TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technology
Department of Software Science

Mari Jääger 153111IVCM
ITC70LT

DEVELOPING RECORDS OF PROCESSING ACTIVITIES IN A SMALL ENTERPISE

Master's thesis

Supervisor: Priit Raspel,
MSc

Tallinn 2018

Author’s declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Mari Jääger

7.05.2018

Abstract

The General Data Protection Regulation (GDPR) is an European Union regulation on the protection on natural persons data. GDPR establishes the baseline of requirements to anyone processing personal data and levels the ground across member states. One of the requirements of GDPR is keeping a record of data processing activities by data categories describing processing purposes, transfer of personal data to another processor, retention period and security measures. In Estonia, such a record has not been a requirement for most organisations, but as interpreted by the local Data Protection Inspectorate, extends to virtually all personal data processors. The goal of this research is developing records of processing activities on the example of a small-sized Estonian enterprise.

GDPR sets the requirements for anyone processing data of natural persons to ensure transparency and sufficient protection while handling personal data. Data volumes processed have exploded over the past decades with the growing range of electronic data processing opportunities such as cloud-computing, and the decrease of data hosting costs. Like with any new industry technical solution, it may be accompanied by misuse in a manner that can damage people concerned. In the cyber realm data protection mechanisms and measures are developed on a daily basis compared to other conventional data processing methods, that have been available for decades and centuries. GDPR also addresses the topics connected to electronic data processing and user profiling based on extensive monitoring of individuals and network behaviour (cookies, IP addresses, device names, location coordinates), which has become so wide-spread in the cyber domain that, it can be regarded as intrusive and violation of privacy.

This research discusses different aspects in personal data processing and protection in order to develop a methodology to create records of processing activities, and use it to create records for the enterprise used as a case study. The methodology is analysed and created taking into account the following: GDPR generic requirements, existing and previous examples of records, efficiency of record-keeping, local law requirements to the

enterprise, and using the records for broader purposes than what is required by GDPR. The records of personal data processing developed as a result of the research describe the activities of personal data processing in the case study enterprise. This enables the enterprise to display compliancy to GDPR and to enable the enterprise to better organise applying relevant security measures to protect the processed data.

This thesis is written in English and is 95 pages long, including five chapters, five figures and seven tables.

Annotatsioon

Isikuandmete kaitse üldmäärus (GDPR) on Euroopa Liidu loodud õigusakt füüsiliste isikute andmete kaitseks. GDPR kirjeldab baasnõuded kõikidele isikuandmete töötlejale ja ühtlustab isikuandmete töötlemist kogu Euroopa Liidus. Üks GDPRi nõuetest on isikuandmete töötlemise registri loomine, milles kirjeldatakse andmekategooriate kaupa andmete töötlemise eesmärgid, edastamine teisele töötlejale, andmete säilitamise tähtajad ja andmete kaitseks rakendatud turvameetmed. Valdavale osale Eesti organisatsioonidest ei ole varem sellise registri loomine olnud kohustuslik. Andmekaitseinspektsiooni hinnangul laieneb nüüd töödeldavate isikuandmete registri loomise kohustus enamikule isikuandmete töötlejatest. Käesoleva magistritöö eesmärk on isikuandmete töötlemise registri välja töötamine Eesti väike-ettevõtte näitel.

GDPR seab nõuded igale isikuandmete töötlejale tähtsustades andmetöötluse läbipaistvust ja andmete kaitset nende töötlemisel. Töödeldavate andmete mahud on viimaste aastakümnetega hüppeliselt kasvanud. Seda toetab lai valik soodsalt kättesaadavaid elektroonilise andmetöötluse vahendeid nagu pilv-andmetöötlus ja andmemajutusteenuse hinna langus. Nagu iga uue tegevusvaldkonna ja tehnilise lahendusega, võib siingi kaasneda oht sellega seotud inimestele. Võrreldes konservatiivsemate andmetöötlusviisidega, mis on olnud aastakümneid laialdaselt kättesaadavad, töötatakse täna kübermaailmas välja andmete katise meetmeid. GDPR juhib tähelepanu elektroonilise andmetöötlusega seotud aspektidele nagu isiku profileerimine võrgukäitumise alusel (küpsised, IP aadressid, seadmete nimed, asukoha koordinaadid), mis on küberruumis nii laialt levinud, et seda peetakse pealetükkivaks ja privaatsust riivavaks.

Käesolev magistritöö analüüsib isikuandmete töötlemise ja kaitsega seonduvaid aspekte eesmärgiga töötada välja metoodika isikuandmete töötlemise registri loomiseks, ja luua metoodika aluseks võttes töötlemise register vaadeldava väike-ettevõtte jaoks. Registri loomisel on arvesse võetud GDPRi üldiselt sõnastatud nõudeid, varasemalt loodud registrite näidiseid, registri haldamise tõhusust ja kohalike õigusaktide nõudeid ettevõttele. Teemat on käsitletud laiemalt kui seda on nõutud GDPRis. Loodud isikuandmete töötlemise register kirjeldab isikuandmete töötlemist konkreetses väike-

ettevõttes võimaldades tõendada selle vastavust GDPRi nõuetele ja optimeerida töödeldavate andmete kaitset selles ettevõttes.

Magistritöö on kirjutatud inglise keeles ning sisaldab teksti 95 leheküljel, viit peatükki, viit joonist ja seitset tabelit.

List of abbreviations and terms[1]

AKI	Data Protection Inspectorate, the supervisory authority of data protection in Estonia (Andmekaitse Inspektsioon)
Controller	Natural or legal person which determines the purpose and means of processing personal data
Data processing	An operation performed on personal data, 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
Data subject	Natural person who is or can be identified based on personal data
Enterprise	The company the research focuses on as a case study
EU	European Union
GDPR	General Data Protection Regulation 2016/679
ICO	Information Commissioner's Office, the United Kingdom national data protection authority
ISACA	A global non-profit organisation formerly known as Information Systems Audit and Control Association,
ISKE	IT baseline security system for the Estonian public sector
IKS	Estonian personal data protection act
Personal data	Any information[2] relating to an identifiable or an identified natural person such as name, identification number, online identifier etc.
Processor	Natural or legal person processing personal data on behalf of the Controller
Register	Records of personal data processing activities as described in article 30 of GDPR
Special categories of personal data, sensitive personal data	Personal data that by its nature is particularly sensitive such as ethnic origin, religious or philosophical beliefs, trade union membership, genetical, biometric, health or sex life.
WP29	The Article 29 Data Protection Working Party, composed of EU member states data protection supervisory authorities representatives and a European Commission representative

[1] Several terms used in the research originate from GDPR and are used as in GDPR. Definitions given here are rephrased to reflect the principal meaning perceived by the Author in the context of this thesis.

[2] The distinction between terms „information" and „data" that is made in information technology, will be disregarded in this thesis due to GDPR cross-using the terms without distinction.

Table of Contents

List of Figures

List of Tables

1 Introduction

The General Data Protection Regulation (hereinafter GDPR) of the European Union enforced on May 24th 2016 affects all member states in personal data processing and protection. Anyone processing personal data shall adhere to GDPR by May 25th 2018, when the regulation will be applied after two years of transitional period for achieving compliance.

The first concern of organisations[3] processing personal data, is whether it concerns them at all? The answer is – yes, it applies to anyone processing personal data. The second question is how does it affect the organisation and what changes are needed in daily operation? The answer depends on many aspects from the organisation size, industry of operation, nature of data processing etc. The main four changes affecting an organisation as perceived by the Author, are appointing a data protection officer, conducting data protection impact assessments, keeping records of data processing activities and ensuring transparency of processing. With the trend of increasing electronic data processing and exploding volumes, the natural person, whose data GDPR aims to protect, has become an object in the rather new cyber domain, where maintaining full control of data processing poses a new set of challenges. Creating transparency of personal data processing with the records required by GDPR, enables visibility for everyone involved: the person the data is about, the authorities supervising data protection, and to the organisation itself. This visibility is a prerequisite to protect the data processed by applying adequate security measures and detecting any deviations from the intended purpose or process.

The motivation for this research is preparation for GDPR and achieving compliance for the case study enterprise (hereinafter Enterprise). The goal of this research is to create records of data processing activities required by GDPR (hereinafter Register) for the

[3] GDPR applies to persons processing data, not just organisations, but that is out of scope of this research and will be disregarded in this research.

Enterprise to enable displaying GDPR compliance and transparency to clients, the authorities, the natural persons and to the Enterprise itself. This research will focus on what is needed to create the Register, what aspects and considerations affect creating it, and reveal further application opportunities and practical benefits of the Register.

The scope of this research is the Register for the Enterprise as required by GDPR with the extension of incorporating local requirements and context of personal data protection. The main constraint of the research is the law in development in Estonia specifying personal data protection on state level. The advancement made in working out local law can affect the Enterprises compliance to the rules defined there, and since relevant law is not finalised, according adjustments may need to be made to the Register after the law is in force. Another significant constraint is the limitation of different publicly available Registers which to use as an example and the limited variation of guidelines interpreting GDPR requirements for Registers. With GDPR application deadline approaching more Registers and guidelines are expected to emerge, that were not available at the time of conducting this research, but the starting point of few examples available increases the value and contribution of this thesis producing a publicly available source of a Register.

The approach taken in this research includes analysing the requirements and guidelines on personal data processing, investigating the aspects and considerations in processing and protecting the data, and customizing the Register to best suit the business needs of the Enterprise. The data sources used in this research span from GDPR itself and data protection authorities' materials, to consultants and auditors assisting organisation in preparing for GDPR, to the contribution of the employees and service providers of the Enterprise.

This research gives an overview of the context and background of personal data processing describing in section 2 the requirements set by GDPR, existing solutions and examples, and discusses alternative solutions contribution for creating a Register. The analysis section 3 begins with defining the steps needed to become GDPR compliant and illustrates the Registers role in the process, followed by GDPR requirements to the content of the Register and to whom it concerns. As the Register shall list processed data categories, approaches of how to categorise personal data will be analysed to create the break-down of the content of the Register. Previous and existing examples of registering

personal data processing will be described, and analysed to what extent these can be (re)used for developing a Register. The requirements for Registers vary for different roles in processing and the effort to uphold different Registers in a single organisation is analysed considering the business efficiency and most value from with reasonable effort. The consequences of giving in to the temptation to process large volumes of data available, and the challenges it presents in determining business sensitive assets, will be discussed. This will provide the Enterprise with insight for further analysis of security measures application, sufficiency and possible reorganisation. Estonian local law poses several obligations to an organisation to process and transfer data to state institutions. Which law applies to the Enterprise will be identified, and the impact to the Register discussed. The Enterprise will be described to characterize the area of operation and the details affecting the Register content for the specific organisation. The results section 4 will firstly describe the steps taken to create the Register, the data processing mapping and the distillation of personal data processing activities from the overall data processing of the Enterprise. Secondly the structure and contents of the Register is described explaining the arguments for data processing activities and business motivation behind that. The section also addresses the possibility and considerations in applying the results in other organisations and lists areas for further research beyond this thesis.

