afterwards through manual checks by expensive consultants (Governatori & Sadiq, 2009; Hashmi, Governatori, & Wynn, 2012). Aligning both perspectives in (near) real time would make compliance more efficient and, more important, less of a burden.

2.5 Compliance by design

2.5.1 Compliance

Compliance by design is an overarching methodology, melting legislation and ethics, by aligning business and control objectives (Sadiq & Governatori, 2010) anchored closely with Business Process Management.

The fundamental interest of the compliance function is in ensuring that an organisation complies with existing external laws and regulations, and internally defined policies and ethical standards. Organisational behaviour that is in accordance with the evolving social norms of all stakeholders. The compliance function is mostly associated with finance, but just like Sarbanes Oxley (SOx), Basel II, Solvency II, and other non-financial regulations, the Data Protection Regulation, is a compliance requirement with control objectives that have to compete with business objectives, for management attention.

Rational decision-making is strategically concerned with the efficient fulfilment of business objectives. Comparing what is actually performed given the available resources of money, time and labour and

determining what actions and resource combinations increase of decrease efficiency. The criterion of efficiency is a priority for organisations and the modus operandi, relegating other commitments or goals to a secondary status in theory and thus in practice. Consequently, it is easy to understand why ethics, and other commitments have secondary, if any, importance in the rational model (Simon, 1976). In rational decision making the price of getting and staying compliant is compared to the chance of getting fined for not doing so. The lack of enforcement, according to the scientific and political community data, makes that protection is suffering from non-compliance. (Burghardt, Bohm, Buchmann, Kuhling, & Sivridis, 2010)

2.5.2 Legislation

Legislation is mostly formulated in a generic way, so that it is applicable in many different situations. A lot of legislation describes a purpose that should be pursued. A purpose that is based on certain ethics; moral principles that govern behaviour or the conducting of an activity. “The field of ethics involves systematizing, defending, and recommending concepts of right and wrong behaviour.” (Fieser, 2009)

The pursuance of legislation itself is not prescribed or dictated. Organisations have to make choices how to implement it in their business processes, in a way that they believe will serve the purpose, and then operationalise it in the underlying information systems. Compliance is then conforming to particular requirements originating from the interpretation of compliance sources (Schumm, Leymann, & Streule, 2010). Compliance requirements are formulated in a set of rules that can be checked during or after the execution of the business process (Lohmann, 2013). It is obvious that the level of compliance is dependent on how good an organisation’ analysis of the legislation is translated into the design of the business processes, implementation in information systems and the governance of it. Given for instance that the Dutch implementation of the EU-Data Protection Directive, the Dutch Data protection law (Wbp), has resulted in a broad omnibus law, leading to problems of complexity and inflexibility and making compliance no easy task (Zwenne, et al., 2007).

2.5.3 Ethical pursuits

The collection, processing and storage of information, personal and otherwise, due to technological advances raises more and more ethical questions to the right to privacy of individuals threatened by it. Considerable effort is required to prevent employees in engaging in non-compliant or unethical behaviour by eliminating weak moral awareness and intent in handling information. Among important drivers to make this happen are clear guidance of executive/ supervisory management, good congruency of words/policies and actual organisational practice and open discussions on incidents that were not so clear (Hener, 2011). Privacy policies, created with legal and regulatory input, play an important role in preventing opportunistic behaviour and as guidance for sound decisions and good business ethics (Smith J. , 1993)

Organisations that invest ample resources in compliance, could be described as having high moral standards. Compliance functions need to put effort into ethics management. This is necessary for a better understanding why legislation is important and what moral factors are pushing it forward. By doing this, the translation of legislation in business process and underlying technology, by those who have to work accordingly, is better secured. A better understanding of the why generally leads to a better execution what needs to be done. But even when it is achieved that employees share the same norms and values it will not be clear cut among them what is to be done, because moral dilemmas are seldom black or white, but more often shades of grey (Nijhof & Rietdijk, 1995). With only 10% of all people always trying to achieve the

morally good and 80% acting according to the circumstances (Hener, 2011), it is of importance to guard for opportunistic behaviour that can lead to unethical business decisions.

Colle and Werhane (2008) state if organisations focused more on ethics, they would be able to encourage their organisations' managers and professionals to do the right thing because they should, not because it is the law, adding that research has shown that a good ethics program is better at creating compliance than a mere compliance program.

The Netherlands Authority for the Financial Markets (AFM) for instance requires from financial institutions not only to be compliant in the strict sense of rules and laws and look after their reputation from a mere shareholder perspective, they also are expected to demonstrate the pursuance of values in the interest of their customers. The integrity of an organisation to all stakeholders (customers, employees, …) is at stake and needs to be evenly balanced (Beusekom & Raaijmakers, 2010)

2.5.4 Privacy Risk management

To reach objectives organisations create opportunities and take risks. Organisations must build in controls to address these risks and opportunities. Because how good the intentions might be from the start of an opportunity, humans are less competent when it comes to containing the risks (Simon, 1978). Guidance, amidst all opportunity, is necessary to keep an eye open for unwanted effects coming from the vulnerabilities and threats to the organisation.

Risk management is the balancing act of all risks coming from unwanted and uncertain effects, from either a business or control perspective, that are willingly accepted, avoided, transferred. Becoming and staying compliant is for most organisations a choice that is based on the time, money and resources to do so and the risk of getting caught if they don't. For a regulation like the data protection law, the amount of time and effort put in the design of internal controls determines the willingness to comply. The level of willingness in a sense reflects the risk appetite of an organisation (Governatori & Sadiq, 2009). Within the new data protection law so called Privacy Impact Analysis' (PIA) will be proof of the preparedness to comply. A PIA is a process to identify and evaluate risks to privacy, and check for compliance with privacy legislation (Wright & de Hert, 2012).

2.6 Right of Subject Access

The principle of informational privacy, runs as a thread through data protection law, making it possible for everyone to check where data is recorded and processed. (Putker-Blees & Meulenveld, Inzicht in het inzagerecht, 2006).This transparency is conditional for the right to correct or object to the recording and processing of one's personal data (Putker-Blees & Berkhout, 2008). The checking of personal data is known as the right of subject access. This right of subject access, commonly referred to as Subject Access (SA) means that everybody can make a request to any organisation processing one's personal data, to be informed about the collection and processing of one's personal data.

The high paced technological developments are leading to more and more automatic processing and storage of personal data. A research conducted for the CBP (Dutch Data Protection Authority) shows that the 'average' Dutch citizen has 250 to 500 registrations to his name within the government alone. According to Kohnstamm, the chairman of the CBP, to only have 250 registrations to your name, you would have to live like a recluse (Schermer & Wagemans, 2009). Including non-governmental organisations this

number could probably easily reach 1000 registrations in databases for the average individual. All that personal data is increasingly getting mixed and combined into 'high octane' information to predict behaviour and preferences of citizens, customers, patients, students, et cetera. Of course, as the research points out there are no standards or guidelines as to how many registrations are good or bad. Having 10 separate registrations in different databases might well be less intrusive than 2 interconnected ones. Big data being all about finding out new things through exploration, will more likely than not give rise to interconnecting data in search of correlations, or better causation.

It becomes worrisome if correlation of data is confused with causation, leading to incomplete or unfair decisions denying benefits or services. Correlation and causation can happen at the same time, but having a correlation does not imply that there is always causation. The examples of confusion between them are many, leading to wrong conclusion(s) and following wrong decision(s). Critical human judgement of this is of great importance, but not everybody is equally well equipped to spot logical fallacies. The growth of Big Data and subsequent correlations could well result in an avalanche of logical fallacy. Clearly automated decision making can be advantageous for both organisations and individuals, but it also means responsibilities for both sides: For organisations to be transparent and for people to take control (Boston Consultancy Group, 2012).

The best safeguard is a right to see and judge for yourself the logic of (automated) decision making. Fortunately the majority of European Internet users feel responsible themselves for the safe handling of their personal data (Attitudes on data protection and electronic identity in the European Union , 2011). Right of subject access is an important first step to be able to check upon the purpose of data collection and processing, and when necessary correct it (right of rectification) or object against it (right of erasure).

An individual who exercises his right of subject access is, according to the Dutch data protection act, entitled to be:

- Told whether any personal data is being processed;
- Given a complete summary of it;
- Given a description of the personal data, the reasons it is being processed, categories of personal data, and whether it is shared/given/transferred to any other organisations or people;
- Given details of the source(s) of the data.

An individual can also request information about the reasoning behind any automated decisions, such as a computer-generated decision to grant or deny credit, or an assessment of performance at work.

In the Netherlands every adult is entitled to do a SA request on a regular basis, of course within reason, and expect to receive an answer within four weeks.

For this research the Subject Access Right has been divided in logically related tasks and/or activities that must be fulfilled within an organisation to deliver transparency (Trkman, 2010). In the process breakdown structure of right of subject access in Appendix 3, the steps are described to get from a request to an answer.

2.7 Privacy Capability Maturity Model

In search of the disruptive factors within organisations that diminish the ability to respond properly to a SA, and what can be done to eliminate and/or mitigate them, a diagnosis is needed to help identify the

problem areas. In order to address organisational context, policies, processes and people, and point out areas that require improvement, Capability Maturity Models (CMMs) are well suited. CMM has been adopted by many organisations as a means of assessing compliance and performance. It provides an effective tool to assess an organisation's current capabilities and where it wants to be in the (near) future.

The Capability Maturity Model was piloted in 1988, based on data collected from organisations that contracted with the U.S. Department of Defense, and has been in use for almost 25 years. It was originally developed in order to assess the maturity of software development processes and is based on the concept of immature and mature software organisations. The Carnegie Mellon University Software Engineering Institute (SEI) has developed a more general approach to assessing capability maturity, called Capability Maturity Model Integration (CMMI) and can be used to describe entire companies and overall process maturity. For this research a CMM focused on privacy was needed.

Review of the literature and searching the internet for
- "Privacy Capability Maturity Model";
- "Privacy Capabilities Maturity Model";
- "Privacy Maturity Model";
- CMM AND Privacy

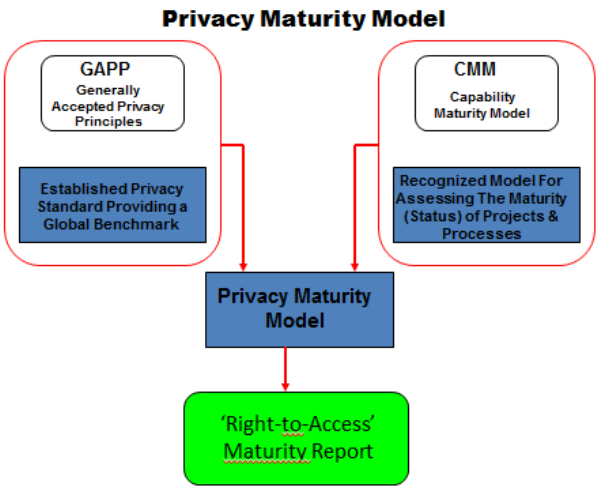
revealed that there currently exists only one fully developed capability maturity model (CMM) that deals specifically with privacy: The AICPA/CICA Privacy Maturity Model.

The AICPA/CICA Privacy Maturity Model (AC-PMM) was introduced at the beginning of 2011 by the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA) based on Generally Accepted Privacy Principles (GAPP), combined with CMM concepts. Although there is reference to the general term privacy the scope of GAPP is focussed on personal data. GAPP was originally published in 2003 and revised in 2009 and has been developed from a business perspective, "to help management create an effective privacy program that addresses privacy risks and obligations as well as business opportunities" (Generally Accepted Privacy Principles, 2009, p1).

AICPA/GAPP has done a comparison of its principles to some domestic and international privacy regulations, laws, and guidelines (Comparison of International Privacy Concepts, n.d.). Including, the afore mentioned OECD guidelines and EU Directive. From this comparison one can see that it very much has a business perspective because of the management principle it has, that the others miss. This being said, does not mean that GAPP is superior to the others. Not in the least because the comparison does not identify any privacy principles which might be covered by other privacy frameworks but might be absent from GAPP.

Nevertheless the Privacy Maturity Model AICPA/CICA provides an interesting concept for organisations to gauge their progress in implementing data protection against specific privacy regulations, laws, and guidelines and not GAPP. This being necessary because of GAPP being an amalgam of "some but by no means all significant local, national and international privacy regulations" (AICPA/CICA , 2011, p.1), and therefore plausible that complying with GAPP, is no guarantee for complying with specific data protection regulations.

So AC-PMM for this research is used as a guideline for doing an assessment of the capability of an organisation specifically for right of subject access. This is done through a selection process of specific principles and criteria. The selected principles and accompanying criteria are the control objectives to assess the achievement of an organisation perceived ability in complying for right of subject access. In the figure below this has been schematically depicted.



3 Research design

This chapter describes the choices made and for what reason, with regards to the available research methods within business science to answer the research (sub)question(s) and so meet the stated objective of obtaining insight in and understanding of the process which leads to a response to a SA request.

3.1 Introduction

The previous chapter explored the theory and concepts with regard to the research questions posed in the first chapter. Now in this chapter a conceptual model is presented and explained which ensures more focus for the research.

Business studies is the branch of science which is concerned with the organisation and the market environment of businesses. A field of study that is practically oriented and concerned with problems within organisations and problems caused by organisations. Real-world problems. The issues of those problems do not stand in isolation and cannot be confined to one single academic discipline for finding answers. The answers must be sought in an interdisciplinary approach. Therefore business studies make use and combine scientific insights from economics, sociology and psychology to analyse and explain real-world situations.

3.2 Qualitative research

Due to the fact that a single person only can exercise his SA from organisations where he is known as being a client, patient, etc. and the fact that the scope of this research is on public and financial organisations (more on this choice later) it was clear from the start that a survey (with many respondents) was not an option and that this research would have to go deeper instead of broader.

So to answer the research question a qualitative research approach was chosen. Qualitative research has a focus on real-life situations, an interest in the meanings of them by learning about the perspectives and understandings of the participants. Using an inductive research approach focussing on process, meaning and understanding (Gillham, 2005, p.9; Denzin & Lincoln, 2005, p.3; Potter, 1996).

However, the term qualitative research is a general definition that includes many different methods used in understanding and explaining social phenomena. As a result, there is great variation in approaches for doing qualitative research. The four methods stated below are the most commonly used to acquire data, analyse them and get a better understanding of a phenomenon.

