An automated rule based system for checking GDPR compliance

Master thesis by Joost Krapels BSc.

VU Amsterdam
De Boelelaan 1105, 1081 HV Amsterdam
j.n.krapels@student.vu.nl
July 15th 2018

Supervised by dr. Henrik Leopold and dr. Sieuwert van Otterloo

Table of Contents

Abstract **1**
Preface **2**
1. Introduction **3**
2. Background **4**
2.1 The GDPR 4
2.2 Definitions 5
2.3 The RVO tool 7
2.4 Related work 8
3. Methodology **10**
3.1 The DSRM 10
3.2 Objective of the solution 11
4. Development of the tool **11**
4.1 The structure 11
4.2 Design choices 17
4.3 Initial exploratory interviews 17
5. The Experiment **21**
5.1 Experimental setup 21
5.2 Test run 24
5.3 Tools and software 26
6. Results **27**
6.1 Duration 27
6.2 Perceived compliance improvement 28
6.3 Confidence improvement 29
6.4 The average perceived compliance and confidence per topic 30
6.5 Combining perceived compliance and confidence with overall confidence 31
6.6 Accurately determining compliance 32
6.7 Has the tool put people to action? 32
6.8 Net Promoter Score 35
6.9 Improvements from the initial interviews 36
7. Discussion **38**
7.1 Participants' overall impression of the tools 38
7.2 Revisiting the criteria and research problem 38
7.3 Future improvements to the tools 40
7.3.1 Improvements to the Compliance Scan 40
7.3.2 Improvements to the RVO tool 41
7.4 Possible influences on the experiment results 41
7.5 Main takeaways 42
8. Conclusion **43**
Bibliography **45**
Appendix **47**
Dutch and English names of the ten topics 47
Full structured view of the chapter *register of processing activities* 48
Full set of example questions from the chapter *register of processing activities* 49
Two chapters of an example Compliance Scan report 50
The BPMN models of the rights of data subjects 51
The full set of the initial interview questions, in both English and Dutch 59
The form given to participants during the experiment 63

An automated rule based system for checking GDPR compliance

Joost Krapels BSc.

VU Amsterdam,
De Boelelaan 1105, 1081 HV Amsterdam
j.n.krapels@student.vu.nl

Abstract. On May 25th 2018, the GDPR, or General Data Protection Regulation, became applicable for all EU member states and all organizations located and/or operating in them. For organizations it appears to be difficult to know what activities they are performing correctly and what not, since the Regulation has many aspects and no organization is the same. The Dutch Information Supervisory Authority Autoriteit Persoonsgegevens has, together with the RVO (Netherlands Enterprise Agency), developed a high-level GDPR readiness scan, which is useful to a certain extent but remains generic and contains walls of text. In this master thesis I develop and test a rule based system for checking GDPR compliance that gives well structured feedback on compliance and areas of improvement. After a literature study on compliance and the GDPR, interviews to identify important real world problems were held and a first version was built. A test run was done to find out how the tool could be improved, which was followed by an experiment where seven participants used either the current RVO tool or the newly developed Compliance Scan, testing for perceived compliance improvement and confidence improvement. The RVO tool took less time to complete and caused a slightly higher perceived compliance improvement, while the developed C-Scan caused a higher improvement in confidence. There are reasons to assume that the C-Scan taught its users more on the level of their GDPR compliance than the RVO tool, but future research is needed to confirm this. Next to fulfilling the criteria for a successfully developed tool set out in this paper, the Compliance Scan satisfies accuracy and ease of use for the intended target group. It has laid the basis for a structural GDPR compliance analysis method, and may assist more organizations even better in the future.

Keywords: GDPR, AVG, compliance, data protection, privacy, personal data

Preface

Acknowledgements:
First of all, I would like to thank my parents and sister for supporting me and, most of all, forcing me to take breaks throughout the six months it took to complete this master thesis project.

Secondly, I would like to express my gratefulness to my external supervisor dr. Sieuwert van Otterloo (ICT Institute) and internal supervisor dr. Henrik Leopold (VU Amsterdam). Dr. van Otterloo has supported and supervised me on a daily basis. He gave me an open insight in ICT Institute and IT advisory and allowed me to learn as much about them as I wanted, observed and advised with a sharp eye for detail, and helped connect me to the right organizations. Dr. Leopold guided me through the minefield called academic research, while at the same time providing me with lots of freedom to find the topic that interested me and explore it.

Next, for their direct contribution to this thesis I would like to thank:

- Marc Abbink, Marilena Tsigkou, and Marco van Burken from ISO2Handle for the provision of their platform and services, and the very close and pleasant collaboration that turned an idea into a real product
- Dr. Floris van den Broek from ICT Institute for the connections, and dr. Joost Schalken-Pinkster (also from ICT Institute) for the feedback on my experimental design
- Freke van Dijk for the proofreading
- Bert Wassink for helping discover some pesky bugs and giving valuable feedback

Fourth, a special mention for their indirect contribution:

- Wiebe Tijsma for the participant connection and interesting DPO experiences
- Noah Korevaar for the many new insights, distraction where appropriate, and setting the example for work ethic
- Peter Bennink for the interesting GDPR dilemmas and discussions

Finally, I would like to extend my gratitude to all organizations and people having participated in the initial interviews or experiment. Even though I would love to mention and thank you all by name, I will keep the promise to leave you anonymous. This thesis would not have been possible without you!

Joost Krapels, 15-07-2018

1 Introduction

The General Data Protection regulation, or GDPR for short, is a new European Regulation that aims to protect the personal data of EU citizens and simplify the handling of personal data protection for organizations.

Since the GDPR is a fairly new Regulation affecting all departments and levels of organizations, it can be difficult to apply. There is no case law yet, and guidelines still have to be furtherly developed. Just like the pre-cursing Dutch Data Protection Act, it will take quite some time for the Regulation to take shape in practice. [Winter et al., 2008] Any organization that works with personal data is affected by and has to comply with the Regulation, or risk a hefty fine. The Regulation replaces national laws and a nearly 25 year old European Directive, so organizations need to be aware of the changes to stay compliant with data protection legislation. It contains 99, often fairly complex, articles which researchers such as Koops [2014] find to defeat the purpose of simplifying data protection.

The Dutch Information Supervisory Authority Autoriteit Persoonsgegevens (from here on referred to as AP) set out a ten step plan [AutoriteitPersoonsgegevens, 2017] that covers the most important topics that need to be checked on to determine GDPR compliance. As a way for organizations to do a quick self-check, the AP also developed a high-level GDPR readiness scan together with the RVO (Netherlands Enterprise Agency). The documentation accompanying the ten step plan and readiness scan is detailed and elaborate, which is also its main weak point. The walls of text make it difficult to use, and not intuitive for the user whether he or she is compliant.

The aim of this paper is to improve the user experience and efficiency of the AP plan and RVO tool by constructing an automated rule based checklist system with hands-on feedback that assists in applying the complex new General Data Protection Regulation. Since a regular research question would not do the process of developing an Information System justice, I have followed the approach of Wieringa [2014] for Design Science Research to formulate the following technical research problem:

The design of a checklist that satisfies accuracy and ease of use so that GDPR compliance can be checked in business processes.

The research in this paper is structured according to Peffers et al. [2007] 's Design Science Research Methodology. This methodology provides a solid foundation for developing an Information Technology system, due to the fact that emphasis is put on a step-wise approach and iterations are encouraged.

With the motivation and right methodology found, an initial version of the tool was developed. Five organizations were then interviewed to determine on what aspects focus needs to be put and with that, a good connection to the work floor can be assured. The tool was developed further, had a test run, was improved, was tested in an experiment against the current RVO tool using two groups of seven participants, and was finally evaluated.

The value of a successfully designed product is trifold: organizations will be able to handle data protection and privacy with more care, their level of contentment with the new Regulation and confidence in their compliance to it will increase, and automating and simplifying a seemingly difficult aspect of doing business saves time and resources. In chapter 3.2, I will elaborate on this goal by presenting the objective of the solution.

Comparing the Compliance Scan tool to the RVO tool yielded several new insights. The RVO tool took considerably less time to complete and made the users feel slightly more GDPR compliant, but not as confident in the given answer as the C-Scan tool did. The Compliance Scan took longer to complete but provided concrete feedback and is likely to have caused the users to actually learn about their current level of GDPR compliance. It has been determined to be a useful way to gain insight in one's GDPR compliance by SMEs from various sectors, and fulfilled the criteria set out for it in this paper. Both tools could profit from more real-world examples and even more clarification on used terms.

2 Background

2.1 The GDPR

The GDPR (EU 2016/679) entered into force on May 24th of 2016, with a transition period of two years. From May 25th of 2018 on, the Regulation applies to each and every organization in the member states of the European Union that processes personal data, and organizations outside it that process personal data of individuals within the EU. The Regulation replaces a Directive from 1995, the DPD (95/46/EC). Next to the educated guess we can all make that legislation based on the state of Information Technology of 23 years ago is outdated by now, the change from a Directive to a Regulation is less trivial than it might sound. The Regulation simply became applicable in all EU member states, and binds together all data protection legislation on the European and national level instead of setting a goal that has to be achieved according to own insight. The GDPR does, however, leave room for member states to fill in certain details to assure the Regulation ties in as smoothly as possible with national laws. As the GDPR states in Recital 10:
"*This Regulation also provides a margin of manoeuvre for Member States to specify its rules, including for the processing of special categories of personal data ('sensitive data').*"

This is often done by means of a national Implementing Law. Taking the Netherlands as an example; the Implementing Law is called the UAVG, where the U stands for Uitvoeringswet (Implementing Law) and AVG for Algemene Verordening Gegevensbescherming (GDPR).

2.2 Definitions

To avoid ambiguity with important terms, they have to be properly defined. Below a collection of the terms often used in this work, how they are described in the GDPR, and where:

Personal data
Personal data is any information relating to an identified or identifiable natural person ('data subject'). (p. 33)

Data subject / identifiable natural person
A data subject is a natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. (p. 33)

Consent
Consent is any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. (p. 34)

Processing
Under the term processing falls any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. (p. 33)

Personal data breach
A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. (p. 34)

Controller
Considering personal data, the controller is the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law. (p. 33)

Processor
Also considering personal data, a processor is a natural or legal person, public

authority, agency or other body which processes personal data on behalf of the controller. (p. 33)

Data Protection Officer (DPO)
In Recital 97, the Data Protection officer is described as a person with expert knowledge of data protection law and practices. (p. 18) This person should, according to Article 39, inform and advise their employer and its data processing employees of the obligations set by the GDPR, monitor compliance with the Regulation and other data protection laws, advice on or perform DPIA's, and be the face of their employer and point of contact towards the Supervisory Authority.

Data privacy Impact Assessment (DPIA/PIA)
A DPIA is an assessment of the impact of the envisaged processing operations on the protection of personal data. (p. 53) It needs to be carried out when a type of processing, in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons.

Supervisory Authority
A Supervisory Authority is an independent public authority which is established by a Member State pursuant to Article 51 (p. 34) Article 51 states that each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union (p. 65) and that every Supervisory Authority shall contribute to the application of the Regulation and cooperate with each other and the European Commission. Examples of Supervisory Authorities are the Dutch Autoriteit Persoonsgegevens and the UK's ICO.

Special categories of personal data
The GDPR makes a distinction between several categories of personal data. They deem some categories to be special, namely personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. (p. 38) The restrictions on the processing of these types of personal data are much higher than the 'normal' types, since mishandling them could have much more severe consequences for the rights and freedom of people.

Risk and High Risk
The GDPR is not very clear on what constitutes high or low risk (processing) activities, even though these terms are used quite frequently. No percentage of

likelihood is mentioned, the only semi-clear definition is given in Recital 76, namely: Risk should be evaluated on the basis of an objective assessment, by which it is established whether data processing operations involve a risk or a high risk. (p. 15) According to Recital 77, risk and mitigation identification can be provided by approved codes of conduct, approved certifications, guidelines provided by the Board or indications provided by a Data Protection Officer. (p.15) Recital 94 states that high risk is likely to result from certain types of processing and the extent and frequency of processing, which may result also in a realization of damage or interference with the rights and freedoms of the natural person. (p. 18)

Compliance
No direct definition of compliance is used. For this reason I shall use the Oxford dictionary definition 1.2 of compliance[1], namely: "The state or fact of according with or meeting rules or standards".

2.3 The RVO tool

The Rijksdienst Voor Ondernemend Nederland (RVO) has, together with the Dutch Supervisory Authority Autoriteit Persoonsgegevens, developed a checklist tool for GDPR compliance. The RVO is part of the Dutch Ministry of Economic Affairs and Climate Policies, and calls themselves the Netherlands Enterprise Agency in English. The scope of the tool has been shrunk to just data controllers, it is written in Dutch, and consists of the following chapters:

Welcome

1. Your Processing Activities
2. The Lawful Bases of Processing
3. The DPO
4. The DPIA
5. Data Protection by Design and Data Protection by Default
6. Register of Processing Activities
7. Security
8. Processing Agreements
9. Informing Data Subjects
10. Rights of Data Subjects

Your advice

According to the introduction page, the information is concise and meant for own use. I have used this tool as the comparative tool in my research since it is quite close to the tool I planned to develop; a checklist type tool with a customized report in the end. The RVO tool also contains ten chapters, but not all

[1] compliance — Definition of compliance in English by Oxford Dictionaries. https://en.oxforddictionaries.com/definition/compliance.

chapters are the same as the ones used in the Compliance Scan. More on this can be found in chapter 5.1. The main strength of the RVO tool is the fact that it has been developed in collaboration with the Dutch Supervisory Authority. The Authority has an elaborate website[2] with ample information on the GDPR, and is objectively the most trustworthy source of GDPR information for Dutch citizens and organizations falling under the AP's authority.

2.4 Related work

Kingston [2017] states that AI can assist with GDPR compliance by "*asking all and only the relevant questions; monitoring activities; and carrying out assessments*" (p. 429) and that AI can help reach compliance by, among others, following compliance checklists and help in risk assessment. For following compliance checklists, he uses an example organizational level checklist by Evans [2016], and explains how rule-based AI technology can help implement its pointers. For risk assessment, he describes that an AI system could assess the risks and make the connection between the level of risk and what mitigation measure would be appropriate. The GDPR often refers to high risk activities, so it is vital to know when this is the case. A checklist can help identifying these activities in an easy and inexpensive manner compared to e.g. a full Data Protection Impact Assessment.

Current checklists for GDPR compliance in business processes
There is, at the time of writing, no checklist that thoroughly checks for GDPR compliance in business processes, but there is plenty of work on GDPR compliance on software system- and organizational level. Research on implementing GDPR compliance on software system level has been done by e.g. integrating privacy best practices into a privacy engineering methodology [Notario et al., 2015] and developing PIA templates [Iwaya et al., 2016] based on the European Commission's DPIA framework. [EuropeanCommission, 2011] Research on GDPR compliance on an organizational level is often done by consulting firms, law firms [Evans, 2016], or Information Supervisory Authorities such as the British ICO [ICO, 2017] and the aforementioned Dutch AP, which provide a GDPR summary or general checklist to assess where one's organization stands at the moment.

Compliance
This assessing of one's current stance on regulatory compliance falls under compliance management. In 2008, El Kharbili et al. proposed a technical framework for compliance management in business processes, which is mentioned often in papers on the topic. In 2012, El Kharbili made a comprehensive summary on Business Process Regulatory Compliance Management Solution Frameworks, comparing similar frameworks to date effectively from a BPM perspective. Recently, in 2016, an abstract formal framework was proposed by Hashmi et al.,

[2] "Autoriteit Persoonsgegevens —." https://www.autoriteitpersoonsgegevens.nl/. Opened on 7 Jul.. 2018.

who, in an elaborate overview of previous work on evaluation frameworks, mention among others the 2012 literature review of El Kharbili as the most recent in this field and how norms, imposed from laws, should be interpreted to reach actual compliance. Compliance detection can, according to Sadiq et al. [2007], be either *after-the-fact* or *before-the-fact*, where they preferred the latter due to a severe difficulty to evolve and maintain of the former. The checklist will do an *after-the-fact* compliance check, but advise an *before-the-fact* approach for improvement.

The influence of the GDPR on business processes
Research on the direct influence of the GDPR on business processes is scarce, but the GDPR seems to influence business processes in mainly two ways. Processes will have to be adapted to become compliant, and new processes might have to be established for compliance on an organisational level. In 2017, Heuck et al. used a certain process modelling notation to digitize the GDPR, and by applying the self made model to a business process, a new activity was discovered that needed implementation, showing that the Regulation can call for the extension of business processes with new activities. The need for establishment of new processes, such as the need for a DPIA (Sec. 3, Art. 35) and taken measures to be assessed on a regular basis (Sec. 2, Art. 32) stems from the Regulation itself, as well as from research. [Buchmann and Anke, 2017] It is underlined by security experts, such as Tankard [2016] who describes the need "*to implement appropriate technological and operational safeguards for securing data, including putting in place strong privacy controls.*". (p. 6)

Privacy in business processes
Several attempts have been made to implement privacy [Labda et al., 2014] and GDPR compliance [Bartolini et al., 2015] into Business Process Modeling. These are examples of Data Protection by Design, which is together with Data Protection by Default a requirement of the GDPR. Buchmann and Anke [2017] built forward on the idea of privacy in workflows. They propose Workflow Privacy Patterns, and how to integrate these into the existing tool-chain. They describe that data privacy must be considered in workflows by means of Privacy Processes (several processes need to be established, such as handling requests of data subjects), Crosscutting Privacy Patterns (processes where personal data is involved need to be updated to comply with the GDPR), and Meta Privacy Processes (certain demands set out in the GDPR influence processes directly such as minimal data collection and separation of duty).

Even though, in total, quite some research on compliance, privacy in business processes, the influence of data protection legislation, and the influence of GDPR on software systems has been conducted, there seems to have been no study that combines all these aspects. This thesis closes that gap by combining knowledge from these fields and results from its studies and incorporates it in a rule based system that checks for GDPR compliance.

