UNIVERSITY OF TARTU

Institute of Computer Science

Computer Science Curriculum

Steven Leego

An approach for evaluating organizational data processing activities for GDPR compliance

Bachelor's Thesis (9 EAP)

Supervisor: Jake Tom

Tartu

2018

Organisatsiooniliste andmetöötlustoimingute hindamise lähenemine GDPR vastavuse saavutamiseks

Lühikokkuvõte:

Selle lõputöö eesmärk oli leida lähenemine, mille abil hinnata GDPR vastavust ning seda lähenemist reaalse ettevõtte peal proovida. Teoreetilises osas analüüsiti GDPR-i põhilisi väljakutseid ning mõningaid juhiseid, mille põhjal kavandati sobilik lähenemine. Lähenemist prooviti väikese B2B mudeliga ettevõtte peal, mille käigus kaardistati isikuandmete töötlusega seotud äriprotsessid ja koostati register töötlemistoimingutest. Ettevõttele pakuti välja ka edasised sammud saavutamaks täielikku GDPR vastavust.

Võtmesõnad: GDPR, äriprotsesside kaardistamine, vastavusanalüüs, ärianalüüs

CERCS: P170 Arvutiteadus, arvutusmeetodid, süsteemid, juhtimine (automaatjuhtimisteooria)

An approach for evaluating organizational data processing activities for GDPR compliance

Abstract:

The goal of the thesis was to find an approach to assess GDPR compliance and test the approach on an actual company. In the theoretical part, GDPR's main challenges and several guidelines were analysed, and a suitable approach was devised. The approach was tested on a small business-to-business company, during which business processes related to personal data were mapped and a registry containing data processing activities was created. The company was also given recommendations in achieving full compliance.

Keywords: GDPR, business process mapping, compliance analysis, business analysis

CERCS: P170 Computer science, numerical analysis, systems, control

Table of contents:

1. Introduction

After four years of preparation and debate the General Data Protection Regulation (EU) 2016/679 (henceforth GDPR) [1] was finally approved by the EU Parliament on 14 April 2016. The regulation will be enforced on 25 May 2018.

GDPR replaces the Data Protection Directive 95/46/EC [2] and was designed to harmonize data privacy laws across Europe, to improve data privacy of all EU citizens, give them more control over their data and to reshape the way organizations across the region approach data privacy [3].

GDPR applies to companies that control or process personal data. In essence, it applies to almost every company, although severity and requirements vary upon the nature of personal data processed and the size of the company. The authority tasked with information privacy which includes enforcing GDPR is called a Data Protection Authority (DPA). Under the GDPR, a DPA will receive a wide range of tools of enforcement. These include issuing warnings and reprimands; imposing a temporary or permanent ban on data processing; ordering the rectification, restriction or erasure of data; and suspending data transfers to third countries [4]. In Estonia the DPA is the Estonian Data Protection Inspectorate [5].

To avoid penalties, companies all over Europe were looking for ways to ensure that they are compliant with the new regulation. At the time of writing, a standardized approach had not been released and different parties had different opinions on how to tackle the problem. The goal of the thesis is to assess GDPR compliance and test the selected approach on an actual company.

Main research question: **How to assess GDPR compliance on a company?**

1. What are the current approaches available to assessing GDPR compliance?
2. From the approaches what is the suitable approach for this company?
3. What actions need to be taken to ensure GDPR compliance within the thesis scope?

While a complete evaluation of GDPR compliance lies beyond the scope of this thesis, according to several sources [6] [7] [8] [9] [10], one of the key activities for assessing GDPR compliance is mapping the data processing activities and fitting them into a registry that is by itself a requirement under GDPR article 30 [1]. Therefore, the goal of this thesis is to develop an approach for evaluating data processing activities and creating this registry.

The general approach consists of identifying and mapping processes of a company that are related to data processing activities. Relevant processes are identified through an interview with the CEO and the details are specified through interviews with department leaders. The processes and data flow are modelled using Business Process Modelling Notation (BPMN) [11]. For structuring the data identified from data processing activities, a registry is created, which is an adaptation of one provided by U.K.'s data protection authority, the Information Commissioner's Office [12]. The registry is also used to identify deficiencies in processing activities and further assessment needs. Based on the deficiencies and traits of Leego Hansson, recommendations are provided and validated.

The company chosen for assessment is Leego Hansson OÜ, whose core services are IT management and consultancy. Leego Hansson is a small business-to-business company that has less than 10 employees and does not meet the criteria of needing to fulfil many of the GDPR requirements. In the context of GDPR, Leego Hansson is the controller of the personal data of its employees and business client representatives. The author is also employed at Leego Hansson and found that the company is suitable for small-scale testing of the approach.

2. Background

This chapter gives background information about GDPR in general. Section 2.1 describes key definitions in the context of GDPR. Section 2.2 discusses key changes that GDPR bring along. Section 2.3 gives an overview of documentation requirements that GDPR article 30 states.

2.1. Key definitions of GDPR

The following definitions are crucial in the context of GDPR:

1. Controller – the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data. [1] (Art.4(7))
2. Processor – the natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller. [1] (Art.4(8))
3. Personal data – any information relating to an identified or identifiable natural person; an identifiable person is one who can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person. [1] (Rec.26; Art.4(1))
4. Special categories of personal data – personal data, revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership; data concerning health or sex life and sexual orientation; genetic data or biometric data. [1] (Rec.10, 34, 35, 51; Art.9(1))
5. Data relating to criminal offences and convictions is not considered personal data, although it may only be processed by national authorities. [1](Art.10)
6. Anonymous data – the GDPR does not apply to data that are rendered anonymous in such a way that individuals cannot be identified from the data. [1](Rec.26)
7. Processing – any operation or set of operations performed upon personal data or 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. [1](Art.4(2))

8. The consent of the data subject – any freely given, specific, informed and unambiguous indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed. [1] (Rec.32; Art.4(11))
9. 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. [1](Art.4(12))
10. Data concerning health – personal data relating to the physical or mental health of an individual, including the provision of health care services, which reveal information about his or her health status. It expressly covers both physical and mental health. [1](Rec. 35, 53-54; Art.4(15))

2.2. Key principles of GDPR

Some of the key changes that GDPR brings along, according to an article by D. Gabel and T. Hickman [13] are the following:

1. Territorial application – GDPR applies to non-EU organisations that conduct business in EU.
2. Consent – acquiring and maintaining consent becomes harder for organisations.
3. Rights of data subjects – data subjects gain new rights by the GDPR (e.g. right to data portability, right to be forgotten). It also complicates lawful processing of data for companies.
4. 72-hour data breach notification – businesses will be required to report any data breach to the DPA within 72 hours of detection.
5. Increased compliance obligations for controllers – data controllers will have to follow several new rules. For example, they are required to implement appropriate policies, keep records of data processing, ensure privacy by design
6. Direct compliance obligations for processors – data processors are now introduced to compliance obligations as well.
7. Appointing a DPO - organisations that regularly and systematically monitor data subjects, or process special categories of personal data on a large scale, must appoint a Data Protection Officer (DPO)

8. Cross-Border Data Transfers – the GDPR increases consistency of intra-organizational transfer of personal data across borders through Binding Corporate Rules (BCR). It also recognises a number of other data transfer mechanisms.
9. The One-Stop-Shop – organisations, that span across multiple countries can now have a "lead DPA", which means they can avoid having to deal with multiple DPA-s regarding regulatory issues.
10. Increased harmonisation – under the GDPR, compliance requirements across EU will be more consistent. National variations in some areas, will however persist.
11. Remedies and sanctions – consequences of breaching data protection law under GDPR will be dramatically higher. The maximum fine for a single breach can be up to the greatest of €20 million, or four percent of annual worldwide turnover, whichever is higher.