- Observation
- Interviews
- Documentary analysis
- Questionnaires

3.3 Choice of Methods

For answering the main research question:

How can the Right of subject access (SA) process within organisations be improved to deliver timely and adequate responses?

three sub questions were defined for which answers (data) had to be acquired. This was done in two ways.

3.3.1 Documentary analysis

To find an answer to sub question:

What is the quality of a response to a 'right of subject access' request in accordance with the legal requirements?

documentary analysis was the method of choice.

The response to a SA was first obtained before respondents (organisations) were asked for an interview. This was important to do and the only way to prevent SA's from getting special attention and treatment and to make sure that the request was handled in a way that truly represented the best effort of an organisation.

3.3.2 Interviewing

For the sub question:

What circumstances and bottlenecks surrounding the response process can there be identified within an organisation?

this was done by interviewing the employees responsible for the response to the SA request to get to know the circumstances and bottlenecks surrounding the process from their point of view.

To avoid that categorisation afterwards was done in a way, consciously or unconsciously, to fit the answers one was expecting, interviewing was set up in a semi-structured way and preliminary hypotheses, deducted from a conceptual model, were used as guidance.

3.4 The conceptual model

From the research question a conceptual model is constructed and hypotheses deduced.

How can the Right of subject access (SA) process within organisations be improved to deliver timely and adequate responses?

The identified concepts within the research question:

- Right-to-Subject Access process (SA process).
- Timeliness of a response.
- Adequacy of a response.

3.4.1 SA process

In the light of a response to a SA, the SA process is defined as follows:

A SA process is a series of actions, that can be more or less procedural, in order to produce a response of a certain quality and within a certain timeframe.

In Appendix 2 there is a graphical representation (SA request Business Process Model and Notation) specifying a standard SA process. The SA process is measured by determining the maturity levels of selected criteria. The selected SA criteria are a subset of the AICPA/CICA Privacy Maturity Model (AC-PMM) criteria. From these the mean SA maturity level is determined as an indicator of the predictability, effectiveness, and control of an organisation's process to respond to a SA request.
(See section 4.4. Research interviewing, Rating)

The maturity levels are:

Level	Description
1. **Ad Hoc**	Processes and procedures are generally informal, incomplete and inconsistently applied. At this level procedures or processes are typically undocumented and in a state of change, tending to be driven in an ad hoc, uncontrolled and reactive manner by users or events. This provides a chaotic or unstable environment for the process.
2. **Repeatable**	Processes and procedures exist; however, they are not fully documented and do not cover all relevant aspects. It is characteristic of processes at this level that some processes are repeatable, possibly with consistent results. Process discipline is unlikely to be rigorous, but where it exists it may help to ensure that existing processes are maintained during times of stress.
3. **Defined**	Processes and procedures are fully documented and implemented, and cover all relevant aspects. It is characteristic of processes at this level that there are sets of defined and documented standard processes established and subject to some degree of improvement over time. These standard processes are in place and used to establish consistency of process performance across the organisation.
4. **Managed**	Reviews are conducted to assess the effectiveness of the controls in place. It is characteristic of processes at this level that, using process metrics, management can effectively control the business process. In particular, management can identify ways to adjust and adapt the process to particular projects without measurable losses of quality or deviations from specifications. Process Capability is established from this level.
5. **Optimised**	Regular review and feedback are used to ensure continuous improvement towards optimization of the given process. It is a characteristic of processes at this level that the focus is on continually improving process performance through both incremental and innovative technological changes/improvements.

(AICPA/CICA Privacy Maturity Model, 2011)

So a SA process results in a certain performance, which is described as SA performance.

3.4.2 Timeliness and adequacy

The SA response is determined by its timeliness and adequacy (= quality).

- Timeliness of a response: time between sending out of an SA and receiving the response. The legal requirement is within 4 weeks.
- Adequacy of a response: guidelines and instructions on the adequacy of a response, as set by law.

From this we derive four SA response categories:

a. In time & adequate
b. Out-of-time & adequate
c. In time & inadequate
d. Out-of-time & inadequate

A is the optimum result and better than b, that is better than c, that in turn is better than d. So it is importunately considered better to get an adequate response out-of-time than getting an inadequate answer within time.

3.4.3 Process improvement capability

In a research project from the University of Utrecht (UU) 'Business Process Management Maturity in the Netherlands 2011' (Spekschoor, 2012) one of the capability areas, called constructs, identified for BPM was Process Improvement. The research also showed that the difference in capability 'Process improvement' is significantly better for the finance branch then the public branch. It was determined to use this as a discriminator for the selection of SA criteria from the Privacy Maturity Model.

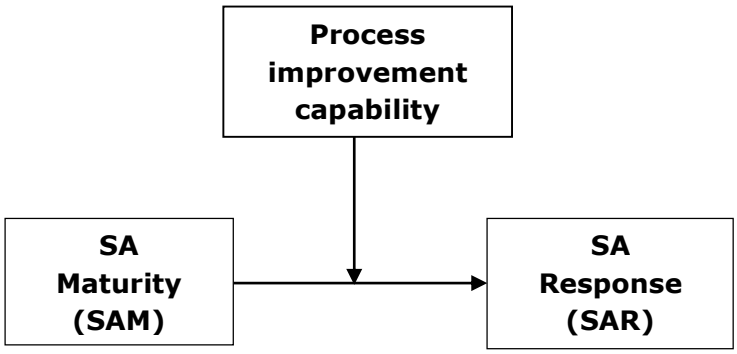
A capability area consists of several theorems. For Process Improvement they are:

- If a process needs to be improved or modified, it is clear who is responsible.
- Management has an active role in improving processes.
- Continuous improvement is pursued by means of improvement planning and control, focusing on quantitative measurable process improvement: Plan-Do-Check-Act cycle.
- The organisation uses methods like Lean and/or Six Sigma and/or Theory of Constraints, to improve processes.
- Employees are actively and frequently involved in improving their processes.
- Relevant stakeholders are sufficiently involved in the process and process improvement.

In the research the inter-item correlation for Process Improvement was determined to see whether the construct consisted of theorems that are alike. The higher the correlation between the different theorems, the stronger the construct. The research showed that the difference on the capability 'Process Improvement' was significantly better for the finance branch than the public branch. On the basis of this finding it was decided that the cases to be studied for SA process and performance would be financial and governmental organisations.

A closer look at the maturity levels for 'process improvement capability' keywords in the descriptions are overall, in terms of maturity level, more to be found in levels 4 and 5 (managed and optimised). In the lower maturity levels (ad hoc, repeatable, defined) there is less or no management attention, focus on improvement and less clear where responsibility lies. See Appendix 3 for the details of the key-word matching.

Conceptual model:



3.4.4 Hypotheses

We have the three components for hypotheses:

1. The variables: the three variables as depicted in the conceptual model.
2. The population: financial and governmental organisations.
3. The relationship between the variables: as depicted in the conceptual model.

Hypothesis 1
An organisation with a good SA process in place (= independent variable) has less difficulty responding to SA requests than an organisation with a flawed SA process and therefore will show better SA Response (= dependent variable).

Hypothesis 2
SA maturity level 5 is more to be expected for financial organisations than for public organisations. The levels to be found for public organisations are expected to be maturity level 4 or less. So finance organisations with a higher propensity for (continuous) process improvement are expected to show more SAR Category “in time & adequate” kind of results than the public organisations.

From the determined maturity levels on the subset of SA criteria the circumstances and bottlenecks for the SA response process are expected to be inferred. This is only valid when the determination of maturity level is aligned with the expected result as stated in the hypotheses. So when for instance an organisation shows not to be expected causality, e.g. SA maturity level 4 and “d” (“Out-of-time & inadequate”), then deduction is not really justifiable.

4 Operationalisation

Operationalisation is the 'translation' of the research in tooling, indicators and instructions (Verschuren & Doorewaard, 2010, p145). This chapter describes how the research questions will be answered, what sources and methods will be used and how will be measured and in what ways the validity and reliability will be secured.

4.1 Expert consultation

Two Data Protection Officers were separately consulted on the research design.

- FG 1 worked for a Top-5 System Integrator in the Netherlands;
- FG 2 worked for an Academic Hospital.

The focus of the consultation was to seek confirmation on:

- The breakdown of the SA process (Appendix 2);
- The conceptual model;
- The hypothesis that for an organisation with a higher/lower SA Maturity level it is less/more difficult to respond to a SA request;
- How from the AC-PMM a 'SA Maturity' subset could be derived;
- The evaluation of the SA responses (grading);
- Their willingness to 'co-grade' SA responses.

The consultations provided confirmation that what was tried to establish with this research and the way it was thought to get the answers from the organisations, based on a SA Maturity Model criteria, made sense to them.

An important piece of advice that both gave was that the criteria set for the structured interview should not take longer than an hour of a respondent's time. This resulted in cutting the criteria set nearly in half.

A very important outcome of the consultation was their willingness to participate in the evaluation of SA responses.

4.2 Case Study

Case studies are about real life situations and involve an in-depth observation of a "case" such as an event, process or person. This research investigates the process of responding SA requests with which numerous organisations experience difficulty with fulfilling: Either in time or/and as legally required.

4.2.1 Hypotheses

From the conceptual model it was expected that there would be a difference for the ratings on the independent variable between financial and public organisations. So the organisations selected as cases were chosen in these segments. The other criterion for the selection of cases was the size of an organisation. Besides the fact that the UU research (Spekschoor, 2012) showed that 'process improvement'

is significantly better for the finance branch than the public branch, it also showed that very large organisations (>5000) are significantly more mature on improvement methods as compared to medium (101-1000) and large organisations (1001-4999).

A limiting factor was the fact that as an individual I could only exercise my right of subject access from organisations that I am known to as a citizen/customer/patient/student. Being only customer of two banks and two insurance companies, these were the only financial organisations I could send a SA request and after receipt ask to participate in my research. For the governmental organisations the municipality I live in was too small, another public organisation, the 'Centraal Justiaal Incassobureau', from which I unfortunately sometimes receive speeding tickets, has 1100 employees and some others that I could think of were either too small (Kadaster) or I had no relation with (e.g. UWV). In my case this only left two other potential governmental organisations I could send a SA request to. I decided also to add the 'Sociale Verzekeringsbank', with 3200 civil servants nearly a 'very large' organisation.

The organisations that participated in this research requested to stay anonymous and therefore they have a code name. The ones that did not wish or could not participate are not anonymised.

Selected organisations:

Large Financial Organisations (LFO)	**Large Governmental Organisations (LGO)**
LFO1 (insurance)	LGO1
LFO2 (bank)	LGO2
Nationale Nederlanden	Sociale Verzekeringsbank
ABNAMRO	

To obtain insight in and understanding of the circumstances and bottlenecks concerning the process of composing a response for the requests made to the above stated organisations, the methods of choice were interviewing of employees and/or managers involved in coming to a response and analysis of the responses received. The ideal research situation would be interviewing anyone, employees and managers, within an organisation who was (in-)directly involved in the response to my SA request.

4.3 Research interviewing

Conducting interviews is one of the most important gathering tools in qualitative research. By interviewing people they are allowed to convey a situation, e.g. the SA response process, from their own perspective and in their own words.

4.3.1 Semi-structured interviews

The choice was made for semi-structured interviewing because of the possibility to have informants comment on the SA process from their own perspective and in their own words if they wanted to elaborate on a rating choice made, the structured part. Semi-structured interviewing allows asking specifying ("What did you think then?" , …), probing ("Could you say something more about that?", "Do you have further examples of this?",…) or interpreting ("You then mean that….?" "Is it correct that you feel that…?", …) questions.

This flexibility to explore and look for clarification, balanced by the structure of a guiding questionnaire with answers to the same questions, prevents superficiality and makes the quality of data obtained broader and much richer.

4.3.2 Rating

As described in Section 3.4 (The Conceptual model) the Privacy Maturity Model (PMM) is based on GAPP and the Capability Maturity Model (CMM). GAPP operationalises complex privacy requirements into a single privacy objective that is supported by 10 privacy principles (see Appendix 1). Each principle is supported by objective, measurable criteria that form the basis for effective management of privacy risk and compliance in an organisation. For every principle there are criteria set in the form of statements. Adding up to a total of 73 criteria. For each criterion a level of maturity has to be rated. The maturity levels being, either: Ad Hoc, Repeatable, Defined, Managed or Optimised .

The SA Process, as a subset, was determined on the basis of a selection of the 10 principles and 73 criteria from GAPP/CMM. To determine this subset all criteria from all principles were 'screened' for relevance to Right of subject access. The selection of criteria was done by cross referencing for process improvement as represented in the conceptual model. In Appendix 3 the selection process is described in detail.

The objective of this research was to learn from as many people as possible, who are involved in the SA response process and to learn what in their view the capability maturity is of their organisation responding to SA requests. This could be specifically on the basis of their experience, perception and involvement in my particular request or on the basis of general experience and or knowledge of the SA requests process. More capability maturity assessments per organisation were expected to provide a more (overall) objective 'SA-capability maturity' picture and together with the quality of the response for a SA request determine the SA response quality of an organisation.

4.3.3 Protocol

After receiving back a SA response a telephone call was made to the signatory of the response. To him/her it was explained that the SA request was part of a master thesis research and if they were willing to participate by being interviewed. (See Appendix 4). If one agreed he/she was sent an email with further details on the purpose of the research, the preferred way of interviewing, permission for recording the interview and the assurance of confidentiality. The day before an interview the informant was sent the SA questionnaire and SA Process Breakdown Structure (see Appendix 2), with the request to get acquainted with it in advance.

The introductory part of the interview was used to 'loosen up' the informant and could take up between 5 or 15 minutes. The topic would be my research and/or privacy in general and proved useful for context when analysing the maturity levels. If the introduction phase did not go smoothly towards privacy in general and SA in particular I would zoom in on the SA Process Breakdown Structure.

4.3.4 Informants

Informants for the interviews were employees and managers that were at some point involved in responding to the SA request, be it as a 'passing station' or 'answering body'. The 'passing stations' being organisational units or persons specifically appointed to 'process' the request forward or even more

interesting sections or persons that got involved accidently. The 'answering body' being all those, persons and/or organisational units, essential for input for the response.

Too many handovers ('passing stations'), intentionally or accidently, and an ad hoc or an efficient answering body are meaningful to learn more about the maturity of the SA process. All people involved either in the capacity of 'passing station' or 'answering body', were to be asked what their role had been in the process.