2 Background and Related Literature

Organisations processing sensitive information such as business confidential data, intellectual property, trade secret, are generally aware of the need to protect the information for the organisation to remain operational and achieve set goals. If that data leaked, the organisation may lose its' competitive advantage, market share and after decreased income business survival could be at risk. Personal data at first glance may not seem as the object of utmost protection in the form of person's name or picture because if misused it will probably not result in significant monetary loss to businesses or the natural person. But taking into consideration the sensitivity of some personal data such as health related, racial, religious, biometric; and convictions related data, when misused it could lead to serious adverse effect on the data subject – prejudice, discrimination, loss of livelihood and even threat for life.

The General Data Protection Regulation (GDPR) is a regulation of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data [36]. It is a relatively new regulation that has been introduced and explained in many articles and papers by the EU authorities in EU and abroad. The discussion remains on a general level to whom GDPR applies to, what are the changes it brings on and where to start in ensuring adherence to the requirements.

This research is important because of the scale of entities processing the data (all EU and beyond) and the struggle for applying sufficient security measures of majority of entities processing personal data. Organisations are struggling to achieve compliance with GDPR requirements and interpreting the regulation, because it is, as stated in its name, *general* and does not give too specific guidelines how exactly it should be implemented.

The practical tools to deploy to become compliant with GDPR, are few and scarce with different European data protection authorities tackling to produce guidelines and examples. At the time of this research, the most detailed guidelines and practical examples have been issued by the Information Commissioner's Office (hereinafter ICO), the United Kingdom national data protection authority, and more general by other states authorities. In the course of this research only one publicly available example of a record of personal data processing activities in Estonia was identified.

This section will describe the basis and the starting point from which to depart in creating a Register, with further details and references concerning specific details discussed in the following section 3 Analysis.

2.1 Goal and Method of Research

The initial concern of the Enterprise is where to start in GDPR compliance preparation and how. Being unaware of the extent to which the organisation activities are affected by GDPR and the specific requirements GDPR introduces, the first concern is to identify steps in dealing with GDPR adherence. This research focuses on creating records of processing activities (Register) for a small-sized[4] enterprise as required by GDPR.

Problem 1: create a Register for the Enterprise.

The research aspires to create tools for data processing map and register, based on which security measures can be analysed and implemented. Based on the example the goal is to generalise the result achieved so that it can be used as a model to be adjusted and implemented in other small or medium-sized organisations. The goal of the research is to develop a *method* of creating a Register for the Enterprise, and by deploying the method, deliver *the Register* structure and content for the Enterprise as required by GDPR.

Problem 2: establish the steps to create a Register.

The research aims to create a practical use and implementation of a Register in achieving GDPR compliance for the Enterprise, but also providing an example of the consideration and argumentation for other small organisations developing their own Registers in Estonia and abroad. Personal data processing in each organisation varies widely and personal data protection is tailored to each organisation, but some models and tools to use in becoming GDPR compliant can support data processors.

Problem 3: publish the Register and the process of its development as an example for other small and medium-sized organisations.

---

[4] GDPR enables a derogation for organisations with fewer than 250 employees regarding record-keeping, taking account the specific situation of micro, small and medium-sized enterprises [36]. This research considers a less than 250 employing organisation to be small-sized.

This research will analyse the Register requirements for a small-sized enterprise, approaches and considerations to map and protect processed personal data, the Register content based on the role of the processor, and relevant regulation and law applicable to personal data protection for the Enterprise in Estonia. The methods for research will include documentation analysis (literature, law), analysis of guidelines and implementations (examples, existing Registers), case study of the enterprise (observation and analysis of data processing, interviews) etc.

2.2 General Data Protection Regulation and the Register

GDPR is a European Union (hereinafter EU) level regulation applicable across the EU and all its member states. The regulation entered into force on May 24th 2016 and will apply from May 25th 2018 having given two years to prepare to adhere to the requirements GDPR has set [36]. GDPR reflects the principles of the Directive 95/46/EC, the basis of GDPR in the approximate extent of 80-90% [34]. Personal data protection law on state level will be repealed and replaced with GDPR, leaving the flexibility and the opportunity to specify some topics on state level law (employment context, national identification number, data subject under the age of 16, convictions related data).

GDPR applies to all organisations processing personal data in EU, of citizens of EU and data subjects in EU [35]. GDPR harmonizes data protection laws across the EU the rules for protection of personal data processing between the member states of the European Union, laying ground for more equivalent base for the EU to support the economy. Personal data processing beyond EU with a third country outside EU or with an international organisation is allowed with the adequacy decision of the European Commission or the supervisory authority in a member state [36] and personal data transfer outside EU is under scrutiny to ensure adequate protection.

GDPR approach is protection by design and protection by default that is required from all organisations processing personal data with principles defined to follow are [36]:

a) lawfulness – data shall be processed according to law and be transparent to the data subject;

b) purpose limitation – data shall be processed for specific and defined purposes and will not be processed for purposes beyond that;

c) data minimisation – data processing is limited only to what is needed for fulfilling the purpose of processing;

d) accuracy – data is correct and updated, measures are taken to delete or rectify data without delay[5];

e) storage limitation – data is stored in a manner that enables identifying a person only until fulfilling the purpose of processing;

f) integrity – data is processed in a secure manner using relevant technical and other means from unauthorised processing, accidental loss, deletion or damage;

g) accountability – the Controller is responsible for protecting data and is able to prove it.

GDPR states that sufficient lawful basis for personal data processing is given by one of the following [36]:

a) contract or preparation of it;

b) performing public duties;

c) legitimate interest;

d) data subject consent;

e) vital interests of the data subject.

GDPR draws attention to some types of data that are more sensitive or require special care during processing – special categories of personal data, such as health related data -

[5] This can be applied to the extent of effort and abilities of the data processor assuming the data presented by the data source is accurate and true. If the data source presents incorrect information, it can be cnsidered the data processor's due diligence to investigate the vaidity of the data, but if the data is intentionally corrupted, the processor can dispute the responsibility for data accuracy.

which is not allowed to process unless given the right or obligation by lawful basis for processing.

GDPR distinguishes the roles of a Controller and a Processor, where the Controller defines the purpose and conditions of personal data processing and using a Processor (such as a service provider), defines the boundaries and rules for the Processor to operate within [36]. Joint Controllers is a model of processing where all organisations processing personal data are Controllers and bare the relevant responsibility.

"In order to demonstrate compliance with this Regulation [GDPR], the controller or processor should maintain records of processing activities under its responsibility" [36] to be able to transparently demonstrate adherence. GDPR applies to all organisations processing personal data, but alleviates data processors of less than 250 employees to be considered with derogation regarding record-keeping where the processing is [36]:

a) Occasional;

b) Does not include sensitive (special categories) or criminal offences related data;

c) Processing is not likely to result in a risk to the rights and freedoms of data subjects.

The Register shall include [36]:

a) Name and contacts of the controller(s), its representative and data protection officer;

b) Purposes of data processing;

c) Description of data subjects and categories of personal data and/or categories of processing[6];

d) Categories of recipients the data is disclosed to;

[6] Contents of Register varies depending on the organisation role in the processing (Processor or Controller). The differences will be addressed and analysed in due course.

e) Transfers of data to third country or international organisation;

f) General description of technical and organisational security measures;

g) Envisaged time limits of erasure of different categories of data (where possible).

The natural person, the data subject, is given rights concerning their personal data [36]:

a) Right of access – to data and activities of processing;

b) Right to rectification – to correct or update data;

c) Right to erasure (right to be forgotten) – deletion or removal of data relating to the natural person;

d) Right to restriction of processing – limiting data processing by physical, technical or other means;

e) Right to data portability – extracting existing data from the processor to enable handing it over to another processor;

f) Right to object – data subject can prohibit processing their personal data.

Personal data breach management and mitigation is addressed in GDPR, defining conditions of notification to the authorities and to data subjects concerned. The notification shall include where possible the categories and approximate number of data subjects and data records concerned [36].

2.3 Existing Instructions and Examples

Data protection authorities, law firms, consultation service providers across Europe and abroad are devising programs or projects to achieve GDPR compliance proposing courses of actions for an organisation to initiate. Most sources begin with mapping data processed, but some take the risk-based approach starting with data protection impact assessment.

The Irish data protection authority lists the GDPR preparation steps as follows [15]:

a) Review and enhance risk management processes;

b) Make an inventory of the data you hold;

c) Communicate data privacy notices within the organisation and to service consumers;

d) Ensure data subjects' rights enabling procedures;

e) Plan data subject request handling;

f) Define lawful basis for data processing;

g) Review data processing on the basis of consent;

h) Children's data processing review;

i) Data breach reporting;

j) Data protection impact assessment;

k) Appoint data protection officers;

l) Data processing internationally.

The Article 29 Working Party (hereinafter WP29) of the European Commission [12] has issued guidelines and explanations interpreting GDPR regarding data portability, data protection officers, data protection impact assessments, automated decision making [13], but creating a Register has not been in focus.

ICO has published templates for Controllers and Processors to use in creating a Register required by GDPR. Presented in Appendix 5 – ICO Example of Records of Processing Activities – Processor [25] and Appendix 6 – ICO Example of Records of Processing Activities – Controller [24], the templates include the compulsory components by GDPR described in the previous section and local law requirements in addition giving some brief examples of describing the processing of some categories. Based on the ICO templates for Controllers and Processors, AKI has translated and illustrated the examples in Estonian [10], the same has been done by Finnish data protection authority [42] covering the compulsory components required by GDPR. ICO differentiates the Registers of Controller and Processor as has done AKI, but the Finnish authority does not.

Some examples of personal data registers descriptions have been published for sensitive data processors to assist them in registering with the Data Inspectorate in Estonia as

required by law. These guide the processors on their mission to define and specify personal data processing purposes, categories and safeguards, but that only covers one area of the Register required by GDPR. The entirety of the Register will still have to drawn up by each processor considering their data processing specifics and extent. To ease that, any practical example would be valuable.

A Register created by an Estonian business media group Äripäev AS [44] is presented in Appendix 4 – Records of Processing Activities of Äripäev. The content of the Register covers most of GDPR required components (transfer to third countries and international organisations can be deducted, for these are not clearly defined) with the addition of lawful basis and Processor names. The categories of data subjects in the Register of Äripäev include customers, subscribers, web-page visitors, employees, and data types include contact, subscription, call recordings, usage statistics, correspondence history, payment discipline, personal identification code. Purposes of data processing include registration for events, fulfilling subscription orders, promotion, sales proposals, reporting, user activity monitoring, client feedback. The Register also includes components not obligatory by GDPR – list of Processors, which is separated from recipients, and lawful basis for processing. Lawful basis for processing includes contracts, consent, legitimate interests, direct marketing as mentioned in GDPR.

The Handbook of European data protection law lists specific topics addressed by different European data protection laws: electronic communications, employment relationships, medical data, clinical trials, statistics and financial data [23]. These topics are regulated on EU level and reflected on state local law described in AKI guideline [4]. A large extent of personal data processed is compulsory by law to process and forward personal data to relevant state institutions. According to Personal Data Protection Act draft, there are over 80 local acts affected by GDPR and repelling the IKS in force [28] and for an organisation it is rather difficult to get one’s bearing in the myriad of acts. The acts affecting personal data and the protection of it by local law specific paragraphs are largely covered in AKI guideline [5].