2.3. Article 30 documentation requirements for controllers

Article 30 of GDPR [1] states that controllers must document the following:

1. Organisation's name and contact details;
2. If applicable, the name and contact details of the data protection officer, the controller's representative and the joint controller;
3. The purposes of the processing;
4. Categories of data subjects and of personal data;
5. Categories of recipients of personal data;
6. If applicable, the name of any third countries or international organisations where the personal data is transferred to;
7. If applicable, the safeguards in place for any exceptional transfers of personal data to any third countries or international organisations;
8. If possible, the retention schedules for different categories of personal data;
9. If possible, a general description of technical and organisational security measures.

The article also states that the records must be kept in writing, including in electronic form.

3. Choosing the approach

The chapter's purpose is to examine main GDPR challenges and different approaches that have been proposed for achieving GDPR compliance and formulate a suitable approach for the thesis. Section 3.1 partially answers the main research question. Section 3.2 fully answers research question 1. Section 3.3 fully answers research question 2 and partially research question 3.

3.1. GDPR main challenges

Achieving compliance with GDPR is not an easy process. The complexity and steps taken vary upon several different factors – the amount of personal data processed, number of employees and the intent of processing. For example, a data protection impact assessment (DPIA) must be conducted in cases where personal data is automatically processed, large amounts of special categories of data is processed or a publicly accessible area is systematically monitored on large scale [1](Art.35(3)).

Under the GDPR each personal data processing activity must have a lawful basis – consent, contract, legal obligation, vital interests, public task, legitimate interest [1](Art.6(1)). Furthermore, processing activities must be compliant with new rights to individuals – the right to be informed [1](Art.13,14,19), the right of access [1](Art.15), the right of rectification [1](Art.16), the right to erasure [1](Art.17), the right to restrict processing [1](Art.18), the right to data portability [1](Art.20), the right to object [1](Art.21), and rights in relation to automated decision making and profiling [1](Art.22).

GDPR states that the data controller shall be responsible for following the principles and requires it to be able to demonstrate compliance [1](Art.5). To demonstrate compliance, a company must implement relevant technical and organisational measures, have processing activities documented, ensure data protection by design and by default and carry out DPIA-s where necessary. [7]

The regulation's [1] article 30 requires almost all personal data controllers to keep structured records of data processing activities.

3.2. Existing approaches for evaluation

A news outlet, CSO, who provides news, analysis and research on security and risk management, [14] has brought out the following steps for achieving GDPR compliance [9]:

1. Thoroughly understand what are the obligations that GDPR sets upon organisations;
2. Perform a data discovery and document all the findings;
3. Assess how data is classified and how it is processed;

4. Assess the critical risks to data, review policies and procedures. Apply security measures where needed.
5. Investigate any other risks and repeat the fourth step until all the risks have been handled.

Metacompliance, a company, that has been developing software and content for cyber security and compliance market since 2005, [15] has created a GDPR best practices implementation guide [8]. In the guide they have divided achieving GDPR compliance into three main phases:

1. Prepare – main goal is to ensure that the organisation is ready for GDPR and key stakeholders are involved in the process
2. Operate – main goal is to implement procedures that GDPR requires and bring existing processes to compliance
3. Maintain – main goal is to demonstrate and sustain ongoing compliance with the GDPR

Estonia's data protection authority (AKI) has advised companies to act in 3 key points:

1. Seek competent help – AKI recommends seeking competent help in achieving compliance even if one's company is not required to assign a DPO;
2. Do a full data processing audit – AKI recommends evaluating every aspect of business where data processing takes place, e.g. information systems, documentation, work processes;
3. Assess data portability – AKI recommends putting emphasis on being compliant with article 20, which requires that personal data must be transmittable to another system in a structured, commonly used and machine-readable format. [6]

U.K.'s data protection authority (ICO) has created a detailed guidance on how to handle every aspect of GDPR. They have also combined their advice into 12 steps to take to prepare for the GDPR [10]:

1. Raise awareness in the organisation and get key stakeholders to support achieving compliance;
2. Document what kind of personal information is held;
3. Review privacy notices – GDPR brings along several new requirements that need to be implemented in privacy notices;
4. Verify that procedures are compliant with new rights to individuals under GDPR;
5. Establish a procedure for handling individuals' requests for their information;
6. Identify lawful basis for processing activities and document it;
7. Review procedure of acquiring and maintaining consent for personal data processing;

8. Assess whether it is necessary to verify individual's ages and to obtain parental or guardian consent for any data processing activity;
9. Ensure that procedures are in place to detect, report and investigate a data breach;
10. Ensure data protection by design and by default. Also carry out a DPIA where it is necessary;
11. Assign someone who is responsible for data protection compliance, even if a DPO is not required for the organisation;
12. Determine a lead data protection authority in case the organisation is international.

3.3. Choosing the approach

The common denominator among different approaches and a good starting point in assessing compliance is mapping and documenting data processing activities. Creating a registry of data processing activities is by itself a requirement under the GDPR article 30 [1] and it applies to all companies where personal data processing is not occasional. As most of the companies process at least their employee data, they must create and maintain said registry.

Creating the registry also allows to further assess compliance of several other requirements under the GDPR as many of them are related to specific data processing activities, e.g. lawful basis for processing, DPIA necessity. The registry can furthermore be used as a central repository of links to relevant documentation. MetaCompliance has said in their guide that "the registry becomes the company's centralised 'single source of truth'" [8].

ICO has created an Excel template for said registry [12]. ICO structured the Excel in a way that it contains all the information required by article 30. Each of the rows contain granularly types of personal data that are grouped by categories of individuals and the purpose of processing. ICO chose to use this representation to add numerous other columns to the Excel which map compliance to other aspects of GDPR or are otherwise useful, e.g. lawful basis for processing, location of personal data, links to relevant documentation. A month before GDPR enforcement, Estonia's data protection authority published their own template which seems to also be based on ICO's template, but only focuses on article 30.

The author chose the focus of the thesis as following - mapping the data processing activities of a company and tailoring the Excel registry to only contain relevant additional columns and then filling it with information.

3.4. Summary

In the first section the main challenges of GDPR, that require action were explored. The second section was used to analyse proposed guidelines by a news outlet, a cyber security company, the Estonian data protection authority and the U.K.'s data protection authority. In the third section the author explained the reasoning behind chosen approach.