3 Methodology

3.1 The DSRM

To structurize this thesis and research, I will be following Peffers et al. [2007] 's DSRM methodology. The DSRM, or Design Science Research Methodology, is a structured approach for conducting Design Science research. A schematic version of it can be found in figure 1, which also clearly shows how welcome iterations are. The methodology is specifically focused on and developed for the field of Information Systems, and consists of the following six stages:

Step 1: Problem identification and motivation
Step 2: Definition of the objectives of a solution
Step 3: Design and Development
Step 4: Demonstration
Step 5: Evaluation
Step 6: Communication

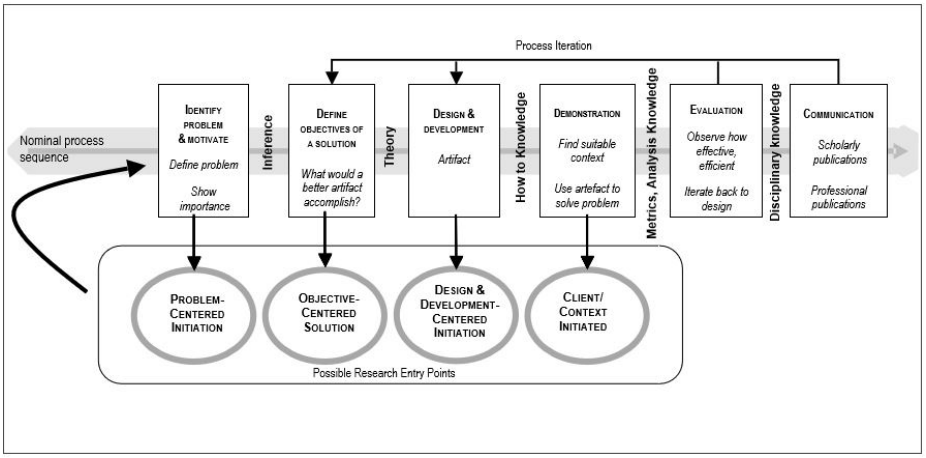


Fig. 1. DSRM Process Model

The first stage, Problem Identification and Motivation, has been addressed in the introduction of this thesis, as well as a state of the art of the related literature in chapter two. The following sub chapter (3.2) sets out the Objective of the Solution. Chapters four and five provide the Design and Development stage, in chapters six and seven the Demonstration and Evaluation will be discussed, and this thesis as a whole will serve as the final stage, Communication.

I have gratefully used the opportunity for iterations in stages five and six by first developing an Minimal Viable Product, which was then tested during the first evaluation stage. In this thesis, I have called this first evaluation the Test

Run. After the Test Run, the gathered improvements are implemented during a final Design and Development phase and the final three stages are completed. Further improvements gathered during this part are described in a separate chapter at the end of the thesis. Should this tool be further improved in the future, another iteration back to the Design and Development stage (or even stage two) can be done with the newly found improvements.

3.2 Objective of the solution

As stated in the introduction, the goal of this paper is to develop an automated rule-based system (checklist) that satisfies accuracy and ease of use so that GDPR compliance can be checked in business processes. The term business processes is used since it best describes the way organizations operate. The processes might be implicit, but everything that happens in an organization can be split in separate processes. GDPR compliance intertwines with nearly all processes and even constitutes several processes itself, which makes the development of a successful tool a challenge. To determine whether the developed product can be considered a success, several criteria need to be established:

- The tool needs to be useful for organizations of all sizes
- The tool needs to be usable by non experts
- The tool needs to accurately determine (non) compliance to all parts of the ten step plan
- The tool needs to advise on improvements towards compliance using (where appropriate) business process models

4 Development of the tool

4.1 The structure

The rule based checklist consists of twelve blocks; one block of introduction questions to find out which questions are (not) needed, one block for every AP step, and the results. Each one of the ten middle blocks contains a set of questions. The answers can influence what will be asked in this or the next block(s). The introduction questions are asked using the knockout heuristic, to end the checklist as quick as possible if needed. The results are shown as a report. The report will, for every step, contain what has been deduced from the answers. This can, for example, be that a certain mandatory part is done correctly or that something is missing and how it can be improved.

The checklist has been developed in cooperation with ISO2Handle, in particular with Marilena Tsigkou and Marc Abbink. The tool was built on their platform, which has the ideal structure for the intended tool. First, I deduced a list of questions from the GDPR for every topic and indicated how they should be linked. Ms. Tsigkou created a structured view for every chapter, such as the one that can be seen in figure 2. Finally, the chapters and report were implemented into the platform, and tested on content and flow correctness. In figure

3, the questions belonging to the chapter *Register of Processing Activities* can be seen. The full versions of both figures can be found in the appedix.

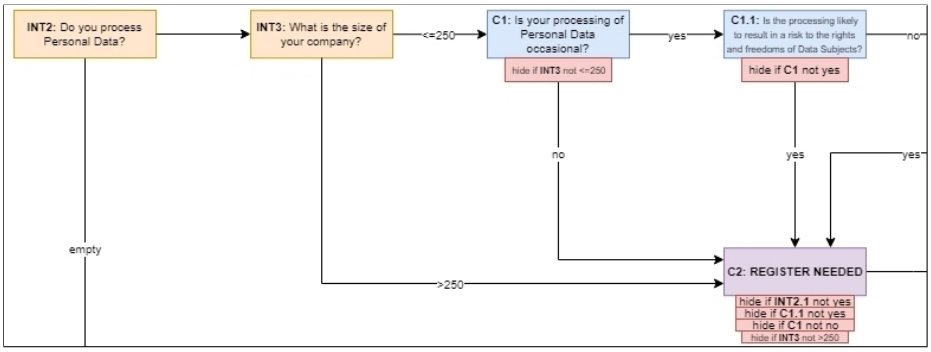


Fig. 2. Snapshot of the structured view of the chapter *Register of Processing Activities*

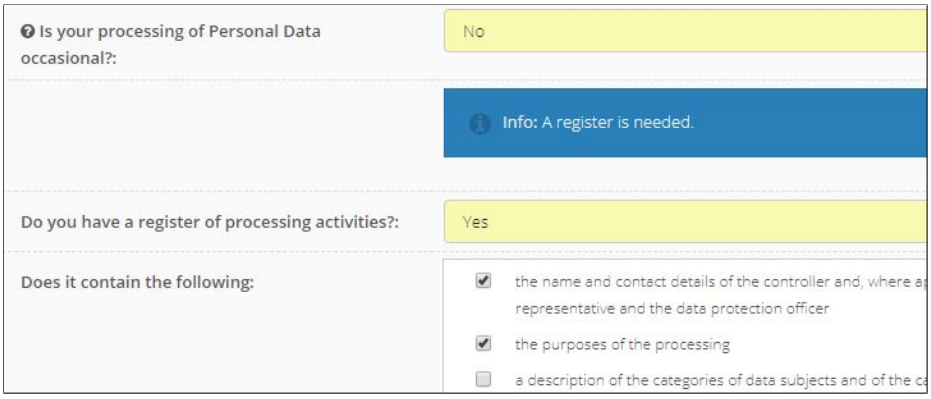


Fig. 3. Snapshot of the questions of the chapter *Register of Processing Activities*

Introduction:
When using the platform for the first time, the user starts with the questionnaire to determine the current level of GDPR compliance. First, several introduction questions are asked to determine, among others, whether the GDPR even applies to the user, what kind of data is processed, and whether the user is a data controller or data processor. The answers to these questions are stored, and used later on in other sections to show/hide certain questions.

Register of processing activities
Using the answer from the introduction question about the organization's size and several other questions, the tool determines whether the user needs a register of processing activities. If the user needs it and has one, questions are asked to determine whether it contains all the mandatory points from the GDPR article. The need for a register is determined following the logic found in figure 4.

As an added feature, I have developed a Register of Processing Activities. This register is not used during the experiment, but adds value to the product as a whole.

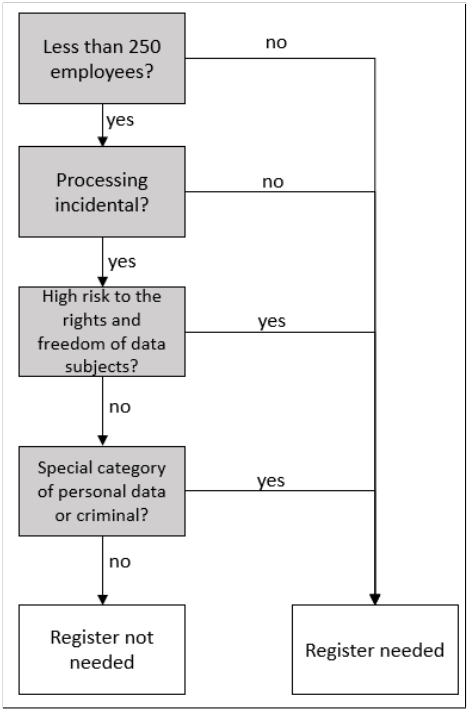


Fig. 4. Determining the need for a register of processing activities

The Data Protection Officer
Under certain conditions, a Data Protection Officer is required. The GDPR states requirements for a DPO, and what tasks this person should at least perform. The position of the DPO in an organization has requirements attached to it as well. This part of the tool therefore determines whether the user needs a DPO, if they do whether they actually have one in place, and whether the position of the DPO in the organization is as it should be. The need for a DPO is determined following the logic found in figure 5.

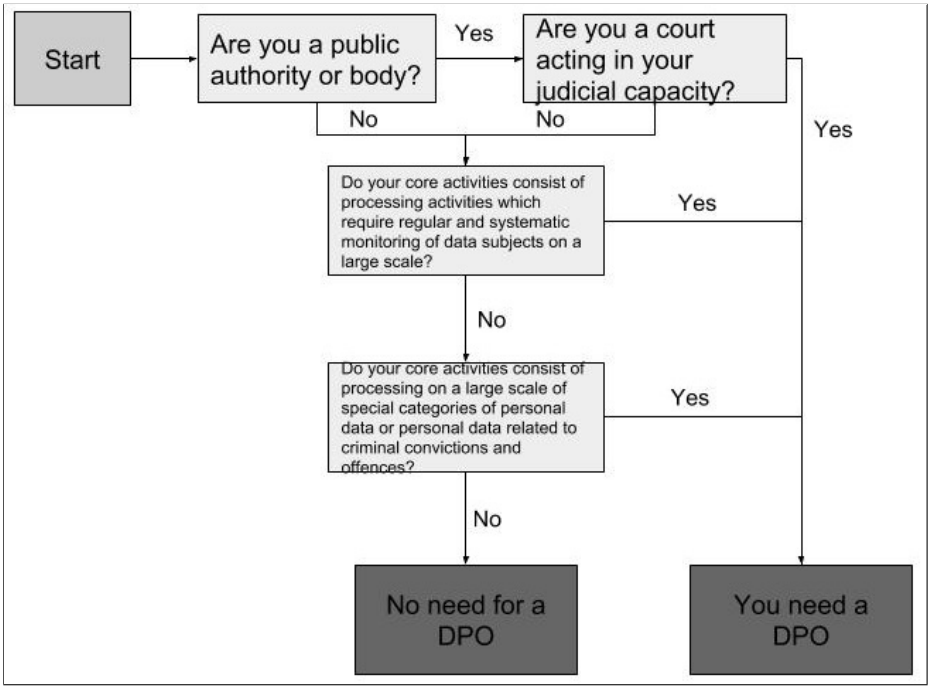


Fig. 5. Determining the need for a DPO

Data Protection Impact Assessment
To check compliance with the topic of Data Protection Impact Assessments, the tool first asks the user whether they do a DPIA for new processing activities or changes in current ones that are likely to result in a high risk to the rights and freedoms of data subjects. If they indicate not to do that (even though they should), the tool skips to the next chapter. The user is then asked whether their organization has a template for DPIA's. If there is no template, the chance of doing a DPIA correctly is close to nil. If there is a template, the tool asks the user whether the template contains the mandatory points (presented as a check-box list). Next, the amount of DPIA's that are done are asked. I advise to have done at least one, so one knows how to do it. Finally, if the user has answered earlier that he/she has a DPO, the tool checks whether the DPO's advice is sought when doing DPIA's.

Rights of Data Subjects
On the rights of data subjects, three main questions are asked. First, the tool asks whether the user knows when to allow data subjects to execute their rights. If the user does not know when to allow/deny the execution of a right, the rest of the questions cannot be answered correctly and the tool skips to the next step. Otherwise, the tool presents the user with all the rights, and asks whether

(and if yes, how) the rights can be executed at their organization. Since not all organizations use automated decision making, the question about that right may also be answered with Not Applicable.

Personal Data Breaches
The next chapter is personal data breaches. Just like the previous chapter, the tool first checks whether there is a protocol. If there is, the user is asked whether they know when to contact the Supervisory Authority. A positive answers leads to the user being presented with a short list of requirements the GDPR has for a notification of a PDB to the Supervisory Authority, to which the user must answer whether their notification contains all points it should. Next, the same is done for the notification to data subjects. As the final question, the tool asks the user whether all personal data breaches are documented.

Processing Agreements
Processing agreements is the topic of the next chapter. First, the tool asks the user whether they have a processing agreement with all parties personal data is exchanged with. The user can answer Yes, Some of them, and No. In case one of the first two is answered, the tool lists the points a correct processing agreement has to contain and the user has to select which ones their own agreements contain.

The second added feature to the Compliance Scan is a processing agreement generator. From the register of processing activities, the user can select a controller and a processor that are already stored in the register. They can be either one of those themselves. Once both parties are picked, a processing activity needs to be selected and the agreement is generated.

Determining the Lead Supervisory Authority
To determine which party is the user's Lead Supervisory Authority, the tool asks whether the user's organization has multiple establishments, whether cross-border processing takes place, where the decisions around the means and purposes are made, and whether there is a regional or only a national Supervisory Authority.

Lawful bases of processing
Here, the user is first presented with the six lawful bases of processing. They have to select which ones apply to the processing activities of their organization, after which they must answer whether they can prove to the Supervisory Authority why this basis applies. I have chosen this structure due to the emphasis the GDPR puts on the need for a lawful basis. To prevent people for choosing a basis without a second thought, I ask them whether they can explain to the Supervisory Authority why this choice/these choices is/are made. This is also the rationale behind the final question "*Are all your Processing Activities based on a lawful basis?*".

Data Protection by Design and Data Protection by Default
Even though the principles of data protection by design and data protection by default are vital aspects of data protection according to the GDPR, the Regulation is not very elaborate on the way they should be applied. In this tool, I have chosen to stick to the limited information on the topics that is provided by the GDPR itself and refrain from using suggested clarifications from research, such as the ones by Colesky et al. [2016]. The tool first asks whether the user works by the principles, which can lead to either continuing to the following questions or the following chapter. The following questions actually determine whether the organization follows the principles by asking e.g. whether data minimization is implemented.

Awareness
The final chapter is Awareness. Even though the GDPR does not contain any guidelines on awareness, it remains the backbone of data protection. Humans are still often the weak link in an Information System, and organization wide awareness can help prevent personal data breaches and the acceptance of the new 'rules'. If the user has indicated their organization has a Data Protection Officer, the tool asks them about the only GDPR rule on awareness: "*Is the Data Protection Officer responsible for raising awareness in your organization?*".

The report
The report shows the user their answers, how they scored, and what can be improved. Items in red show where they need to make improvements to become compliant, orange indicate that they are suggested to improve this part, and green means that they are doing well on this aspect. The report is organized by chapter, and contains extra information for every subject. Part of a chapter of an example report can be found in figure 6, with a more elaborate overview of two chapters of an example report in figure 13 in the appendix.

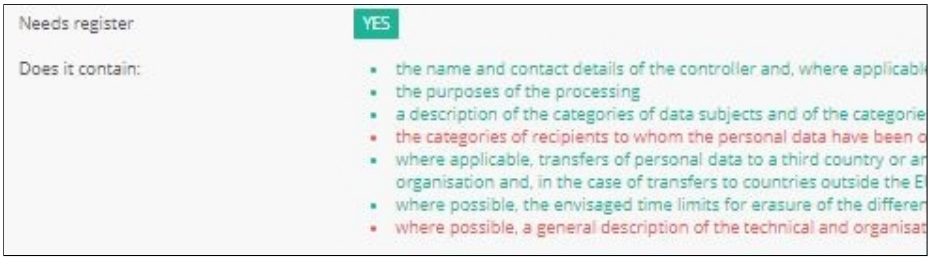


Fig. 6. Snapshot of an example report

Note: if a certain question or part does not apply to the user now, that does not mean it cannot change in the future. New processing activities might involve a

different kind of personal data, and new collaborations might require a processing agreement.

4.2 Design choices

In the used BPMN models, I have chosen not to use swimlanes, artifacts, and message events.[3] The current level of abstraction better fits the spirit of hands-on and easy to understand advice. For both implementation and organizations taking care of the most important aspects of the GDPR first, I have chosen a particular order that differs from the original ten step plan. This order is based on how mandatory a step is, the practical implications of not having it, and lastly usefulness. The steps will be presented to the user in the following order:

1. Register of Processing Activities
2. Data Protection Officer
3. Data Protection Impact Assessment
4. Rights of Data Subjects
5. Personal Data Breaches
6. Processing Agreements
7. Determining the Lead Supervisory Authority
8. Consent
9. Data Protection by Design and by Default
10. Awareness

4.3 Initial exploratory interviews

Goal
The aim of the initial interviews was to find out the following three main things:

1. What is the current stance on GDPR/privacy awareness?
2. How prepared are the interviewed organizations for the GDPR topics?
3. What are important real-world focus points for the tool?

The interview consisted of fourteen questions and an opportunity for questions or remarks from the interviewee's side. The interviews were held between the end of February and mid-March 2018, where the GDPR was already in effect but still three months away from applying, meaning that from this point in time,the organizations still had three months to become fully compliant. The following was discovered:

1. What is the current stance on GDPR/privacy awareness?
The distribution of GDPR awareness seems to differ quite a bit. Some organizations had informed all employees, while the knowledge and awareness seemed to be more concentrated in one or two people in other organizations. At the

[3] https://cloud.trisotech.com/bpmnquickguide/index.html?bpmn_examples_2.htm Retrieved on 14-07-2018

time of the interviews (end of February to mid-March 2018), there seemed to be no compliance stress in the interviewed organizations. *I should advise users of the tool to spread awareness among all levels of employees as much as possible.*

2.&3. How prepared are the interviewed organizations for the GDPR topics and what are important focus points for the tool?