To learn who the people were that were involved in the SA process at some point in time in either capacity, 'passing station' or answering body', was done through back tracking. The person who was first interviewed, most likely the signatory of a SA response, was asked from whom he got the request, and that person was asked the same question, and so forth. Back tracking is also known as reverse snowball sampling: enlarging the target group of respondents by getting introduced to other respondents.

4.3.5 Interview method

The SA Process was evaluated on the basis of a selection of the 10 principles and 73 criteria. To determine the (SA-)subset all criteria from all principles were 'screened' for relevance to Right of subject access. From the first screening 20+ criteria were picked, but the expert consultations learned that these were too many if the interviews should not take longer than an hour. So the number of maturity criteria was limited by the estimated average time per criterion to come to an answer. An answer including the structured part of determining the maturity level for a criterion and time for additional comments or remarks. This was set on an average of 5 minutes per criterion, resulting in 10 criteria.

The 10 criteria had the following format:

Criteria	Criteria Description	Ad Hoc	Repeatable	Defined	Managed	Optimised	Familiarity
Access	**The entity provides individuals with access to their personal information for review and update.**						Very Good/ Good/Adeq/ Moderate/Bad
Access by Individuals to their Personal Information	**Individuals are able to determine whether the entity maintains personal information about them and, upon request, may obtain access to their personal information.**	The entity has informal procedures granting individuals access to their information; however, such procedures are not documented and may not be consistently applied.	Some procedures are in place to allow individuals to access their personal information, but are not consistent and uniform.	Procedures granting individuals access to their information have been documented and are available to them. The procedures have been provided to employees and are consistently and uniformly applied.	Procedures are in place to ensure individuals receive timely communication of what information the entity maintains about them and how they can obtain access. The entity monitors information and access requests to ensure appropriate access to such personal information is provided.	The entity reviews the appropriateness and usability of its communications procedures to ensure individuals are informed of their right to access information. Such monitoring may result in improvements in the communication message and/or techniques.	

All 10 criteria, only the first two columns stating and explaining the criterion, were send to the informants to read in advance. In the interview the informants had to choose which maturity level, in their opinion, represented their organisation in the best way. Informants were also asked to give their valuation and opinion on a criterion from their experience and to state their familiarity towards a criterion. The latter was asked to be able to give responses more or less weight in the analysis if the expertise differed substantially between informants within an organisation.

4.4 Transcription

The transcript helps qualitative researchers make sense of and understand informants' experiences and perceptions. Transcription is a process of interpretation. What is transcribed, what not, and how the transcript is structured very much influences the analysis process (MacQueen & Milstein, 1999). Here we describe what transcription choices were made and why.

4.4.1 Selective transcription

As stated transcription is an important step towards the demanding process of interpretive analysis. Verbatim transcripts are important to identify from unstructured in-depth interviews the apparent themes or categories. For this particular research the themes had been determined in advance and the choice was made to address them by means of the semi-structured interviewing method. From the Privacy Maturity Model the selected principles and selected criteria were determined that would contribute to the SA response. The selected criteria also differed in relative importance. See table below and Appendices 1 and 3.

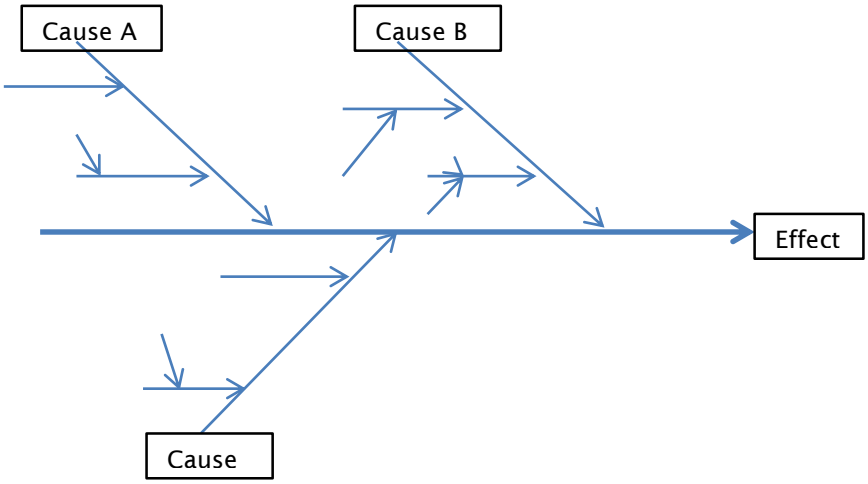
Principle	Definition
Management	The entity defines, documents, communicates and assigns accountability for its privacy policies and procedures.
Collection	The entity collects personal information only for the purposes identified in the notice.
Access	The entity provides individuals with access to their personal information for review and update.

What to include in the transcription should always be driven by the research question that an analysis attempts to answer. If a research is not focussed on in-depth description of the knowledge, attitudes, values, beliefs, or experiences of an individual, a group of individuals, or groups of individuals, the exploration of general themes and patterns can be undertaken with less text (McLellan, MacQueen, & Neidig, 2003 Vol.15).

Identifying in advance the main causes/principles of analysis for this research made that selective transcription (Emerson, Fretz, & Shaw, 1995) of remarks/comments on top of an informants choice for a maturity level would suffice. This was done with a special focus on remarks and/or comments that led to insights that added extra meaning or dimension to a cause. Those insights were seen as sub-causes underlying the pre-determined principles (e.g. causes). The Causes A, B and C being the principles: Management, Collection and Access and the SA response being the 'effect'.

4.4.2 Transcription template

Coding for transcription was done manually. An initial consideration was to do this on the basis of an Ishikawa diagram as suggested by one of the DPO's (Data Protection Officer) of the expert consultation. An Ishikawa provides a graphically and orderly, easy-to-read format to diagram cause-and-effect relationships, illustrating the relationship between a given outcome and factors within a cause, influencing the outcome. This way each transcript would have an identical structure and appearance. See below.



Although Ishikawa's have their merit it became during analysis clear that a software program designed for computer-assisted qualitative text analysis (MAXQDA) was more suited to gain insight from the interviews. Together with using tables this provided a better way to oversee categories (Access, Management, Collection) for LFO or LGO, the 10 principles, given maturity levels of informants and the differences between them. In Chapter 5 'Results' this is explained in more detail.

4.5 Analysis .

To determine the SA Overall performance of an organisation, in line with the conceptual model, the SA-Maturity (SAM) and SA-Response (SAR) were combined in a total score, by multiplying both mean scores with each other. To be able to do this it was first necessary to check if the individual results for SAM and SAR could be averaged. This was checked through Analysis of Variance (ANOVA) and Hartley's test (Bertram, 2013; Kirkwood & Sterne, 2003).

4.5.1 Hartley's test (Fmax)

Hartley's test computes the ratio of the largest group variance, S^2max to the smallest group variance, S^2min. The resulting ratio, Fmax, is then compared to a critical value from the Fmax sampling distribution table. If the computed ratio is less than the critical value, the groups are assumed to have similar or equal variances.

4.5.2 Analysis of Variance (ANOVA)

ANOVA provides a statistical test of whether or not the means of several groups are equal and are useful in comparing three or more means (groups or variables) for statistical significance. It has to be proved that there is no significant difference between and within the scores of the informants.

In the typical application of ANOVA, the null hypothesis is that all groups are simply random samples of the same population and that there is no relationship between measured phenomena. Rejection of the null hypothesis is grounds for assuming a relationship between phenomena. For this research acceptance of the null hypothesis is the goal to prove that all groups are random samples. This is proven when the F-test score is below the Critical Value at a 95% threshold.

4.6 SA-Maturity score (SAM)

The SAM score of an organisation is based upon the individual maturity-level scores of the informants within an organisation. The SAM score for every informant is determined by summing up the scores of chosen maturity levels. Ad Hoc being the lowest score and Optimised the highest (see below). On the basis of the 10 chosen criteria, this results in a score between 10 (min. score) to 50 (max. score).

Ad Hoc =1	Repeatable =2	Defined =3	Managed =4	Optimised =5

Steps in determining Mean SAM score organisation

a. Hartley's test. If valid then ANOVA;
b. ANOVA for all informant scores;
c. When ANOVA checked out as reliable the mean of the informant scores would be calculated;
d. The 'mean of the informants scores' divided by the total of criteria = Mean SAM organisation.

For the maturity levels defined, managed and optimised it was determined that no difficulties or problems for the SA process of an organisation were to be expected. The difference between the three levels is seen as a management choice between good enough, better and best practice. Maturity levels ad hoc and repeatable could be potential bottlenecks and therefore were paid closer attention to. But when two or more informants from the organisation differed in their maturity assessment of a criterion, this could be an indicator of a bottleneck in the SA process. This is the case when the difference of chosen maturity levels on the same criterion by informants within the same organisation is two levels or more. For example: One informant has chosen optimised and the other defined, or managed vs repeatable. The latter being more 'serious' than the other one.

4.7 SA-Response (SAR) score

On 20 December 2012 to four Large Financial Organisations and three Large Governmental Organisations a SA request was sent.

For the organisations to compose a correct 'Right of Subject Access response, the following (Dutch) legal requirements are stated:

- A complete synopsis of the processed personal information of the person concerned. ***(1)***
- A definition of :

- *The purpose(s) of data processing;* ***(2)***
- *The categories of data related to the processing of it;* ***(3)***
- *The recipients or categories of recipients.* ***(4)***

- All available information on the origin of the personal data. ***(5)***
- When specifically asked for an organisation also must explain the systematics of the automation of data processing. ***(6)***

All the above has to be formulated in a clear and comprehensible manner ***(7)*** *and within four weeks of receiving the request* ***(8)****.* (Sauerwein, L.B.; Linneman, J.J., 2002)

See Appendix 5 for the standard SA request that was sent to these organisations. Note that in the requests sent out it was specifically requested to elaborate on the systematics of the automation of data processing. Because this is not an explicit legal requirement, and if not specifically requested, no answer is to be expected.

The responses received were analysed and rated for the above eight requirements. A record of the dates the responses were received and checked was kept to see if requirement 8 was met. See Appendix 4.
The other 7 legal requirements were all turned into statements for which the response was checked to the extent to which it complied. This was done by the same tow experienced data protection officers mentioned before and myself on the basis of Likert-type scales.

The seven statements derived from the legal requirements.

1	The response contains, as reasonably can be overlooked, a complete overview of the processed personal data of the requestor.
2	The response describes the purpose(s) of the collection and/or the processing of the requestors personal data.
3	The response defines categories of data for which the processing of requestors personal data is covered.
4	The response describes recipients or categories of recipients.
5	The response explains the origin(s) of the personal data.
6	The response explains, as requested, the systematics of the automation of data processing.
7	The response has been provided in a clear and comprehensible manner.

4.7.1 Likert Scale

A Likert scale (Bertram, 2013) is an approach to response categories that measures the extent of a person's satisfaction or agreement with a set of statements or questions. A "Likert Item" is one of the above statements that the respondent is asked to evaluate. The table as a whole is the Likert scale. So the "scale" in "Likert scale" refers to the total sum of all Likert items and not the 1-5 range you see for each item.

Statement 1…

Totally disagree =1	Disagree=2	Neutral (neither agree or disagree) = 3	Agree= 4	Totally agree= 5

Every response from an organisation was rated for the seven items by for every evaluator, which resulted in a score between 7 (min. score) to 35 (max. score).

When a criterion was discarded a legal requirement is not fulfilled and therefore the given response is incomplete/inadequate. When two or more of the three evaluators deemed a criterion inapplicable then that criterion was discarded.

The determination of the SA-Response (SAR) score of an organisation, is done as follows:
a. Hartley's test;
b. An ANOVA for the scores of the three evaluators is done. When 'good';
c. The Mean Total Score is calculated;
d. The 'Mean Total Score' divided by the total of criteria = Mean SAR organisation.

4.7.2 Timeframe and adequacy

Timeliness is obviously a very important goal of a process, if not one of the main reasons why a process is implemented. For a SA request it is an important criterion that, as legally required, a response is provided within four weeks. If there is no proper SA process in place then there is no telling when a response will be finished and sent out. The 'in time' criterion is rather binary, yes or no, while for the other legal requirements a choice was made from five evaluation scores (Likert scale) to determine the adequacy of the requirements for a response. If no answer was given for a criterion and it was not explicitly stated in the response that this was done on purpose than it was designated a 'totally disagree'. If it was on purpose and as such stated, the criterion was discarded.

It is determined that:

- If Mean SAR >3 = Adequate
- If Mean SAR <3 = Inadequate

On this basis the following four SAR categories were identified:

a) In time & adequate
b) Not-in-time & adequate
c) In time & inadequate
d) Not-in-time & inadequate

'In time & adequate' (a) is the optimum result and better than b, that is better than c, that in turn is better than d. So it is importunately considered better to get an adequate response not-in-time (b) than getting an inadequate answer within time (c). Of course not-in-time being within reason. When an adequate response is a week later this is deemed acceptable. But acceptable from a requestor's perspective, does not make it acceptable from an organisation's perspective. An organisation should strive to provide a response in time as legally required. On the basis of this and combining it with a response being in time or not, the SAR categories have been given the following scores:

SAR Category score:

	In time	Not-in-time
Adequate	4	3
Inadequate	2	1

4.8 SA Overall Performance

By multiplying the 'SAR Category score' with the 'mean SAM score' the SA Overall Performance Indicator is determined.

SAR category	Mean SAM				
	Ad Hoc (=1)	Repeatable (=2)	Defined (=3)	Managed (=4)	Optimised (=5)
Not-in-time & in-adequate (=1)	1	2	3	4	5
In time & inadequate (=2)	2	4	6	8	10
Not-in-time & adequate (=3)	3	6	9	12	15
In time & adequate (=4)	4	8	12	16	20

For the scores the following categorisation is made:
- 1 - 7,5 = Low SA Performance (L)
- 7,5 - 15 = Medium SA Performance (M)
- 15 - 25 = High SA Performance (H)

Or differently

SAR category	Mean SAM				
	Ad Hoc (=1)	Repeatable (=2)	Defined (=3)	Managed (=4)	Optimised (=5)
Not-in-time & in-adequate (=1)	L	L	L	L	L
In time & inadequate (=2)	L	L	L	M	M
Not-in-time & adequate (=3)	L	L	M	M	M
In time & adequate (=4)	L	M	M	H	H

4.9 Construct validity and reliability

To realise good construct validity, really measuring what is being assessed, namely the maturity of the SA process, a selection was made from the set of GAPP criteria for rating Privacy Maturity. The GAPP Maturity model is to measure the overall privacy competency of an organisation, in its most broadest sense. For this research the primary interest was in the Right of Subject Access (SA) aspect of privacy. As described earlier the selection of criteria focussed on that aspect.