2.4 Alternative Approaches and Sources

The challenge in mapping personal data to create a Register, is identifying and locating the personal data. There are data discovery and analysis tools and solutions to identify

personal data in structured and unstructured repositories (databases, file servers, e-mail servers), which deliver coarse-grain data overall view that is good to benchmark business required data against, but cannot be relied to map the entire perspective of an organisation. These tools are also not applicable to all media types used to process data, for example, audio, video and especially paper are more difficult to analyse. Another obstacle is different lingual context with dozens of official languages used in the EU member states and developing tools to crunch all languages is a resource consuming task. Using these tools would only provide the transparency only to the extent of existing electronic processing activities not covering the justification for processing or transferring. In the era of big data another expected GDPR non-compliant result using such an approach would be to find that data retention is not limited.

A source for mapping personal data processed is found in information systems or IT infrastructure documentation if such exists. Larger organisations developing their own custom-made information systems have documented processes, requirements for information systems processing data and may reveal sources where, how and why personal data is processed. This kind of information obtained from a variety of sources and level of detail would require levelling the detail, but would still not cover the purposes and retention period required for GDPR.

These alternative solutions are perceived by the Enterprise to be too resource costly to implement compared to developing the Register on the basis of GDPR requirements. Therefore alternative solutions are not within the scope of this research.

3 Analysis

Implementing GDPR requirements and becoming compliant includes for most organisations creating a Register. For some organisations GDPR imposes other obligations like data protection impact assessment and assigning a data protection officer. With more sensitive personal data and more extensive processing, further requirements for the organisation shall be fulfilled.

The complexity of implementing GDPR for a data processor, is that GDPR is as is stated in its name – *general* – and does not regulate *how,* but *what* to protect. It provides the principles and guidelines for data processing and protection, but not the practical support data processors crave for in implementing adjustments brought on by GDPR. The practical implementation is left to the sole discretion of the implementor. What are the needed changes and how to go about them, are the questions each organisation will ask in the context of GDPR and is looking for answers, guidelines examples of material to assist making the necessary changes. A high-level regulation, such as GDPR, extending across European states, cultures and organisations, should be presented to be adjustable to a wide range of organisations in different industries and sizes, from a small family business to large international groups or corporations. GDPR going into detail would face a challenging highly complex task defining rules to fit all sizes and characteristics, staying general it remains. Developing the necessary mechanisms, processes, documentation and skills is something each data processor should take upon themselves with the best knowledge they have or expertise they can involve.

GDPR emphasises the principle of purpose for personal data processing, which for most data processors cannot be easily copied. Creating the Register, it cannot be copied or transferred from one organisation to another and each organisation has to develop the Register best befitting the specific organisation, industry, local regulation and business model. The structure of the Register can to some extent be reused learning from the organisations already have devised it. The willingness to share it outside the organisation, is another matter, since the contents of the Register can to some extent be considered sensitive information including contractors and service providers, collaboration cross EU borders and the description of security measures. Another aspect is the cost of developing mechanisms to meet GDPR requirements because operational efficiency in many

industries is the prime competitive advantage. Having implemented the relevant processes and measures to fulfil GDPR requirements, having spent time and money on developing them, organisations may not be motivated to help others prevent making the same investment.

Validation of a tool developed is an issue with any tool acquired. Existing tools can cover the basic needs for whom the tool is devised, but the implementation solution and the specifics of the implementer differ and may be even unique for each case. Out-of-the-box solutions are implemented largely at the risk of the implementer and the producers of out-of-the-box products can only offer some support with the expertise in the product, not the implementers operation. Tools to deploy or implement after which the organisation is GDPR compliant are scarcely published or tightly tied to a lingual context. Interpreting GDPR for each organisation specific context and developing the necessary changes involves analysis, business and legal acumen, so using an out-of-the-box solution is unachievable. GDPR encourages certification mechanisms to prove adherence, but such have not been created in Estonia nor referenced by the Data Protection Inspectorate (hereinafter AKI) as the state supervisory institution on data protection.

Disclosing information about the operation and data assets of an organisation may not be in the interest of the organisation, let alone if the data asset is the core asset or intellectual property of the organisation, for example strategic service providers contact list for an events organising company or a product design or pricing mechanism. Revealing this asset to a competing organisation could mean grave monetary loss (if not the bankruptcy) for the enterprise. Not to even mention security measures disclosing the weaknesses of an organisation and listing the measures taken to protect them, which would be fascinating for anyone with a malicious intent mapping the possible attack or entry points.

The reasoning where to start in preparation for GDPR compliance is discussed analysing the approaches to begin GDPR preparations in an organisation (section 3.1 GDPR Compliance Programs) and elements of a Register is listed in GDPR and application obligation to the Enterprise is analysed (3.2 Records of Processing Activities). In a situation where there is no previous enterprise information architecture documented, identifying personal data processing is a challenge where some data or processing can remain off the map. The approach to identify personal data needs to be determined (3.3 Data Assets and Categories) and the responsible party identified for protecting the data

(3.4 Data Ownership and Responsibility). On the brink of GDPR application, in the beginning of 2018, there is very few practical guidelines and examples made public to learn from, but some examples are identifiable that can be followed (3.5 Previous Examples of Register and 3.6 Current Examples of Content of Records). The effort to make in creating a Register is differentiated considering the responsibility of the organisation processing the data. Any organisation acting at level of responsibility, will calculate the least effort for maximum result for the organisation in fulfilling GDPR requirements (3.7 Combining Records of Controllers and Processors). The appropriate safeguards applied in the of context of data value and impact if compromised shall also be analysed and calculated (3.8 Data Content and Protection Considerations). The Register created in this thesis, is based on a small Estonian enterprise considering the characteristics of its data processing (section 3.10 The Enterprise). GDPR applies in all of EU member states, but leaves some areas open to be specified or regulated on state local level. In addition to GDPR, an organisation shall comply to state local law, which in many regards is intertwined with personal data processing. Personal data processing and protection according to local law should be analysed by the Enterprise (section 3.9 Regulation and Law).

3.1 GDPR Compliance Programs

WP29 providing some tools and recommendations, does not give general guidelines of planning the steps to take to become GDPR compliant and the different sources that do, vary in their advice. The Director General of AKI listed 5 steps to follow to be compliant to GDPR [3]:

1) Not to panic, because the foundation of data protection rules, is the same as before;
2) Conduct an integrated assessment of your data processing, if personal data is processed on a large scale or involves considerable risks;
3) Observe your entire work order, information systems, and document blanks from the perspective of the new data protection rule;
4) Check the data portability in your work processes and information systems;
5) Find a specialist to assist and if needed appoint a data protection officer.

The first step in the overall program for GDPR compliance by ISACA GDPR implementation guide [37] is identification and registering (Figure 1 GDPR Program Workstream, Identifying PD and PD Register).

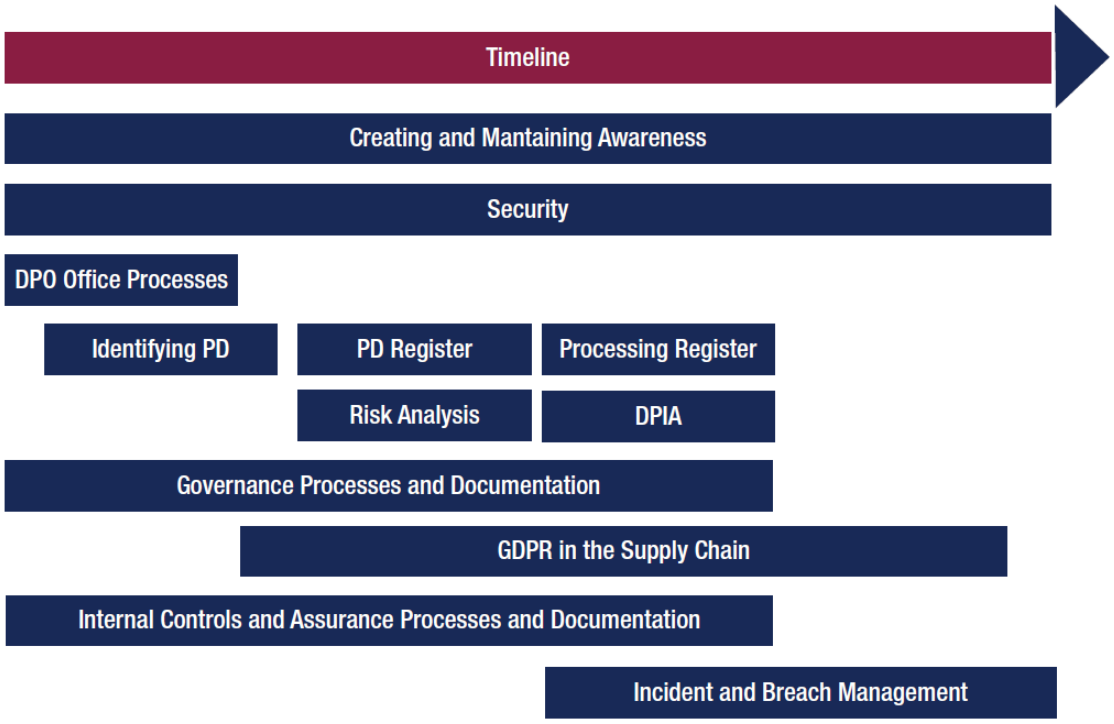


Figure 1 GDPR Program Workstream

The Irish data protection authority [15] as referred in section 2.3 suggests to start with data inventory, proceed with defining lawful basis for processing and to leave data protection impact assessment for further stages.

Information Security Forum describes the approach for GDPR compliance [27] in the following phases and steps:

Phase 1: Prepare for GDPR compliance:

a) Discover personal data: define personal data and maintain records of the processing;

b) Determine compliance status;

c) Define GDPR compliance scope.

Phase 2: Implement a GDPR compliance programme:

a) Satisfy role requirements;

b) Protect personal data;

c) Manage DPIAs[7];

d) Demonstrate lawful processing;

e) Uphold data subject rights;

f) Meet data transfer requirements;

g) Respond to personal data breaches.

GDPR Tech, a fully GDPR focused solution provider lists the steps to take for GDPR compliance [38] in another sequence starting from personal data impact assessment as step 1, to developing the organisation to be able to respond to data subjects requests automatically in step 5 (Figure 2 GDPR Whiteboard). In step 4 of creating classification, the first question to answer is identifying personal data from the whole dataset processed.

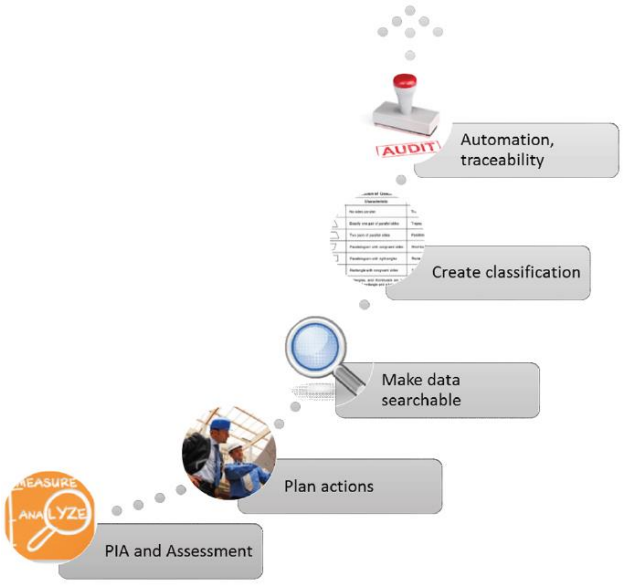


Figure 2 GDPR Whiteboard

[7] (D)PIA refers to data protection impact assessment required by GDPR.