Register of Processing Activities
Interviewed organizations that followed a certain security training already had a register of processing activities. The others did not. One interviewee that did not have a register knew that it will be required under the GDPR, but hoped it will not be too much work. *The register should be easy to fill out, and it should not take long.*

DPO
Not all interviewed organizations looked into the need for a DPO. Three out of the five looked into it, and made the conscious decision one is not needed. The other two assumed a DPO was not needed, but had not made the formal decision yet. *I should make sure the formal decision for a DPO is made and stored.*

DPIA
None out of the five interviewed organizations had done a DPIA. PIA's have been done by some, and others seemed to have no protocol for a PIA or DPIA. First of all, the GDPR has strict demands on what a DPIA should contain. Second, a good DPIA is only useful when it is used in the right conditions. *I need to make sure the mandatory points are easy to check, and make it clear when a DPIA is needed.*

Rights of data subjects
The interviewed organizations were mostly aware of the rights of data subjects. This might be attributed to external GDPR trainings, where the topic is discussed. Especially in the smaller organizations, the rights could not easily be executed, and if they could it had to be done manually. *I should inform users on a way to (partly) automate requests from data subjects. For processors this could be to automatically forward the request to the right controller.*

Personal Data Breaches
None of five interviewed organizations have had a personal data breach in the past twelve months. There seemed to always be, at the minimum, a general idea of what needs to be done but there was not always a protocol. *I will provide a standard protocol, based on what the GDPR says needs to be done.*

Processing Agreements
Since it is currently mandatory under Dutch law to have processing agreements, all organizations had at least a few processing agreements, and some had agree-

ments with all parties personal data is exchanged with. *I will make clear that processing agreements with all parties personal data is exchanged with should be in place, and that for every party worked with needs to be determined whether personal data is involved.*

Lead Supervisory Authority
The Lead Supervisory Authority was either known, or guessed correctly by the interviewee when confronted with the topic. The correct guess is not representable for knowledge, since the correct answer was always the Autoriteit Persoonsgegevens. This is the only, and most well known Supervisory Authority of the Netherlands. *Since it is important to be absolutely sure who the LSA(s) is/are, I will advise the users to explicitly document the involved LSA. I will also help them determine it.*

Consent
Not all organizations had processing activities with consent as the legal basis. Reasons for this were the use of other bases (such as performance of a contract) or the avoidance of a processing activity (choice to not use certain Google Analytics plugin) to circumvent the issue. *I will make the users aware consent is a good basis for processing, but not always the easiest or only one. Since the GDPR is quite strict on how consent must be requested, I will make sure to inform the users well of this.*

Data Protection by Design and by Default
Adhering to the principles of Data Protection by design and Data Protection by default has not been asked to all interviewees. *Information on this topic is missing. I shall conduct more literature research, so more examples can be given.*

Table 1 depicts deductions I have made based on the answers to the questions. I have determined whether the interviewees were compliant with the respective GDPR articles of the ten Autoriteit Persoonsgegevens' steps. Table 2 explains what constitutes a Y or N for every topic. The columns labeled 1-10 in table 1 correspond to the rows in table 2; 1 corresponds to *Awareness*, 2 to *Rights of Data Subjects*, etc.

Table 1. Compliance to the ten steps before the experiment

ID	1	2	3	4	5	6	7	8	9	10
02211	Y	Y	Y	N	Y	Y	Y	Y	N	-
03091	Y	Y	N	Y	-	Y	Y	Y	Y	N/A
03161	Y	Y	N	Y	-	Y	Y	Y	Y	N/A
03191	N	Y	N	N	-	N	N	N	N	N/A
03211	Y	Y	Y	N	N	N	Y	Y	N	N

Table 2. Obtaining a Y or N in table 1

Subject	Condition for "Yes"	Condition for "No"
Awareness	(nearly) All employees are privacy and GDPR aware	No or just one employee is privacy and GDPR aware
Rights of Data Subjects	Aware of the rights and they can all be executed	Not aware of the rights and/or they cannot be executed
Register of Processing Activities	There is a register of processing activities where there should be one	There is no register of processing activities where there should be one
DPIA	There is a protocol for doing DPIA's, and they are done when needed	There is no protocol for doing DPIA's, and/or they are not done when needed
Data Protection by Design and by Default	The principles are followed or processors are instructed to do so	The principles are not followed nor are processors instructed to do so
DPO	A correct and explicit decision on the need for a DPO has been made, and one is appointed when needed	An incorrect or implicit decision on the need for a DPO has been made, or no DPO is appointed when one is needed
Personal Data Breaches	There is a protocol for PBD's that will lead to a SA notification when needed, explicit or implicit	There is no protocol, it is not clear who will take action, or the SA can/ will not be notified
Processing Agreements	There are processing agreements with all parties PD is exchanged with, or these are in the making	There are no processing agreements, or not with all parties PD is exchanged with
Lead Supervisory Authority	The Lead Supervisory Authority has been explicitly correctly determined	The Lead Supervisory Authority has not been explicitly determined, or this is done incorrectly
Consent	Where consent has been used as the legal basis for processing, it has been done correctly.	Where consent has been used as the legal basis for processing, it has not been done correctly or no consent is asked while it actually should.

Note: Compliance to the articles is based on many factors, and not conclusive for every topic. Full compliance to every respective article has not been spotted in any of the interviewed organizations. For this reason, I have based the conditions for compliance on the spirit of every topic.

The full set of questions can be found in the appendix (figures 22-25).

5 The Experiment

5.1 Experimental setup

To properly test the Compliance Scan against the RVO tool, some alterations had to be made. As can be seen in table 3, the RVO tool does not contain all chapters from the original ten step article. For this reason, the chapters *Awareness, Personal Data Breaches*, and *Lead Supervisory Authority* of the Compliance Scan are not used in the experiment, and neither are the chapters *Personal data processing*, *Security*, and *Informing data subjects* of the RVO tool. Participants using the Compliance Scan are not presented with the omitted chapters, and participants using the RVO tool are asked to skip the omitted chapters.

Table 3. Overlap and difference in chapters of both tools

Compliance scan	RVO Tool
Rights of Data Subjects	Rights of Data Subjects
Register of Processing Activities	Register of Processing Activities
DPIA	DPIA
Data Protection by Design and by Default	Privacy by design and by default
DPO	DPO
Processing Agreements	Processing Agreements
Lawful Bases of Processing	Lawful Bases of Processing
Awareness	Personal data processing
Personal Data Breaches	Security
Lead Supervisory Authority	Informing Data Subjects

In this experiment, fourteen SMEs were involved. They were selected by hand, and are either business partners of ICT Institute, known by J. Krapels, or contacted by him through acquaintances. They were given an ID, and then randomly split into two equal groups. Group A received the RVO tool and group B received the tool that was developed for this thesis. The experiment consisted of six phases, and the questions and information as presented to the participants can be found in the appendix (figures 26-32).

Before the tool
Before using a tool, the participants will all get to read the original ten step plan written by the Autoriteit Persoonsgegevens [AutoriteitPersoonsgegevens, 2017], minus the omitted chapters (phase 1). This way, all participants will have at least a basic understanding of the topic. After that, all participants fill out a short questionnaire to determine self perceived compliance, and how confident they are about the given answers (phase 2).

Using the tool
Next, the participants get to use the tool allocated to them (phase 3). During the use of the tool, I made notes of problems participants face, which will be used as suggestions for improvement. For the sake of the experiment, I pointed them in the right direction if they happened to get stuck. I have not answered any questions about the content, as this influences the understanding of the tool. I also kept track of the time each participant needed to complete the tool.

After the tool
After the tool has been used, the participants are presented with the report generated by their tool and have ten minutes to study it (phase 4). Next (phase 5), they have to fill out the same small questionnaire as in phase 2. This way, the performance before and afterwards can be compared. Finally, additional questions on the user experience and questions to determine the effect of the tool are asked. (phase six)

Experiment Goal
The goal of this experiment is to compare an existing tool (the RVO tool) to the tool that has been developed during this thesis. To determine whether the new tool is an improvement over the RVO tool, the following needs to be measured:

1. Has the perceived compliance of the user improved more than the RVO group?
2. Has the compliance confidence of the user improved more than the RVO group?

Previously determined criteria for the development of a successful tool need to be fulfilled as well. The tool needs to:

- Be useful for organizations of all sizes
- Be usable by non-experts
- Accurately determine non-compliance to all parts of the ten step plan (minus personal data breaches, the lead supervisory authority, and awareness)
- Advise on improvements towards compliance using, where appropriate, business process models

Data collection
Quantitative
Quantitative data is collected during phase 2 and phase 5 by asking the participants the same two questions on seven topics before and after using the tool. The questions are:

A) Is your organization compliant with the GDPR requirements surrounding this topic?
B) How confident are you about this?

To question A, the participants can answer "Yes", "Don't know", or "No". Perceived compliance improvement is a "No" or "Don't know" before using the tool, and a "Yes" afterwards.

For question B, the participants rate their perceived compliance confidence for every topic by grading it on a scale from 1 to 5 (completely unconfident to completely confident). Confidence improvement is a higher self reported confidence score after using the tool than before using the tool. In phase 6, I also ask the following question: On a scale of 1-10, how likely is it that you will recommend this tool to others?

Qualitative
Qualitative data is collected by means of the following open questions:

1. What are your overall impressions of the tool?
2. How could the tool be improved?
3. Do you feel more confident on your overall GDPR compliance?
4. Is your organization going to implement a register of processing activities or change the current one? Why?
5. Will your organization perform a DPIA in the next two months? Why?
6. Has your decision on the need for a DPO changed? Why?
7. Will your organization be changing the way rights of data subjects are handled? Why?

Data analysis
Analysis of quantitative data
The total improvement in perceived compliance for the respective tools is calculated by adding up all perceived compliance improvements of participants using those tools. This amount can be higher for the RVO tool, equally high, or higher for the new tool.

The total improvement in confidence for the respective tools is calculated using the formula below for every topic of every participant using that tool, and adding this all up.

ConfidenceImprovement = (confidence score afterwards - confidence score before)

From this amount two conclusion can be drawn. The first conclusion is whether the perceived compliance confidence has improved while using one of the tools, and the second conclusion is which tool had the largest increase in confidence.

The recommendation question is to establish the Net Promoter Score. Imperative for this is that enough participants use the tools, which is difficult. If more participants are found than planned, the NPS can also be used to determine which tool is perceived to be better.

Analysis of qualitative data
Answers to the first open question will show the user experience. Answers to the second question will help determine how the Compliance Scan can be improved

in the future. The third question is to check whether a possible problematic situation has occurred. Participants could gain GDPR knowledge, which makes them doubt whether they are actually compliant. This will show as a lowered perceived compliance and confidence score. The participant is asked to explain why he/she does (not) feel confident overall, which confirms or rejects the possible problematic situation. Questions four to seven indicate whether the tool has informed participants well enough to mobilized them to make steps towards becoming GDPR compliant.

5.2 Test run

After the tool was about 90% finished, I have invited one of the participant candidates to participate in the evaluation of the first iteration; the Test Run. During this run I was hoping to find out where the tool and perhaps experimental setup would result in issues in a real setting. The results from this test run (see table 4 on the next page) are used in the data analysis, and to improve the tool and be better prepared for the following real experiment. Any issues that came up did not influence the way the participant answered the questions.

Table 4. Experiment test run with the Compliance Scan

What happened	What can be learned from this
Participant questions	
I determine the means of processing, but someone else the purpose. What am I?	After questions "who determines" and user answering someone else, also ask "just them or together with you?"
Is developing software for another organization also processing?	Describe processing more clearly
In the introduction. "Do you process personal data?" do you mean regularly or at all?	Change question to "Do you process any personal data?"
In the introduction, what does "the processing" mean in the question "Is the processing your main activity?"	Change question to: "Is processing the main purpose of your assignment?"
What is a public body?	Add translation and maybe example
Does "Do you perform a DPIA" mean whether I do it now or will be doing in the future? (filled out incorrect)	Change question to "Does your organization perform a DPIA ..."
In design/default, what exactly is a measure?	Help text with: (maatregelen) Measure such as standard settings for software and a policy stating this is done
When arriving at the report, what do I do now?	Write a small piece of text to explain what the report is, and display it on top
What do the Yes and No and other things mean?	Write a small piece of text to explain what the report is, and display it on top
Problems participants ran into	
The questions are in English, but the information text in Dutch	Add the Dutch translation of the ten topics. (See table 13 in the appendix)
Participant thinks he is a processor, but the tool says he is a controller	This happened due to the fact that the participant processed PD for a controller, but the processing was not the main assignment. According to the GDPR, the participant is therefore the controller of the personal data. This should be explained after the question and in the report
In design/default, the first question of design is unclear	Change question to: Is only the bare minimum of personal data used for processing?
Participant remarks	
In the introduction, it wasn't clear whether "Someone else" meant inside my company, or another company	Change to "my organization or another party"
It is good to see what exactly is important for the topics in the report. For some topics, I was not sure about it beforehand	Will be added to future improvements
The colouring of No is not consistent with what you would expect; sometimes a hard no is orange while you would expect it to be red, and a soft no is red while you would expect it to not be that big of a problem	Make all hard No's red, and soft No's (less problematic) orange
Maybe it is a nice idea to make a top three/top five actions the user should take, not clear what is a priority right now	Will be added to future improvements

Observer remarks	
There is no need for a right to automated, participant filled in "no"	Add option of "no automated decision making processing" or "N/A"
There were still quite some translation issues	Add more help text, or allow the observer (myself) to translate on the spot
When the final questions have been answered and the participant was presented with the report, they did not know what to do with it	Write a small piece of text to explain what the report is, and display it on top
The Yes and No in the report raised questions, it was not clear what this meant	Write a small piece of text to explain what the report is, and display it on top
While answering the questions in the tool, the user was thinking well and hard. It is a good thing that the tool makes the user think	Pay attention to this in the real experiments
While filling out the second questionnaire, the participant looked at the report they were presented with. The observer did not state whether this was allowed or not	I shall allow it, since they are only looking back on what they learned from the tool
The user skipped a lot of information texts in the tool	If other participants do this, ask why they did not do it

Since the tool will be slightly improved using the findings of the test run, I need to watch out that this does not result in a slight overfit of the tool for the experiment.

5.3 Tools and software

The following tools and software was used during this thesis:

- Google Drive
- Google Docs, Slides, Spreadsheets
- Dropbox
- Skype
- Slack
- The ISO2Handle platform
- Signavio
- GanttProject
- Microsoft Office
- Regelhulp Algemene Verordening Gegevensbescherming[4]

[4]https://rvo.regelhulpenvoorbedrijven.nl/avg/ Retrieved 21-06-2018

6 Results

6.1 Duration

Figure 7 shows the time it took the participants to walk through all steps of the respective tool. The participants of the RVO tool walked through ten steps, and the participants of the C-Scan walked through seven steps. As can be seen in Table 5, the C-Scan took on average more than twice the time to complete. The time to complete (TTC) was more consistent in the RVO tool than in the C-Scan. The highest TTC was during a C-Scan experiment where there was unclarity about the situation of the organization (public authority or not, joint controller/controller) and several questions about the meaning of terms or explanation of GDPR topics. The quickest RVO participant had the highest self reported compliance (7x Yes) and the second highest confidence before the experiment. The quickest C-Scan participant had the highest self reported compliance (5x Yes, 1x Don't Know, 1x No) and the fourth highest confidence before the experiment.

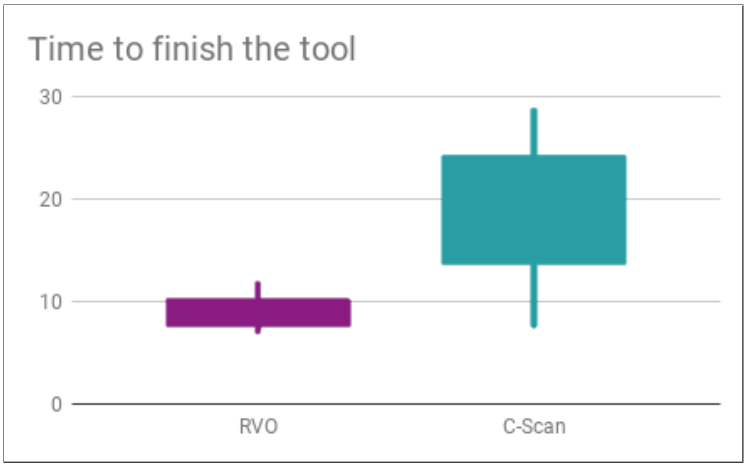


Fig. 7. Time in minutes to walk through all steps of either tool

Table 5. Duration metrics of both tools

	RVO tool	**C-Scan**
Minimum	6.9 min	7.5 min
Lower quartile (25%)	7.7 min	13.8 min
Average	9.0 min	18.5 min
Median	9.1 min	17.5 min
Upper quartile (75%)	10.0 min	24.0 min
Maximum	11.9 min	28.8 min

6.2 Perceived compliance improvement

As can be seen in figure 8, the RVO tool had a slightly higher average perceived compliance improvement. The compliance change was calculated by subtracting the compliance scores before the tool from the ones afterwards. From the data, no clear reason can be found for this. An analysis on more participants might shine light on the underlying reason, or even change the outcome due to the current low amount of participants.

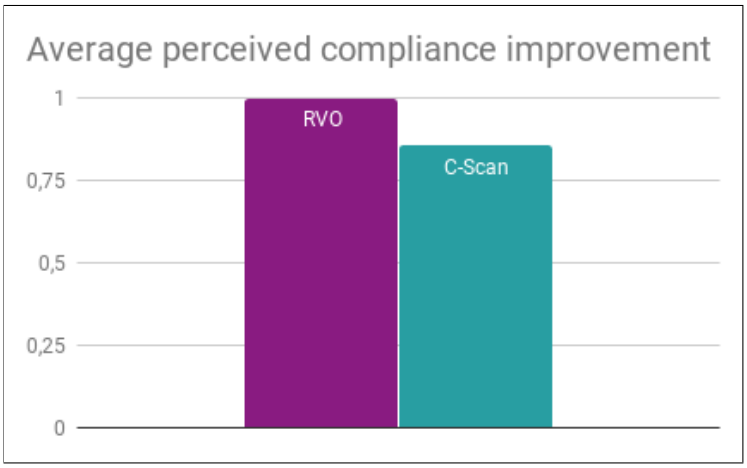


Fig. 8. Average perceived compliance improvement of both groups

When looking at the separate participants, there seems to be a different distribution in the perceived compliance change. The users of the RVO tool seemed to have either no or quite some improvement. The C-Scan participants varied more:

RVO participant perceived compliance change: 0,0,0,0,1,3,3
C-Scan participant perceived compliance change: -1,0,1,1,1,2,2

6.3 Confidence improvement

On average, the C-Scan tool managed to increase the participants' confidence more than the RVO tool did. The confidence change was calculated by subtracting the confidence scores before the tool from the ones afterwards. This is then averaged for each tool, which can be seen in figure 9. As will be discussed in chapter 6.4, the confidence change by itself does not tell the full tale. Both groups had one participant that was fully confident in their answers on all topics. Both the highest loss as well as the highest gain in confidence was with RVO group participants. The highest loss was an average of -0.86 per GDPR topic, the highest gain was an average of 1.00 per GDPR topic.