The selected SA criteria were presented to as many informants as possible within an organisation, who had been involved in some way or another in composing a response for the SA request. The 'rigid' structure of the SA criteria and rating classifications ensured that the results were accurate and stable, could be repeated by others and the results will be, more than likely, the same.

Case study research is very useful as a means to learn more in depth about a phenomenon. Topics of case study can be programs, events, persons, processes, institutions and social groups. So although the 'breadth' of insights is much smaller for research on the base of a few cases , its advantage is to learn more in depth about the (process) steps and governance coming to a SA response. The weakness of the limited breadth of insights ("small-n" data) is that conventional empirical techniques cannot be used because mostly there is not enough data to meet requirements for statistical significance. To make this research more sturdier for construct and internal validity and reliability, it was decided to: seek after multiple cases, triangulate, use embedded units of analysis and by adhering to a maturity framework as guidance for conducting interviews (Swanborn, 2008).

Two cases are preferred above one and three is more preferred than two. More cases means more data and this helps in identifying what aspects are specific for a certain case and what are more general aspects. With triangulation different methodologies are used to check for the same phenomenon for the cases. For this research this was done by interviewing and document analysis. As guidance for conducting the interviews they were set up semi-structured and based upon a maturity framework.

The unit of analysis is an organisation for which sub-units will be investigated: being the people within the organisation involved or responsible in formulating a SA response.

To make the data from this research as meaningful as possible and applicable to more general situations, the SA process is to be investigated for multiple cases and within those cases interviewed multiple persons for their insights on the maturity of the SA process. The responses to the SA request were not analysed until after all interviews were done. This was done to prevent any bias when interviewing persons within an organisation. Of course it was known if a response was received in time, but this was not to be remarked to prevent defensive behaviour or other reactions that could disturb the interview.

5 Findings, Analysis & Results

The results of the process of analysis followed is answering the research questions. Seven organisations were selected and sent a right of Subject Access request. Through (semi-structured) interviewing insight was obtained in the process of coming to a response for the request and a qualification was made of the maturity level of the process. The maturity level of an organisation was juxtaposed to the quality of response. The meanings and understandings of the informants regarding the choices made for maturity levels are analysed to better understand the way the Subject Access request has been organised as a process.

5.1 Research outline

5.1.1 Chronology

Four Large Financial Organisations (LFO's) and three Large Governmental Organisations (LGOs) were sent a SA request. In Appendix 4 the chronology of the requests sent out, the responses received and the decision to be interviewed or not, can be found.

5.1.2 General remarks

- Two organisations responded within the four week deadline.
- Four of the seven organisations failed to respond to the first SA request.
- One Large Financial Organisation failed to respond even after two requests.
- Achieving participation for the research was difficult and finally resulted in only 4 willing to cooperate.
- Snow ball sampling to interview as many people as possible involved in the SA request formulation process proved to be either difficult or not appropriate as anticipated.

5.2 Coding

The goal was to come to an understanding from the informant's perspective. Circumstances and bottlenecks follow from the chosen maturity levels for the categories Management, Collection and Access on the basis of 10 selected SA criteria.

5.2.1 Key & sub codes

This was operationalised by using the qualitative analysis software from MAXQDA. With it important information gathered through the interviews could be organised, sorted and categorised. (See Appendix 6 for a screenshot).

The categories and their criteria are:

Category	**ACCESS**	**MANAGEMENT**	**COLLECTION**
Criteria	1,2	3,4,5,6,9	7,8,10

Description of criteria

Criterion	Description
1	Individuals are informed about how they may obtain access to their personal information to review, update and correct.
2	Individuals are able to determine whether the entity maintains personal information about them and, upon request, may obtain access to their personal information.
3	Resources are provided by the entity to implement and support its privacy policies.
4	The types of personal information and sensitive personal information and the related processes, systems, and third parties involved in the handling of such information are identified. Such information is covered by the entity's privacy and related security policies and procedures.
5	The potential privacy impact is assessed when new processes involving personal information are implemented, and when changes are made to such processes (including any such activities outsourced to third parties or contractors), and personal information continues to be protected in accordance with the privacy policies. For this purpose, processes involving personal information include the design, acquisition, development, implementation, configuration, modification and management of the following: • Infrastructure • Systems • Applications • Web sites • Procedures • Products and services • Data bases and information repositories • Mobile computing and other similar electronic devices The use of personal information in process and system test and development is prohibited unless such information is anonymised or otherwise protected in accordance with the entity's privacy policies and procedures.
6	Policies and procedures are reviewed and compared to the requirements of applicable laws and regulations at least annually and whenever changes to such laws and regulations are made. Privacy policies and procedures are revised to conform with the requirements of applicable laws and regulations.
7	Management confirms that third parties from whom personal information is collected (that is, sources other than the individual) are reliable sources that collect information fairly and lawfully.
8	Individuals are informed that personal information is collected only for the purposes identified in the notice.

9	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 monitoring and enforcement.
10	Individuals are informed if the entity develops or acquires additional information about them for its use.

Coding was done on the basis of the three categories (= Key Codes in MAXQDA) and their sub codes, which were based on the criteria belonging to a category.

5.2.1.1 Access sub codes

The definition for Access as derived from GAPP, for the questions is: 'The entity provides individuals with access to their personal information for review and update.' For Access with regards to the SA process two criteria were selected: Criteria 1 and 2 (See Table 'Description of criteria' above)

On the basis of these two criteria three sub codes 'statutory deadline', 'transparency' and 'accessibility' were determined as important for the qualitative analysis for the key code Access.

5.2.1.2 Management sub codes

The definition for Management is: 'The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures.' For management the following criteria were selected: Criteria 3, 4, 5, 6 and 9 (9 follows 6 intentionally).

Sub codes of Key code Management: 'Training', 'Processes & Procedures', 'Resources', 'Compliance & Control', 'Responsibility'.

5.2.1.3 Collection sub codes

Definition: 'The entity collects personal information only for the purposes identified in the notice.' For collection the following criteria were selected: 7, 8 and 10.

Sub codes: Notification, Information, Purpose

Code Overview

Key codes (= categories)	**ACCESS**	**MANAGEMENT**	**COLLECTION**
Sub codes	- Statutory deadline - Transparency - Accessibility	- Training - Processes & Procedures - Resources - Compliance & Control - Responsibility	- Notification - Information - Purpose

Juxtaposing key- and sub codes for informants and type of organisation (Fin., Gov.) made it possible, to compare the given answers and perceptions, to identify patterns, connections and themes. But there also was looked for paradoxes and evidence that challenged the interpretations as stated through the hypotheses.

5.3 Qualitative Analysis

This was done by analysing the categories for the large financial and governmental organisations on the basis of respondents' choice of maturity scores in combination with the comments and remarks made in the interview to learn more about the circumstances and possible bottlenecks.

5.3.1 Analysis guidelines

As stated before, bottlenecks were not directly expected for the maturity levels defined, managed and optimised . The difference between the three is seen as a management choice between good enough, better and best (practice). Maturity levels ad hoc and repeatable can be potential bottlenecks and therefore were paid closer attention to. But also when two or more informants differed in their maturity assessment of a criterion, this could well be an indicator for a bottleneck. Special attention was paid when the difference in chosen maturity levels on the same criterion by informants differed two levels or more. For example: One informant had chosen optimised and the other defined, or managed vs repeatable.

This is even more interesting for the more important criteria than lesser important ones (see Appendix 3). For the top four most important criteria, Access criteria 1,2 and Management criteria 3 and 4, the maturity level 'defined' were more scrutinised. For the more important criteria the choice made by management were expected to be higher than just the maturity level defined (='good enough').

Also was taken into account the stated familiarity of an informant for determining the maturity level of a criterion. When the familiarity with a criterion was satisfactory or less and the chosen maturity level differed much with that of the other informant(s), who had stated their familiarity as higher than satisfactory, this was more scrutinised.

For every organisation the maturity level per criterion and the familiarity with the subject was put in a table.

Maturity levels		**Familiarity with criterion**	
Ad Hoc	= a	Very good	= vg
Repeatable	= r	Good	= g
Defined	= d	Satisfactory	= s
Managed	= m	Moderate	= mo
Optimised	= o	Poor	= p

The interviewed (informants) were coded as follows: LFO1, LFO2, LGO1 and LGO2 followed by their initials (e.g LFO2-xx). So in the table below for example LFO1-jp and d in bold and g within parentheses, means: LFO1-jp was familiar (good) with the criterion and rated it with a 'defined', which has been marked bold in

this case because it was decided to pay special attention to criteria 1 to 4 when it differed 'two steps' from the rating of another informant (LFO1-ga, optimised)

5.3.2 Large Financial Organisations (LFO)

	Access		Management					Collection			SAM
LFO1	**1**	**2**	**3**	**4**	**5**	**6**	**9**	**7**	**8**	**10**	**4.1**
LFO1-jp	**d** (g)	m (g)	m (g)	**d** (g)	d **(s)**	o (g)	o (g)	m (g)	**d** (g)	m (g)	
LFO1-ga	**o** (g)	**d** (g)	o (g)	**o** (g)	m **(s)**	m (g)	o (g)	m (g)	**o** (g)	m (g)	
LFO2											**4**
LFO2-rh	m (g)	m (g)	m (g)	m (g)	m (g)	m (g)	m (g)	m (g)	m (g)	N.A.	

* Be aware that number 6 is followed intentionally by 9

At first glance for LFO1:
- 1, 2, 4, determined as the relative more important criteria, have a 'defined' (d) and therefore were paid closer attention to;
- 1,4,8 were interesting because of two levels difference in maturity level assessment;
- None of the chosen maturity levels are ad hoc or repeatable, and therefore at face value there were no indications of possible bottlenecks.
- For 5 'Infrastructure and Systems Management' both drop their familiarity on this criterion from good to satisfactory.

For LFO2:
- All criteria are well under control (managed)

5.3.2.1 Access conditions

LFO1 has millions of customers to whom they sell to seven different brands (so-called labels). The different brands compete on the same markets but differ in their proposition and market approach. For two of the labels, with hundreds of thousands of customers, LFO1-ga supervises the SA process. For those two labels she receives (only) about 20 requests a year. For which the statutory deadline always is met.

As for Access, the informants dissent on how their organisation provides individuals with access to their personal information for review and update. LFO1-ga states that LFO1 does not pro-actively communicate to its customers that there is a SA process that can be used. This would lead to too many requests. LFO1-ga states: "If we would do that then we definitely need to employ more FTE." The choice of jp says otherwise: The SA is communicated pro-actively to emphasise that inquiries are the way to correct personal information that LFO1 is keeping.

The second Large Financial Organisation, which also has millions of customers, estimates that there are no more than ten SA requests per month. In contrast to LFO1, LFO2 has no separate labels and all requests are funnelled to one location and unit, where the requests are handled by two employees who have this responsibility.

Before there was the one centralised location and unit for handling SA requests, they were received all through the organisation and the statutory deadline was never met. This made it necessary to organise it in such a way that the requests are received in one location, with a minimum of delay. The privacy statement is a means for funnelling requests to the one location, through the company's home page, various terms and agreements and the call centre that refer to it. It is rh responsibility to keep the privacy statement up to date.

In the experience of rh only half of the SA request is "pure". That is to only learn through a request about any personal information held by an organisation on someone, with no other intentions behind it. The other half have other intentions underlying. The request in those cases are used as a "lever" to discover new insights (arguments) in running disputes on, for example, security transactions. Rulings from the court on the widened usage of SA requests have determined that this is justifiable. So when 'non-pure' SA requests are received for copies of voice recordings of security transactions this is provided accordingly. This application of the SA request procedure made it necessary to adjust the response process accordingly.

Circumstances and/or bottlenecks

- *The key to control the SA process and comply, is guidance and centralisation: Making sure that SA requests are received at one place and if not that they are forwarded internally as soon as possible for expedient processing.*

5.3.2.2 Management conditions

Almost everyone within LFO1 works one way or another with PII. The coordination of the organisations privacy policy is challenging. Although the SA process is standardised for all labels/brands within LFO1, LFO1-jp, who has a more overall point of view on the SA process, says it is a coordination challenge to keep it going accordingly because of ongoing organisational changes (restructuring, employee promotion or resignation, etc.). Because of this it is always possible that privacy within certain projects is not recognised properly as an aspect to be taken into consideration. LFO1 has learned that it is beneficial to find a balance between tightening procedures and heightening overall privacy awareness. Privacy Policy e-learning modules are important to raise awareness and ease on procedures.

Anyway compliance and regular audits are important to make sure 'the right things' are done. Governmental guidelines on data protection, in which it is explained how authorities judge the compliancy of an organisation are important in making organisational and procedural choices. New developments, publications, insights, etc. on privacy and data protection are regularly discussed in a so-called 'privacy roundtable' between managers who have privacy as a managerial responsibility.

In the LFO1 Control Framework it is established that once a year privacy policy and procedures are audited. LFO2's privacy policy is checked at least once every two year. LFO2-rh assesses the SA response process yearly and everybody in any way involved is invited to provide feedback. This is also important to see if colleagues are still 'on board' and part of the process. Keeping tabs on colleagues through meetings is also significant for LFO1-jp to learn if the process chain is broken. When issues arise then measures are taken and if necessary procedures are adapted accordingly. LFO1-ga states that senior management is very much privacy focussed and will not hesitate to act promptly when required.

Although the SA process is standardised, LFO1-ga is particular in establishing that the procedures, necessary to fulfil the statutory deadline of four weeks, are followed up in a timely manner by different departmental units who have to provide the required input for a valid SA response. When departmental units hamper the process, she does not hesitate to bring it to the attention of the 'privacy roundtable'.

LFO1 has a Lean programme running, called SENSE (A Dutch acronym that translates in 'Together Effectively Successful') and for which employees can get accreditations. LFO1-ga has a 'one star' accreditation, which contributes to her diligent pursuits to have the SA process 'up to specs' at all times. Resulting in a response time for SA request in less than two weeks. A response that was rated with a respectable 3.8 (see table in 5.4.3).

LFO1-jp and LFO2-rh both note that despite of clear procedures, it always is possible that some projects with privacy issues concerning the collection of personal data will not get the proper attention that is required. Employees can be ignorant, oblivious, under pressure, etc., and willingly or unwillingly forget about it. As LFO2-rh states: "It's a big organisation with a lot of enthusiastic marketers' with wild plans, but for most of them (initiatives) we get involved."