Triniti Estonia, a business law firm has listed the steps in preparing for GDPR [34]:

1) Data – identify what data is processed and where;
2) Identify third parties – who is the data collected for and with whom is it shared;
3) Impact assessment – establish a formal impact assessment process;
4) Processing – map and prioritise data processing activities and risks;
5) Breach notification – create a plan of action for data breach management and procedures for notification compliant to 72 hours requirement;
6) Individuals' rights – develop processes for replying to data subjects' requests, complaints, respond within required timeframe.

Out of the different approaches to start preparation for GDPR requirements fulfilment - from starting with data records to another with impact assessment - it is the Author's belief that an impact cannot be assessed without specifying the object behind the force and the effect – the processed data itself. Mapping the data processed and identifying personal data within the specific organisation context is the preliminary condition of any well-informed decisions or plans beyond that. This research will be focusing on identifying personal data by Triniti Estonia preparation model step 1, creating personal data register by ISACA model (Figure 1 GDPR Program Workstream), discovering personal data by ISF approach phase 1 step a) [27] and classifying it by GDPR Tech whiteboard model step 3 (Figure 2 GDPR Whiteboard).

3.2 Records of Processing Activities

GDPR lists the compulsory components of records of processing activities, which should be maintained and made available to the supervisory authority [11]. AKI recommends maintaining the Register in electronic form using free software tools [9]. The requirements for keeping records of data processing are listed in GDPR article 30, where the contents vary to a small extent depending on the role of the processor.

GDPR states that the Controller, who defines the data processing purposes and means, shall maintain a record of processing activities under its responsibility containing the following:

a) Name and contacts of the controller, its representative and data protection officer;

b) Purposes of data processing;

c) Description of data subjects and categories of personal data;

d) Categories of recipients the data is disclosed to;

e) Transfers of data to third country or international organisation (which should be identified) and documentation to safeguards in absence of adequacy decision by the European Commission (where applicable);

f) Envisaged time limits of erasure of different categories of data (where possible).

The Processor, acting within the limits of the contract with the Controller and GDPR, shall maintain a record of processing activities containing the following:

a) Name and contacts of the processor and each controller, their representatives and data protection officers;

b) Categories of processing carried out for each controller;

c) Transfers of data to third country or international organisation (which should be identified) and documentation to safeguards in absence of adequacy decision by the European Commission (where applicable);

d) General description of technical and organisational security measures (where possible).

Compared to ICO template, AKI and the Finnish supervisory authority has excluded the components not obligatory by GDPR that were included in ICO template: consent documentation reference, data location reference for access request, privacy notices content, data protection impact assessment, data breach documentation and local data protection bill. As seen by ICO template, additional creating a transparent overall picture

for the organisation data processing, will provide practical elements to use the register to manage compliance to data protection regulation as a whole, not just GDPR.

GDPR allows an exception in the obligation to uphold the Register to Controllers employing under 250 persons unless the processing is:

a) Likely to result in a risk to the data subject,

b) Not occasional,

c) Including special categories of data.

AKI has interpreted that the aim of this exception to relieve small and medium-sized organisations from the obligation to create a Register to reduce administrative burden, is deceptive and that all processors are obligated to maintain the Register [9].

3.3 Data Assets and Categories

Mapping data assets and developing data categories, it is important to create a common vocabulary of terms and an understanding of the underlying goal. To comply with GDPR, a rather superficial Register can suffice, but with the organisation delving into details beyond formalities ISACA refines a more detailed approach proposing an example of types of personal data (Figure 3 Types of Personal Data).

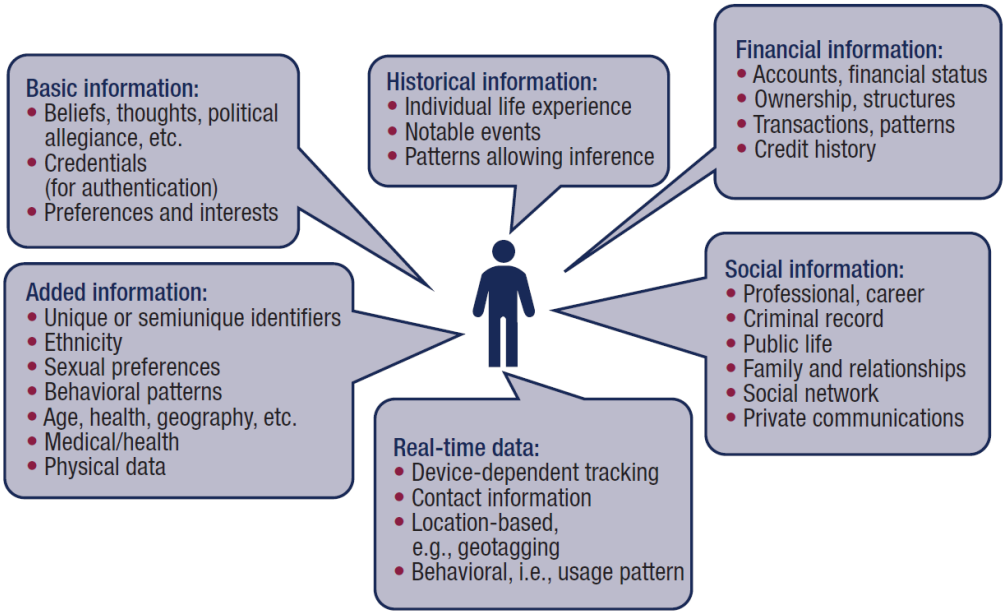


Figure 3 Types of Personal Data

In the GDPR Implementation Guide [37] ISACA distinguishes personal data register from processing register. The guide defines personal data register as "containing metadata that lists or catalogues the type, amount and processing context of personal data within the enterprise…" (Table 1 Personal Data Register).

Item	Example / Remarks
Primary key	Use numeric or alphanumeric key; could be name of personal data set.
Information type	
Information owner	
Information custodian (if any) as delegated by owner	
Information source	
Special categories (if any)	
Protection level	
Information format	Electronic, paper-based, microfiche, permanent, transient, screenshot, etc.
Purpose of collecting and processing	Insert GDPR-conformant statement of purpose(s).
Type of storage	Physical, hard disk or tape, SAN/NAS, cloud, etc.
Storage instance	Specify storage array or other unique identifier(s) for precise location(s) of personal data.
Processing jurisdiction(s)	Describe all jurisdictions in which personal data processing takes place, including backup locations, etc.
Storage jurisdiction(s)	Describe all jurisdictions in which personal data may be stored, including backup locations, etc.
Retention period	Specific purpose-dependent (maximum) retention. Include any overriding retention requirements that may prolong retention (e.g., tax purposes).
Right and reason of access	Provide appropriate information from identity and access management function, preferably linking to their tools to obtain up-to-date information.
File exports / further processing	Specify any exports or mutations of data (e.g., into XLS or CSV) and further processing (e.g., sending a copy by mail), including the specific purpose and justification.
Sharing with third parties (if any)	List all third parties that may receive the personal data asset, including the rationale for sharing (must be covered by purpose); where possible, link to processing agreement with the third party.
Mode of sharing with third parties (if any)	Specify the mode and format for sharing, e.g. remote access, mail attachment, encrypted database sharing, etc.
Additional jurisdictions	Specify any jurisdictions in which third parties might process or store the data asset; include adequacy, additional safeguards, binding corporate rules, etc., for each case.

Table 1 Personal Data Register

The guide [37] defines a processing register as "containing metadata about processes using personal data…" (Table 2 Processing Register).

Item	Example / Remarks
Primary key	Use numeric or alphanumeric key; could be name of personal data set.
Process	Link to the standardized process name or identifier.
Process owner	
Process step	
Personal data used (specify assets)	Insert reference to all personal data assets in the personal data register that are used to perform this process (or process step).
Purpose(s) for using the assets	Explain the purpose of processing in terms of the process—what is the business rationale or transaction, why is the information needed, etc.
Process result	Describe the expected result of the processing (e.g., identity established and forwarded to payments).
Upstream processes or process steps	Where does this process (step) get information from, and which personal data assets are sent from upstream processes?
Downstream processes or process steps	Which downstream processes (steps) is this process or step feeding into, and which personal data assets are being sent?
Process jurisdiction(s)	Specify the jurisdiction(s) in which the process (or process step) takes place; match against personal data register to ensure referential integrity and consistency.
Third parties (if any)	List all third parties performing part or all of this process (step).

Table 2 Processing Register

As can be seen ISACA guide [37] recommends registering data processing in much more detail than required by GDPR, focusing in-depth on business processes, ownership and responsibility, and storage specifics. ISACA refers the described registers in the manual to be a source for risk management, controls management, data governance, processor/controller management, access control management etc. valuable in use for large organisations with thousands of employees with such processes in place or in focus. For small and medium sized organisations this approach would be exceedingly draining and the author considers it to be excessive to implement with such granularity in small or medium sized organisations.

3.4 Data Ownership and Responsibility

Who owns the data? Who is responsible for it? GDPR states that the Controller determines the purpose and the means of processing personal data [36]. To some extent the responsibility can be shared with the data subject, the natural person, the data is about, via consent, contracts and other lawful grounds of processing the data. Through that the data subject authorises the Controller to use and potentially monetise the personal data in return of receiving a service or a product. But from a certain point forward, the processor should consider the individuals ability to comprehend data processing complexity and take responsibility for protecting it. Releasing the data for marketing purposes of adjacent services could be transparent enough to the individual, but for example European energy

grid demand and supply balance calculation might exceed the average person's awareness and understanding.

In general, an owner of an asset is interested and often responsible for preserving and protecting the asset. The asset of personal data appears more complex to handle and the owner of the data to identify in the era of big data and cloud computing. In product development, it might appear rather straightforward who owns the technology – the one who designs and builds the components – and to protect the intellectual property of the design can apply to licence it. In the era of electronic data processing, duplicating and transferring data is much easier, and identifying the owner of the data after it has been passed on is much more complex than with physical property. The definition of personal data by GDPR is "any information relating to an identified or an identifiable natural person…who can be identified directly or indirectly…" [36]. So, that means piece, or a combination of pieces of data that relate to one specific person, is personal data. This could be the description of a person, their behavioural patterns, unique origin or traits. Personal data belongs to the individual, because it is about the individual [14], if the person did not exist, the data would not exist. "Personal data belongs to the individual and they have "borrowed" it to be used for business purposes, and like with any loan, they can reclaim it." [35]. "When processing your data organisations have to provide you with clear information relating to the use of your data" [21]. On the other hand, placing the responsibility of processing or protecting the data to the individual, is likely to become overwhelming with the speed of light considering the free flow of data and the availability of processing tools. Not to mention the business of exchanging, purchasing or selling data (such as direct-marketing contacts). An example where processing and ownership of data should not be placed on the individual can be drawn from the energy sector. The consumers of electricity, the average households, are offered convenience services related to electricity including smart-meters, where the consumer now does not have to report the meter readings to the electricity provider, but they are collected by smart-metering devices and reported to the service provider without human intervention. This data is used for billing purposes and calculating the invoice of that specific consumer, but the same data can also be incorporated in trends analysis for demand across the energy grid of the whole of Europe or beyond. The energy sector is a good example of interdependent markets, where no country, let alone a single electricity provider, can afford operating autonomously. It is a complex resource optimisation exercise daily, with a myriad of

consumers and their habits dictating the demand the producers react to. Can an individual household as an electricity producer be expected to comprehend the trends and economics of European or global energy market production and demand dynamics? Because their data is a small piece the demand relies on and is based upon. Can the individual be considered as responsible for their data in these circumstances? The responsibility should not be placed on the individual, because they might not understand the big picture and market mechanisms [14].