4. Mapping data processing activities

This chapter's purpose is to devise and fulfil a specific approach on how to map data processing activities. This chapter partially answers sub research question 3.

4.1. Identifying processing activities

To identify potential processing activities an open-format interview with the company's CEO was conducted. The CEO was tasked with analysing day-to-day processes and from that he formulated a list of possible processes which include personal data processing. The list of potential business functions that use personal data was the following – payroll, personnel file, recruitment, sales, service providing.

The mentioned functions in Leego Hansson are the responsibility of the human relations (HR) representative, financial (FIN) representative and the sales manager. For the data processing activities regarding payroll, personnel file and recruitment - an interview with the HR and FIN representatives and for the sales and service providing processes, an interview with the sales manager was organized. An interview with the CEO was also held to validate the results from a general viewpoint.

4.2. Preparing for interviews

To be better prepared for the interviews the author analysed different requirements for the data in the processing activity registry brought out in paragraph 2.3. From the analysis, several key topics were identified that need to be followed through during the interview. The topics were the following:

1. Personal data – what kind of personal data is used in the process;
2. Data purpose – why is the data processed;
3. Data source – where does the data originate from;
4. Data location – where is the data stored;
5. Data subjects – whose data is processed;
6. Data recipients – with whom is the data shared with;
7. Data security – how is the data kept secure;
8. Data retention – how long is the data kept.

4.3. Conducting interviews

Interviews were conducted with the sales manager, the human relations representative, the financial representative and the CEO. The interviews were audio-recorded, and the interviewer was taking notes while conducting the interview.

The approach chosen for the interviews was semi-structured – key topics were prepared beforehand although the interviewing was conducted with open-ended questions. According to Zorn [16] semi-structured interviews are the most useful format when doing qualitative research, as it gives the interview a structure, but also allows delving deeper into unforeseen topics.

The interviews started with the interviewer explaining the goal of the interview, background of GDPR and the role of the interviewee. He also asked permission to record the meeting. During the core part of the interview, interviewer asked the interviewee to describe the process at hand. While the process was described, the interviewer ensured that all the predetermined topics were covered by asking clarifying questions. In the end of the meetings, the interviewer summarised what was covered, brought out what would be the next steps and thanked for their contribution.

4.4. Mapping processes using BPMN

The author chose to visualize data processing activities using BPMN [11] and the software Bizagi Modeler [17]. In author's opinion BPMN efficiently captures data processing activities in everyday processes and allows to emphasize personal data occurrence in them. BPMN also simplifies validation process with the client as it follows a real-life flow. The processes do not fully reflect the whole real-life process as the focus was only on the parts where personal data is handled.

The author identified, modelled and described the following processes:

1. The sales process starts with the sales manager identifying a lead, finding a contact person and recording contact information. The contact data is stored in Pipedrive. When a lead is solid, contact is made and the potential customer is met with. If the customer is interested in conducting business, the sales manager will create and negotiate a proposal. If the customer is satisfied with the proposal, the project is started.
2. The recruitment process starts with the potential candidate writing an application and a motivation letter and sending them to Leego Hansson via email. HR representative stores the documents in the file management system and creates an analysis document to compare different applicants. If a candidate is suitable, he/she is interviewed. Based on interviews the analysis document is complemented and a final candidate is chosen. Work terms are negotiated with the potential employee and once he/she is employed, the employee data is stored in different documents in the file management system and national registries are updated with employment information.

3. The salary payment process starts with the beginning of the month with the financial representative compiling and sending the salary and vacation data of all employees via email to the accounting firm. The accountant records the data and compiles declarations, which are then submitted into national registries. When the declarations are compiled, financial representative will pay salaries and send a payslip to all the employees.
4. The employee data update process begins when the employee presents new information to the HR. HR representative then records new information in appropriate registries on the file management system.
5. The time tracking process is an everyday process which is acted upon every time an employee starts or finishes an activity. The employee fills their work-related activities inside Toggl.
6. Compensation management process starts at the start of the month with employees collecting their checks and receipts and storing them in the file management system. FIN representative organizes documents and compiles the compensation data, which is sent via an email to the accountant. The accountant records the data and compiles declarations which are submitted to national registries. When the declarations are compiled, financial representative will pay the compensations.
7. The billing process takes places at the end of the month. The consultant creates time reports and FIN representative creates a bill and sends the documents to the client. The process repeats until the project is finished.