Combining these results with the results from chapter 6.1 (duration), there might be a connection. A possible explanation for the longer time it took and larger increase in confidence with the C-Scan group could be that the participants learned more than the RVO participants, which takes times. Future research could investigate whether there is in fact a link.

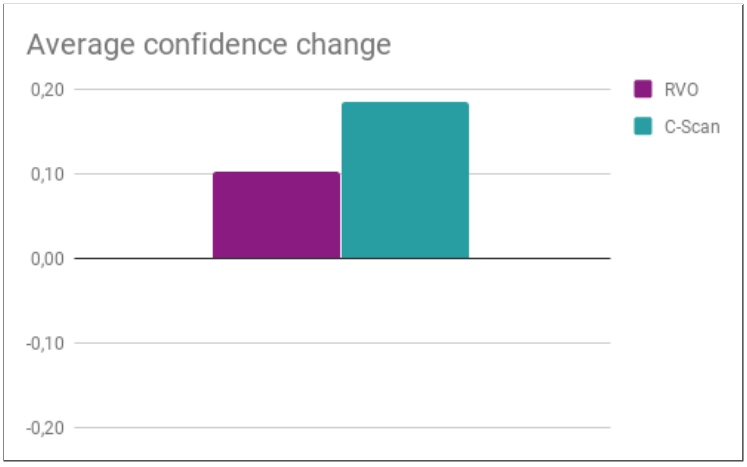


Fig. 9. Average confidence improvement of both group

6.4 The average perceived compliance and confidence per topic

In this subchapter, I will compare the average perceived compliance improvement per topic to the average confidence improvement per topic, which can be seen in figure 10. Every participant equates a 0.14 change in both graphs. Due to the low amount of participants, I will only zoom in on the topics where the perceived compliance and confidence do not seem to match up at all.

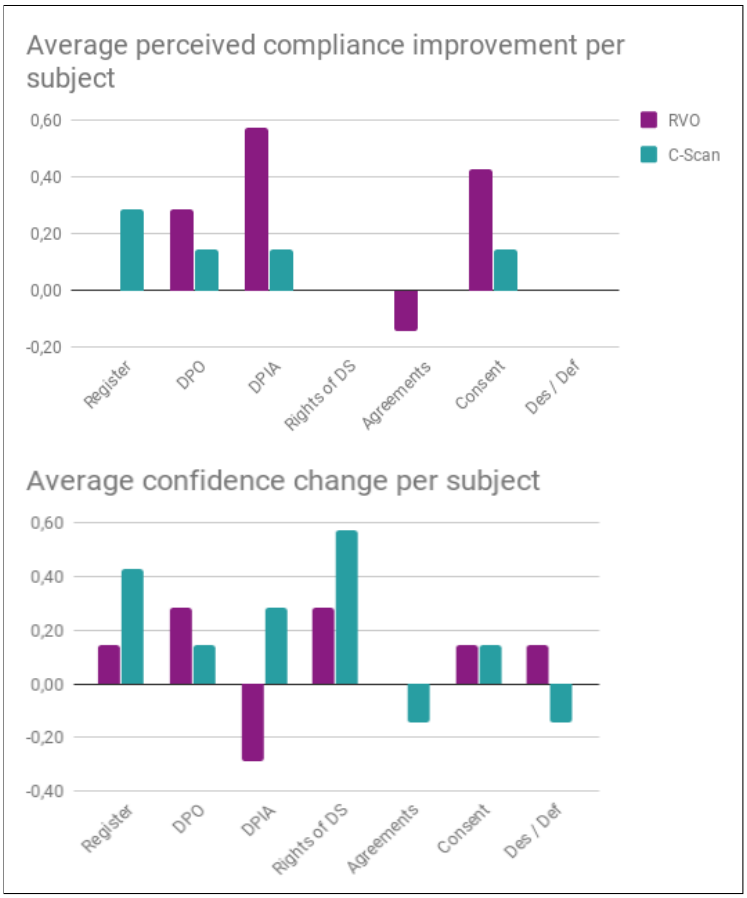


Fig. 10. Average perceived compliance and confidence change of both groups, per topic

Notable results:
Inconsistency in the topic DPIA:
In the RVO group, a substantial increase in perceived compliance was paired with a notable drop in confidence. Four out of seven participants using the RVO

tool went from No to Yes, while most became slightly less confident or remained just as (un)confident as before. The open question on whether the participant will do a DPIA in the next two months might provide more insight. This will be discussed in chapter 6.7

Inconsistency in the topic Rights of Data Subjects:
In both the RVO group and the C-Scan group, there was on average no perceived compliance change in the topic *Rights of Data Subjects*. One C-Scan user felt less compliant and one C-Scan user felt more compliant afterwards. The perceived compliance of the RVO group participants did not change. The confidence has, however, increased quite a bit for both groups. One RVO participant felt more confident, while three C-Scan participants felt more confident and one C-Scan participant felt less confident. Not feeling more/less compliant but feeling more confident might indicate that the participants were already well educated on the topic and had their thoughts confirmed by the tools.

6.5 Combining perceived compliance and confidence with overall confidence

In this chapter I would like to zoom in on cases where the participant reported a higher perceived compliance, but a lower confidence score. For these cases, I will take a look at how it correlated to their answers to overall confidence. In both cases, the participants used the RVO tool.

In the first case, the participant lost two confidence points on *DPIA*, two on *Consent*, two on *Design & Default*, and one on *Processing Agreements*. In all cases, the perceived compliance to the topics changed from No to Yes. When asked whether the participant felt more compliant overall after using the tool and why, they responded: "Yes, the tool indicates that several things are not required for us"'. This participant has therefore 'lost confidence', but still profited from the tool by learning from it.

In the second case, the participant lost one confidence point on *DPIA*, and one on *DPO*. In both cases, the compliance to the topics changed from No to Yes. When asked whether the participant felt more compliant overall after using the tool and why, they responded: "Yes. I am more aware of what we already have and what we still need to do". This participant has therefore also 'lost confidence' but still profited from the tool by learning from it.

This does, however, not mean that learning has to be accompanied by a loss in confidence. The clearest objectively observed learning moment took place during an experiment where a C-Scan participant gained confidence, and indicated to feel more confident overall. The participant was selecting the tasks they knew their DPO fulfilled, and saw a task in the lists they themselves were not aware of. The DPO, luckily, was aware of it.

6.6 Accurately determining compliance

A way to check whether the tool accurately determined (non) compliance is to focus on an easy to judge topic. This topic is the need for a DPO, since the GDPR is quite clear with its criteria. By comparing the judgment of the tool to the three criteria of the GDPR, discrepancies can be found.

According to Article 37 GDPR, if one or several of the following occurs, a DPO is needed:

1. The processing is carried out by a public authority or body, except for courts acting in their judicial capacity
2. The core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale
3. The core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offenses referred to in Article 10

Only two discrepancies were found, one for the RVO tool and one for the C-Scan. Both were due to the fact that the responsible persons made a decision on what they determined to be a *large scale*. Since the GDPR gives no ballpark figure to determine what a large scale is, this will not be seen as shortcomings of the tools.

The same problem occurred when trying to find discrepancies in the need for a register of processing activities. The main reason organizations need a register of processing activities is that they either have more than 250 people employed or their processing of personal data is non-occasional. The former is easy to check and fairly impossible to get wrong, but the latter requires interpretation.

6.7 Has the tool put people to action?

One way to determine whether a tool has had a positive effect, is to see whether the tool was able to motivate users to improve their GDPR compliance. Open questions four to seven of experiment phase six indicate whether the tool has informed participants well enough to mobilized them to make steps towards becoming GDPR compliant on the topics *Register of Processing Activities, DPIA's, DPO*, and *Rights of Data Subjects*. The exact questions were:

4. Is your organization going to implement a register of processing activities or change the current one? Why?
5. Will your organization perform a DPIA in the next two months? Why?
6. Has your decision on the need for a DPO changed? Why?
7. Will your organization be changing the way rights of data subjects are handled? Why?

A Yes means that the participant will perform the action, but this may only be seen as being put to action when it was not already planned before using the tool, hence the question for the motivation. A No means that the participant will not perform the action, but this may only be seen as not being put to action when the participant should perform the action but has decided not to. Deciding not to perform an action because the participant is already compliant on the topic is completely fine.

RVO tool
Table 6 shows the answers to the questions participants using the RVO tool gave, minus the explanation. Below the table is a selection of the given reasons for answering Yes or No, where answers by different participants are separated by commas.

Table 6. RVO participants' answer to whether they will improve compliance on four GDPR topics

	Register	**DPIA**	**DPO**	**Rights of DS**
Yes	5	1 + 1 maybe	2	1
No	2	5	5	6

Is your organization going to implement a register of processing activities or change the current one?
Yes: We have to and were already working on one before the experiment, it is mandatory, do not have one now.
No: Already in order.

Will your organization perform a DPIA in the next two months?
Yes: Definitely have 1/9 criteria, but better safe than sorry.
No: Do not expect there will be a need for this, do not need to do according to the tool, currently waiting for a DPIA model, don't process lots of data.
Maybe: Going to check with legal advisor.

Has your decision on the need for a DPO changed?
Yes: Image for our clients, I now know we don't need one.
No: Has been confirmed by our legal advisor, it still looks like we do not need this.

Will your organization be changing the way rights of data subjects are handled?
Yes: Provide a more on point privacy statement.
No: Already in order, we only process data for our clients, this already happens according to our pre-existing protocol, The design will change, but the way of processing will not.

Compliance Scan
Table 7 shows the answers to the questions participants using the C-Scan gave, minus the explanation. Below the table is a selection of the given reasons for answering Yes or No.

Table 7. C-Scan participants' answer to whether they will improve compliance on four GDPR topics

	Register	**DPIA**	**DPO**	**Rights of DS**
Yes	4	6	1	3 + 1 maybe
No	3	1 not sure	6	3

Is your organization going to implement a register of Processing Activities or change the current one?
Yes: We already have a compliant register, because it is mandatory, good for our own / users overview.
No: Probably prefer to spend the time differently, the current one is compliant enough.

Will your organization perform a DPIA in the next two months?
Yes: For GDPR compliance, we already planned to, will perform it to know how it works to be prepared as soon as we really need one, depends on new businesses/projects/innovations.
Not sure: Maybe for one of our special activities.

Has your decision on the need for a DPO changed?
No: Small firm that does not process special data, don't need any, do not need it and if we do we will "use" the DPO of our mother company, formally not necessary and do not see the need, already assigned, not needed but will be appointing a dedicated internal owner.

Will your organization be changing the way rights of data subjects are handled?
Yes: Will want to comply with their rights, we currently lack a policy for it, we will capture it better in our policy.
No: We will only automate it when it takes too much time to do it manually in comparison to automating it, rights can already be executed.
Maybe: Might change restriction of processing.

The comparison
The only noticeable difference when looking at both tables can be found in the topic DPIA. In the RVO tool, one participant said they will be performing a DPIA in the next two months while five said they would not. The rationale behind the decisions to not do it was a combination of being told/sure it is not required, and thinking it is not needed. The answers were a combination of de-

cided before and after the tool. For the Compliance Scan, this was nearly the opposite: six participants said they will be performing a DPIA in the next two months, while one said they will not. The rationale behind the decision to do a DPIA was a combination of wanting to comply with the GDPR and just doing one to know how it works. It was not clear whether these decisions were made before or after using the Compliance Scan.

A possible explanation for the higher number of participants that will perform a DPIA in the next two months may be the fact that the RVO tool explicitly tells participants a DPIA might not be needed for them, while the C-Scan does not. Another factor might be that the C-Scan explicitly advises to do at least one. Even though the GDPR does not require you to do a DPIA when you do not need it, doing a risk assessment at least once can create awareness and show that data protection is the norm.

As stated earlier, when examining the quantitative results one should keep in mind that only seven participants used each tool.

6.8 Net Promoter Score

The Net Promoter Score is a way to calculate a customer/user's experience with one's product or service.[5] Participants are asked how likely they are to recommend the product on a scale from 0-10. The given grades fall into three categories: detractors, passive, and promoters. Cultural differences influence the grade participants give[6],which is why there is an NPS, and an NPS-EU (see table 8). European customers are in general less excited and more critical, shifting the grading categories slightly.

Table 8. Cultural difference in NPS

	NPS grades	**NPS-EU grades**
Detractors	0-6	0-5
Passive	7-8	6-7
Promoters	9-10	8-10

The NPS(-EU) is calculated as follows: NPS(-EU) = %promoters - %detractors

The result will be a real number, between -100 and 100. Normally it would be compared to an industry standard, but due to the relatively low amount of participants the scores will only be compared to each other. The NPS-EU scores of the RVO tool and Compliance Scan can be found in table 9.

[5]https://www.medallia.com/net-promoter-score/ Retrieved on 14-07-2018

[6]https://www.allesovermarktonderzoek.nl/onderzoeksmethoden/net-promoter-score/ Retrieved on 14-06-2018

Table 9. NPS-EU of both tools

	RVO	**C-Scan**
Detractors	14%	14%
Passive	43%	43%
Promoters	43%	43%
NPS-EU	**29**	**29**

Due to the low amount of participants in both groups, one participant can change the score drastically. If one detractor were a promoter instead, the score would nearly double. The scores given by all participants can be found in table 10. The RVO tool received a slightly higher score on average. Just like the NPS-EU score, an average score given by seven participants can easily change with a participant giving a slightly higher or lower score. With this in mind, the tools scored virtually the same.

Table 10. Scores given and average

	RVO	**C-Scan**
	4	5
	6	6
	7	7
	7	7
	8	8
	9	8
	10	9
Avg.	**7.3**	**7.1**

6.9 Improvements from the initial interviews

Table 11 shows whether the insights gained from the initial exploratory interviews were successfully implemented.

Table 11. Improvements gathered from the interviews

Step	Plan	Status
1	I should advise users of the tool to spread awareness among all levels of employees as much as possible	Done, added in the extra information at the final report step
2	I should inform users on a way to (partly) automate requests from data subjects. For processors this could be to automatically forward the request to the right controller	I have developed BPMN models for handling requests. These models can easily be converted to a workflow or process
3	The register should be easy to fill out, and it should not take long	The register is currently being tested by independent consultants and their clients. The feedback on usability is good so far
4	I need to make sure the mandatory points are easy to check, and make it clear when a DPIA is needed	In the DPIA questions, the mandatory points are checked systematically. In the report, the user sees a conclusion whether DPIA's are done when needed and whether these contain all mandatory points
5	Information on this topic is missing. I shall conduct more literature research, so more examples can be given	More research on the topic has been done. It will be implemented in the tool at a later stage
6	I should make sure the formal decision for a DPO is made and stored	The Compliance Scan helps determine whether the user needs a DPO. This is stored and shown in the report
7	I will provide a standard protocol, based on what the GDPR says needs to be done	I have informed the users on the importance of a good protocol. Under Extra Information in the report, the user can read what the notifications to data subjects and the Supervisory Authority needs to contain and when these need to be notified
8	I will make clear that processing agreements with all parties personal data is exchanged with should be in place, and that for every party worked with needs to be determined whether personal data is involved	I have made this a literal question in the Compliance Scan. There is a choice between No, Some, and All. Both Some and No result in a red mark in the report, and only All results in a green mark
9	Since it is important to be absolutely sure who the LSA(s) is/are, I will advise the users to explicitly document the involved LSA. I will also help them determine it	The Compliance scan informs the user which party is their Supervisory Authority or that the user may choose one. The tool informs the user whether the national or regional Supervisory Authority is the one for them
10	I will make the users aware consent is a good base for processing, but not always the easiest or only one. Since the GDPR is quite strict on how consent must be requested, I will make sure to inform the users well of this	I have made the choice to rename the chapter Lawful Bases of Processing. This way, more than just Consent is captured, and the users become aware that there is more than one lawful basis. In the experiment I only asked about consent due to the AP article

7 Discussion

7.1 Participants' overall impression of the tools

After the participants gave their perceived compliance and confidence score for the second time, they were presented with some open questions. The first open question was: "*What are your overall impressions of the tool?*". The answers to this question can give insights to the strong points of both tools and where there is room for improvement. The second open question directly asked what could be improved, this will be discussed in chapter 7.3.

RVO tool:
The general impression of the RVO tool differed quite a bit. Some participants deemed it to be a bit too generic, while others found it to be too technical. The used language was experienced as vague by several, they felt the tool was actively trying to avoid statements like "You do not need a DPO" but used terms like "You do most likely not need a DPO". The participants found it easy to use and overall at least slightly useful. One participant found the "congratulations" and "well done" to be condescending, and thought it was weird the tool said the participant distinguished themselves positively from other organizations while compliance should be the norm.

C-Scan:
The general impression of the Compliance Scan was more uniform. The most used terms to describe the experience with the tool were "on point" and "to the point". The dashboard with red and green points was received well, but the flow and used language should be improved. One participant had used the RVO tool a while ago, and found the results the C-Scan presented much clearer.

7.2 Revisiting the criteria and research problem

Usefulness for companies of all sizes
As can be seen in table 12, the Compliance scan tool has been tested with organizations of various sizes.

Table 12. Organization size of participants

RVO Group	C-Scan Group
5	5
7	6 + 10 detach
10	8
10 + 60 freel.	15
11	20
23	40
150 + 650 teachers	200 + 350 flex

A final experiment in an organization with 2500 employees was done after the data collection, but only the insights for improving the tool are used from this. Micro-organizations with only one or two employees were considered to be out of scope.
Taking into account the category and size of organizations, the conclusions drawn in this paper apply to Small to Medium-sized Enterprises focused on software services and software development, health care, communication services, and social services.