The discussion of data ownership remains unsettled and open for further debate, but the requirements defined by GDPR are at this point the Controllers obligations and data subjects rights.

3.5 Previous Examples of Registering Personal Data Processing

Preceding GDPR in Estonia AKI has provided samples of data processing records with categories by industries for organisations that have been under the obligation to register their data processing according to the law. Before the ICO templates were created for GDPR required Register, these were the baseline in Estonia to describe personal data processing activities. The examples provide the structure for the registration application for health, communication [7], credit and financial [6], and security [8] service providers. Comparing the structure and components of the registers described by AKI to the Register required by GDPR it can be seen that they are not equivalent as described in Table 3 Components Comparison of GDPR and Estonian Data Processing Register and cannot be claimed to adhere to GDPR requirements.

Component of Register	**GDPR**	**AKI**
Name and contacts of Controllers/Processors and representative	Yes	Yes
Name and contacts of data protection officer	Yes	*No*
Identification or registry code of the Controllers/Processors, location or area of operation	*No*	Yes
Lawful basis for data processing	*No*	Yes
Purposes of data processing	Yes	Yes
Description of data subjects and categories of personal data	Yes	Yes

Component of Register	GDPR	AKI
Sources of personal data	*No*	Yes
Categories of processing for Controller	Yes	*No*
Categories of recipients of data	Yes	Yes
Transfers to a third country or an international organisation and documentation of safeguards (where possible)	Yes	*No*
Time limits of erasure of data	Yes	*No*
General description of security measures	Yes	*No*

Table 3 Components Comparison of GDPR and Estonian Data Processing Register

If an organisation had created a personal data processing register that was necessary to obtain the right to process delicate (special categories) of data from AKI, they would merely add a few components to it and could be considered GDPR compliant. As notified by AKI, these registers will no longer be required to obtain the right to process special categories of data [2], but as GDPR requires a Register from all who process personal data, the organisations creating the register can still learn from AKI previous examples. Looking at AKI examples of contents for the data processing register as described in Table 4 Examples of Data Processing Register Contents, these do correlate to ICO given examples [26] to some extent in the relevant components and categories and can be reused for GDPR required Register. The nature and extent of a specific organisation data processing can be based on these examples but requires customisation to reflect the environment and actual data processing within an organisation.

Component of data processing register	Examples by AKI
Lawful basis for data processing	Electronic communications act, employment contracts act, data subject consent, security act
Purposes of data processing	Providing high quality security services, providing financial services, providing high quality communications services
Content of personal data	Name, personal identification number, date of birth, income, location, education, medical history, marital status, convictions, ethnical origin, biometric data, need for social care

Component of data processing register	Examples by AKI
Categories of data subjects	Clients, personnel, client official representatives
Sources of personal data	Identification card, state databases, data subject, medical history documents, court documents, translation services providers, Health Insurance Fund, forensic investigators
Categories of recipients of data	Court, Ministry of Economic Affairs and Communications, AKI, insurance provider, state databases, other enterprises in the group, communication service providers, Police and Boarder Guard Board, beneficiaries determined by the data subject

Table 4 Examples of Data Processing Register Contents

3.6 Current Examples of Content of Records

Records of personal data processing activities publicly available are scarce considering the operation and functioning of any organisation is generally business confidential or a trade secret. In some cases, where data is the core asset of the business (like in the telecommunications industry or cloud computing service providers), it has been recommended to publish the Register to make data processing transparent to all parties involved [34]. The organisations having developed the Register, have been cautious in making their Register public, it appears they are holding back and waiting to see what will happen in May when GDPR will be applied [34]. The motivation not to publish Registers due to intellectual property or trade secret provides a possible explanation for that. Not publishing existing Registers imposes a barrier for organisations initiating to identify the requirements and the effect of GDPR to their specific operation.

An Estonian business media group Äripäev AS has published their records of personal data processing activities [44] displayed in Appendix 4 – Records of Processing Activities of Äripäev. The Register of Äripäev is divided into sections by the group enterprise by the business function such as customer service, advertisement sales, client training, conferences etc. It contains the components of a Processor's Register - purpose of data processing, data subjects and data categories, recipients, retention deadline, but it does not cover the organisations role or responsibilities as a Processor or a Joint Controller. The Register does not mention any data being transferred to a third country or an

international organisation regardless of Äripäev using a global service provider Google while being a member of a group operating beyond Europe [43]. Analysis of Äripäev interpretation of GDPR requirements based on their Register and the accordance to the supervisory authority is a topic for further research and will not be addressed in further detail in this thesis.

In Estonia where all state institutions activities and information is public information by principle, unless given a legal ground for declaring the information confidential, Registers of state and local administration organisations should be made public upon a request. One source of acquiring examples is submitting relevant requests to ministries, but it is likely that in their preparation for GDPR, they have not yet progressed far enough to present one.

The Author expects that with time, more Registers will become publicly available by the initiative of trade associations and with the contribution data protection enthusiasts in enterprises making the effort to display transparent data processing. But the pace and amount of them becoming public is difficult to prognose.

3.7 Combining Records of Controllers and Processors

Although the Register requirements vary for Controller and Processor, the author proposes to combine the Registers of Controller and Processor because virtually all Processors are simultaneously Controllers, especially in case of small and medium sized organisations that combine the functions larger corporations who may choose to segregate into separate organisations for better business management. As a Controller, it is unlikely that an organisation does not involve any Processors or Joint Controllers. Nowadays it is quite rare that an organisation is entirely autonomous processing personal data without any contact with a service provider to support some functions delegated to an external party, such as accounting, IT, legal advice. Larger organisations may perform these functions by themselves, but then it is more likely that due to the complexity of the organisation, requirements imposed by the state or other international bodies, they involve expertise from specialised service providers. The Author perceives that each small and medium sized organisation, that by first glance may act as a Processor, also acts as a Controller regarding data only required for the organisation itself, such as employee data, and it would require additional inefficient effort to maintain two separate

Registers for small and medium sized Processors. In order to combine the information in the Register as a Controller and as a Processor, the first step is to identify the difference in the requirements between the two, interpret the underlying content, keeping in mind the value and intent (transparency, substantiation and validation) of the Register, and then to combine them. The components of Registers for Controller and Processor vary as described in Table 5 Comparison of Contents of Records Requirements.

Component of Register	**Controller**	**Processor**
Name and contacts of Controllers/Processors, representative and data protection officer	Yes	Yes
Purposes of data processing	Yes	*No*
Description of data subjects and categories of personal data	Yes	*No*
Categories of processing for Controller	*No*	Yes
Categories of recipients of data	Yes	*No*
Transfers to a third country or an international organisation and documentation of safeguards (where possible)	Yes	Yes
Time limits of erasure of data	Yes	*No*
General description of security measures	*No*	Yes

Table 5 Comparison of Contents of Records Requirements

Name and contacts of Controller(s) and Processor(s) are included for both roles. For Controller, the next two components are purposes of data processing and categories of data subjects which correspond with the categories of processing for the Processor. The Author suggests including these components to cover both roles[8]. Although a Processor is not responsible for defining the purpose of processing, it is necessary to be aware of the data subjects the processing concerns, to support the Processor. For example, in data breach management the Processor is likely to inquire about data subjects affected in case

[8] As Joint Controllers, both involved are responsible for defining the purposes, but the purposes can be different due to the industry and line of business. Categories of processing reflects the line of business or a service of a Processor, so the line between a Processor and a Controller holds room for different interpretations.

of an incident, and categories of processing can reflect the extent of data subjects in addition to means of processing. To cover the data processing across different organisations regardless of the perceived roles, more comprehensive outlook is gained from defining the purpose and range of data subjects affected beyond GDPR defined roles in the GDPR general approach. Documenting the recipients, the data is disclosed to, is compulsory for the Controller, and to ensure transparency of the whole data processing, identifying further recipients at the Processor (or any further Processors), empowers the Controller with added awareness and the data subject with transparency through the whole data processing sequence and involved organisations as service providers. Transfer to a third country or an international organisation is included in Registers both for the Controller and the Processor, so are the security measures and safeguards description.

Majority of Registers components are the same for Controllers and Processors and the rest can be combined into a single register covering the requirements for both roles.

3.8 Data Content and Protection Considerations

Personal data processing volume has exploded alongside with data processing in general during the past decades in Estonia as well as across the globe. Data has become *the gold* and an essential asset for many businesses with tools to process it having become widely available and being developed extensively for a wide range of purposes. Data hosting cost (in data centres regarding disk space) has dramatically decreased using modern technology such as cloud computing, diminishing the concern of optimising data volumes processed for business purposes. It would appear that with data, the more you have it, the better, enabling primary business operation complemented by long-term historical data multi-source hybrid analysis. There is little motivation for data processors to delete data, it is more alluring to preserve existing and even acquire it from different sources. This has led to the status quo where there are so many “digital fingerprints” of a person in the cyber domain, it requires additional effort to ensure privacy of an individual, because “Google knows all about you anyways” and “the Internet will never forget”. The General Data Protection Regulation [36] or *GDPR* as it is referred to in the media, in specialist circles and by the officials, takes a firm step towards enforcing personal data processors to map, assess and mitigate the effect of their actions on the natural person. It requires for

the data processor to map their processing activities and assess the impact of the processing activities to the natural person or the *data subject*.

Network security has been addressed previously on the international scale in EU with the NIS Directive[9], but the asset passed through networks – data – requires further means of protection. Network security measures do not penetrate to the level of content protection nor deal with protecting the business asset extent, value and continuity. The fortress of network protection can be impenetrable, but valuating the need of securing the fortress comes down to a business decision of risk appetite and mitigation cost of the asset. ISACA distinguishes personal data register from processing records - "In terms of controls, the personal data register is the most important source of information assets... It is important to align any controls to the corresponding personal data sets. … personal data register shows what the personal data are and how they are distributed across information assets, the [GDPR] processing register forms the other half of the equation by specifying what is done to the data." [37]. If there is no treasure in a fortress, there is no need to secure it. GDPR is about the asset and making sure it is at its minimal to serve the purpose needed lifting the business the need to apply excessive protective measures. Creating security is an art in itself but in the practical world of limited resources exists only to serve the business needs and the needs of those they concern and deliver value to. From business perspective every expense made should justify the value returned, every risk taken must be taken with full awareness and accounted for, in case it is realises.