According to LFO2 access by Individuals to their Personal Information (criterion 1) is not really a "senior management thing". But when asked about resources (criterion 3) to implement and support its privacy policies and the answer is given in the context of the effort done by Compliance, Risk and Legal affairs, privacy is said to be a topic that has very much the attention of senior management. Anyway LFO1-rh states that with the new EU regulation much higher penalties are at stake and this certainly will raise the attention for privacy.

The legal rulings that the right of access had to be broadly interpreted, made it that LGO2 decided to make the SA Response a two-stage process. Only when someone, after receiving the first general response, asks for more and detailed information, like voice loggings, this is then provided.

LFO2-rh describes the SA process as "a tiny process". Privacy overall is most of the time part of some bigger business process, with regard to identification or some other privacy aspect. It is quite a challenge for LFO2-rh to sustain attention on privacy. Mainly because: "It is not the coolest topic around." It is therefore that LFO2-rh is glad that the Audit unit checks upon privacy compliance on a regular basis. This ensures that privacy is not forgotten and taken into consideration.

Circumstances and/or bottlenecks

- *The coordination of employees/colleagues involved in privacy processes like SA, can be challenging due to dynamics because of constant organisational changes. This needs to be actively pursued, if not then privacy (processes) falls more often than not through the cracks.*
- *Raising privacy awareness through e-learning make that employees better understand why their involvement is important.*
- *Involvement of senior management is important. Not only reactive involvement when stricter laws come into effect.*
- *The court rulings widening the usage of SA requests makes the SA request, at least for one Financial organisation, more burdensome and suspicious of the real intentions, resulting in a 'two-step' request process.*

- *Auditing is an important measure to keep the focus on privacy.*

5.3.2.3 Collection conditions

With regards to the collection of personal data and the processing of it, the purpose must have been specified and notified to the appropriate supervisory authority (Cbp). This requirement is in LFO2 designated as something legal and therefore to be handled by Legal Affairs. In order to prevent that notifications need to be updated on a regular basis, they are so broadly defined that this is circumvented. Within this notification it is also stated that profiling is done. LFO2 differentiates between hard (Name, Address, Domicile) and soft (behavioural profiles) customer data. LFO1 yearly checks with all those responsible for the collection and processing of personal data for a label if the notification to the supervisory authority is still valid or needs to be adjusted.

In both LFO's the purchase of 'hard customer data' of suspects and prospects always has to be done through a designated marketing unit. LFO2 builds customer profiles on the basis of log-in behaviour and cookies around their e-banking portal. This provides them with more than enough customer intelligence, that there is hardly no need to purchase supplemental personal data from specialized third parties. This is different for LFO1 that regularly purchases 'hard customer data' from third parties and is strongly promoting their 'Digital Insurance Portal'. It seems LFO1 wants to achieve what LFO2 already has accomplished with their e-banking portal: Intimate customer profiles.

LFO1-ga expects that customer data, from customers with different products from different labels, are combined. How extensive and elaborate this is the case, she does not know, but anyhow customers are not informed on this matter.

LFO1-ga says that when the purchased 'hard customer data' has served its purpose for a certain marketing campaign, it is not kept any longer than necessary. This is done for a very pragmatic reason: If a suspect does not become a customer within the timeframe of the marketing campaign, then over time the personal situation of a suspect changes and makes the acquired data 'useless'.

The principle of limited retention of data makes it necessary to delete data as soon as it are no longer needed for the purposes for which it was collected and therefore eventually must be erased. For the IT legacy systems, within both LFO's apparently, it is hard to delete 'old' personal data. LFO1-jp has had several discussions with IT management on the necessity of doing this, but keeps getting told that this is not possible. He keeps failing to understand why this would not be possible and gets the distinct feeling that the issue is not taken seriously. This might well be the reason that with regards to familiarity on IT Management the choice is made satisfactory (s) and not good (g) like in all other cases. Also LFO2-rh notices that especially with legacy systems deletion is problematic. But because legacy is more and more replaced, there is improvement with respect to the limited retention principle. LFO2-rh, in comparison to LFO1-jp and ga, seemed more comfortable with IT matters in relation to privacy.

Circumstances and/or bottlenecks

- *The overall inclination throughout an organisation to collect as much personal data as possible and turning it into customer information (profiles) makes it more difficult to know what is going on everywhere in large organisations.*

- *Privacy professionals need the support of IT (-security) to accomplish certain objectives. But IT is not always willing to understand what is required from them to reach those objectives.*

5.3.3 Large Governmental Organisations (LGO)

	Access		Management					Collection		
LGO1	**1**	**2**	**3**	**4**	**5**	**6**	**9**	***7**	**8**	***10**
LGO1-za	d (vg)	d (vg)	m (g)	o (s)	D (s)	m (g)	d (g)	o (g)	o (g)	d (g)
LGO2										
LGO2-vc	d (g)	d (g)	m (g)	m (g)	O (g)	M (g)	o (g)	n.a.	m (g)	n.a.
LGO2-sk	m (g)	d (s)	m (g)	o (g)	O (g)	D (g)	m (g)	n.a.	o (g)	n.a.
LGO2-mv	a (s)	d (s)	m (s/g)	m (g)	D (mo)	M (g)	o (g)	d (mo)	d (s)	o (mo)

* Because two of the three evaluators of LGO2 deemed criteria 7 and 10 not applicable (n.a.), those criterions are discarded.

At first glance:
- 1 and 2, as the more important criteria have a 'defined'.
- 1,5,8 differ two levels in maturity level assessment. But 5 is left out for LGO2 because LGO2-mv, just starting in her job as a privacy coordinator, assesses her judgement as moderate and the two other more experienced assessors as good. The lack of experience is confirmed by the answering of 7 and 10 by mv, while the other two independently judged them as not applicable.

5.3.3.1 Access conditions

See below the difference between defined and managed for questions 1 and 2

[1-Defined] Procedures granting individuals access to their information have been documented and are available to them. The procedures have been provided to employees and are consistently and uniformly applied
[1-Managed] Procedures are in place to ensure individuals receive timely communication of what information the entity maintains about them and how they can obtain access. The entity monitors information and access requests to ensure appropriate access to such personal information is provided.

For criterion 1, the difference can be summarised in reactive versus proactive.

[2-Defined] Confirmation/ authentication methods are in place to uniformly and consistently confirm the identity of individuals requesting access to their personal information. The methods include various forms of authentication depending upon the circumstances (in-person, interactive voice response, call centre, web, e-mail, etc.).
[2-Managed] Procedures are in place to track the confirmation/ authentication of individuals before they are granted access to personal information and also track the validity of granting access to such personal information.

The difference is that for 'managed' there is one authentication procedure instead of various forms and that the validity of granting access is tracked.

According to LGO1-za there are very few SA requests from the "outside in", being from civilians. LGO1-za believes the reason for this is that there is a general administrative law (Algemene wet bestuursrecht, Awb) that enables citizens to object to decisions made by LGO1. Citizens are more interested in decisions made and the process coming to a decision than in gaining insight in what personal data is collected and for what reasons. The Awb provides insight on what grounds decisions have been made. LGO1-za thinks that the 'misuse' of the SA right as stated by LFO2 is that they do not have such a 'convenient' procedure as the Awb.

When LGO1 receives a SA request it is important to figure out what it is that someone is trying to gain insight in. This is important for LGO1 to determine where to look within the organisation and in what systems. If this would not be done then LGO1 would have to check approximately 80 systems for every SA request to determine in which a requestor might be registered. LGO1 has once tested how long it would take to do this: It took a full time employee one month to look for and through all systems and gather the information for one test case.

Just like LFO2 designates the SA process as a 'small one', LGO1 designates it is a 'thin workflow'. The main challenge with a SA request is the determination of being one. A SA request is not required to be a letter with those words in capital letters on it. If someone at the counter would say "I would be interested to know what personal data you have collected of me" this formally qualifies as an SA request and should be handled accordingly by referring someone to the proper channels.

Unlike the LFO's LGO1 has not centralised the receipt of SA requests. SA requests are to be directed at the local branches of LFO1. Throughout the organisation there are 22 employees in the local branches who are assigned 'privacy duties', like taking care of SA requests. The legal timeframe for sending out a response to a SA request is perceived as difficult to accomplish. LGO1-za remarks: "One cannot do much more than one's best. That is what it boils down to, I suppose."

In contrast to LGO1, which deals with millions of citizens, this is not the case for LGO2. Ninety percent of the SA requests come from their own employees. LGO2 civil service does not deal primarily with citizens. Within LGO2 it is required that any system that holds personal data is registered. The LGO1 Data Protection Officer (Functionaris voor de Gegevensbescherming) publishes this so-called 'notification register' on the intranet with the person to contact regarding any questions. That contact is a sort of first line support to answer questions on the purpose of the registration. The main advantage of this way of organising is that when someone, not satisfied by the given answers of the first line of support, pushes forward to do a formal SA request it is known which system is concerned. For LGO2 with more than 250 systems, this is even more crucial than for LGO1. LGO2-sk sees as one of the most important tasks of the Data Protection Officer (DPO) to make collected personal data as accessible as possible. The DPO could advise to build a meta-search system over all 250 systems but does not because this would lead to yet another privacy sensitive system.

Circumstances and/or bottlenecks

- *Access is provided in a more reactive rather than proactive way and the procedures involved could be improved to make it a smoother experience.*
- *There is more interest from inquirers in knowing on what grounds decisions are based than what data is collected.*
- *The challenge with SA requests is the recognition as such.*
- *Not centralising the receipt of SA requests makes it more difficult to answer within the statutory deadline.*
- *A notification register of all systems that is accessible for everyone seems like a sensible thing to do. A logical next step would be to be able to determine all the systems where one is registered. One could argue that such a system would be in the interest of SA requestors to gain a more overall insight in how many different systems they are registered. Of course this might trigger inquisitiveness from potential requestors.*

5.3.3.2 Management circumstances

For LGO1 the SA process is so small, meaning not very much SA requests are received, which made it hard to implement a 'real' process. Because of a campaign of Bits of Freedom a few years ago, the Dutch digital rights organisation, LGO1 was forced to design and implement a SA process. The process has been decentralised in 13 regions and the process is to send a standard letter, which is the best guarantee to comply with the statutory deadline for a response.

LGO2 has drafted a regulation with regards to the Wbp which states what has to be done, but not how it has to be done. Therefore divisions differ in their governance and how processes and procedures are implemented.

LGO2-vc has an independent role and only answers to the secretary, who in the end is accountable for privacy. LGO2-vc has the authority to address privacy related issues to the senior executives. The past years LGO2 has been constantly in a state of reorganisation and privacy has not been a priority for the senior executives. LGO2-vc therefore has to remember them, as often as possible, not to forget about it. As LGO2-vc states: "Believe me, not everybody dreams of privacy". With the 'continuous' reorganisations, outsourcing is an important driver to cut costs. It is especially with the transfer of personal data of employees to outsourcers that LGO2-vc pays close attention that this happens correctly. He does this by checking closely the terms and conditions with regards to the data protection aspects of some of outsourcing deals where there is a lot of personal data involved.

The so-called Wbp-coordinators play an important role within the divisions to build and sustain privacy awareness. They need to proactively get involved in projects or issues where data privacy play a role. But how well they do this is not checked. And in my case where my SA request 'bounced' through the organisation and finally got in the hands of, through an intervention of LGO2-vc, LGO2-mv complained about the lack of organisational support in responding to it.

My SA request, which 'bounced' through LGO2, made LGO2-vc clear that the SA response process needed some adjustment when a request from a civilian like me, who also is a part time employee of LGO2, needs to be 'routed' differently. One could say that this is proof of the fact that the SA response process was not mature (yet) because not all 'request variations' were known.

Circumstances and/or bottlenecks:

- *Building privacy-awareness is not easy, especially when it is not deemed as pressing as other management matters. It helps both LGO1 & 2 to have a DPO who has the right and authority to ask, inform and challenge senior management.*
- *When outsourcing is an important strategy to cut costs, it is also important to make sure that with regards to transferred personal data solid arrangements are made.*

5.3.3.3 Collection circumstances

LGO2, mainly collects personal data of their own employees and has, in comparison to LGO1, nearly no personal data of citizens. The core business of LGO1 is to collect as much personal data (of citizens) as necessary to perform their statutory duty. It is in the interest of LGO1 to be as secretive as possible about what and when they collect, because knowing this would be a clear indicator how they detect fraud. When necessary LGO1 will rephrase the legal requirement to state the purpose of collection. Fortunately the Wbp is so broadly formulated that this can be done. “On some matters there is disclosure and on some matters there is not”.

Circumstances and/or bottlenecks:
When deemed necessary the purpose of collection will (and can) be changed.

5.3.4 Process Improvement

Within the two LGO’s process improvement methodologies like Lean were unfamiliar and not known to be used to improve Privacy process like the SA response process.

The informants of the two LFO’s were acquainted with Lean and indicated that the methodology was used to improve processes and done so for the SA Process. Being Lean and improving processes is ongoing for both organisations.

5.4 Results

For answering the research question:

> **How can the right of Subject Access (SA) process within organisations be improved to deliver timely and adequate responses?**

Three sub questions were to be answered.

5.4.1 First research sub question

> **1.What circumstances and bottlenecks surrounding the response process can be identified within an organisation?**

The structured part of the interviews resulted in scores for subject access maturity levels, as perceived by (an) employee(s) who was part of the SA process (→ SAM). From the analysis of the interviews (the unstructured part) the insights as described above were gathered.

The level of privacy maturity is expected to influence the quality of a response. The research shows:

	LFO1	**LGO1**	**LFO2**	**LGO2**
Mean SAM	4,1	3,8	4	3,8

LFO1
LFO1 has set up a 'SA response process' guidance, to be implemented throughout the organisation. LFO1 is also very process conscious, with a Lean methodology geared to the organisation called SENS (acronym for 'together effectively establishing success'). Despite this process orientation and the way it is actively carried out to look for possible improvements only makes that the SA response was received in time, but not at all responded in a way according to legal requirements.

LFO2
LFO2 which receives approximately ten SA requests per month has organised the communication as effectively as possible to prevent receiving them throughout the organisation. Because LFO2 has experienced that (half of the) customers who send in a SA request do this for other reasons than to learn about the usage of their PII, this has resulted in a SA process that is set up 'perfectly' avoiding being 'misused' by customers, but sending out SA responses which are not compliant with the legal requirements of what information to provide and also not within time. Because of this focus on not wasting resources in order to prevent 'misuse', the other 'sincere half' of SA requesters suffer from this measure. This is especially so because in the response no statement was made, as affirmed in the interview, that further more detailed inquiries were welcomed.