Usability by non-experts
The Compliance Scan tool has been tested by participants of varying levels of GDPR knowledge. All participants using the C-Scan tool had at least some prior knowledge of the GDPR, and some were near experts on the GDPR. The person with the most limited experience needed extra explanation of the terms, but all this has been collected for future improvement. Most questions received from participants during the use of the tool was concerning the rights of data subjects. Participants, for example, did not know what a certain right was.
When more help text is added and participants have at least a basic understanding of the GDPR, the tool can be easily used by non-experts.

Accurately determine non-compliance to all parts of the ten step plan (minus personal data breaches, the lead supervisory authority, and awareness)
It proved to be quite difficult to check whether the tool has accurately determined. The tool has been developed by the main author of this thesis, which is the same person that interpreted the results. The only type of evidence that can be used is anecdotal; the observations made while participants used the tool. The only situation where the tool 'did not accurately determine compliance', was when a question was difficult to understand. By being unclear, the tool had therefore not accurately determined the actual compliance of the participant. An example of this is the following observation I made:
"Participant was not sure what Data Protection by Design and Data Protection by Default was, so entered no".
A positive reaction regarding accurate determination given by a participant was: "The tool shows me the same improvement points as an expert did previously".
From this I can conclude that the tool does most likely accurately determine (non) compliance to all parts of the ten step plan.

Advise on improvements towards compliance using, where appropriate, business process models
Advising on improvements towards compliance has worked out as planned. I have not been able to test the business process models with users. After one experiment, I have used one model to explain when a data subject's request needs to be honored, which seemed to clarify it for the participant. The developed BPMN models can be found in the appendix (figures 14-21).
Testing and improving the modeled processes would be future work.

Combining these conclusions on the criteria for success, the tool can be considered to be a moderate success. Holding it back from being called a full success is the fact that I cannot say with a full 100% certainty that the tool determines (non) compliance to all ten steps accurately, and the BPMN models have not been put to the test.

Revisiting the Research Problem:
In the first chapter, the technical research problem, *The design of a checklist that satisfies accuracy and ease of use so that GDPR compliance can be checked in business processes*, was introduced. Since the tool is considered to have been successfully developed, the approach taken in this thesis combined with the found improvements can be seen as the solution to the research problem. The most vital parts in this process were: Determining the scope (topics used), using the law itself as the source, interviewing organizations for insights, implementing the feedback, and testing against a similar tool. The iterative approach payed off.

Ease of use in a successful checklist stems from clearly formulated questions, plenty real-world examples, no vagueness and ambiguity, a clear scope, and a well structured report.

7.3 Future improvements to the tools

7.3.1 Improvements to the Compliance Scan

1. A top three or top five list of actions to take in the report, based on priority
2. Have the tool in Dutch (already done after experiments)
3. Being able to change the font size for readability
4. Sometimes a bit abstract, adding examples might help
5. Make the distinction between your own answer and the recommendation more clear
6. Certain questions and/or sentences were too long, shortening these would help
7. The tool should determine whether the user actually needs to perform a DPIA and base its advice on that
8. Extend the topic of Data Protection by Design and Data Protection by Default using e.g. the found research by Colesky et al. [2016]
9. Assist the users more on the rights of data subjects

7.3.2 Improvements to the RVO Tool

1. The questions are not detailed enough
2. Questions are quite general (nothing about underage data subjects for example)
3. Some questions are vague
4. It might be a good idea to work with sub-questions
5. The advice should be more accurate
6. Remove errors
7. The question about incidental processing (need for register) was unclear due to the double negative
8. Even when one indicates not to process data related to criminal convictions, the tool tells the user to stop processing this type of data
9. The tool could use more examples
10. The tool should state more clearly what type of organizations it is meant for
11. When selecting the lawful bases for processing, the user can select any of the six bases and the option of no base. This should not be possible

7.4 Possible influences on the experiment results

- During the experiment, both groups only contained seven participants. This low amount means that no statistical analysis can be done on the quantitative results, and I had to be careful with conclusions
- Selecting of participants was not completely random, since they knew ICTI and/or Joost Krapels (in)directly
- The participants were aware of the tool they were using; it was not a double blind test setup
- The participants could only indicate Yes, Don't Know, and No to the questions "Are you compliant on the topic of ...?". Some participants indicated they would have preferred a 1-5 scale on how close to compliance they thought to be. 80% compliance on a topic is now a clear no, and full compliance to the GDPR is difficult. A scale of 1-5 with an extra option of Don't Know would indeed paint a more fair picture of perceived GDPR compliance
- Participants might think that multi select questions with a lot of text in the options were cumbersome, and did not completely read them before selecting. A fix to this could be to check whether the user has his/her full attention on the tool by adding an option like "If you are still awake, do not select this option"
- It turned out to be difficult to give a confidence score when the compliance questions on that topic was answered with a Don't Know
- During two experiments with the C-Scan tool, some minor technical errors occurred
- The RVO tool was in Dutch, and the C-Scan tool was in English. Dutch is the mother tongue of all participants, which may have influenced the speed, perceived compliance, confidence, and NPS-EU scores. To combat this, I was present during all experiments and translated difficult terms on the spot

– The experiments were done over the course of six weeks, from mid April to the end of May. Later experiments were closer to the 'deadline' of May 25th, and some were even after the deadline. Early participants might have improved their compliance in the meantime
– The tool was improved after the test run, this might have resulted in a slight overfit

7.5 Main takeaways

Taking all discoveries about the Compliance Scan into account,three main takeaways arise:

1. The developed tool can help support and educate on GDPR compliance
2. The the tool is useful for SMEs in the branches software services and software development, health care, communication services, and social services
3. The main improvements are adding examples and improving readability

The developed tool can help support and educate on GDPR compliance
Even though the GDPR can prove to be a difficult topic, the tool developed following the strategy described in this paper was able to teach participants some new things, help them become more confident on their view of their own compliance, and present them with clear insights in their GDPR compliance. This was seen in the results as an overall positive confidence improvement and in the answers to the open questions.

The tool is useful for SMEs in the branches software services and software development, health care, and social services
The seven participants that used the Compliance Scan develop software, provide a software service, provide a communication service, provide health care, or provide a social service. The size of the organizations they work at range from five full-time employees to 200 full-time + 350 part-time/flex workers. The research results shows and the overall consensus was that the tool was a useful way to learn more about the GDPR and one's own compliance.

The main improvements are adding examples and improving readability
Even though the tool was considered useful by organizations of different sizes and by people of different expertise levels, the tool could definitely benefit from more clear real-world examples and easier to read/understand questions. The goal is to make the tool more intuitive, so that users instantly understand what is asked and can translate this to their own situation.

8 Conclusion

Summary
In this paper I have described the development of the Compliance Scan; a rule based system for checking GDPR compliance. Its design was structured following the DSRM, and the content was based on the ten most important GDPR topics according to the Dutch Supervisory Authority. Since an Information System was going to be developed, the choice was made to formulate a technical research problem instead of a research question. This technical research problem, *The design of a checklist that satisfies accuracy and ease of use so that GDPR compliance can be checked in business processes*, indicates the goal of this paper; the solution to a gap in research and existing tools. To further specify the goal and remain true to the DSRM, a more detailed objective of the solution was established before the Design and Development stage.
The developed Compliance Scan contains a set of questions for each topic and ends with an automatically generated custom report that shows strong points and improvements. During initial development, focus points were gathered by structurally interviewing five organizations that fell in scope due to their size and industry. A test run of the experiment was done, and its results were used to improve the tool. The system was then compared, on seven overlapping topics, to an already existing ruled based system made by the Dutch Supervisory Authority and the RVO. Seven participants were presented with one tool, and seven with the other tool. The measured variables were perceived compliance and confidence, which were measured by collecting a combination of quantitative and qualitative data.

Deduction from the results
The RVO tool seemed to cause a slightly higher perceived compliance change, but the Compliance Scan caused a higher confidence improvement on average. It took participants a lot longer to complete the Compliance Scan, but combined with the higher confidence improvement I suspect this indicates that the participants learned more from the Compliance Scan than from the RVO tool. The impression of the C-Scan was that it is to the point and has a useful way of presenting the results, as indicated by the participants of varying GDPR expertise levels that represented SMEs in the areas of software development, software service provision, communication service provision, health care, and social service provision. The main areas of improvement for the tool are the lack of real world examples and the fact that some questions need to be simplified. Overall, the tool seemed to be a useful way to support and educate on GDPR compliance. The criteria attached to the research problem have been met, so the solution to the technical research problem would be the approach taken in this paper that lead to a successfully developed tool. Summarized in one sentence, this would be to determine a strong scope, use the most reliable source (GDPR itself) for the content, gain insights using interviews, implement all feedback, and test against a comparable pre-existing tool.

Limitations to the conducted research
When examining the results, one has to keep in mind that only seven participants have used either tool. For this reason, the focus was more on the qualitative side than on the quantitative during the analysis. Another limitation to keep in mind is that the experiments were done over the course of six weeks, with the final experiments taking place after the GDPR went into effect. The participants for the research were not randomly selected from the total pool of all Dutch SMEs, but were randomly assigned to either one of the two groups.

Future research
Future research on the topic of GDPR compliance tools could use the anecdotal feedback, the found strong points, and the points for improvement from this paper, and could build forward on the now newly existing tool by doing another iteration in the DSRM. More chapters and exceptions from the GDPR could be implemented, and tests can be done on the best way of presenting feedback to the user. The BPMN models developed for and implemented in the tool need to be tested on ease of use and usefulness in general, since as of now it is unclear whether they can provide the extra support on the topic of Rights of Data Subjects the participants seem to require. Continuing in the footsteps of Kingston [2017], the decision making in this tool might at some point be extended with AI to assist in GDPR compliance by "*asking all and only the relevant questions, monitoring activities, and carrying out assessments*". The developed Compliance Scan tool has laid the basis for a structural GDPR compliance analysis method, and may assist more organizations even better in the future.

Bibliography

AutoriteitPersoonsgegevens. In 10 stappen voorbereid op de avg. nov 2017. URL https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving/voorbereiding-op-de-avg.

C Bartolini, R Muthuri, and C Santos. Using ontologies to model data protection requirements in workflows. In Mihoko Otake, Setsuya Kurahashi, Yuiko Ota, Ken Satoh, and Daisuke Bekki, editors, *New frontiers in artificial intelligence*, volume 10091 of *Lecture notes in computer science*, pages 233–248. Springer International Publishing, Cham, 2015. ISBN 978-3-319-50952-5. doi: 10.1007/978-3-319-50953-2_17. URL http://link.springer.com/10.1007/978-3-319-50953-2_17.

E Buchmann and J Anke. *GI DL - Privacy Patterns in Business Processes*. Gesellschaft fr Informatik, Bonn, 2017. ISBN 978-3-88579-669-5. URL https://dl.gi.de/handle/20.500.12116/4101.

M Colesky, J Hoepman, and C Hillen. A critical analysis of privacy design strategies. In *Security and Privacy Workshops (SPW), 2016 IEEE*, pages 33–40. IEEE, 2016.

M El Kharbili. Business process regulatory compliance management solution frameworks: a comparative evaluation. In APCCM '12 Proceedings of the Eighth Asia-Pacific Conference on Conceptual Modelling , editor, *APCCM '12 Proceedings of the Eighth Asia-Pacific Conference on Conceptual Modelling*, volume 130, pages 22–32. Australian Computer Society, Inc., 2012. ISBN 978-1-921770-11-1. URL https://dl.acm.org/citation.cfm?id=2523786.

M El Kharbili, S Stein, I Markovic, and E Pulvermuller. Towards a framework for semantic business process compliance management. *Proceedings of GRCIS*, 2008. URL http://ai2-s2-pdfs.s3.amazonaws.com/febb/99f0b652fd4e311487c6470e1dbf6570d19a.pdf.

EuropeanCommission. Privacy and data protection impact assessment framework for rfid applications. 2011. URL https://ec.europa.eu/digital-single-market/en/news/privacy-and-data-protection-impact-assessment-framework-rfid-applications.

M Evans. Gdpr checklist. 2016. URL http://www.nortonrosefulbright.com/les/gdpr-checklist-139465.pdf.

M Hashmi, G Governatori, and M T. Wynn. Normative requirements for regulatory compliance: An abstract formal framework. *Inf Syst Front*, 18(3): 429–455, jun 2016. ISSN 1387-3326. doi: 10.1007/s10796-015-9558-1. URL http://link.springer.com/10.1007/s10796-015-9558-1.

E Heuck, T Hildebrandt, R Kiaerulff Lerche, M Marquard, H Normann, R Iven Stromsted, and B Weber. Digitalising the general data protection regulation with dynamic condition response graphs. In *Proceedings of the BPM 2017 Industry Track co-located with the 15th International Conference on Business Process Management (BPM 2017)*, pages 124–134. 2017.

ICO. Preparing for the general data protection regulation (gdpr): 12 steps to take now. 2017. URL https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf.

LH Iwaya, LA Martucci, and S Fischer-Hubner. Towards a privacy impact assessment template for mobile health data collection systems. *Conference on M4D Mobile Communication Technology for Development*, pages 189–200, 2016. URL http://www.diva-portal.org/smash/get/diva2:1056790/FULLTEXT02.pdf#page=192.

J Kingston. Using artificial intelligence to support compliance with the general data protection regulation. *Artif Intell Law*, 25(4):429–443, dec 2017. ISSN 0924-8463. doi: 10.1007/s10506-017-9206-9. URL http://link.springer.com/10.1007/s10506-017-9206-9.

B Koops. The trouble with european data protection law. *International Data Privacy Law*, 4(4):250–261, 2014.

W Labda, N Mehandjiev, and P Sampaio. Modeling of privacy-aware business processes in bpmn to protect personal data. In *Proceedings of the 29th Annual ACM Symposium on Applied Computing - SAC '14*, pages 1399–1405, New York, New York, USA, mar 2014. ACM Press. ISBN 9781450324694. doi: 10.1145/2554850.2555014. URL http://dl.acm.org/citation.cfm?doid=2554850.2555014.

N Notario, A Crespo, Y Martin, J M. Del Alamo, D Le Metayer, T Antignac, A Kung, I Kroener, and D Wright. Pripare: Integrating privacy best practices into a privacy engineering methodology. In *2015 IEEE Security and Privacy Workshops*, pages 151–158. IEEE, may 2015. ISBN 978-1-4799-9933-0. doi: 10.1109/SPW.2015.22. URL http://ieeexplore.ieee.org/document/7163219/.

K Peffers, T Tuunanen, M A. Rothenberger, and S Chatterjee. A design science research methodology for information systems research. *Journal of Management Information Systems*, 24(3):45–77, dec 2007. ISSN 0742-1222. doi: 10.2753/MIS0742-1222240302. URL http://www.tandfonline.com/doi/full/10.2753/MIS0742-1222240302.

S Sadiq, G Governatori, and K Namiri. Modeling control objectives for business process compliance. In Gustavo Alonso, Peter Dadam, and Michael Rosemann, editors, *Business Process Management*, pages 149–164. Springer Berlin Heidelberg, Berlin, Heidelberg, 2007. ISBN 978-3-540-75182-3. doi: 10.1007/978-3-540-75183-0_12. URL http://link.springer.com/10.1007/978-3-540-75183-0_12.

C Tankard. What the gdpr means for businesses. *Network Security*, 2016(6): 5–8, jun 2016. ISSN 13534858. doi: 10.1016/S1353-4858(16)30056-3. URL http://linkinghub.elsevier.com/retrieve/pii/S1353485816300563.

R J. Wieringa. *Design science methodology for information systems and software engineering*. Springer Berlin Heidelberg, Berlin, Heidelberg, 2014. ISBN 978-3-662-43838-1. doi: 10.1007/978-3-662-43839-8. URL http://link.springer.com/10.1007/978-3-662-43839-8.

HB Winter, PO De Jong, A Sibma, FW Visser, M Herweijer, AM Klingenberg, and H Prakken. Wat niet weet, wat niet deert: een evaluatieonderzoek naar de werking van de wet bescherming persoonsgegevens in de praktijk. 2008.