In the realm of cyber security new threats and weaknesses are presented and identified on a daily basis. Mitigating all of them is an ambitious undertaking few attempt, or are able. Is it worth making a network, an organisation, a business bulletproof, which superficially appears to be the unachievable goal of technical cybersecurity specialists? Is it worthwhile to deploy first rate controls to protect less than critical operations or data asset? It is difficult to identify the desired level of security and substantiated cost unaware of the asset value and magnitude. Records of personal data processing activities required by GDPR is a valuable tool in identifying and mapping the personal data asset extent and volume in an organisation. The categories of personal data support assessing the

[9] Directive 2016/1148/EU of the European Parliament and of the Council concerning measures for a high common level of Security of Network and information systems across the Union.

sensitivity and consequences if compromised. With the awareness of the assets to protect, one can make an informed decision of appropriate security measures to apply. The risk appetite of the processor, the level of uncertainty a processor is willing to accept with the loss assessed, brings on an entirely new layer which is addressed in the data protection impact analysis obligatory to some data processors according to GDPR. Risk appetite and possible impact of consequences would be an area for future research but falls out of the scope of this thesis.

Cybersecurity is about protecting the assets in cyber domain by applying necessary security measures to achieve the desired residual risk level. One of the focal points of cybersecurity is data loss prevention and detection. Protecting digitalised and decentralised data, which has become widespread, is a challenge and assessing the extent and impact of an occurred data breach is something cyber forensics deals with. Findings of cyber forensics in an occurred event is a valuable source for learning to prevent further security breach and assessing the potential consequences of it happening. GDPR is a compliance type of document by which each data processor should assess the impact of their data processing to the data subject [34]. Before processing personal data, AKI advises the Controller to perform personal data protection impact assessment even when it is not an obligation from GDPR [1]. Given the extent of electronic personal data processing assessing the potential impact is closely tied to cyber forensics. GDPR also defines the obligation to document and notify data breaches to the data subject and the supervisory authority. The components of this notification include description of the failure, the categories and approximate number of data subjects concerned. Cyber forensics here is an inseparable component of adequate reconnaissance and transparency. Describing the amount of data subjects concerned as an additional component in the Register, would provide an indication of the range of personal data processing, and tools used to process the data can give valuable information for data breach mitigation techniques and containment.

3.9 Regulation and Law

Besides EU regulation for personal data processing, there are state level acts in Estonia that also define requirements for data processing relevant to the Enterprise industry and operation, and on personal data protection. Requirements from other sources than GDPR

applicable to the Enterprise are reasonable to consider when creating the Register. These additions, as can be seen from Registers examples described in previous sections, are perceived to increase the value and practical use. From the organisations perspective creating the Register, including law applicable to the organisation in the Register, it would become a tool that can be used to map overall law requirements beyond GDPR and monitor compliance. This section will discuss the law related to the principal activities of the Enterprise and identify if and how they affect the Enterprise or can be reflected in the records of personal data processing activities.

Handbook on European data protection law refers to the Directive 95/46/EC as the principal legal instrument on personal data protection aiming to harmonise data protection law at the national level [23]. The Directive [16] by now has evolved to GDPR.

In addition to European level data protection, there is a state law in Estonia addressing data protection and personal data processing. Due to the fragmentation of different norms, the coherence is unsettled, and it is difficult to keep track of the law in applying security measures to information systems [29]. In some industries data processing is regulated on an international level like telecommunications, banking or energy, facilitating stabilisation of the interconnected markets and infrastructure. GDPR is striving to set the baseline for personal data processing, but remains less practical in providing tools, standards or guidelines.

This section describes the content of regulation and legislation affecting the Enterprise and the industry specifying the obligation and manner of processing personal data.

3.9.1 Personal Data Protection Act

Personal data processing in Estonia has been regulated by Personal Data protection Act (hereinafter IKS) [33] which was enforced on January 1st 2008 and the current version in effect, was last updated on January 16th 2016. It applies to all data processing in Estonia except processing data by natural persons for personal purposes and data that is transmitted through Estonian territory without any other processing of the data. The Act defines the conditions of processing personal data state-wide: personal data processing principles and processors' obligations, data subjects' rights, protection measures, delicate personal data processing and registration with the supervisory authority, and supervision. IKS will be replaced by a new full text after GDPR application May 25th 2018 removing

the duplicating clauses of the Directive 95/46/EC and specifying the allowed flexibility on state local level.

IKS covers the content and essence of GDPR extensively in reflecting the requirements of personal data processing. In this sense there should not be a large shift in protecting personal data for the processors. But the problem is that IKS implementation is rather modest beyond the public sector and most of the private sector, especially the numerous small and medium-sized companies in Estonia, is not compliant to IKS[10]. Therefore, the GDPR "campaign" for the data processor in Estonia in essence is a fraction novelty and a lion's share of upgrading to the law in force previously.

The major changes GDPR brings compared to the IKS in effect presently are:

a) While GDPR approaches data protection from the data processing transparency and prevention angle, IKS has previously been more aftermath oriented of proving compliance and sufficient measures upon request or following an incident. GDPR makes the Controller accountable for *whole* data processing cycle and the Controller shall be able to prove compliance;
b) Each data processor shall maintain records of personal data processing activities;
c) Data protection impact assessment and assigning a data protection officer is made compulsory by GDPR to some data processors;
d) GDPR lists a set of compulsory clauses to the contracts between the Controller and the Processor;
e) Information of data processing provided to the data subject is expanded;
f) Data subject will gain the right for portability of personal data and the right to be forgotten is specified;
g) GPDR sets more demanding deadlines to data processing breaches and expands the range of parties to be notified;
h) GDPR increases fines of failure to comply.

[10] The perception of majority enterprises not being compliant to IKS, is deducted from personal and proffessional experience of the Author by the numerous uninvited intrusive sales calls and e-mails received daily and regarded as spam.

With GDPR being compulsory to adopt in each member state by May 25th 2018, Estonia has drawn up the implementation act Draft Personal Data Protection Act specifying some topics as allowed in GDPR, but mainly excluding what is already regulated on EU level. The new full text draft of IKS was published on November 24th 2017 [18]. The Draft Application Act of the Personal Data Protection Act [18], which describes the changes in local law resulting from GDPR application and IKS, was issued for information and feedback on March 15th 2018 and discussions risen have not finalised into proposals or changes in the act at the time of finalising this thesis.

IKS addresses some specific forms of data processing giving the data processor the right to process personal data without consent in using surveillance equipment. IKS §14 section 3 states that using surveillance equipment transmitting and recording for protection of persons or property is allowed based on data subjects consent. If the usage of the surveillance equipment is clearly communicated to the data subject along with the name and contact details of the data processor, the data subjects consent is substituted.

3.9.2 Guidelines from Data Protection Inspectorate

The Data Protection Inspectorate of Estonia (AKI) reflects the developments of data protection regulation within Estonia and EU. As the supervisory authority described in GDPR, AKI issues guidelines and instructions in addition to supervision conclusions on data protection. Concerning GDPR implementation in Estonia AKI has described GDPR related statements among which is the obligation of registering personal data processing activities, assigning a data protection officer (e.g. insurance providers, telecommunications or network security services, hotels, banks, direct marketing services, location data processors) and performing data impact assessments (network behaviour or location monitoring for example network security enterprises, smart device service providers, telecommunications and security services providers).

According to AKI network security and monitoring service providers data processing carries out high risk to the data subject, the Enterprise is obligated to create records of processing activities, even though employing less than 250 people, it could be exempt from it just by the size of the enterprise as allowed in GDPR article 30(5).

3.9.3 Personal Data in Employment Relationship

Employing people, the employer shall comply with many rules set by the state it operates in, regarding taxes, health safety etc. The acts requiring personal data processing and forwarding to the state are primarily Occupational Health and Safety Act [32] and Employment Contracts Act [20]. In Estonia this also includes personal data about employees, and not only personal data, but special categories personal data the employer shall collect and forward to others as set by the law. This includes data such as about employee medical leave and work-related health examinations. Delicate personal data obligatory to process and forward to relevant state institutions are described in Employment Contracts Act and the Occupational Health and Safety Act. This addresses data such as temporary incapacity to work (due to illness), pregnancy and maternity leave, medical health examinations for employees whose health may be affected in course of work process, but also health safety. The Occupational Health Act §13 section 1(7) sets the responsibility of the employer to organise medical examinations for employees whose health may be affected in the course of the work process. In the Occupational Health Act occupational accidents, diseases and other work-related illnesses are addressed in §22 and §23. The employer is compelled to pay sickness benefit as described in §12[2].

The Employment Contracts Act §15 section 1(10) defines the responsibility of the employee to notify of temporary incapacity to work, and §19 section 2 the right to refuse to work due to temporary incapacity. The Employment Contracts Act regulates the payment of wages and §38 defines the payment of wages upon impediment to work. The basis of paying wages upon impediment of work is notification as described in the Occupational Health Act. Pregnancy related work time issues and remuneration are also addressed.

3.9.4 Accounting Act

The accounting act defines the rules of processing financial information and documents of enterprises in order to comply with state tax and reporting principle in Estonia. The accounting act is important because it defines the retention period of accounting source documents, which impacts the Register to a large extent of personal data retention period of 7 years after the creation of the source document.

3.9.5 Public Information Act

Public information processing in Estonia is regulated by the Public Information Act. It defines the usage and access to public information, requests for information management, disclosure of information, restricting information management, public information databases and supervision. The Public Information Act states that all information obtained or created by performing public duties is public information unless restricted by law. All data is public unless restricted approach can be perceived as diametrically opposite approach from GDPR, where all data is restricted unless made public on lawful grounds. This discrepancy is a research topic for the author in the future. The Enterprise is a privately-owned company not performing any public duties, therefore the act will not apply to the Enterprise.

3.9.6 Draft Cyber Security Act

Regulation connected to more technical cybersecurity in Estonia includes the implementation of the NIS Directive which is reflected in the Draft Cyber Security Act. This act defines information society service providers obligations in network and information systems managing, responsibility and supervision requirements in providing information society services. The draft act has been approved by the Government of Estonia and has reached the discussion rounds of the State Defence Commission of the Parliament of Estonia. There has been much discussion and opposing opinions as to the reach, the impact and the authority given by of the act, since it is arguably not apparent from the draft act, and the list of service providers it applies to will be published approximately 6 months later than the act is enforced.

The topics the act covers are cyber security management principles; service providers obligations security measures; cyber incidents prevention, management and reporting to Information System Authority of Estonia; and state supervision. It also imposes the service provider to conduct a risk analysis and establishes a database of cyber incidents managed by the Information Systems Authority.

The initial draft [17] of 26.09.2017 was published for feedback for state institutions and industry organisations and secondary draft of 1.03.2018 issued for feedback to the Parliament of Estonia and industry organisations. In the first draft the scope of service providers was wide and unspecified and raised a wide interest in specifying the

organisations it applies to. The second draft specified that it applies to organisations with significant effect to state information society services and does not apply to service providers of under 50 employees and revenue of less than 10 million euros. At the time of writing this thesis the act is in the state of development still and has not been decleared entering into force. The second draft makes it clear not applying to the Enterprise of this thesis and therefor will not be focused on in further detail.