LGO1
For LGO1, which has a decentralised approach for answering SA requests, the response was not too far from being adequate but in time. Just like LFO2 LGO1 wants to prevent wasting resources needed to investigate in what systems a requestor is registered.

LGO2
LGO2 which has set up a more generic privacy policy & governance document what is expected to be done by different identified roles throughout the organisation and not stating how something like the SA response process should be implemented on decentralised level, also resulted in a proper SA response. The reason that LGO2 does not have a real 'SA response process' is that requests mainly, but very few, come from their own employees and they can consult on the intranet an 'application registration system' of all applications that register personal data and check what the reason, goal, etc. of it is. When there still remain questions there is the possibility to contact the application owner. And if this is not proving sufficient a SA request can be sent. For LGO2 the proper response received, is not so much the result of a defined process but of the responsible person for the response and the support she had to look for. The reason that the response was not received in time was because the SA request was misinterpreted and sent to a different department for answering. When it became clear that the request did not belong there and

was forwarded to the right person, there was not enough time left to send a decent response and also before the deadline.

This leads to the second research question.

5.4.2 Second research sub question

2. What is the quality of a response to a 'right of Subject Access' (SA) request in accordance with the legal requirements?

To find an answer to this sub question, documentary analysis was the method of choice (See Appendix 7). The result of this are the following SAR scores for the organisations (See Section 4.7 for calculation method).

	LFO1	**LGO1**	**LFO2**	**LGO2**
Mean SAR	0,8	2,6	0,6	3,8

It was determined that:

- If Mean SAR >3 = Adequate
- If Mean SAR <3 = Inadequate

This leads to the third research question.

5.4.3 Third research sub question

3. What can be learned from the comparison of the analysis of the findings on privacy maturity (SAM) and response quality (SAR) to come to recommendations for an effective process around right of subject access?

SAM is compared with SAR and evaluated on the basis of the hypotheses made. This could only be done for the organisations that participated in the research.

Overview

	Participating				**Non-participating**		
	LFO1	**LGO1**	**LFO2**	**LGO2**	**Nat. Ned**	**ABN AMRO**	**SVB**
Interviews	2	1	1	3	X	X	X
Mean SAM	4,1	3,8	4	3,8	X	X	X
Mean SAR	0,8	2,6	0,6	3,8	X	4	1
In time	Yes	Yes	No	No	X	No	No
SAR Category Score	2	2	1	3			

SA Overall Performance	8,2= Medium	7,6= Medium	4= Low	11,4= Medium			
Number of SAR criteria <u>not</u> answered	0	0	6	1		1	5

For the calculation and determination of Mean SAM and Mean SAR, see Sections 4.5 to 4.7. See Appendix 7 for the results.

SAR Category Score determination :

	In time	Not-in-time
Adequate	4	3
Inadequate	2	1

'Mean SAM' x 'SAR category score' = 'SA overall performance'

SAR category	Mean SAM				
	Ad Hoc (=1)	Repeatable (=2)	Defined (=3)	Managed (=4)	Optimised (=5)
Not-in-time & in-adequate (=1)	1	2	3	4 **LFO2**	5
In time & inadequate (=2)	2	4	6 **LGO1**	8 **LFO1**	10
Not-in-time & adequate (=3)	3	6	9	12 **LGO2**	15
In time & adequate (=4)	4	8	12	16	20

From the four cases none of them falls in the category "in time & adequate". These results are in line with the results of previous SA response research.

Hypotheses were posed to guide the search for patterns and common themes emerging in the maturity choices made and accompanying explanations during the interviews. SAM/SAR and LFO/LGO are compared on the basis of the hypotheses made.

- Hypothesis 1

An organisation with a good SA process in place (high SAM; independent variable) has less difficulty responding to Right of subject access requests than an organisation with a flawed SA process and therefore will show a better SA Response (=dependent variable).

- Hypothesis 2

SA maturity levels 4 & 5 are more to be expected for financial organisations than for public organisations. The levels to be found for public organisations are expected to be maturity levels 4 or less. So finance

organisations with a higher propensity for (continuous) process improvement (Lean c.s.) are expected to show more SAR Category "4" ("in time & adequate") kind of results than the public organisations.

When these hypotheses are juxtaposed to the above overview table, it becomes clear, that:
- Not one of the cases evaluates its own SA maturity level lower than 3. The governmental and financial organisations each evaluate their SA maturity as 'more or less' managed (=4).
- The LFO's judge their SA maturity slightly higher and also showed more propensity towards process improvement than the LGO's, but still have a much worse result for the SA responses.
- Three of the four organisations show a substantial difference between the perceived SA maturity and the SA response. The two LFO's from these three even show the worst responses and in no way near to "in time & adequate".

This leads to the conclusion that there is little validation for both hypotheses.

Of course the results cannot be generalised to all large financial and governmental organisations due to the qualitative character of this study. The goal was to gain a more intimate insight and learn from the similarities and differences between the organisations.

6 Conclusion & Discussion

As stated in the introduction of this thesis "when something online is free, you're not the consumer, you're the product." And being the product is based on the personal data that is collected from individuals. Personal data is the digital currency of the 21st century. Knowing what interests and triggers someone is worth money. Although a growing number of people are beginning to understand this, they are not yet doing so much by checking their 'digital currency' account by means of a SA request. Also the investigated financial and governmental organisations will not pro-actively promote SA Requests any time soon.

For the answer and conclusion to the research question the results from the previous chapter are the basis.

> **How can the right of Subject Access (SA) process within organisations be improved to deliver timely and adequate responses?**

Any thoughts and ideas that result from the conclusion and not directly based on the results will be part of the discussion section of this chapter.

6.1 Conclusion

This case study shows that to improve the right of SA process, it is important to:

- Centralise request receipt;
- Standardise the SA response on the basis of the legal requirements. Build a Response template and use that as the basis for a reverse process design;
- Build and maintain an Application register for all PII handling systems ('View of the Wood');
- Develop a Meta data application to discover and find in which applications someone is registered ('View of the trees');
- Audit regularly and keep the 'privacy spirit' alive;
- Senior management involvement and commitment;
- Appointment of a Chief Privacy Officer;
- Not just reactive involvement when stricter laws come into effect;
- Create a (virtual) Privacy Office and appoint 'privacy advocates' (super-users) throughout the organisation.

The cases in this research make it clear that as the collected data grows exponentially and is processed and stored in a growing number of systems, it becomes harder to pinpoint PII on an individual level for customers and deliver a timely and adequate response if requested. All four organisations state it as a challenge and a burden to find out exactly in which systems a requestor's personal data is collected and for what specific purpose. Therefore the propensity currently is to minimise the request 'demand' for SA's as much as possible and not so much to build a 'faster and better' response process.

Only when an organisation (like LGO2) keeps a register of all applications throughout the organisation and the purpose of each one of them, then it is possible to find the necessary answers. This will increasingly become more relevant when personal data in information systems is incorrect, outdated or incomplete and becomes a source of serious hindrance because of exclusion from certain services or facilities someone is perfectly entitled to. In a lot of situations it is undesirable not to see the forest for the trees but for privacy this is not the case: it is necessary to see all the trees. When the 'Computer says no' (Little Britain,

Youtube) it is important to be able to exercise one's right to object to decisions being taken by automated means. This starts with looking for the information systems where things went wrong and the Right of Subject Access is instrumental for this.

That LGO2 keeps a register is due to the DPO who has made this happen. This is in contrast to the other organisations that rather are compliant by stating a general data collection purpose rule that is so broadly formulated that it is a 'license' to implement as many 'PII-handling' systems as they see fit. Which of course should not be restricted in any way, but done in a more cautious manner. This makes a case for the pending General Data Protection Regulation (GDPR) that requires that data protection is designed into business processes and the supporting information systems. Data minimisation is a leading 'privacy by design' principle and should be institutionalized in the expansion of existing systems and new systems, eventually resulting in 'just enough' PII within the organisation to accomplish their goals. A 'Just enough' PII strategy would reduce the required protection measures and thereby resulting in a more efficient Information Security approach. As would a governance structure of 'Privacy advocates' throughout the organisation lead indirectly to an enhanced security awareness because privacy needs security.

Funnelling SA requests to a designated point (letterbox, e-mail address) or person(s) within the organisation is crucial for a good head start to accomplish a timely response. To accomplish that the different organisations communicate this mainly through their websites where requestors can find the details. This approach can help requestors and an organisation, but cannot be made obligatory. If a request is not mentioned as such, it should be treated so if it is clear that someone is asking for their own personal data. Of course this makes recognising a request as difficult and for which most organisations are not up to. This case study shows that the organisations investigated are not particular keen on spending any more time and effort in providing access than necessary and therefore it is kept 'quiet' to keep the number of requests as low as possible and prevent the right of Subject Access to become too popular.

This is even more the case for the financial organisations than the governmental organisations. They might be more process oriented but it does not seem to help when it comes to delivering adequate and timely responses. Even process improvements initiatives (Lean, etc.) that are more known and actively implemented in the financial business environment does not seem to have much effect in doing a better job. Effectively the LFO's have a managed (maturity level) response process for a substandard response. Unfortunately to prove one is compliant it is often enough to show one has a process in place and not so much that the process leads to the desired results.

Auditing is an important measure to keep attention and focus on privacy alive. Unfortunately privacy in general and Right of SA specifically are not regarded as topics that can win the trust of customers and therefore done in a hastened way to be done with it.

Effective processes need dedicated people and a lot of that dedication comes from committed leaders pushing forward. A dedicated privacy leader being someone who has the authority to motivate and make people understand to do 'the right thing'. Senior management must lead the way by actively addressing it and appointing a (Chief) 'Privacy Officer'. A sort of specialised DPO with PII in mind. A dedicated Chief or Officer can make the difference because he is entitled to challenge his peer chiefs on the matter and expected to drive privacy forward in the organisation by creating a (virtual) Privacy office by appointing 'privacy advocates'. The latter are important to be of assistance and engrain privacy into the corporate

culture. When in time this is established a SA process makes more sense and will not be broken so easily and provide for better results.

A Chief Privacy Officer plays also an important role through teaming with the Chief Information Security Officer (CISO) to make his staff more privacy minded. Privacy relies for a great part on IT (-security) but informants have stated that it is not easy or even difficult to engage IT(-security) in their efforts to accomplish certain privacy goals. They encounter pseudo or false technological objections, because of a certain reluctance to organise IT in a way that privacy becomes part of the IT-designs/architectures.

The poor quality of responses witnessed in this case study for the financial organisations and although in no way representative for the whole sector, the client base of both organisations is tens of millions of individuals. The right of SA is fundamental to data protection and it will never be reasonable to deny access to the requested information merely because responding to the request may be inconvenient , labour-intensive and bad for the bottom line. It will become increasingly important to check the accuracy of one's personal data and where it is incorrect, especially when it is leading to unwarranted decisions, to request a correction. The SA request process should more be perceived as an 'open source' for improving information systems and business processes in the 'second machine age' we are now entering (Brynjolfsson & McAfee, 2014).

6.2 Discussion

As the number of databases an average individual is registered in could easily reach 1000, one can expect it will increasingly become impossible to control one's personal data. Nonetheless this does not mean that it is should not be given any thought how more transparency can be accomplished for individuals. Technological advancements in Big Data and Cloud Computing will inevitably lead to more and more dynamics around personal data. The first leading to better and faster decisions for most of us but also to wrong decisions for some of us (false negatives) and the second one to personal data flying around the globe for the best possible storage location within its tracks cyber criminals looking for windows of opportunity to lay their hands on personal data. The SA request should mature within organisations and for citizens, through actively pursued compliance and nudging by the government, to a necessary means to keep tabs on PII, derived profiles and how (automated) decisions are come to.

An analogy

In 2008 it became mandatory for Insurance companies to provide an overview of the retirement claims of individuals in a standardised way (a 'Uniform Retirement Summary'). This was deemed not feasible or even impossible to accomplish. For many years it was postponed and stalled until through legislation it was required to do so and it was realised within two years. Of course this was no small and cheap operation but nonetheless very necessary to provide insight for individuals in the payments to come and to know if something had to be done now to prevent financial problems in the future. A special portal has been created to provide the information where every citizen can log in and get a clear and total picture of their financial retirement situation.

Fast forward: 2020

Personal data a.k.a. digital currency which now resides in a sort of shadow economy should also be brought out in the open in the same way as done with retirement plans, enabling individuals to find out where and

what PII is held about them and request more information in a standardised way (a 'Uniform Privacy Summary') and better understand why and what is the case with their personal data and to what consequences. This would also motivate organisations to delete personal data that is of no more use or relevance. What you do not have you cannot be asked about and just holding on to personal data, because it is technically so easy, could also be too expensive in terms of unnecessary risk exposure in case of a possible data breach. So also on an organisational level there is a sort of right to be forgotten. Starting any time soon would make it possible to have in 2020 a PII-Portal where citizens could check their digital shadows.

7 BIBLIOGRAPHY

Acquisti, A., Friedman, A., & Telang, R. (2006). Is there a cost to privacy breaches? An event study. Cambridge UK: Fifth Workshop on the Economics of Information Security.

(2011). *AICPA/CICA Privacy Maturity Model.* American Institute of Certified Public Accountants (AICPA) and Canadian Institute of Chartered Accountants (CICA).

Arnbak, A., & Van Den Berg, B. (2011). *Jaarboek Ict En Samenleving 2011. De transparante samenleving.* Media Update Vakpublicaties.

Article 29 Data Protection Working Party. (2007). *Opinion 4/2007 on the concept of personal data.* Retrieved June 2013, from ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf

(2011). *Attitudes on data protection and electronic identity in the European Union .* Brussel: Special Eurobarometer 359 .

Bertram, D. (n.d.). *Likert Scales.* Retrieved July 2013, from The Faculty of Mathematics. University of Belgrade: http://poincare.matf.bg.ac.rs/~kristina/topic-dane-likert.pdf

Beusekom, v. H., & Raaijmakers, K. (2010, Oktober). Waarom iedereen in 2015 compliance officer wil zijn.

Blarkom, V. G., Borking, J., & Olk, J. (2003). *Handbook of Privacy and Privacy enhancing technologies- The case of Intelligent Software Agents.* The Hague, The Netherlands: College bescherming persoonsgegevens.