Appendix

The appendix consists of the following:

1. A table with the Dutch and English names for the ten topics from the scope
2. The full structured view of the chapter *Register of Processing Activities*
3. The full set of example questions from the chapter *Register of Processing Activities*
4. Two chapters of an example Compliance Scan report
5. The BPMN models of the rights of data subjects
6. The full set of the initial interview questions, in both English and Dutch
7. The form given to participants during the experiment

Table 13. The Dutch and English names of the ten topics from the scope

English Translation	Original Dutch terms used
Awareness	Bewustwording
Rights of Data Subjects	Rechten van betrokkenen
Register of Processing Activities	Register van verwerkingsactiviteiten
Data Protection Impact Assessment	Data Protection Impact Assessment
Data Protection by Design and Data Protection by Default	Privacy by Design & Privacy by Default
Data Protection Officer	Functionaris voor de Gegevensbescherming
Personal Data Breaches	Meldplicht Datalekken
Processing Agreements	Verwerkersovereenkomsten
Lead Supervisory Authority	Leidende Toezichthouder
Consent	Toestemming

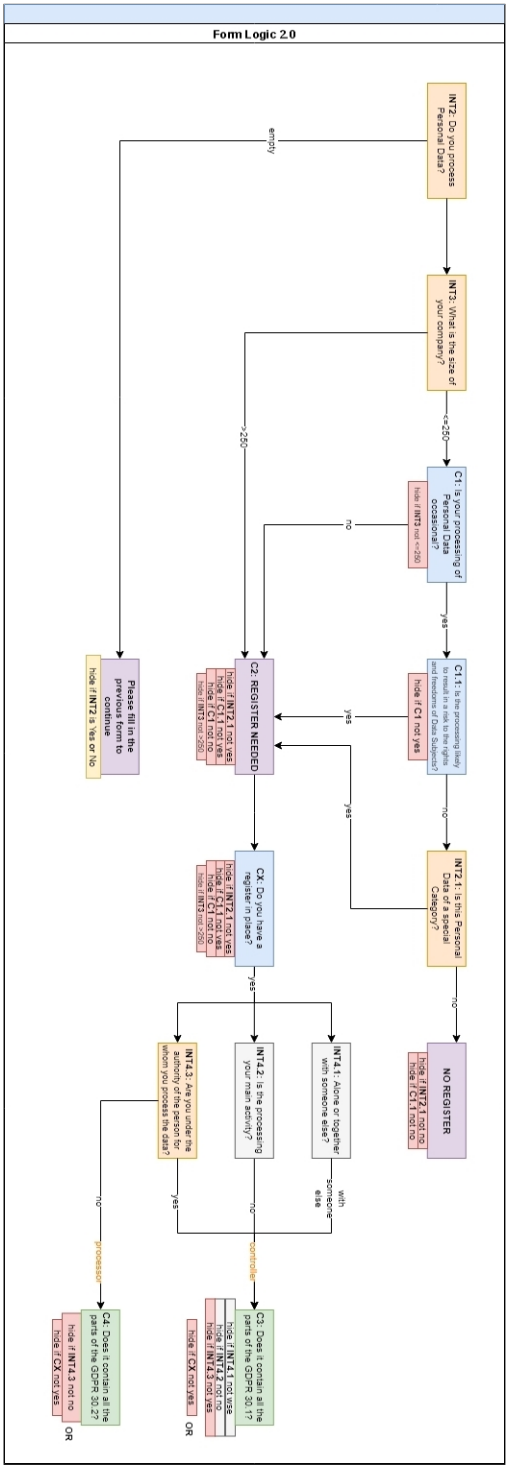


Fig. 11. The full structured view of the chapter *Register of Processing Activities*

Fig. 12. The full set of example questions from the chapter *Register of Processing Activities*

Fig. 13. Two chapters of an example Compliance Scan report

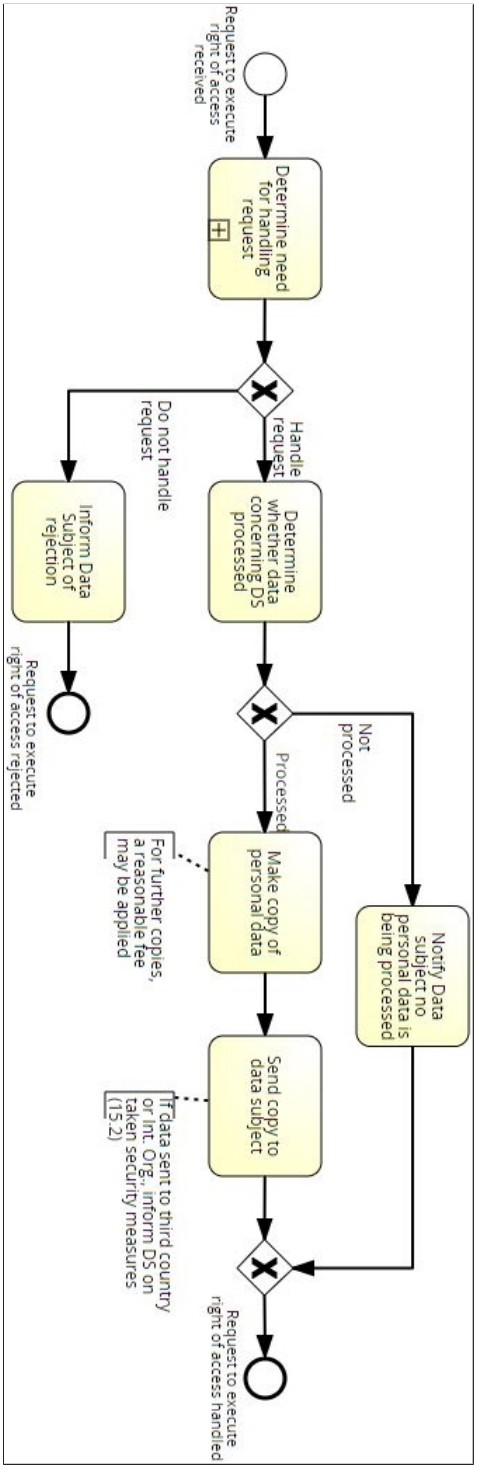


Fig. 14. The right of access in BPMN

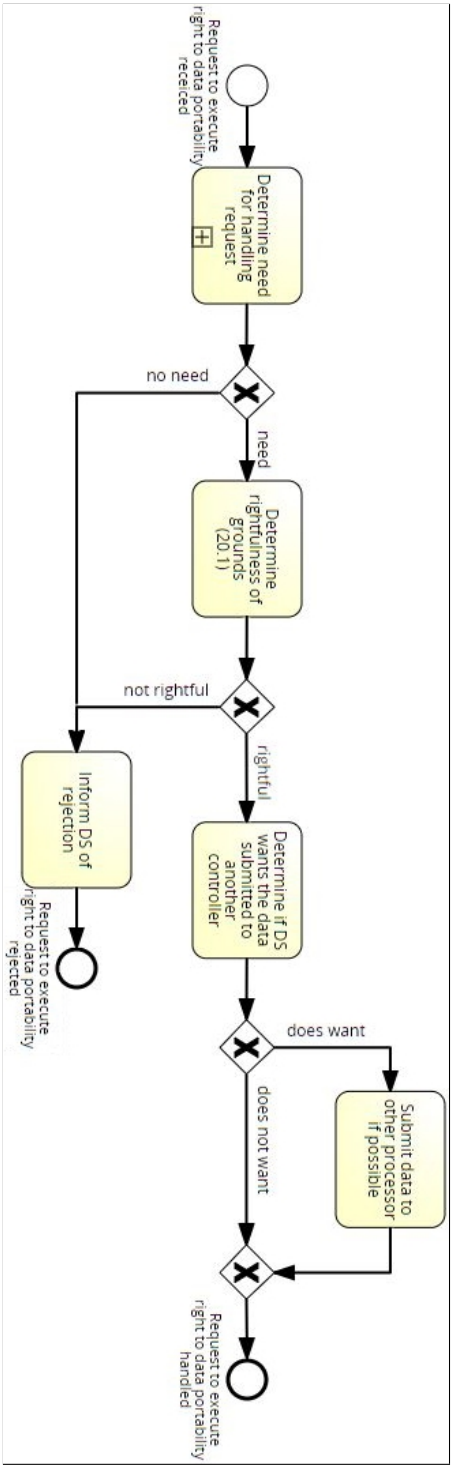


Fig. 15. The right to data portability in BPMN

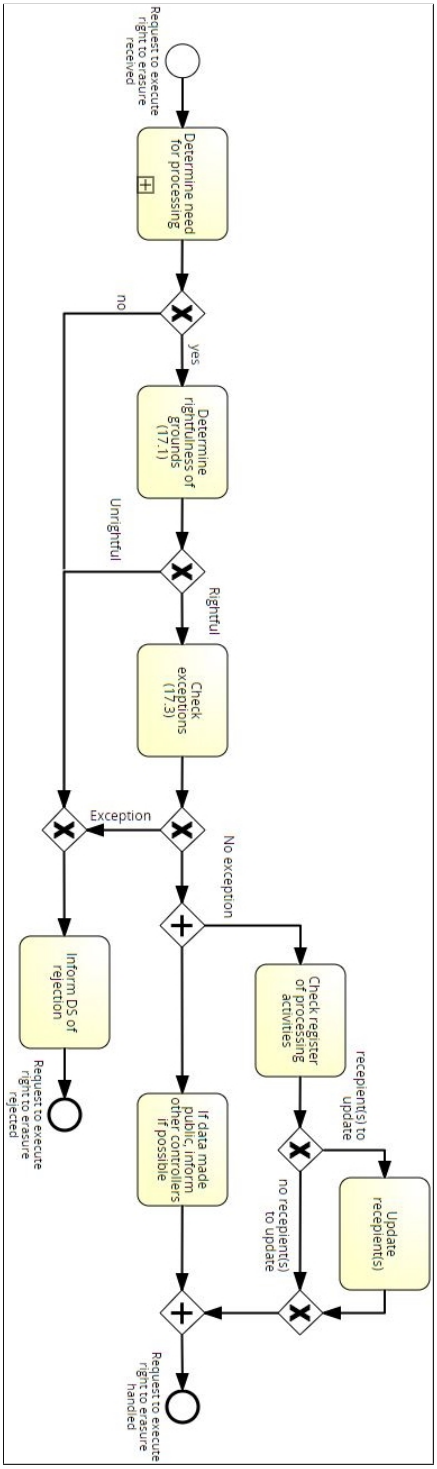


Fig. 16. The right to erasure in BPMN

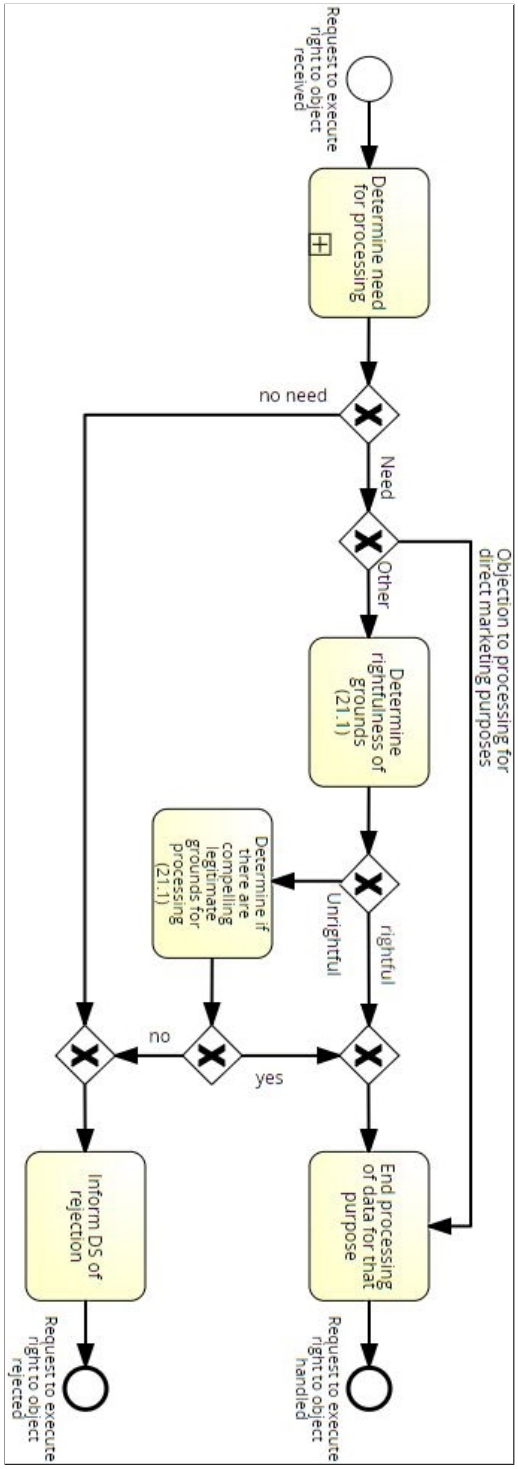


Fig. 17. The right to objection in BPMN

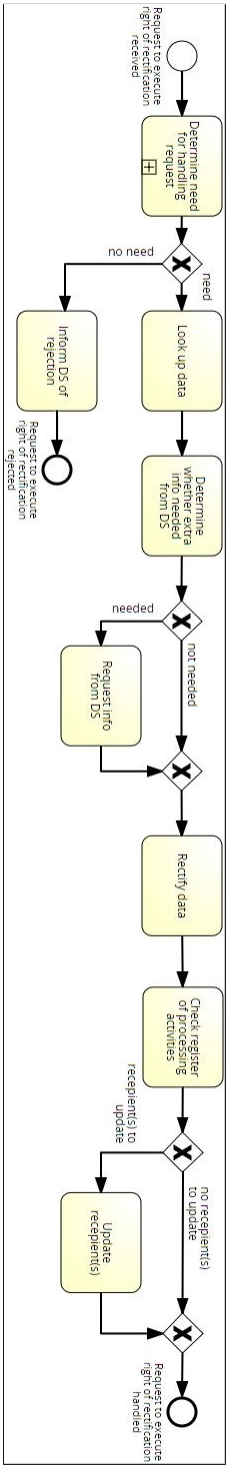


Fig. 18. The right to rectification in BPMN

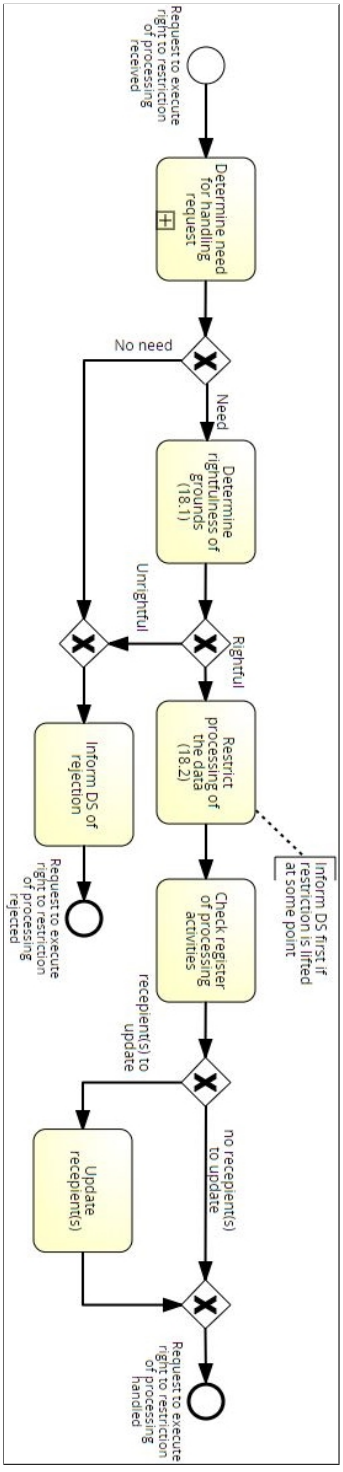


Fig. 19. The right to restriction of processing in BPMN

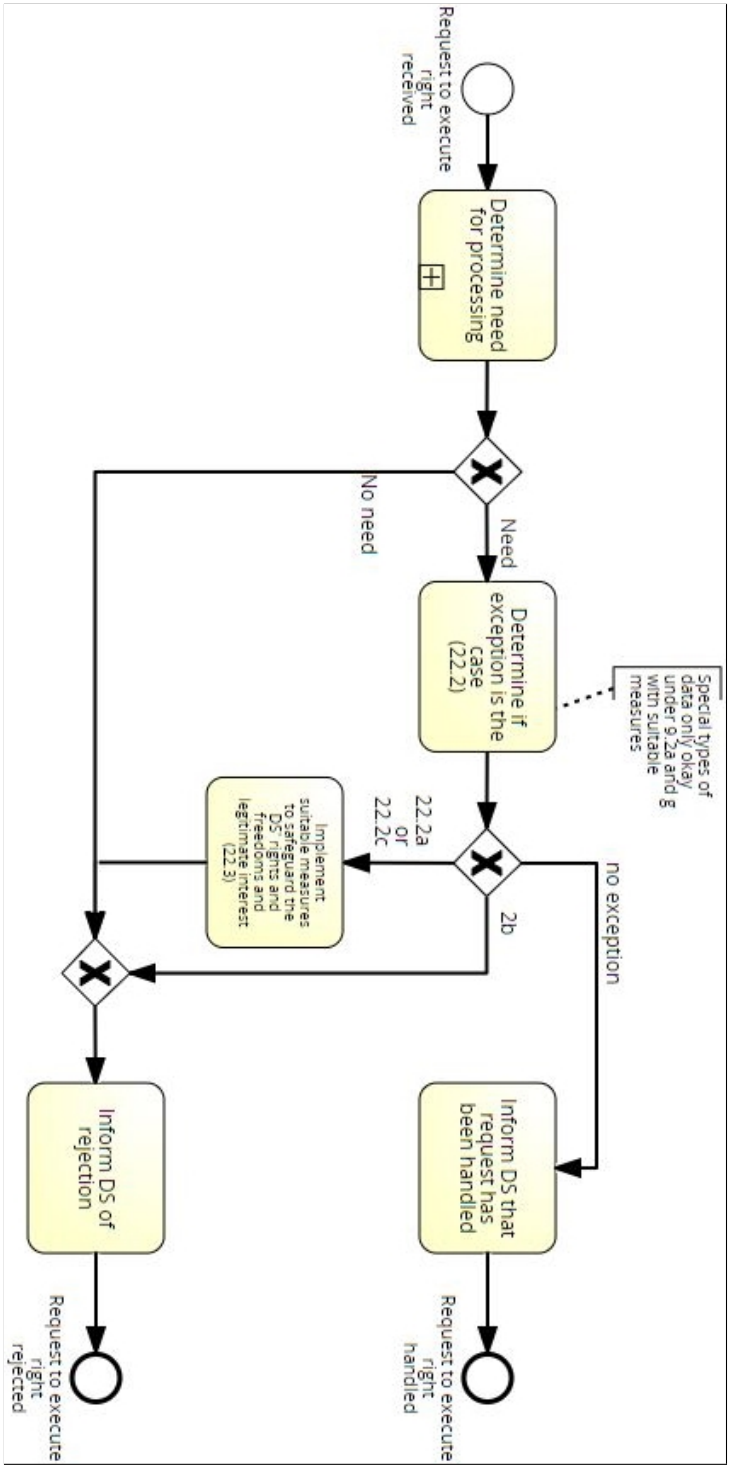


Fig. 20. The right to not be subjected to automated decision making in BPMN

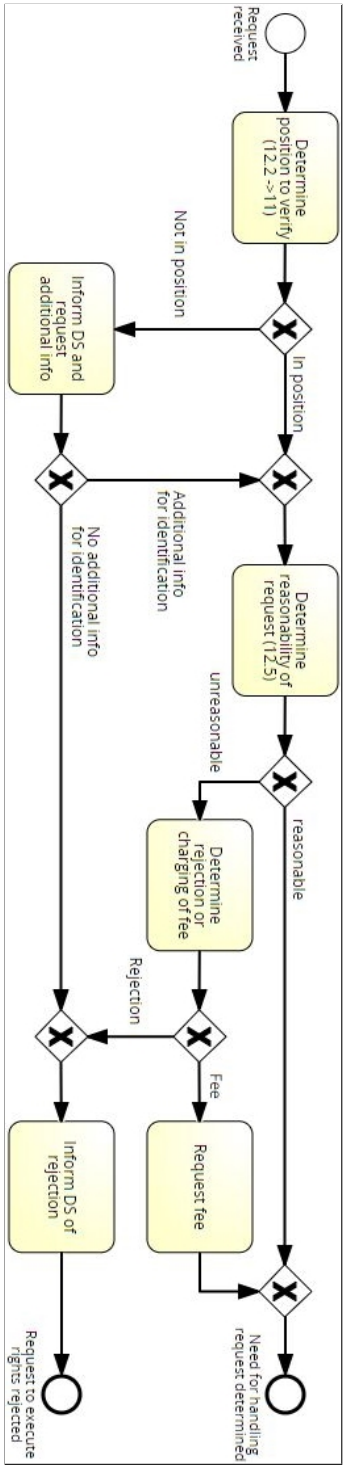


Fig. 21. The subprocess "Determine need for processing"

Interview Master Thesis on GDPR compliance

For my Master Thesis, I am developing an automated rule-based system that checks for high-level GDPR compliance and gives hands-on tips on how to improve it. I am interested in the current stance of GDPR readiness and compliance, and aim to gather information to make sure the system will capture real life scenarios as accurate as possible.