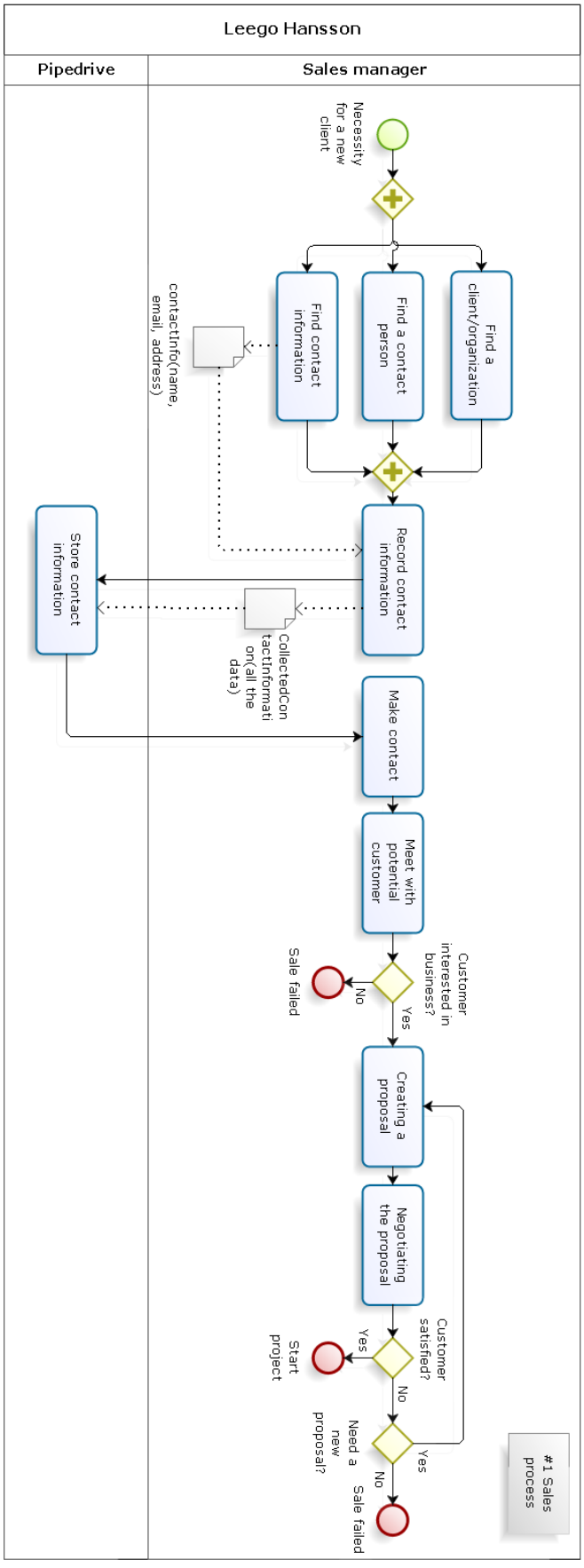

Fig 1: Sales process

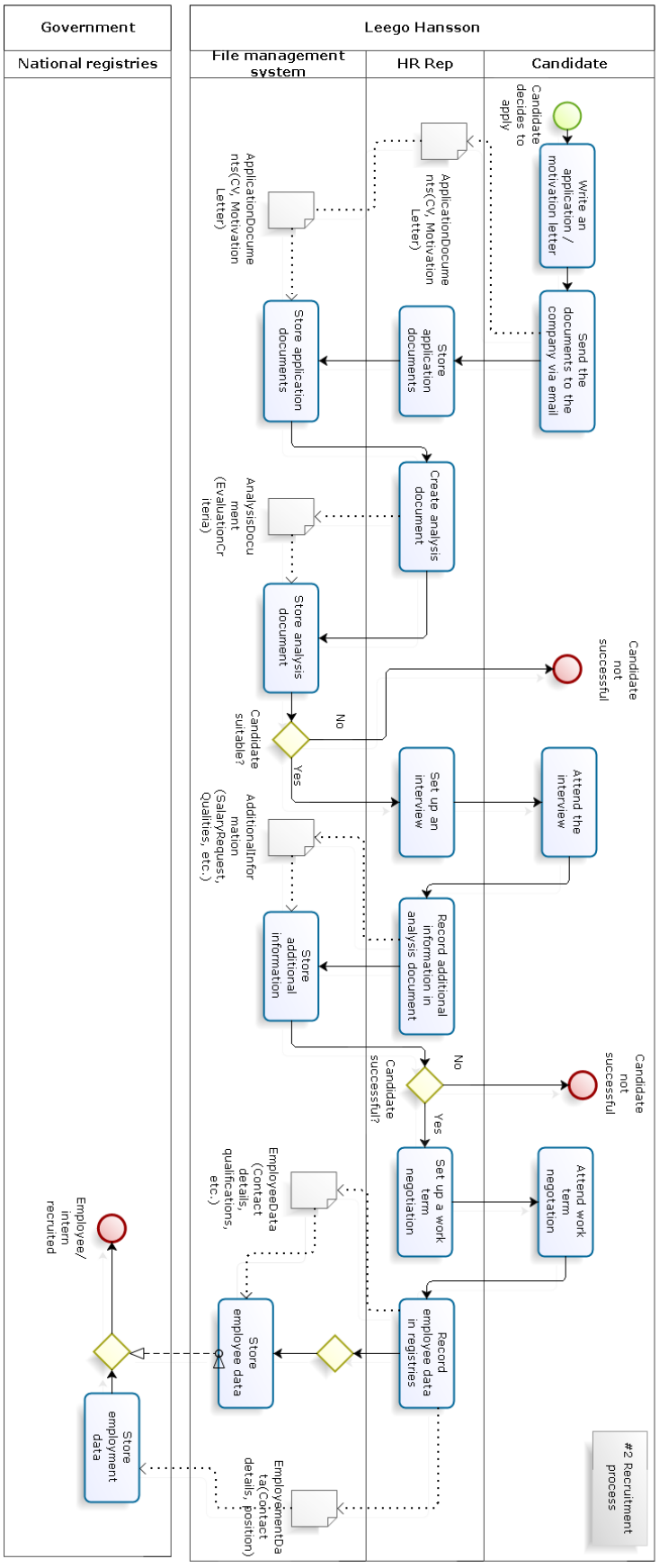

Fig 2: Recruitment process

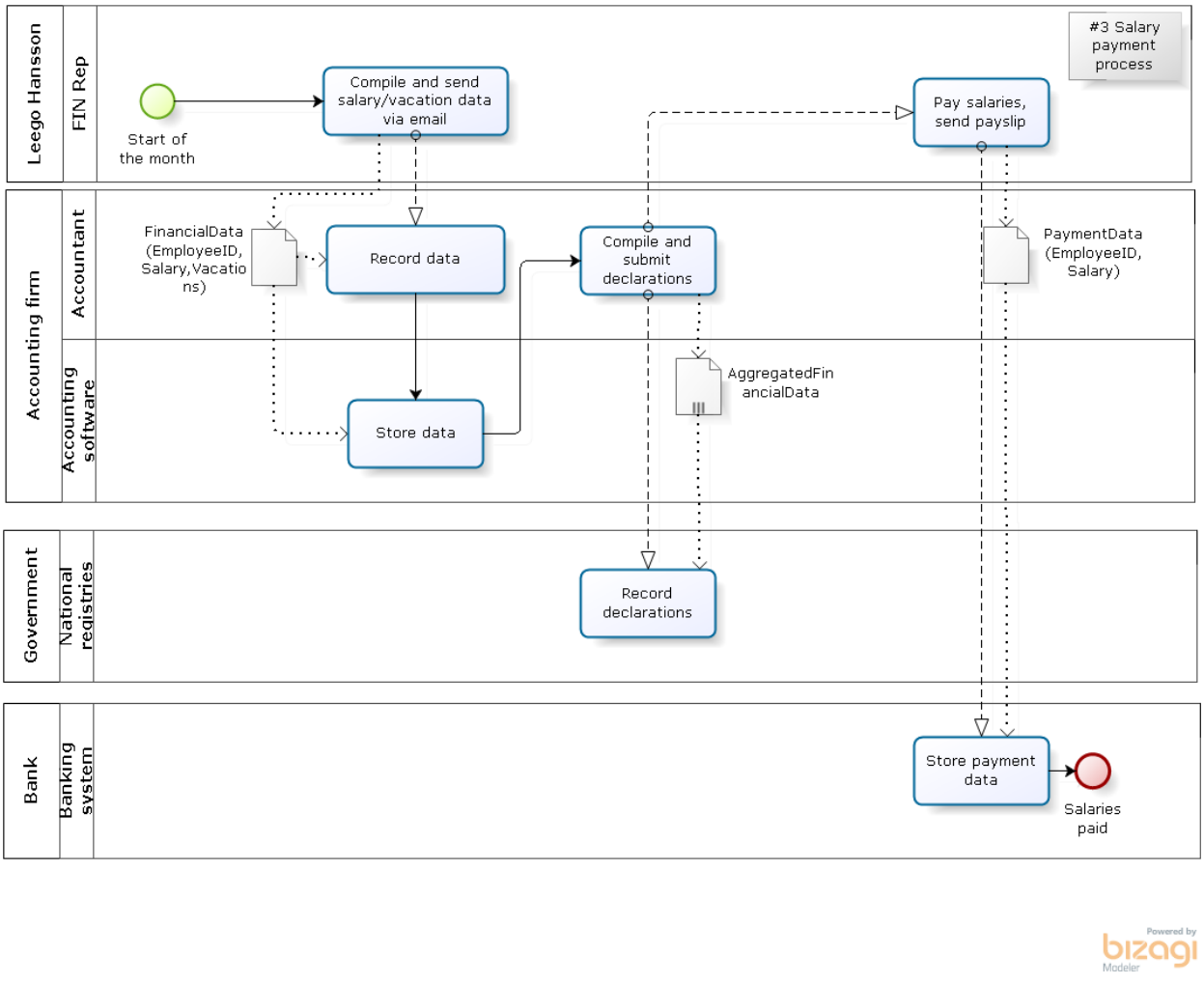

Fig 3: Salary payment process

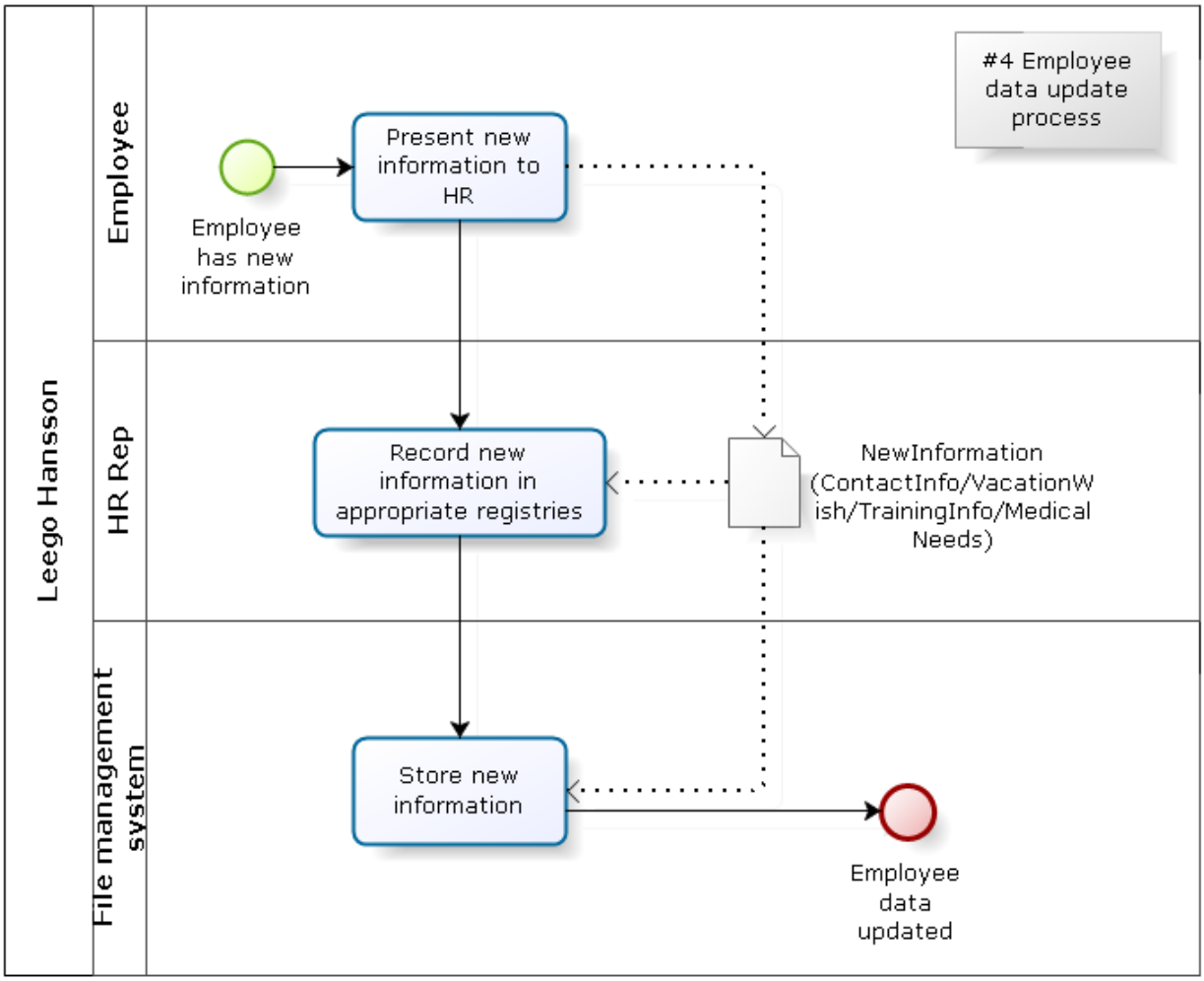

Fig 4: Employee data update process

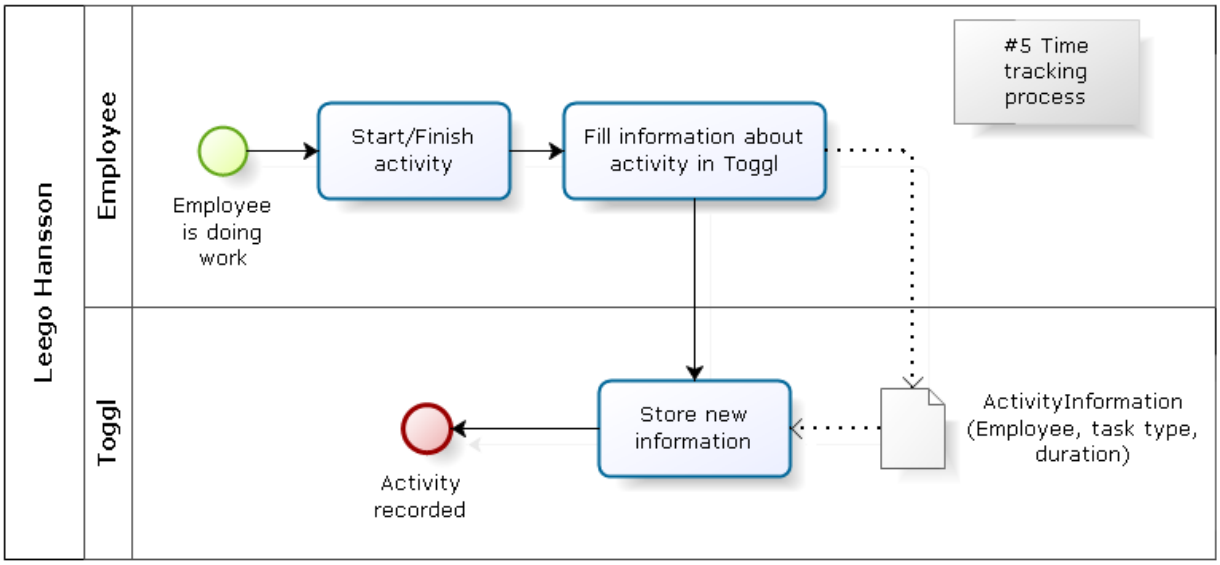