Bloem, J., Van Doorn, M., Duivestein, S., Van Manen, T., & Van Ommeren, E. (2012). *Big Social. Predicting behavior with Big Data.* Groningen: LINE UP boek en media.

Bloem, J., Van Doorn, M., Duivestein, S., Van Manen, T., & Van Ommeren, E. (2013). *Privacy, technologie en de wet. Big Data voor iedereen door goed design.* Sogeti.

Boston Consultancy Group. (2012, November 20). The value of our digital identity.

Brynjolfsson, E., & McAfee, A. (2014). *The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies.* W. W. Norton & Company.

Burghardt, T., Bohm, K., Buchmann, E., Kuhling, J., & Sivridis, A. (2010). A Study on the Lack of Enforcement of Data Protection Acts. In A. B. Sideridis, & C. Z. Patrikakis, *Next Generation Society Technological and Legal Issues* (pp. 3-12). Springer Berlin Heidelberg.

Cavoukian, A. (2012). *Privacy by Design and the emerging personal data ecosystem.* Retrieved from Privacybydesign: http://privacybydesign.ca/content/uploads/2012/10/pbd-pde.

Cavoukian, A. (2013). *Privacy and Security by Design: A Convergence of Paradigms.* Retrieved from Information & Privacy Commissioner Ontario Canada: http://www.ipc.on.ca/images/resources/pbd-convergenceofparadigms.pdf

Child Labour. (n.d.). Retrieved Feb 2014, from Wikipedia: https://en.wikipedia.org/wiki/Child_labour

Colle, S., & Werhane, P. H. (2008). Moral motivation across ethical theories: What can we learn for designing corporate ethics programs? *Journal of Business Ethics*, 751-764.

College Bescherming Persoonsgegevens. (2014, February). *Raamwerk Privacy Audit.* Retrieved from www.cbpweb.nl: http://www.cbpweb.nl/Pages/ind_wetten_zelfr_compliance_rpa.aspx

Comparison of International Privacy Concepts. (n.d.). Retrieved from AICPA: http://www.aicpa.org/InterestAreas/InformationTechnology/Resources/Privacy/GenerallyAcceptedPrivacyPrinciples/Pages/InternationalPrivacyConcepts.aspx

Culnan, M. J., & Armstrong, P. K. (1999). Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation. *Organization Science*, 104-115.

Davies, S. (2010, p.6, October 27). Why Privacy by Design is the next crucial step for privacy protection.

Degeling, M., & Loser, K.-U. (n.d.). *An Approach to introduce Privacy by Design in Agile App-Development.* Retrieved June 2013, from http://prescient-project.eu/: http://prescient-project.eu/prescient/inhalte/download/3-Degeling.pdf

Denzin, N. K., & Lincoln, Y. S. (2005). *The SAGE Handbook of Qualitative Research.* by Norman K. Denzin (Editor), Yvonna S. Lincoln (Editor).

Dix, A. (2010). Built-in privacy—no panacea, but a necessary condition for effective privacy protection. *Identity in the Information Society*, 257-265.

Druschel, P., Backes, M., & Tirtea, R. (2011). *The right to be forgotten – between expectations and practice.*

Emerson, R. M., Fretz, R. I., & Shaw, L. (1995). *Writing ethnographic fieldnotes.* Chicago: University of Chicago Press.

Fieser, J. (2009, May). *Ethics*. Retrieved July 2013, from Internet Encyclopedia of Philosophy: http://www.iep.utm.edu/ethics/

Garfinkel, S. (2000). *Database Nation: The death of privacy in the 21st century.* O'reilly Media.

Generally Accepted Privacy Principles. CPA and PA Practioner Version. (2009, August). Retrieved from AICPA: http://www.aicpa.org/InterestAreas/InformationTechnology/Resources/Privacy/GenerallyAcceptedPrivacyPrinciples/DownloadableDocuments/GAPP_PRAC_%200909.pdf

Gillham, B. (2005). *Research Interviewing: The Range of Techniques.* McGraw-Hill International.

Governatori, G., & Sadiq, S. (2009). The Journey to Business Process Compliance. In J. Cardoso, & W. Van der Aalst, *Handbook of Research on Business Process Modeling* (pp. 426-445). IGI Global.

Hashmi, M., Governatori, G., & Wynn, M. (2012). Business Process Data Compliance. *Lecture Notes in Computer Science Series* (pp. 32-46.). Montpellier, France: Springer.

Hener, M. (2011, March). What makes good people do bad things. *Compliance & Integriteit*, pp. 5-6.

Hern, A. (2014, june 4). *EU commissioner: right to be forgotten is no harder to enforce than copyright*. Retrieved from http://www.theguardian.com/: http://www.theguardian.com/technology/2014/jun/04/eu-commissioner-right-to-be-forgotten-enforce-copyright-google

How will the EU's data protection reform benefit European businesses? (n.d.). Retrieved Feb 2014, from European Commission: http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/7_en.pdf

Hulstijn, J. (2012). Compliance by design. *RegelMaat*, 88-100.

International Telecommunication Union. (2012). *World Telecommunication/ICT Indicators Database.* http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx: International Telecommunication Union.

Kirkwood, B. R., & Sterne, J. A. (2003). *Essential medical statistics.* Oxford: Blackwell.

Lohmann, N. (2013, June). Compliance by design for artifact-centric business processes. *Information Systems*, 606–618.

MacQueen, K., & Milstein, B. (1999). A systems approach to qualitative data management and analysis. *Field Methods Vol.11*, 27–39.

Mayer-Schönberger, V. (2011). *Delete: The Virtue of Forgetting in the Digital Age .* Princeton University Press.

McLellan, E., MacQueen, K., & Neidig, J. (2003 Vol.15). Beyond the Qualitative Interview: Data preparation and transcription. *Field Method*, 63-84.

Muhlen, M. z., & Shapiro, R. (2010). Business process analytics. In J. v. Brocke, & M. Rosemann (Eds.), *Handbook on Business Process Management 2: Strategic Alignment, Governance, People and Culture* (pp. 137-157). Springer.

Nijhof, A. H., & Rietdijk, M. M. (1995). An ABC-analysis of Ethical Organizational Behavior. *Journal of Business Ethics*, 39-50.

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. (n.d.). Retrieved June 2013, from oecd.org: http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

Potter, J. W. (1996). *An Analysis of Thinking and Research about Qualitative Methods.* Lawrence Erlbaum Associates.

Privacy and Data Protection by country. (2013). Retrieved May 2013, from Forrester: http://heatmap.forrestertools.com/

Process Mining Manifesto. (2012). *Lecture Notes in Business Information Processing*, 169-194.

Putker-Blees, A., & Berkhout, D. (2008). Privacywetgeving: troebel en 'troubles' in plaats van transparantie. *Arbeidsrecht*, 10-14.

Putker-Blees, A., & Meulenveld, A. (2006). Inzicht in het inzagerecht. *Sociaal Recht*, 294-300.

Rost, M., & Bock, K. (2011). Privacy By Design und die Neuen Schutzziele. *DuD - Datenschutz und Datensicherheit*, 30-35.

Rubinstein, I. S. (2011). Regulating Privacy by Design. *Berkeley Technology Law Journal*, 1410-1456.

Sadiq, S., & Governatori, G. (2010). Managing Regulatory Compliance in Business Processes. In J. Vom Brocke, & M. Rosemann (Eds.), *Handbook on Business Process Management 2* (pp. 159-175). Springer Berlin Heidelberg.

Sauerwein, L.B.; Linneman, J.J. (2002, April). *Handleiding wet bescherming persoonsgegevens.* Retrieved Nov. 2013, from www.rijksoverheid.nl: http://www.rijksoverheid.nl/documenten-en-publicaties/brochures/2006/07/13/handleiding-wet-bescherming-persoonsgegevens.html

Schermer, B. W., & Wagemans, T. (2009). *Onze digitale schaduw.* College bescherming persoonsgegevens.

Schumm, D., Leymann, F., & Streule, A. (2010). Process Views to Support Compliance Management in Business Processes. In F. Buccafurri, & G. Semeraro, *E-Commerce and Web Technologies* (pp. 131-142). Springer Berlin Heidelberg.

Simon, H. (1976). *Administrative behavior : a study of decision-making processes in administrative organizations* (3rd ed.). New York: The Free Press.

Simon, H. (1978). *Rational decision making in business organisations.* Opgehaald van Nobelprize.org: http://www.nobelprize.org/nobel_prizes/economic-sciences/laureates/1978/simon-lecture.pdf

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: Measuring individuals'concerns about organizationals practices. *MIS Quarterly*(Vol.20(2)), 167-196.

Smith, J. (1993). Privacy policies and practices: Inside the organizational maze. *Communications of the ACM*(vol.36, no. 12), 105-122.

Solove, D. J. (2006, January). A taxonomy of privacy. *University of Pennsylvania Law Review*, 477-560.

Spekschoor, J. (2012). *Business Process Management Maturity in the Netherlands 2011.* Utrecht.

Stone, E. F., Gardner, E., Gueutal, H., & McClure, S. (1983, p.2, August). A Field Experiment Comparing Information Privacy Valuse, Beliefs and Attitudes Across Several Types of Organizations. *Journal of Applied Psychology*, 459-468.

Swanborn, P. (2008). *Case-study's Wat, wanneer en hoe?* Boom Lemma.

Szilvasi, L. (2012, maart 30). *Apple schaft toegang tot UDID af: Goed voor jouw privacyY?* Opgehaald van www.bof.nl: https://www.bof.nl/2012/03/30/apple-schaft-toegang-tot-udid-af-goed-voor-jouw-privacy/

Tokmetzis, D. (2012). *De Digitale Schaduw .* Spectrum.

Trkman, P. (2010). The critical success factors of business process management. *International Journal of Information Management*, 125-134.

Van der Aalst, W. (2013, okt 10). *Privacy Compliance and Enforcement (PriCE) & Process Mining.* Opgehaald van www.iipvv.nl: https://www.iipvv.nl/sites/stw.demo.infi.nl/files/downloads/PriCE-project-WvdA-NCSRA2013.pdf

Vermeer, R. (2012, maart 27). *Menzis en Nuon weten zich geen raad met privacywet*. Opgehaald van www.webwereld.nl: http://webwereld.nl/e-commerce/220-menzis-en-nuon-weten-zich-geen-raad-met-privacywet

Verschuren, P., & Doorewaard, H. (2010). *Het ontwerpen van een onderzoek.* Boom Lemma.

Wright, D., & de Hert, P. (Eds.). (2012). *Privacy Impact Assessment.* Springer.

Zwenne, G.-J. (2012, February). *Privacy and the protection of personal data in Europe.* Retrieved May 2013, from Zwenneblog: zwenneblog.weblog.leidenuniv.nl/ files/ 2013/ 03/ LLC-Personal-Data-Protection-Feb2013-def.pdf

Zwenne, G.-J., Duthler, A.-W., Groothuis, M., Kielman, H., Koelewijn, W., & Mommer, L. (2007). *Eerste fase evaluatie Wet bescherming persoonsgegevens.* Ministerie van Justitie.

APPENDIX 1

SA PRINCIPLES & CRITERIA SELECTION
In this Appendix it is shown how from the 'general' Privacy Maturity Model a SA Maturity Model has been constructed.

GAPP PRINCIPLES
As described (Chapter 2.7) the Privacy Maturity Model (PMM) is based on GAPP and the Capability Maturity Model (CMM).

"GAPP operationalises complex privacy requirements into a single privacy objective that is supported by 10 privacy principles. Each principle is supported by objective, measurable criteria that form the basis for effective management of privacy risk and compliance in an organisation." (Generally Accepted Privacy Principles. CPA and PA Practioner Version, 2009, p1).

For every principle there are criteria set in the form of statements. There a total of 73 criteria. For each criterion a level of maturity has to be determined. The maturity levels being, either: Ad Hoc, Repeatable, Defined, Managed or Optimised .

The 10 privacy principles :

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
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 regulation 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.

(Generally Accepted Privacy Principles. CPA and PA Practioner Version, 2009)

SA PRINCIPLES

The SA Process was evaluated on the basis of a subset of the above principles, tuned specifically towards the Right of subject access. To determine the subset of principles all criteria from all principles were 'screened' for relevance in some way to Right of subject access.

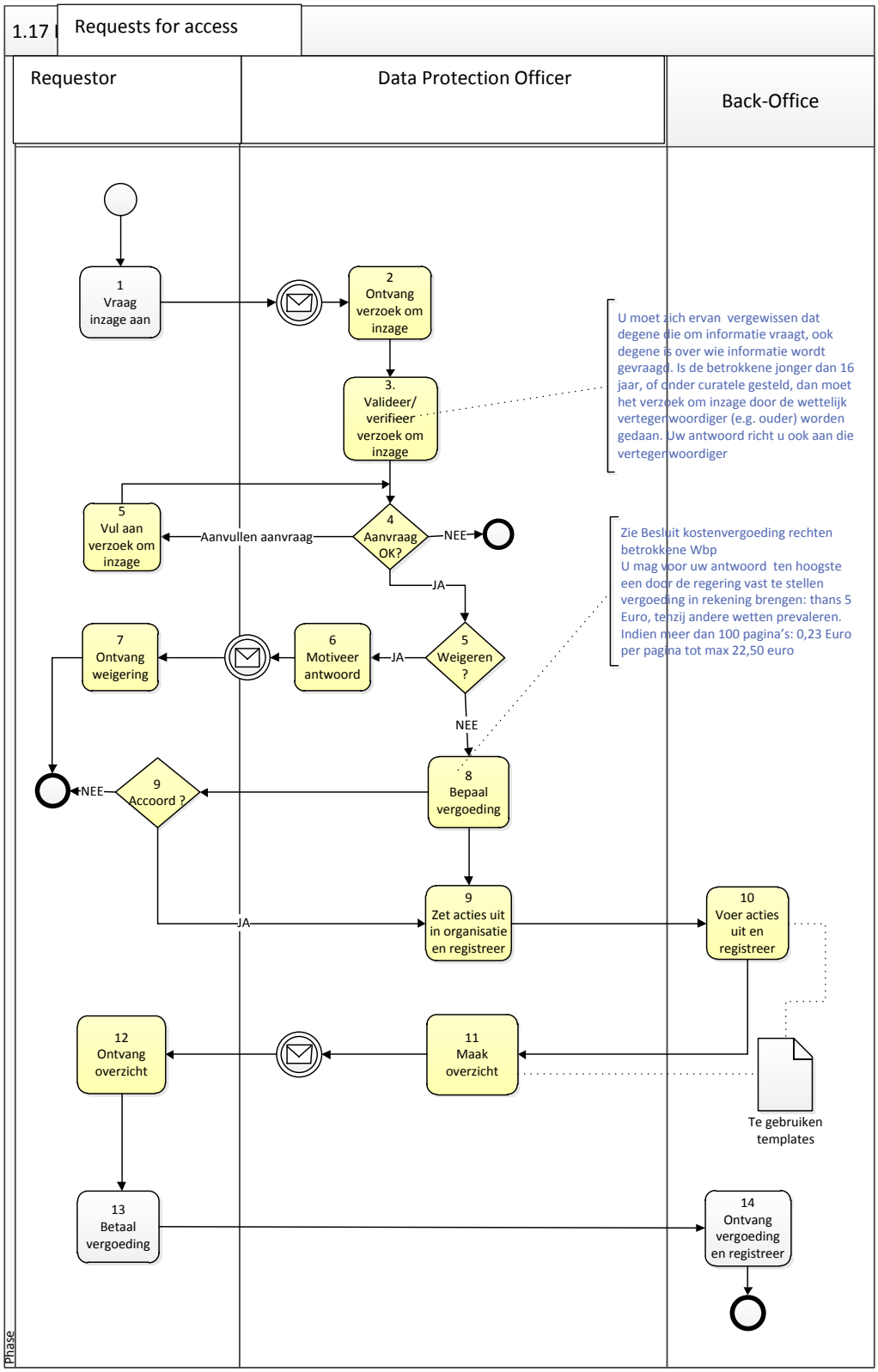
The 10 principles/73 criteria were screened on the basis of the (Dutch) legal requirements of a SA response, being:

- A complete synopsis of the processed personal information of the person concerned.**(1)**
- A definition of :
  - The purpose(s) of data processing; **(2)**
  - The categories of data related to the processing of it; **(3)**
  - The recipients or categories of recipients. **(4)**
- All available information on the origin of the personal information. **(5)**
- When specifically asked for an organisation also must explain the systematics of the automation of data processing. **(6)** (Sauerwein, L.B.; Linneman, J.J., 2002)

APPENDIX 2 SA REQUEST BUSINESS PROCESS MODEL AND NOTATION

In Dutch!

Used when respondent needed to be motivated for interview



APPENDIX 3 KEY WORD MATCHING

The selection of criteria is done by Cross referencing for **process improvement**. See keywords underlined:
- If a process needs to be improved or modified, it is clear who is responsible.
- Management has an active role in improving processes.
- Continuous improvement is pursued by means of improvement planning and control, focusing on quantitative measurable process improvement: Plan-Do-Check-Act cycle.
- The organisation uses methods like Lean and/or Six Sigma and/or Theory of Constraints, to improve processes.
- Employees are actively and frequently involved in improving their processes.
- Relevant stakeholders (customers/patients/…, third parties) are sufficiently involved in the process and process improvement.

Keywords looked up within the GAPP principles

- Keyword: **Management**
1.1.2, 1.2.1. 1.2.2, 1.2.4, 1.2.6, 1.2.7, 1.2.8, 1.2.9, 1.2.10, 2.2.2, 4.1.2, 4.2.2., 4.2.3, 5.2.1, 6.1.1., 8.2.1, 8.2.2, 8.2.4- 8.2.7, 10.1.1, 10.2.1, 10.2.3-10.2.5
- Keyword: **Responsible/Responsibility**
1.1.1, 1.1.2, 1.2.8, 1.2.9, 9.1.1, 9.2.1,
- Keyword: **Improve(ment)/improving**
1.1.1, 1.1.2, 1.2.7, 1.2.9, 2.1.1, 2.2.3, 3.1.1,3.2.1, 3.2.2, 4.1.1, 4.2.3, 5.1.1, 6.1.1, 6.2.1, 7.1.1, 8.2.1, 8.2.4, 8.2.7, 9.2.1, 9.2.2, 10.2.2, 10.2.4, 10.2.5,
- Keyword: **Methods (bpm types)**
None mentioned
- Keyword: **Employees/Stakeholder & involved/involvement**
1.2.3, 1.2.5, 1.2.7, 6.2.6

Final selection of criteria:

1. Principles: **A** (Management), **D** (Collection) and **G** (Access) have the most 'hits' and are therefore determined as leading SA criteria 'providers' and that G >A>D (> = more important)
2. Then criteria with a 'hit' on Process Improvement keywords were determined of more important than criteria without a hit.
3. Then criteria that were selected twice for a legal requirement within a GAPP principle ('2x' criteria) were determined more important than '1x' criteria.

This resulted, in order of importance (1 most important), the following criteria:

1	6.1.1	Individuals are informed about how they may obtain access to their personal information to review, update and correct.
2	6.2.6	
3	6.2.1	Individuals are able to determine whether the entity maintains personal information about them and, upon request, may obtain access to their personal information.

4	1.2.8	Resources are provided by the entity to implement and support its privacy policies.
5	1.2.3	The types of personal information and sensitive personal information and the related processes, systems, and third parties involved in the handling of such information are identified. Such information is covered by the entity's privacy and related security policies and procedures.
6	1.2.6	The potential privacy impact is assessed when new processes involving personal information are implemented, and when changes are made to such processes (including any such activities outsourced to third parties or contractors), and personal information continues to be protected in accordance with the privacy policies. For this purpose, processes involving personal information include the design, acquisition, development, implementation, configuration, modification and management of the following: • Infrastructure • Systems • Applications • Web sites • Procedures • Products and services • Data bases and information repositories • Mobile computing and other similar electronic devices The use of personal information in process and system test and development is prohibited unless such information is anonymized or otherwise protected in accordance with the entity's privacy policies and procedures.
7	1.2.2	Policies and procedures are reviewed and compared to the requirements of applicable laws and regulations at least annually and whenever changes to such laws and regulations are made. Privacy policies and procedures are revised to conform with the requirements of applicable laws and regulations.
8	4.2.3	Management confirms that third parties from whom personal information is collected (that is, sources other than the individual) are reliable sources that collect information fairly and lawfully.
9	4.1.2	Risk classification is already covered with 1.2.3. Because of existing Cookie law in EU this criteria is not relevant.
10	4.1.1	Individuals are informed that personal information is collected only for the purposes identified in the notice.
11	6.2.5	Is correction of PII and not a topic of this research.
12	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 monitoring and enforcement.
13	4.2.4	Individuals are informed if the entity develops or acquires additional information about them for its use.

All 13 were scrutinized again and 2,9, 11 were left out.

APPENDIX 4 CHRONOLOGY FROM REQUEST TO ANSWER

	Organisation	First SA-request	Identification Check (Y/N)	Second SA-request	Called (yes/no)	Response Received (Y/N), To late or In time	Research Participation request	Denied (D), Accepted (A)	Number of interviews
1	ABN AMRO	20-12-2012		10-2-2013	Twice; 2 different persons	Y: 20-03-2013. Too late	10-04-2013	D: 07-05-2013	0
2	Nationale Nederlanden	20-12-2012		10-2-2013		N			0
3	LFO2	20-12-2012	Y:03-01-2013 asked for identification, 06-01 sent to ING. Appr. Receiving date: 08-01	10-2-2013		Y: 13-02-2013 Too late	14-05-2013	A:06-06-2013	1
4	SVB	20-12-2012		10-2-2013		Y: 21-02-2013 Too Late	14-05-2013	D: 14-06-2013	0
5	LGO1	20-12-2012	06-01-2013 identification on request	10-2-2013		Y: 10-01-2013 In time			1
6	LFO1	20-12-2012	03-01-2013 identification on request			Y: 23-01-2013 In time			2
7	LGO2	20-12-2012				Y: 17-04-2013 Too late			3

APPENDIX 5 STANDARD SA REQUEST (In Dutch)

<Naam>
<Adres>
<Postcode, Plaats>
Nederland

Wijk bij Duurstede, 20 december 2012

Betreft: Verzoek om inzage in persoonsgegevens

Geachte heer, mevrouw,

Met verwijzing naar artikel 35 van de Wet bescherming persoonsgegevens verzoek ik u na te gaan of u persoonsgegevens van mij verwerkt. Als u persoonsgegevens van mij verwerkt, wil ik hier graag inzage in hebben.

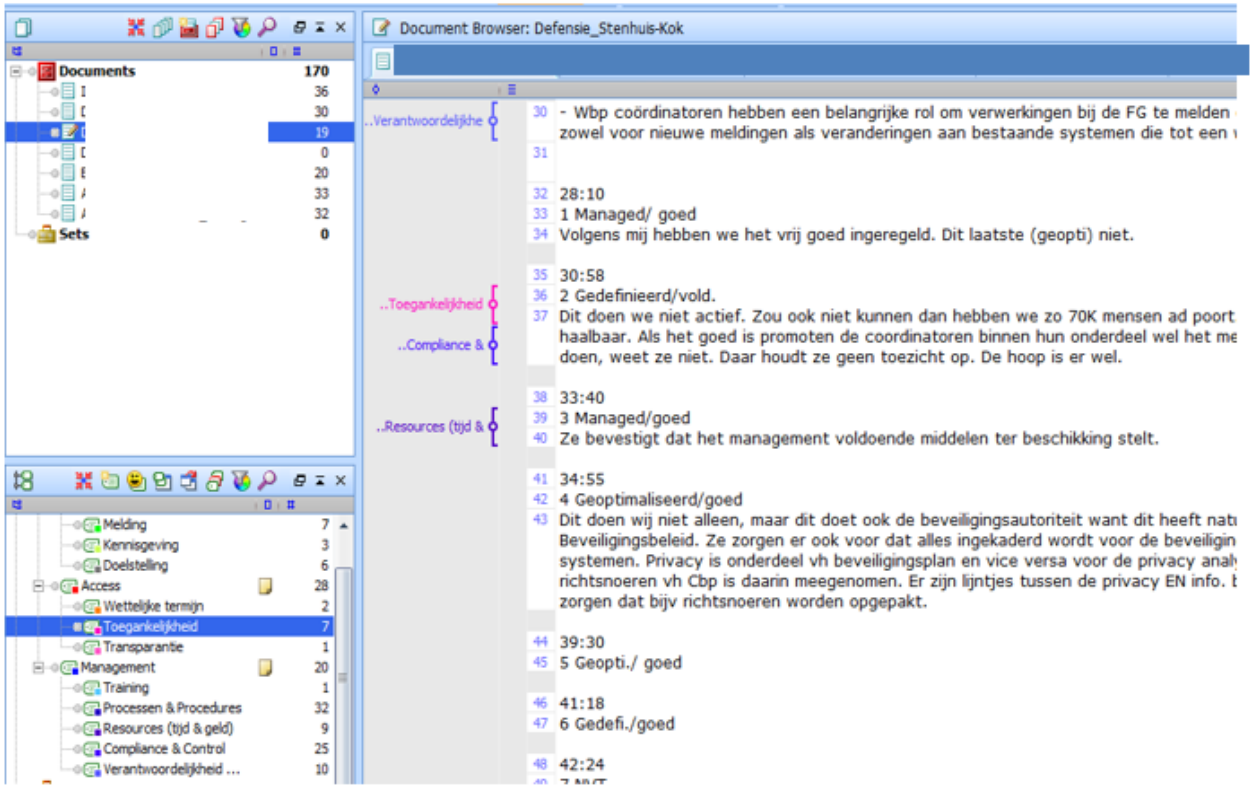
Graag ontvang ik naast inzage ook informatie over de systematiek van uw geautomatiseerde gegevensverwerking. Tot slot verzoek ik u om het nummer van de melding van de verwerking bij het CBP.

Als u met het oog op de vaststelling van mijn identiteit behoefte heeft aan een kopie van een rijbewijs, paspoort of ander identiteitsbewijs, ben ik bereid u deze te verstrekken. Alsook de wettelijke vergoeding te betalen.

Hoogachtend,

Roger Howard

APPENDIX 6 SCREENSHOT MAXQDA



Text in picture has been made invisible to protect the name of organisations and informants.

APPENDIX 7 RESPONSE & MATURITY RESULTS

LFO1 Response

Evaluator	LH	MB	RH
Stelling 1	3	5	3
Stelling 2	0	0	0
Stelling 3	0	0	0
Stelling 4	0	0	0
Stelling 5	0	0	0
Stelling 6	0	0	0
Stelling 7	0	5	0

LFO1 Maturity

Informants	JP	GA
Stelling 1	3	5
Stelling 2	4	3
Stelling 3	4	5
Stelling 4	3	5
Stelling 5	3	4
Stelling 6	5	4
Stelling 7	4	4
Stelling 8	3	5
Stelling 9	5	5
Stelling 10	4	4

LFO2 Response

Evaluators	LH	MB	RH
Stelling 1	0	0	0
Stelling 2	0	0	0
Stelling 3	0	0	0
Stelling 4	0	0	0
Stelling 5	0	0	0
Stelling 6	0	0	0
Stelling 7	5	5	3

LFO2 Maturity

Informants	RH
Stelling 1	4
Stelling 2	4
Stelling 3	4
Stelling 4	4
Stelling 5	4
Stelling 6	4
Stelling 7	4
Stelling 8	4
Stelling 9	4
Stelling 10	4

LGO1 Response

Evalueerders	LH	MB	RH
Stelling 1	0	3	3
Stelling 2	5	5	5
Stelling 3	5	0	0
Stelling 4	5	0	3
Stelling 5	5	0	3
Stelling 6	0	0	0
Stelling 7	5	5	3

LGO1 Maturity

Informants	Zan
Stelling 1	3
Stelling 2	3
Stelling 3	4
Stelling 4	5
Stelling 5	3
Stelling 6	4
Stelling 7	5
Stelling 8	5
Stelling 9	3
Stelling 10	3

LGO2 Response

Evalueerders	LH	MB	RH
Stelling 1	5	5	5
Stelling 2	5	5	5
Stelling 3	5	4	5
Stelling 4	5	5	5
Stelling 5	2	0	3
Stelling 6 = NVT	0	0	0
Stelling 7	5	5	5

LGO2 Maturity

Informants	vdV	S-K	VC
Stelling 1	1	4	3
Stelling 2	3	3	3
Stelling 3	4	4	4
Stelling 4	4	5	4
Stelling 5	3	5	5
Stelling 6	4	3	4
Stelling 7 = NVT			
Stelling 8	3	5	4
Stelling 9	5	4	5
Stelling 10 = NVT			