Your answers will be written down, typed up, and stored digitally under an identifying number. I will have a list that links this number to your company name, so I know which companies I have interviewed and which company to contact should clarification be needed afterwards. The list will be stored separate from the answers. No personal data will be recorded or processed, and no direct transcript from interviews will end up in my thesis.

1. What is the size of your company?
2. In what way has your company been occupied with the GDPR?
3. What is the current level of privacy awareness in your company?
4. How many Personal Data Breaches[1] have you had in the past 12 months?
5. What is your protocol for data leaks, and are all employees aware of this?
6. Have you made the decision on whether to assign a Data Protection Officer[2] after May 2018? What is this decision and how have you made it?
7. What is your protocol for a Data Protection Impact Assessment[3]?
8. How many of these have you conducted in the past 12 months?
9. Are you aware of the rights of Data Subjects[4]? Can they execute these rights with you, and how?
10. Do you have a register of processing activities[5]?
11. Do you have processing agreements[6] with companies you exchange personal data[7] with?
12. Have you determined who your Lead Supervisory Authority[8] is?
13. Do you have processing activities that require user consent[9], and if yes how is this consent requested?
14. Are you ISO27001 certified or working on becoming ISO27001 certified?
15. Do you have any questions or remarks?

Explanation of terms:

1. **Personal Data Breach:**
   A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.
2. **Data Protection Officer:**
   A person with expert knowledge of data protection law and practices that, in certain cases, has to be appointed. He or she is responsible for several privacy related issues inside your company.
3. **Data Protection Impact assessment:**
   An assessment of the impact of the envisaged processing operations on the protection of personal data. It needs to be carried out when a type of processing is likely to result in a high risk to the rights and freedoms of natural persons.

Fig. 22. Initial interview questions in English, first page

4. **Rights of data subjects:**
   Right of access
   Rights to rectification
   Right to erasure
   Right to restriction of processing
   Right to data portability
   Right to object
   Automated individual decision-making, including profiling
5. **Register of Processing Activities:**
   Most companies have to record all the ways they interact with personal data. This includes what is done with the data, how it is protected, and with whom it is shared.
6. **Processing agreement:**
   When personal data is shared to be processed by a third party, there should be an agreement in place stating, among others, the purpose of processing and rules that both parties have to abide by.
7. **Personal Data:**
   Personal data is any information relating to an identified or identifiable natural person (data subject).
8. **Lead Supervisory Authority**
   A Supervisory Authority is an independent public authority that monitors the application of the GDPR, nation wide or region wide. Since several Supervisory Authorities might be involved in one processing activity, one Supervisory Authority takes the lead.
9. **Consent:**
   Consent is any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Fig. 23. Initial interview questions in English, second page

Interview Master Thesis over AVG compliance

Voor mijn Masterscriptie ben ik een geautomatiseerd rule-based systeem aan het ontwikkelen, dat op een hoog niveau AVG compliance checkt en praktische tips geeft voor verbetering. Ik ben geïnteresseerd in de huidige status van AVG compliance en in welke mate bedrijven er klaar voor zijn. Met dit interview wil ik informatie verzamelen om het systeem zo goed mogelijk op de praktijk te gaan laten aansluiten.

Uw antwoorden worden genoteerd, uitgetypt, and digitaal opgeslagen onder een identificatie getal. Ik maak een lijst met daarin dit getal, gekoppeld aan uw bedrijfsnaam. Op deze manier weet ik welke bedrijven ik geïnterviewd heb, welke antwoorden bij welk bedrijf horen en kan ik, mocht het nodig zijn, de juiste persoon benaderen als er achteraf verheldering nodig blijkt. De lijst zal apart opgeslagen worden van de antwoorden. Er zullen geen persoonsgegevens verwerkt worden en er zal geen transcript van het gesprek in mijn scriptie belanden.

1. Wat is de omvang van uw bedrijf?
2. Op welke manier is uw bedrijf tot nu toe bezig geweest met de AVG?
3. Hoe is het momenteel gesteld met het privacy bewustzijn binnen uw bedrijf?
4. Hoeveel datalekken[1] hebben er in de afgelopen 12 maanden plaatsgevonden in uw bedrijf?
5. Wat is uw protocol voor datalekken, en zijn alle medewerkers ervan op de hoogte?
6. Heeft u de beslissing gemaakt of er een Functionaris Gegevensbescherming[2] nodig is vanaf eind Mei? Wat is deze beslissing, en hoe is deze tot stand gekomen?
7. Wat is uw protocol voor een gegevensbeschermingseffectbeoordeling[3] (DPIA)?
8. Hoeveel van deze heeft u in de afgelopen 12 maanden uitgevoerd?
9. Bent u zich bewust van de rechten van betrokkenen[4]? Kunnen zij deze rechten op dit moment bij u uitoefenen?
10. Heeft u een register van verwerkingsactiviteiten[5]?
11. Heeft u bewerkers/verwerkersovereenkomsten[6] met alle partijen waarmee u persoonsgegevens[7] uitwisselt?
12. Heeft u bepaald wie uw Leidende Toezichthouder[8] is?
13. Doet u aan gegevensverwerkingen waar de gebruiker toestemming[9] voor moet geven, en zo ja hoe gebeurt dit?
14. Bent u ISO27001 gecertificeerd of bezig dit te worden?
15. Heeft u nog vragen of opmerkingen?

Toelichting van termen:

1. **Datalek:**
   Een falen van beveiliging dat leidt tot de onvrijwillige of onwettelijke vernietiging, verlies, aanpassing, ongeautoriseerde uitgifte van, of toegang toe verstuurde, opgeslagen of anderwijs verwerkte persoonsgegevens.
2. **Functionaris gegevensbescherming:**
   Een persoon met diepgaande kennis van databeschermingswetgeving (in het bijzonder de AVG) die in sommige gevallen aangesteld moet zijn.

Fig. 24. Initial interview questions in Dutch, first page

3. **Gegevensbeschermingseffectbeoordeling:**
   Een beoordeling van de impact van een beoogde verwerkingsactiviteit op de rechten en vrijheden van betrokkenen. Deze moet uitgevoerd worden als het risico van de eerder genoemde verwachte impact hoog is.
4. **Rechten van de betrokkenen:**
   Recht van inzage
   Recht op rectificatie
   Recht op gegevens wissing
   Recht op beperking van de verwerking
   Recht op overdraagbaarheid van gegevens
   Recht van bezwaar
   Geautomatiseerde individuele besluitvorming, waaronder profilering
5. **Register van verwerkingsactiviteiten:**
   De meeste bedrijven zullen een register bij moeten gaan houden van alle manier waarop zij Persoonsgegevens verwerken. In dit register moet, onder andere, het doel van de verwerking, hoe de gegevens beschermd zijn, en met wie de gegevens gedeeld worden.
6. **Verwerkersovereenkomst:**
   Als persoonsgegevens gedeeld worden met een derde partij moet er een overeenkomst gesloten worden. In deze overeenkomst moet, onder andere, staan wat het doel van de verwerking is en aan welke regels beide partijen zich te houden hebben.
7. **Persoonsgegevens:**
   Persoonsgegevens zijn alle data die gerelateerd zijn aan een geïdentificeerd of identificeerbaar natuurlijk persoon (betrokkene).
8. **Leidend toezichthouder:**
   Een toezichthouder is een onafhankelijke publieke autoriteit die de toepassing van de AVG in de gaten houdt op landelijk of regionaal niveau. Aangezien er meerdere toezichthouders betrokken kunnen zijn bij een verwerking, neemt één toezichthouder de leiding en is daarmee uw aanspreekpunt.
9. **Toestemming:**
   Toestemming is alle vrijwillig gegeven, specifieke, geïnformeerde, en ondubbelzinnige aangeving van de wensen van de betrokkene waarbij hij of zij, middels een statement of duidelijke bevestigende actie, instemt met het verwerken van persoonsgegevens die hem of haar betreffen.

Fig. 25. Initial interview questions in Dutch, second page

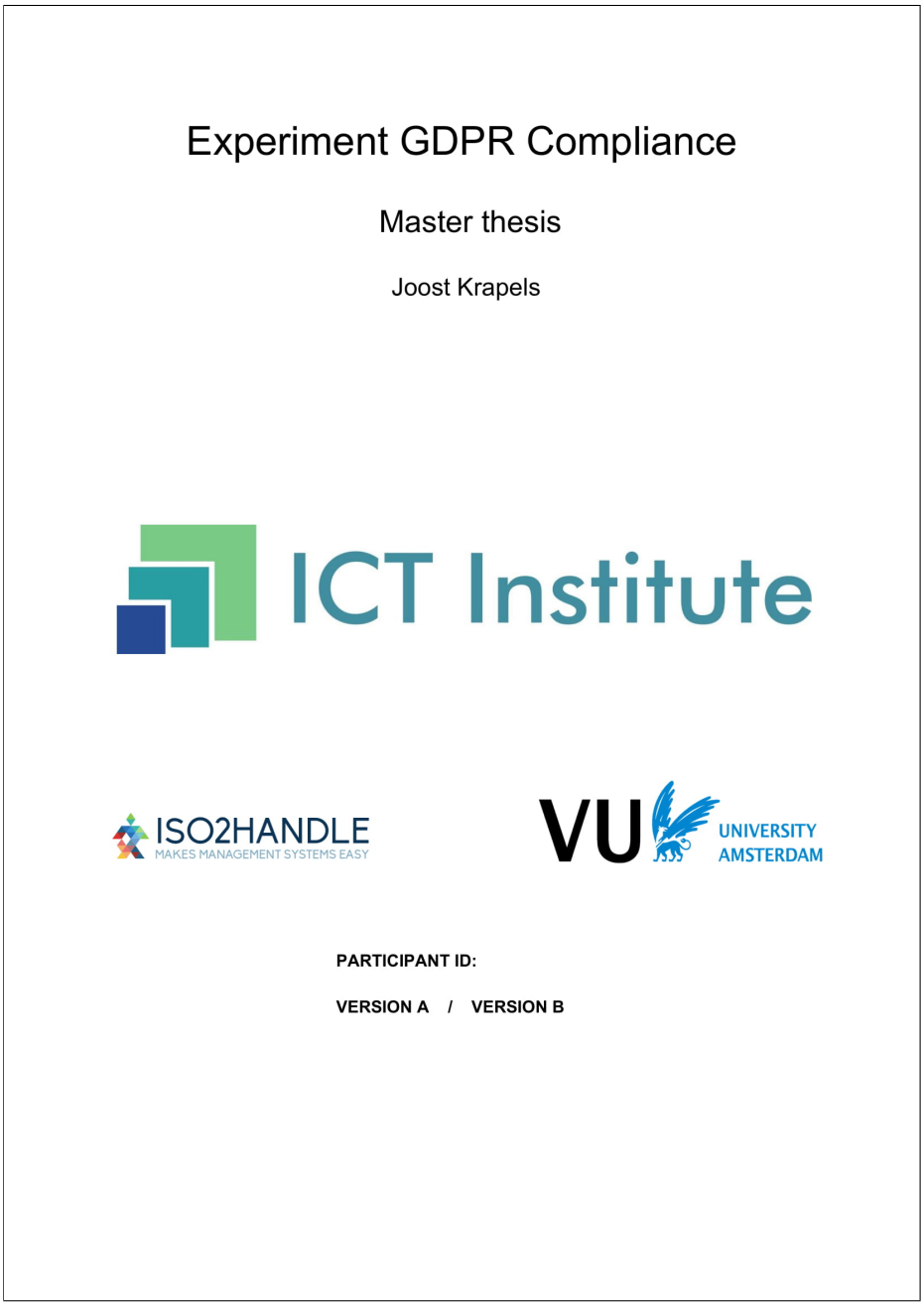
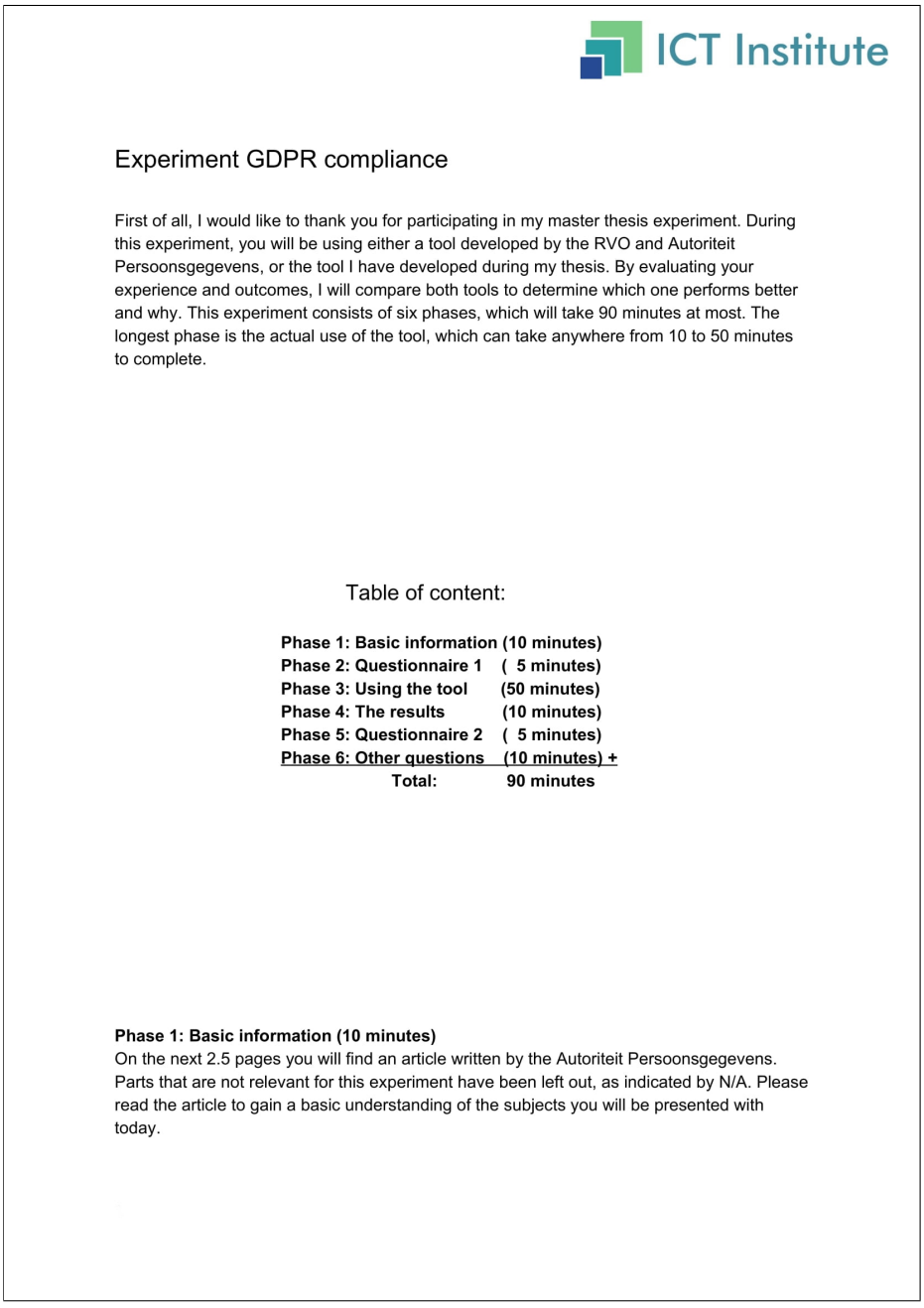


Fig. 26. Experiment form, first page


ICT Institute

Experiment GDPR compliance

First of all, I would like to thank you for participating in my master thesis experiment. During this experiment, you will be using either a tool developed by the RVO and Autoriteit Persoonsgegevens, or the tool I have developed during my thesis. By evaluating your experience and outcomes, I will compare both tools to determine which one performs better and why. This experiment consists of six phases, which will take 90 minutes at most. The longest phase is the actual use of the tool, which can take anywhere from 10 to 50 minutes to complete.

Table of content:

Phase 1: Basic information (10 minutes)
Phase 2: Questionnaire 1 (5 minutes)
Phase 3: Using the tool (50 minutes)
Phase 4: The results (10 minutes)
Phase 5: Questionnaire 2 (5 minutes)
Phase 6: Other questions (10 minutes) +
Total: 90 minutes

Phase 1: Basic information (10 minutes)
On the next 2.5 pages you will find an article written by the Autoriteit Persoonsgegevens. Parts that are not relevant for this experiment have been left out, as indicated by N/A. Please read the article to gain a basic understanding of the subjects you will be presented with today.

Fig. 27. Experiment form, second page


ICT Institute

In 10 stappen voorbereid op de AVG

Vanaf 25 mei 2018 is de Algemene verordening gegevensbescherming (AVG) van toepassing. Dat betekent dat vanaf die datum dezelfde privacywetgeving geldt in de hele Europese Unie (EU). De Wet bescherming persoonsgegevens (Wbp) geldt dan niet meer.

Wat verandert er?
De AVG versterkt de positie van de betrokkenen (de mensen van wie gegevens worden verwerkt). Zij krijgen nieuwe privacyrechten en hun bestaande rechten worden sterker. Organisaties die persoonsgegevens verwerken krijgen meer verplichtingen. De nadruk ligt –meer dan nu –op de verantwoordelijkheid van organisaties om te kunnen aantonen dat zij zich aan de wet houden.