Fig 5: Time tracking process

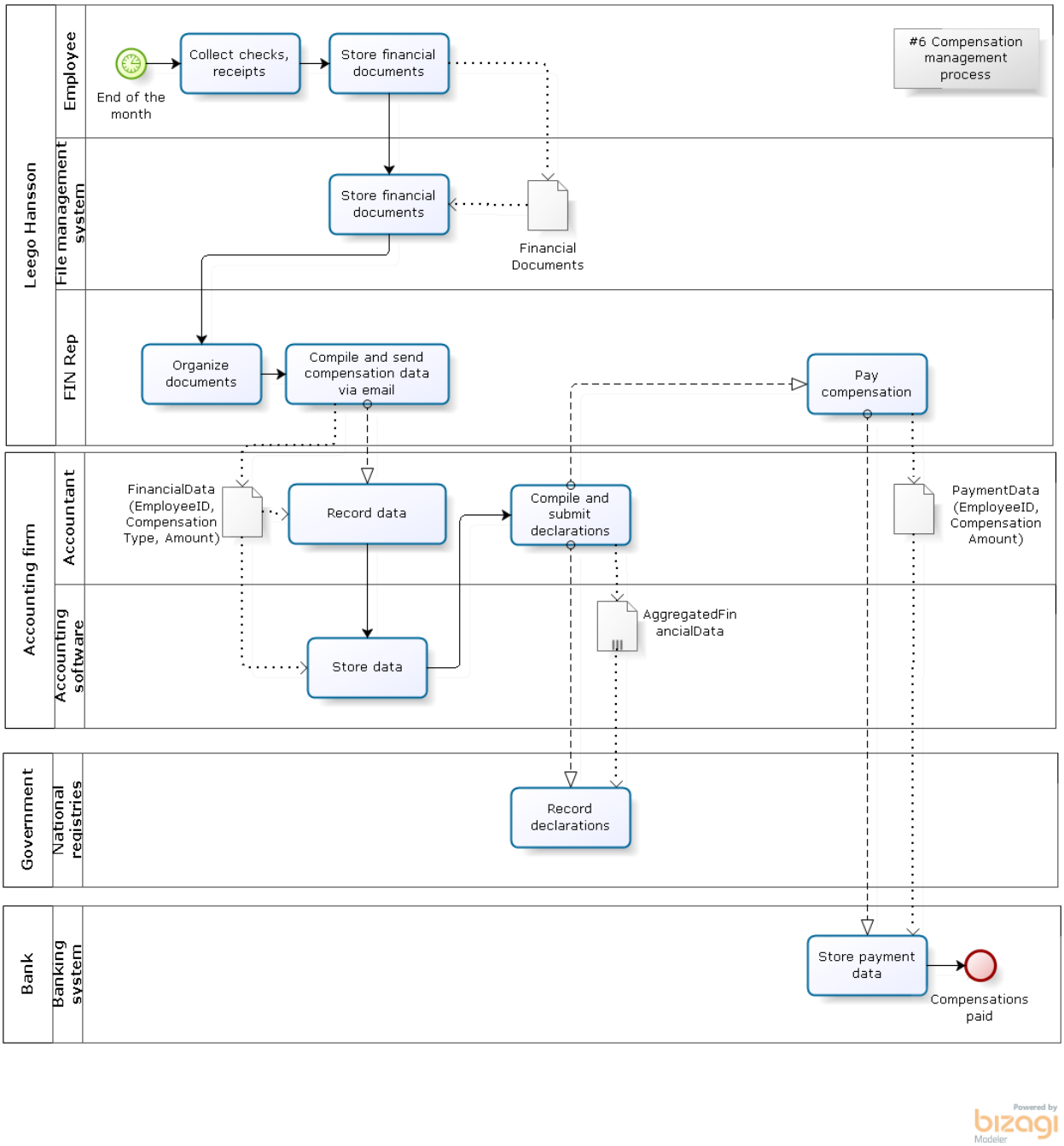

Fig 6: Compensation management process

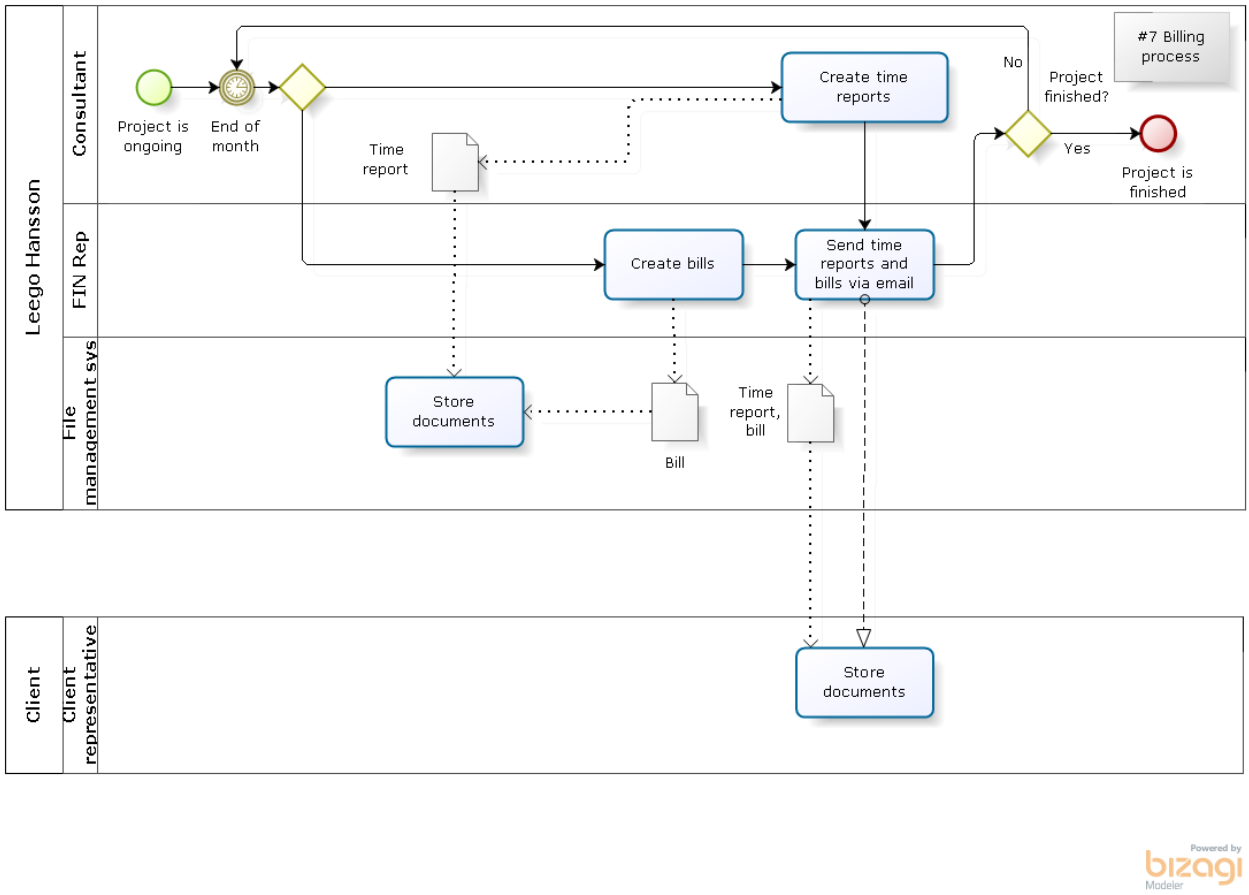

Fig 7: Billing process

4.5. Summary

In the first section a general identification of potential personal data processing activities is done with the help of the CEO of Leego Hansson. In the second section general discussion topics were derived to efficiently prepare for the interviews. The third section describes how the interviews were conducted. The fourth section discusses the reasoning behind choosing BPMN for process modelling and describes the mapped processes.