3.9.7 Electronic Communications Act

The Electronic Communications Act "provides requirements for the public electronic communications networks and publicly available electronic communications services, for the use of electronic contact details for direct marketing, for the conduct of radiocommunication, for the management of radio frequencies and numbering and for radio equipment as well as state supervision over the compliance with these requirements and liability for the violation of these requirements." [19]. The Electronic Communications Act regulates mainly communications network providers, national broadcasting network, naval radio communication and operative radio communication services. Although the Enterprise does not fall under these categories, the act regulates using electronic contact details for direct marketing via electronic channels. The act § 103^1 section 1 states that for direct marketing the subscribers consent is required, and the opportunity given to the subscriber to refuse. The contacts of an existing client can be used to offer similar services they have purchased earlier, if the client is informed of the right to refuse using the contacts by §103^1 section 2.

3.9.8 Security Act

Security Act [39] applies among other areas to security consultation and to operating a monitoring centre. Security consultation as defined in the act is "…the process of identifying the risks arising from the characteristics or peculiarities of a guarded object and providing written recommendations for the prevention or reduction thereof. Recommendations shall be made in the form of a security plan." The definition of a monitoring centre is "…unit for the remote monitoring of information transmitted by security equipment, and the duties of the employees at a monitoring centre are to determine any change to the guarded object or any potential threat to the object in due time, to inform the security guards promptly of any such change or threat, to co-ordinate the activities of the security guards and to apply relevant measures.". The vocabulary used

in Estonian regarding the services and enterprises this act applies to, is closely knitten to physical security services like personal protection (body-guards), maintaining order at events (concerts, public displays) and physical objects surveillance (video cameras, surveillance equipment planning and operation). This leads to the perception that this act does not apply to information security services providers like the Enterprise.

3.9.9 ISKE

Data protection in state institutions and local administration information systems is regulated by the Estonian Government Regulation of Information Systems Security Measures System[11][31]. This regulation describes security classes assignment, measures implementation and auditing based on the IT baseline security system ISKE [30], which is compulsory to the public sector in Estonia. The regulation recommends conducting a data security analysis for security classes assignment and fixes an auditing interval of 2-4 years according to the security level assigned.

ISKE implementation guide includes a description of the aspects of assessing information criticality, and inventory of information assets to choose and implement the relevant security measures to protect the information [30]. ISKE analysis include based on data processed (categories, purposes, extent) assessing the information confidentiality, integrity and availability requirements, with an additional layer of assessing the severity of consequences if any of the previous have been compromised; ISKE inventory lists the assets used to process the data (equipment, medium, people etc.) [30]. European data protection inspectorates list among other components of data protection impact assessment check-list: means, purposes and context of data processing; time limits of data erasure; inventory of processing system (people, appliances etc.); assessment of risks [1]. Having performed ISKE analysis and inventory of information assets the previously listed components can be reused for GDPR data protection impact assessment.

ISKE does not apply to the Enterprise, because it is not performing public duties nor providing input of original documents to state registers with requirements of electronic

[11] Unofficial translation into English available in [22].

data integrity and security that shall be ensured with the means of the Enterprise[12]. ISKE however is significant to the Enterprise because it applies to its potential clients and therefore can be the source of defining some requirements to processing or providing additional information on the protection of the clients' data.

3.10 The Enterprise

Personal data processing record in this research is created on the example of an Estonian company Security Software OÜ. The Enterprise is an information security solutions provider established in 2010 providing services from training and consultation to testing and security operations center.

The Enterprise provides the following services (Figure 4 The Enterprise Service Portfolio) [40]:

a) Product related support and services: custom solutions, licences, support;

b) Security consulting and analysis on minimising risks, analysing and managing cybersecurity, information security process management;

c) Testing vulnerabilities of IT infrastructure and organisation;

d) Security operations centre service: monitoring and supervising (collecting and analysing security events, threat response and defence etc.), developing and administering;

[12] Security of the information provided by an enterprise to state institutions is by electronic means ensured by the relevant state institution. For example in the healthcare industry the state has imposed requirements to private sector systems providing information to the State Health Information System to apply at least the same level of ISKE security class and controls as the state information system to ensure the integrity of the data processed decades later. In the healthcare industry example, it is the responsibility of the private enterprise to ensure the confidentiality, integrity and availability of the information system and data.

e) Security training and awareness: information security awareness, security products implementation and operation (data loss prevention, advanced threat defence etc.), cyber hygiene;

f) Information security technology: endpoint security, infrastructure and cloud security, monitoring and testing equipment, special appliances.

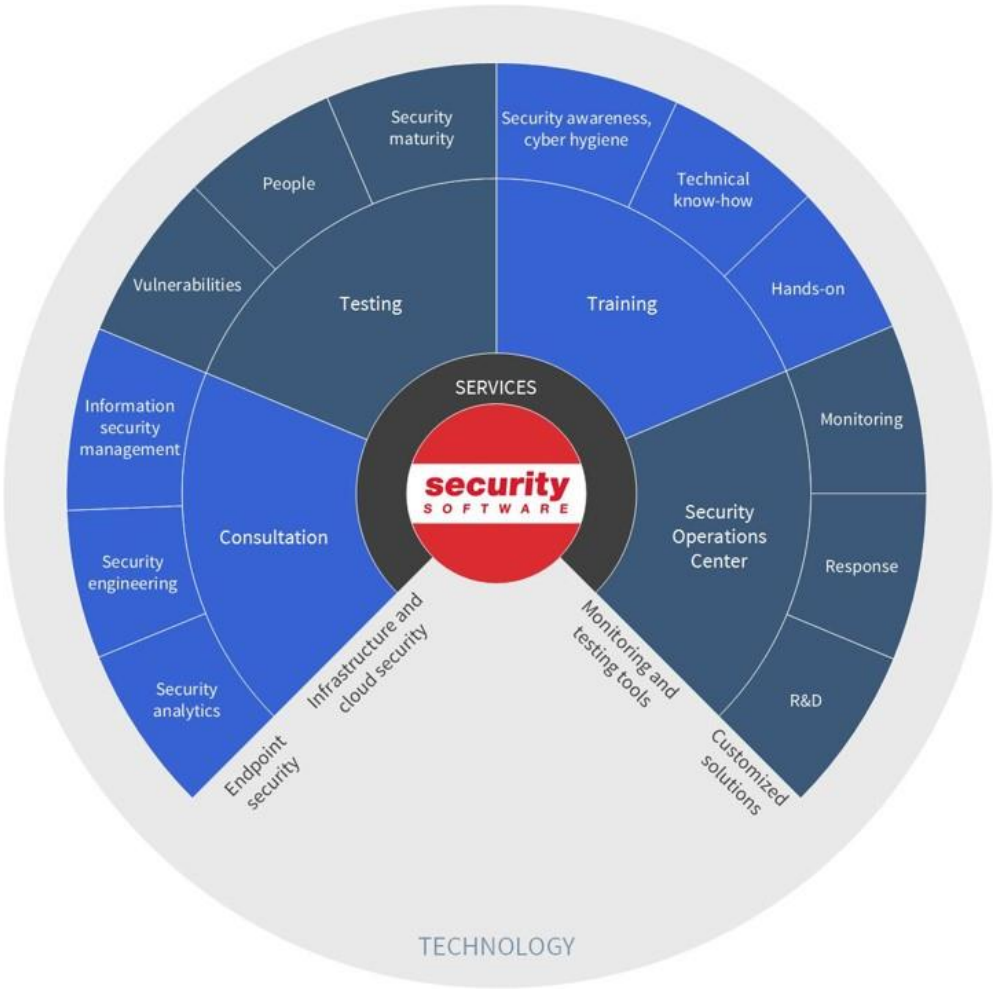


Figure 4 The Enterprise Service Portfolio

The Enterprise operates in Estonia as well as across Europe with customers in the public-sector institutions and privately-owned companies in various sizes and industries (Figure 5 The Enterprise Client Base Parameters) [40]. Contracts with clients include long-term partnerships across the entire service portfolio and well-defined specific projects.

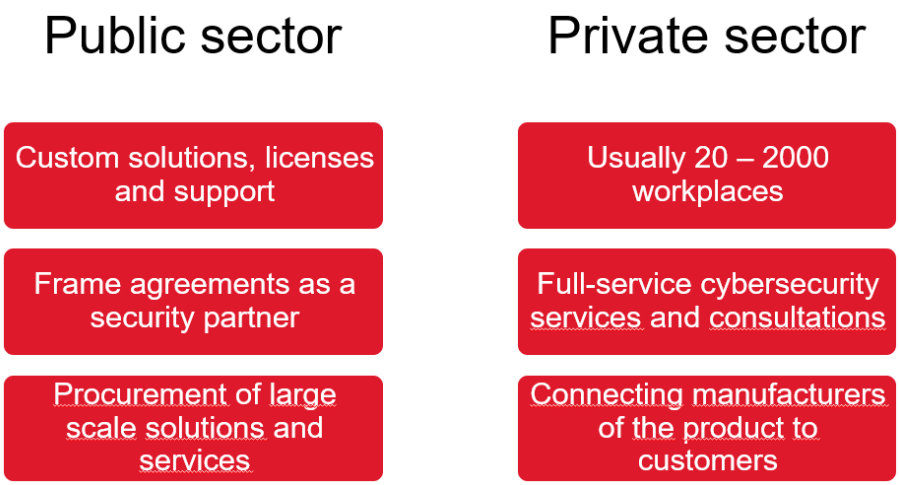


Figure 5 The Enterprise Client Base Parameters

The Enterprise acts as a partner for several vendors and distributors with products and solutions in addition to developing services and products for clients in-house. Solutions are implemented and maintained on client site or configured to extract service relevant data to the Enterprise. Implementations have extended up to 45 000 endpoints and strictly regulated industries like the financial sector.

The Enterprise is a small business with 12 employees [41] and some functions necessary for operating a business are performed by service providers (accounting, marketing etc.).

The Enterprise has not analysed existing requirements applicable to personal data processing and has based personal data processing on what is required by law and contracts with clients, partners and contractors. The Enterprise presumes that it does not fully comply to GDPR requirements and further effort should be made to achieve compliance. The Enterprise does not currently maintain required Register and current data processing in general is not documented. There is some documentation regarding specific areas or topics (accounting, specific products and clients), but the overall picture is uncharted. Information about overall data content, processing details, business considerations required for creating a Register will be acquired in the course of interviews with members of the Enterprise team and service providers they engage.

4 Results

The goal of this research was to create a Register for the Enterprise to be able to demonstrate compliance to GDPR. Due to the scarceness of methods to create a register and existing Registers examples, the methodology was analysed and created in the course of the research. After developing the method, it was applied in the context of a case study to create Register for the Enterprise. Combining these tracks in this research, provided several by-products and additional applications for from knowledge gained from developing a Register.

This research delivers the content of the Register created for the Enterprise reflecting the personal data processing activities while conducting business. Section 3 analysed the requirements and consideration influencing the content of the Register and has clarified the compulsory elements of a Register and provided the reasoning for the additional elements described in the Register of the Enterprise. This corresponds to problem 1 defined in section 2.1 Goal and Method of Research and the results are described in sections 4.3 and 4.4.