Wat kan ik doen?
Als organisatie kunt u nu alvast stappen ondernemen om straks klaar te zijn voor de AVG. Om u hierbij te helpen, heeft de Autoriteit Persoonsgegevens de 10 belangrijkste stappen voor u op een rijtje gezet. In het grote AVG-dossier op de website van de AP vindt u de antwoorden op veelgestelde vragen.

Stap 1: Bewustwording
N/A

Stap 2: Rechten van betrokkenen
Onder de AVG krijgen de mensen van wie u persoonsgegevens verwerkt meer en verbeterde privacyrechten. Zorg er daarom voor dat zij hun privacyrechten goed kunnen uitoefenen.
Denk daarbij aan bestaande rechten, zoals het recht op inzage en het recht op correctie en verwijdering. Maar houd ook alvast rekening met nieuwe rechten, zoals het recht op dataportabiliteit. Bij dit recht moet u ervoor zorgen dat betrokkenen hun gegevens makkelijk kunnen krijgen en vervolgens kunnen doorgeven aan een andere organisatie als ze dat willen.
Ook kunnen mensen bij de AP klachten indienen over de manier waarop u met hun gegevens omgaat. De AP is verplicht deze klachten te behandelen.

Stap 3: Overzicht verwerkingen
Breng uw gegevensverwerkingen in kaart. Documenteer welke persoonsgegevens u verwerkt en met welk doel u dit doet, waar deze gegevens vandaan komen en met wie u ze deelt.
Onder de AVG heeft u een verantwoordingsplicht, wat inhoudt dat u moet kunnen aantonen dat uw organisatie in overeenstemming met de AVG handelt. Het bijhouden van een register van verwerkingsactiviteiten is onderdeel van de verantwoordingsplicht.
U kunt het register ook nodig hebben als betrokkenen hun privacyrechten uitoefenen. Als zij u vragen hun gegevens te corrigeren of verwijderen, moet u dit doorgeven aan de organisaties waarmee u hun gegevens heeft gedeeld.

Fig. 28. Experiment form, third page

ICT Institute

Stap 4: Data Protection Impact Assessment

Onder de AVG kunt u verplicht zijn een zogeheten data protection impact assessment (DPIA) uit te voeren. Dat is een instrument om vooraf de privacyrisico's van een gegevensverwerking in kaart te brengen. En vervolgens maatregelen te kunnen nemen om de risico's te verkleinen.
U moet een DPIA uitvoeren als uw beoogde gegevensverwerking waarschijnlijk een hoog privacyrisico met zich meebrengt. U kunt nu alvast inschatten of u straks DPIA's moet uitvoeren en hoe u dit dan gaat aanpakken.
Komt straks uit een DPIA naar voren dat uw beoogde verwerking een hoog risico oplevert? En lukt het u niet om maatregelen te vinden om dit risico te beperken? Dan moet u met de AP overleggen voordat u met de verwerking start. Dit wordt een voorafgaande raadpleging genoemd. De AP beoordeelt dan of de voorgenomen verwerking in strijd is met de AVG. Is dit het geval, dan ontvangt u een schriftelijk advies van de AP.

Stap 5: Privacy by design & Privacy by default

Maak uw organisatie nu al vertrouwd met de onder de AVG verplichte uitgangspunten van privacy by design en privacy by default en ga na hoe u deze beginselen binnen uw organisatie kunt invoeren.

Privacy by design houdt in dat u er al bij het ontwerpen van producten en diensten voor zorgt dat persoonsgegevens goed worden beschermd. Maar bijvoorbeeld ook dat u niet meer gegevens verzamelt dan noodzakelijk voor het doel van de verwerking. En dat u de gegevens niet langer bewaart dan nodig.

Privacy by default houdt in dat u technische en organisatorische maatregelen moet nemen om ervoor te zorgen dat u, als standaard, alléén persoonsgegevens verwerkt die noodzakelijk zijn voor het specifieke doel dat u wilt bereiken. Bijvoorbeeld door:

- Een app die u aanbiedt niet de locatie van gebruikers te laten registeren als dat niet nodig is
- Op uw website het vakje 'Ja, ik wil aanbiedingen ontvangen' niet vooraf aan te vinken
- Als iemand zich op uw nieuwsbrief wil abonneren niet meer gegevens te vragen dan nodig is.

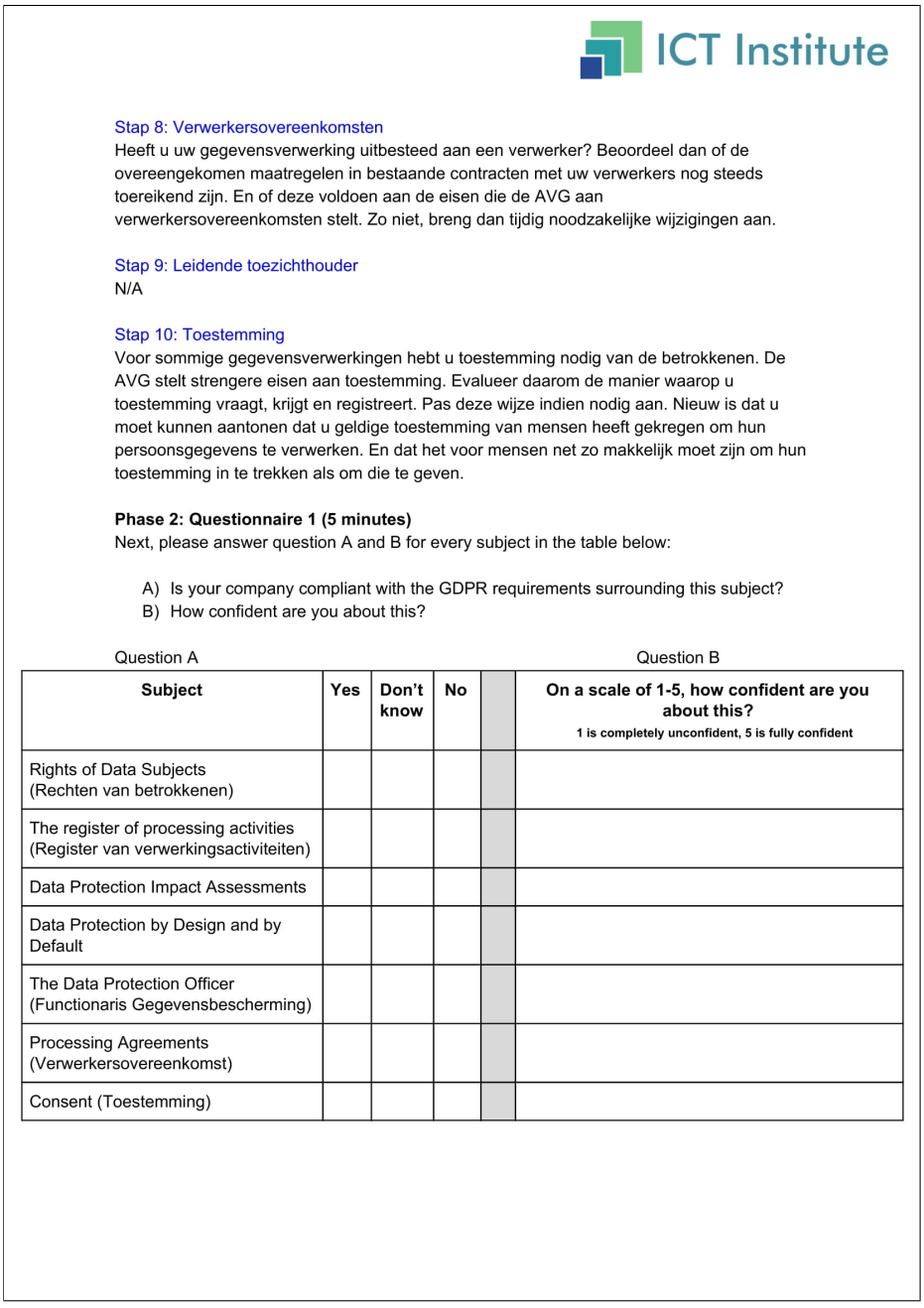
Stap 6: Functionaris voor de gegevensbescherming

Onder de AVG kunnen organisaties verplicht zijn om een functionaris voor de gegevensbescherming (FG) aan te stellen. Bepaal nu alvast of dit voor uw organisatie geldt. Zo ja, wacht dan niet te lang met het werven van een FG. Uiteraard mag uw organisatie ook vrijwillig een FG aanstellen.

Stap 7: Meldplicht datalekken

N/A

Fig. 29. Experiment form, fourth page


ICT Institute

Stap 8: Verwerkersovereenkomsten
Heeft u uw gegevensverwerking uitbesteed aan een verwerker? Beoordeel dan of de overeengekomen maatregelen in bestaande contracten met uw verwerkers nog steeds toereikend zijn. En of deze voldoen aan de eisen die de AVG aan verwerkersovereenkomsten stelt. Zo niet, breng dan tijdig noodzakelijke wijzigingen aan.

Stap 9: Leidende toezichthouder
N/A

Stap 10: Toestemming
Voor sommige gegevensverwerkingen hebt u toestemming nodig van de betrokkenen. De AVG stelt strengere eisen aan toestemming. Evalueer daarom de manier waarop u toestemming vraagt, krijgt en registreert. Pas deze wijze indien nodig aan. Nieuw is dat u moet kunnen aantonen dat u geldige toestemming van mensen heeft gekregen om hun persoonsgegevens te verwerken. En dat het voor mensen net zo makkelijk moet zijn om hun toestemming in te trekken als om die te geven.

Phase 2: Questionnaire 1 (5 minutes)
Next, please answer question A and B for every subject in the table below:

A) Is your company compliant with the GDPR requirements surrounding this subject?
B) How confident are you about this?

Question A | Question B

Subject	**Yes**	**Don't know**	**No**		**On a scale of 1-5, how confident are you about this?** 1 is completely unconfident, 5 is fully confident
Rights of Data Subjects (Rechten van betrokkenen)					
The register of processing activities (Register van verwerkingsactiviteiten)					
Data Protection Impact Assessments					
Data Protection by Design and by Default					
The Data Protection Officer (Functionaris Gegevensbescherming)					
Processing Agreements (Verwerkersovereenkomst)					
Consent (Toestemming)					

Fig. 30. Experiment form, fifth page

ICT Institute

Phase 3: Using the tool (50 min)
During this phase, you will use the tool as presented to you. The tool will be opened on the starting page, and you have 50 minutes to complete every step. When you get stuck, please let me know. I will not answer any questions about the content of the tool, but will help you in case you get stuck. I will be making observations during your use of the tool.

Phase 4: The results (10 min)
Please take a look at the results you are presented with, and read through them.

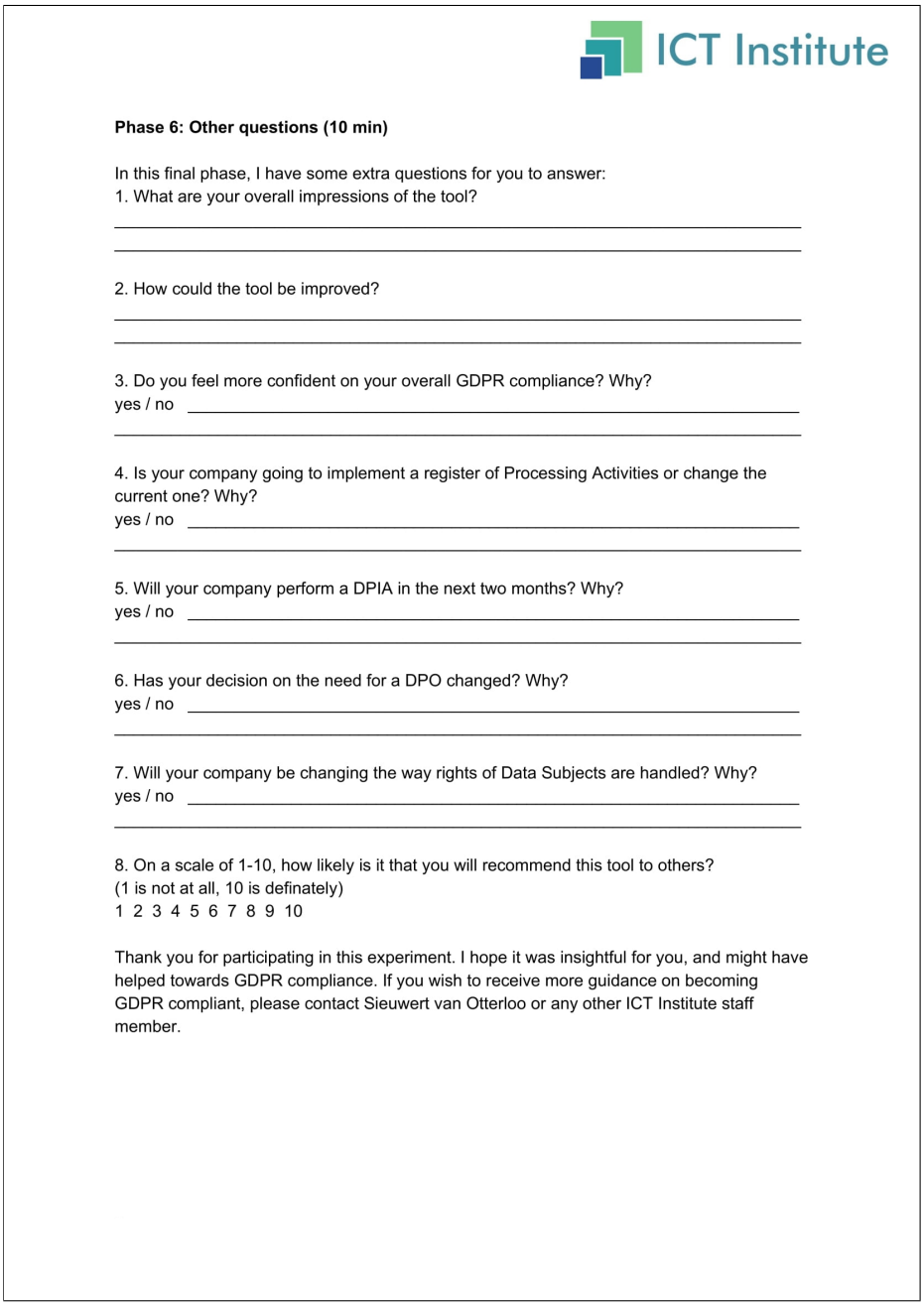
VERSION B: Please skip steps 1, 7, and 9.

Phase 5: Questionnaire 2 (5 minutes)
Now that you have used the tool, please answer question A and B below for every subject in the table below.

A) Is your company compliant with the GDPR requirements surrounding this subject?
B) How confident are you about this?

	Question A				Question B
Subject	**Yes**	**Don't know**	**No**		**On a scale of 1-5, how confident are you about this?** 1 is completely unconfident, 5 is fully confident
Rights of Data Subjects (Rechten van betrokkenen)					
The register of processing activities (Register van verwerkingsactiviteiten)					
Data Protection Impact Assessments					
Data Protection by Design and by Default					
The Data Protection Officer (Functionaris Gegevensbescherming)					
Processing Agreements (Verwerkersovereenkomst)					
Consent (Toestemming)					

Fig. 31. Experiment form, sixth page


ICT Institute

Phase 6: Other questions (10 min)

In this final phase, I have some extra questions for you to answer:
1. What are your overall impressions of the tool?

2. How could the tool be improved?

3. Do you feel more confident on your overall GDPR compliance? Why?
yes / no

4. Is your company going to implement a register of Processing Activities or change the current one? Why?
yes / no

5. Will your company perform a DPIA in the next two months? Why?
yes / no

6. Has your decision on the need for a DPO changed? Why?
yes / no

7. Will your company be changing the way rights of Data Subjects are handled? Why?
yes / no

8. On a scale of 1-10, how likely is it that you will recommend this tool to others?
(1 is not at all, 10 is definately)
1 2 3 4 5 6 7 8 9 10

Thank you for participating in this experiment. I hope it was insightful for you, and might have helped towards GDPR compliance. If you wish to receive more guidance on becoming GDPR compliant, please contact Sieuwert van Otterloo or any other ICT Institute staff member.

Fig. 32. Experiment form, final page

Resume Joost Krapels

About:

Name:	Joost Krapels MSc.
Occupation:	Consultant / privacy expert
Expertise:	ICT, privacy
Interests:	ICT, privacy, NLP, AI
Phone:	06 – 406 11 206
Website:	www.softwarezaken.nl - www.ictinstitute.nl
Email:	joost.krapels@ictinstitute.nl

Education:

- 2017 – 2018 Master Information Sciences (Business Information Systems track), VU Amsterdam
- 2016 – 2016 Minor with courses Cognition, Emotion, and Language & Norwegian Language, Universitet i Oslo
- 2014 – 2017 Bachelor Lifestyle Informatics (Artificial Intelligence), VU Amsterdam

Working experience:

Consultant / privacy expert at ICT Institute
September 2018 - now

Intern Master thesis at ICT Institute
February 2018 – July 2018
MSc. Thesis where I developed a rule-based system to check on high-level GDPR compliance.

Joost Krapels ICT Projecten
July 2017 – September 2018
Software development, websites, ICT related advice.

Teaching Assistant at Vrije Universiteit Amsterdam / VU
April 2016 - June 2016
Responsibilities: teaching students how to create an Android app using Appinventor.

Certificates:

Erasmus+ English language assessment CEFR level C2

For more information on our past projects and available expertise, see:

- https://ictinstitute.nl/about-us
- https://ictinstitute.nl/list-of-projects
- https://ictinstitute.nl/services
- https://ictinstitute.nl/workshops-and-trainings

About ICT Institute

ICT Institute (ICTI BV) is an IT advisory firm with expertise in agile, security, privacy, and software quality. We have a team of experts that work together in small teams. To keep our knowledge up to date, we hire talented people, work together with freelancers, share knowledge in talks and lectures, have an English and Dutch blog and learn from our projects.

All members of our team have extensive IT knowledge and are specialized in different areas. Our consultants with the most privacy knowledge are dr. Sieuwert van Otterloo and Joost Krapels MSc. More information about them and their experience can be found on our website www.ictinstitute.nl and Dutch website www.softwarezaken.nl.

Printed October 2018