5. Compliance analysis

This chapter's purpose is to structure acquired knowledge about data processing in an Excel registry format and derive deficiencies and improvement suggestions. This chapter fully answers sub research question 3 and the main research question.

5.1. Tailoring the registry

The template for the registry published by U.K.'s data protection authority, Information Commissioner's Office [12] is not suitable for Leego Hansson in its original form. The template has a variety of data fields also included in the same template in addition to the original GDPR article 30 requirements. This gives a full overview of any aspects regarding types of personal data although it makes the registry hard to follow and fill. Therefore, the author chose to tailor the registry to minimise the number of columns and only leave data fields that suit the characteristics of Leego Hansson. The following changes were made to the original template:

1. Removed business function field – as a small company, business is not divided into that many functions to justify grouping by it in the registry.
2. Removed the field of joint controller – in the foreseeable future, Leego Hansson will not have a joint controller of personal data.
3. Removed fields that are used to link to documentation – documentation in Leego Hansson is held in a well-structured manner and is easily findable, therefore keeping links in the registry is unnecessary.
4. Removed fields regarding transfer to third countries – in the foreseeable future, Leego Hansson will not be transferring data to third countries or international organisations.
5. Removed the field about processing special category data – the only foreseeable basis for processing special category of personal data in Leego Hansson is employment.
6. Removed fields about data protection impact assessments - in the foreseeable future, Leego Hansson will not be required to conduct one.
7. Removed fields about personal data breaches – the likelihood of personal data breaches is low; therefore, handling them elsewhere is more reasonable.
8. Removed fields about Data Protection Bill – these fields are specific to U.K. and therefore not relevant.

5.2. Filling the registry

The process of filling the registry started with taking a few examples from ICO's registry and analysing the level of detail in every data field. Once the level of detail was clarified, the author took the notes from interviews and started filling the registry row-by-row. As the interviews were conducted with the end goal in mind, most of the data required was structured and easy to fill in the table. In several cases, the data acquired in the interviews was too detailed and to fit the general format, some generalization had to be done – e.g. for each employee, the name, ID number, contact address, contact telephone is collected and the category of personal data can be generalized as contact details.

The more complicated field to fill were the lawful basis for processing personal data and the rights available to individuals. For the lawful basis, the author analysed the examples given by ICO and assessed whether similar categories of personal data would have the same lawful basis in the context of Leego Hansson. The author tried to find a legal basis other than consent for each data category, as getting and maintaining consent is not easy and reasonable for Leego Hansson. In several cases the basis should be a legal obligation [1] (Article 6(1)(c)) or covered by contract [1] (Article 6(1)(b)) and in other cases the author chose legitimate interest [1] (Article 6(1)(f)) as basis. ICO has recommended using legitimate interest as a basis if the following criteria are met:

1. The processing is not required by law but is beneficial to the processor;
2. The privacy impact to the individual is limited;
3. The subject should reasonably expect their data to be used that way;
4. The processor does not wish or cannot ask for consent. [18]

The author found that the legitimate interest basis applies to direct marketing and recruitment, but also collecting lifestyle information about employees. To assess the rights available to individuals the author considered the format and systems the data is stored in, purpose of the data and where applicable, legal obligations.

Once the Excel registry was filled, the author compared all the mapped process and the registry to verify that all categories of personal data was present in the both formats and to ensure that any data was not conflicting.

5.3. Recommendations to achieve compliance

In general, Leego Hansson is processing personal data purposefully, legitimately and securely. Every data processing activity has a reasoned intent and seemingly a lawful basis, which must be verified with a lawyer. Any external systems where Leego Hansson holds personal data have assured they are keeping the data accordingly with GDPR [19] [20]. Leego Hansson's own file management system has ensured privacy and security by design through implementing rigorous access controls. The author could not detect any major discrepancies with GDPR's requirements. Leego Hansson's personal data processing activities are small-scale, infrequent and do not pose a high risk to individual's rights and freedoms. The main risk the author identified is not being able to be compliant with individual's rights (access, erasure, portability, rectification, objection) in situations where personal data is exchanged via email, as identifying data location is complicated.

Considering different guidelines and specifics of Leego Hansson, the author arrived at the following recommendations to achieve GDPR compliance:

1. Validate with a lawyer, whether proposed lawful bases are accurate and valid; and if necessary act, e.g. renew contracts. Current lawful bases were not assessed by a person with legal expertise.
2. Verify whether proposed rights available to individuals are fulfilled and the individual's request procedure is working by testing with a real-life case. Currently proposed rights are hypothetical, and their validity is not tested on real systems.
3. Establish a procedure to detect, report and investigate a data breach. A personal data controller must document any data breach and all the aspects of it. In certain cases, the DPA and subjects affected must also be notified.
4. Compose appropriate privacy notices in situations where the lawful basis for processing data is legitimate interest. In the case of employee lifestyle information, the privacy notice could be stored inside the internal knowledge management system. When recruiting, the privacy notice could be linked in the job offer. The data collected for sales process could be described on the home page.
5. Assign a person that will be responsible for data security and maintaining the personal data processing registry. Although Leego Hansson is not required to assign a data protection officer, specific responsibility assures the matter is not left unattended.

6. Review processes where data is exchanged via email, as complying with individual's rights is complicated. Currently finding all the information about a specific person from numerous mail folders is unachievable in a reasonable manner. Certain automated tools could be used to quickly identify data locations.
7. Educate employees about the principles of proper personal data management. Every employee has some access to personal data and without proper knowledge about the requirements, data is prone to inadvertent mismanagement and breaches.

5.4. Validation with the company

To validate the work with the company, a meeting with the department leaders was organized. The thesis document and the registry were sent to be familiarized with beforehand. The meeting had the following goals:

1. Explain the approach chosen;
2. Verify the correctness of the process models;
3. Explain the different requirements under GDPR;
4. Explain the workings of the personal data registry;
5. Verify the correctness of the personal data registry;
6. Explain the recommendations for achieving compliance;
7. Verify that the thesis does not contain any business secrets and could be publicly published.

The validation meeting started with introducing the goals of the meeting and giving a general summary of thesis results. The approach was introduced in detail and no further questions were asked. To validate the correctness of the process models, the author split the screen and showed process descriptions and models in parallel. While the processes were described, some minor wording and visual improvements were proposed; text was altered instantly and visual changes were implemented later e.g. changing HR representative into FIN representative or adding a missing process step on the model.

Once the processes were validated, the author described the main requirements that GDPR brings along and how they relate to the table. As the next step, the logic of the table was described through discussing general structure and then looking through every column. To validate the correctness of the table, each row was thoroughly passed and discussed; some minor changes were implemented in the process, e.g. adding a missing data location, rephrasing legitimate interest.

To summarise, current status of compliance with GDPR and further steps of action were explained. The company representatives were satisfied with the results and believed in the validity. They thought the recommendations were good and expressed interest in implementing them – the representatives agreed that lawful basis should be validated by a lawyer and promised to assign a person responsible for dealing with other topics. Company board got the assurance that the thesis is general enough and does not give away any competitive edge; therefore, they agreed to the public publishing of the thesis.

5.5. Summary

The first section describes the reasoning and process of tailoring the ICO's template to be suitable for Leego Hansson. The second section describes the process of filling the registry with information acquired from interviews and process mapping. In the third section a general assessment of current GDPR compliance is expressed and specific guidelines for achieving compliance are given. In the fourth section the goals and the process of the validation process are discussed.

6. Concluding remarks

The goal of the thesis was to find an approach to assess GDPR compliance and test the approach on an actual company. The task was divided into 3 sub-research questions and all were fulfilled.

The first goal was to get an understanding of GDPR and explore different approaches in achieving compliance with the regulation. The author delved into the main challenges of GDPR and analysed proposed guidelines by a news outlet, a cyber security company, the Estonian data protection authority and the U.K.'s data protection authority.

The second research question was about finding an approach that would best suit Leego Hansson's characteristics and the scope of a bachelor's thesis. The author reached the conclusion, that mapping the processes and creating a personal data processing activity register would be a good starting place.

The third part of the work was about choosing specific methodologies to implementing the approach on the company. The author chose to use semi-structured interviews to acquire the information and BPMN to visualize the processes. A template, provided by U.K.'s DPA, was tailored to be used to create a data processing activity registry.

The author also identified further actions necessary to achieve full compliance with the GDPR that did not fit inside the scope of the thesis. The author considered the traits of Leego Hansson and guidelines and general knowledge that was acquired during the first research question. Several recommendations in achieving GDPR compliance were proposed.

The results were validated with the company to ensure data correctness, representatives' understanding of the matter and get an approval for public publishing of thesis.

References

1. **European Union Parliament.** Final version of the GDPR, released 6 April 2016. [Online] [Cited: 11 05 2018.] http://data.consilium.europa.eu/doc/document/ST-5419-2016-INIT/en/pdf.

2. **European Parliament.** Data Protection Directive 95/46/EC. [Online] [Cited: 11 05 2018.] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=et.

3. **Trunomi.** Home page of EU GDPR. [Online] [Cited: 11 05 2018.] https://www.eugdpr.org/.

4. **IT Governance.** GDPR enforcement and penalties. [Online] [Cited: 11 05 2018.] https://www.itgovernance.co.uk/dpa-and-gdpr-penalties.

5. **European Commission.** Data Protection Authorities. [Online] [Cited: 11 05 2018.] http://ec.europa.eu/justice/article-29/structure/data-protection-authorities/index_en.htm.

6. **Peep, Viljar.** Andmekaitse Inspektsiooni peadirektori ÜLEVAADE ELi andmekaitsereformi rakendamise seisust Eestis. [Online] 14 10 2016. [Cited: 11 05 2018.] http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/ylevaade_reformist_14102016.pdf.

7. **Information Commissioner's Office.** Guide to the general data protection regulation. [Online] [Cited: 11 05 2018.] https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/.

8. **MetaCompliance.** GDPR Best Practices Implementation Guide. [Online] [Cited: 11 05 2018.] https://www.infosecurityeurope.com/__novadocuments/355669?v=636289786574700000.

9. **MarTech Today.** MarTech Today's Guide to GDPR — The General Data Protection Regulation. [Online] [Cited: 11 05 2018.] https://martechtoday.com/guide/gdpr-the-general-data-protection-regulation.

10. **Information Commissioner's Office.** Preparing for the General (GDPR) 12 steps to take now. [Online] [Cited: 11 05 2018.] https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf.

11. **Object Management Group.** Business Process Model And Notation. Standard Document. [Online] [Cited: 11 05 2018.] http://www.omg.org/spec/BPMN/.

12. **Information Commissioner's Office.** How do we document our processing activities? *Guide to the General Data Protection Regulation (GDPR).* [Online] [Cited: 11 05 2018.] https://ico.org.uk/media/for-organisations/documents/2172937/gdpr-documentation-controller-template.xlsx.

13. **Dr. Detlev Gabel, Tim Hickman.** Chapter 5: Key definitions – Unlocking the EU General Data Protection Regulation. [Online] [Cited: 11 05 2018.] https://www.whitecase.com/publications/article/chapter-5-key-definitions-unlocking-eu-general-data-protection-regulation.

14. **CSO.** About CSO. [Online] [Cited: 11 05 2018.] https://www.csoonline.com/about/about.html.

15. **Metacompliance.** About Metacompliance. [Online] [Cited: 11 05 2018.] https://www.metacompliance.com/company/about/.

16. **Zorn, Ted.** Designing and Conducting Semi-Structured Interviews for Research. [Online] [Cited: 11 05 2018.] http://home.utah.edu/~u0326119/Comm4170-01/resources/Interviewguidelines.pdf.

17. **Bizagi.** Bizagi Modeler Business Process Modeling Software (BPM). [Online] [Cited: 11 05 2018.] https://www.bizagi.com/en/products/bpm-suite/modeler.

18. **Information Commissioner's Office.** When can we rely on legitimate interests? *Guide to the General Data Protection Regulation (GDPR).* [Online] [Cited: 11 05 2018.] https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/when-can-we-rely-on-legitimate-interests/.

19. **Pipedrive.** Privacy Policy. *Pipedrive web site.* [Online] [Cited: 11 05 2018.] https://www.pipedrive.com/en/privacy.

20. **Toggl.** Privacy Policy. *Toggl web site.* [Online] [Cited: 11 05 2018.] https://toggl.com/legal/privacy/.

Appendix

I Personal data processing registry

II Licence

Non-exclusive licence to reproduce thesis and make thesis public

I, **Steven Leego**

1. herewith grant the University of Tartu a free permit (non-exclusive licence) to:

1.1. reproduce, for the purpose of preservation and making available to the public, including for addition to the DSpace digital archives until expiry of the term of validity of the copyright, and

1.2. make available to the public via the web environment of the University of Tartu, including via the DSpace digital archives until expiry of the term of validity of the copyright,

An approach for evaluating organizational data processing activities for GDPR compliance, supervised by **Jake Tom**,

2. I am aware of the fact that the author retains these rights.

3. I certify that granting the non-exclusive licence does not infringe the intellectual property rights or rights arising from the Personal Data Protection Act.

Tartu, 14.05.2018