The process of creating a Register was developed during this research using the existing knowledge of the Enterprise data processing and the materials covered in this research. The process established was used to create the Register for the Enterprise. This corresponds to problem 2 defined in section 2.1 and the results are described in sections 4.1 and 4.2.

While developing a Register for the Enterprise, findings within and beyond the scope of the specific Register provided consideration of what of the Register and the development process can be (re)used in other organisations. This corresponds to problem 3 defined in section 2.1. The limitations of reusing the Register elsewhere, the additional value gained beyond the initial goal of this research and further connected areas of research are described in sections 4.5 and 4.6.

4.1 Research Process and Results Format

Considering the size of the Enterprise and the organisation taking the first steps for GDPR compliance, it would be most efficient for the Enterprise to create a single Register

combining the components as discussed in section 3.7. The level of detail shall remain the same as described in sections 3.5 and 3.6 based on previous and current examples paving the way or the Enterprise increase the level of detail in the future in specific areas if needed to the level described by ISACA in section 3.3. Security measures applied to the processing of personal data will be mapped for the Enterprise on an abstract level considering the argumentation given in section 3.8.

According to the data minimisation principle of GDPR, an organisation shall not process personal data in excess of what is required to fulfil the purpose of processing. On account of that, this research reflects the data processed in the Enterprise during the research. The Register documents the status quo of personal data processing activities in the Enterprise. This research will not address reorganising data processing activities to evolve the adherence to external standards or law in the Enterprise. If there is room for development in compliance with GDPR requirements beyond creating the Register, these will not be solved nor specified in detail, and will remain for further research after this thesis.

The Register presents the general rules of processing for personal data. If the rules are defined differently for a specific project or client in a contract and deviations from general rules are agreed, then these exceptions are not reflected in the Register.

The results created with this research are made public to the extent agreed with the Enterprise. Information in the Register created for the Enterprise that is business, security or client sensitive, is not given in the original level of detail, but abstracted, or marked confidential in the Register, where there is no need-to-know basis within this research. The results of security measures applied is abstracted to the level agreed with the Enterprise to protect revealing the exact details of measures from threats enabling intervention or security breach. The names and contacts of Processors, partners and contractors are abstracted to the level of service type to protect revealing strategic business partnerships. Also the specifics of information systems used by the Enterprise are abstracted to the function they are used to perform to avoid the tools marketing.

4.1.1 Data Mapping and Personal Data Identification

Mapping of the data the Enterprise is processing, was created on the basis on business needs and functions (like sales, marketing, service delivery) focusing on areas where personal data was processed. Data mapping approach taken is top-down creating a model

describing the data processed on a high level and after that specifying the data processed. Besides identifying business functions processing personal data, this enabled to easily identify the purpose for data processing and to develop personal data categories and sub-categories. Business-function based approach to data mapping enabled identifying data transferred to contractors outside the EU for business purposes with strategic partners. If a certain business area or function did not include personal data, the map remained higher level of detail, and areas containing personal data specified the data categories processed.

Data map was structured following the example in Table 6 Example of Data Mapping Structure.

Category	**Sub-category**	**Data (type)**
Enterprise	Employee	Name
		Picture
		E-mail address
	Representative	Name
		Authorisation

Table 6 Example of Data Mapping Structure

4.1.2 Creating Records of Processing Activities

Creating records of processing activities, the first component for each Processor and Controller shall be publishing their name and contacts accompanied with information about their data protection officer(s). Collaborating with external organisations, contractors or providing services to organisations, their names, contacts and data protection officers should be listed by a Processor and described by categories by a Controller. For the Enterprise, the list and contacts of Processors are obtained from contracts, the organisations web-pages or addressing the organisation with a specific inquiry.

Personal data processed was described in the data map by data categories, sub-categories and data type. Considering the same data types can be used for different purposes, retained for different periods of time and transferred to different audiences, the data types were grouped to datasets. For each dataset the information required for the Register was

described – purpose, recipients, retention period etc. A new entry (row) was created if any of the values describing the data (category, sub-category or data type) or the processing (columns) differed as illustrated in Table 7 Example of Register Content.

Category	**Sub-category**	**Data (type)**	**Purpose**	**Retention**	**Recipients**
Enterprise	Employee	Name, personal identification code, e-mail address	Sales and marketing	End of contract	Prospective customers
		Name, bank account number	Fulfilling employment contract	10 years after end of contract	Relevant state institutions
	Representative	Name, authorisation	Providing a service	7 years after end of contract	Respective client

Table 7 Example of Register Content

Creating the records of processing activities, there are factors that influence the obligatory contents required by GDPR and can useful if be documented in the Register. By adding additional pieces of information to the Register, it can also be used within the new processes brought on by GDPR like data protection impact assessment or data breach management. In preparation for GDPR and requirements beyond records of processing activities, the Register can provide a valuable source for information used in other processes connected to personal data processing:

a) breach management;

b) data subjects' rights support and request fulfilment;

c) data protection impact assessment;

d) controller-processor roles defining and agreements management;

e) used IT tools review;

f) security measures mapping and assessment;

g) special categories data processing constrictions;

h) amount of data subjects affected by processing activities.

In addition to GDPR compliance, there are state local requirements applicable to enterprises by the local state and these also should be paid attention to. Local law in Estonia requires processing, retention and transfer of data GDPR in general does not allow, for example in employment relations, where GDPR enables states to specify an approach and requirements different from GDPR. For this reason, obligations arising from local law should be specified in the Register to substantiate processing data that otherwise is not allowed, like special categories of data concerning employee health checks, parental leave etc. Mapping of lawful basis for data processing provides a useful tool for managing data subjects' rights and requests enabling documenting the purpose for data processing, retention period and transfer to other Controllers or Processors. For example, if data is processed as a requirement by law, a data subject may not be able to exercise the "right to be forgotten" or the right to data portability to another organisation even if the source of the data is the data subject. Including relevant local law reduces the sources for the Controller and Processor concerning personal data processing. GDPR required purposes of data processing is expanded in the Register of the Enterprise with *lawful basis for processing*, *reference to local law condition* and *data source*.

Identifying the external Controllers and Processors, the Controller can define their role and clarify it with service providers defining security measures. Having identified the Processors, it can assist in identifying transfer of data to a third country or an international organisation. For example, using a web-based cloud IT service provided by a global organisation, it can be deducted with a certain level of confidence, that hosting the data processed, may not take place within the EU and GDPR requirements may not be satisfied. To get confirmation about the Processors processing activities and applied security measures sufficiency, the Controller can initiate a dialogue with the service provider. The Processor itself may knowingly and intentionally choose a service provider processing data outside EU and deal with risk management or adequacy issues, but the Processor choice could have been made years ago based on the IT tool functional use unaware of GDPR being enforced after that. In that case the Processor shall assess the circumstances and decide to switch service providers and choose one operating in EU and compliant with GDPR. GDPR required transfer to third country or international

organisation in the Register of the Enterprise is divided in two parts - *transfer to third country or international organisation for business purposes* and *transfer to third country or international organisation by technical limitation*. To differentiate between these two transfer purposes, the Register is expanded with *information system* the data is processed in. Service providers of information systems platforms that can confirm processing EU clients' data on EU soil, and information systems that are hosted by the Enterprise, are described not transferring data to third country or international organisation[13]. Service providers, partners and contractors that are operating outside the EU or are not able to confirm not sending data outside EU, are considered to transfer data to a third country or international organisation.

Acting as a Processor, the name and contact of representatives and data protection officers for each Controller and Processor shall be documented in the Register. In order to identify the role of a Processor or a Controller and the need to document the contacts of another organisation, GDPR required name and contacts of Processor and Controller is expanded in the Register of the Enterprise with the Enterprises *role in processing* and *controller*. Controller providing services to several clients over the course of several projects and years, the contact list of Controllers and Processors can increase to a level difficult to manage in the Register. To maintain an updated list of relevant Controllers and Processors contacts, it would be better to document references to sources where updated contacts are stored. GDPR required name and contacts of processors and controllers is substituted in the Register of the Enterprise with *reference to controllers' and processors' contacts* and service providers with more permanent nature are added to the Register front page besides the Enterprise contacts. Other Controllers and Processors contacts are documented in relevant contracts and entered into the accounting or sales information system and will not be included in the Register.

Assessing the appropriate security measures for each personal data category is closely dependent on the amount of data subjects involved and the sensitivity of the personal data processed. Assigning the appropriate security measures should be decided based on the data protection impact and the effort to mitigate the risks. The residual risk and the extent

[13] The validity of the service providers, partners and contractors' confirmation has not been checked, certified or audited, which can be considered as a Security measure for personal data processing, but falls out of the scope of this thesis.

of the impact is important in breach management, which have tight deadlines for communication and notification. The supervisory authority notification within 72 hours of a breach shall include the categories and the approximate number of data subjects concerned (GDPR article 33 (3a)) and affected data subjects communication should be made to the data subjects concerned being aware of the proportionateness of the effort. GDPR required Register is expanded for the Enterprise with *inclusion of special categories* and *approximate amount of data subjects*.

The Register will describe the overall approach of the Enterprise from business perspective to processing data and will not present exact details of contracts that can deviate per client. The Register shall cover the data processed by the Enterprise for business purposes and not cover data that does not concern the purposes and operation of the Enterprise. For example, criminal convictions or offences data is not required, identified or requested for and during the operation of the Enterprise or fulfilling its purpose. If such data should fall into the hands of the Enterprise, it shall happen only by the Controller of such data. This data shall be processed in accordance with the personal data processing rules set in the Enterprise and notified to the public and the relevant agreements with the controller, if such have been made. The Enterprise will rely on the Controller bearing the responsibility in disclosing such data, being aware and accepting the Enterprises terms for such data processing.

4.2 Data Mapping and Personal Data Identification

In this section the data processing in the Enterprise is mapped covering information essential for the operation of the business. Comprehensive data mapping is important for the Enterprise in the long run, but is covered superficially during the course of this research, focusing in detail on areas of personal data processing in order to create records of processing required by GDPR. The areas most personal data is processed are described (in Estonian) in Appendix 2 – Data Processing Map – Enterprise and Appendix 3 – Data Processing Map – Clients, Marketing and Sales, and areas of less personal data processing following the same pattern refer to these descriptions.

The data processed for the daily operation of the Enterprise includes data from different sources both internally created, obtained from external sources and forwarded to external

organisations required by law, contracts or other grounds. The following sections will describe the nature, content and categories of data processed.

Data processed in the Enterprise is divided to the following categories:

a) Enterprise;

b) Clients;

c) Marketing and sales;

d) Products and services;

e) Partners and contractors.

Enterprise data will not be mapped to exhaustive detail, but only to the extent required for the identification of personal data. For example, products and services related data - lifecycle, pricing models, collaboration channels with partners - will not be specified further, because they do not contain personal data. As another example partners and contractors' data will include contact persons with their names, e-mail addresses etc. which is described in the Clients section and will not be duplicated in Partners and contractors section.

4.2.1 Enterprise

Enterprise data is data necessary for the Enterprise to operate as an organisation in Estonia, as an employer and as a place of conducting business. The data processed in the Enterprise is divided into the following areas:

a) General information;

b) Organisation operation;

c) Employees;

d) Work environment and tools.

General information about the Enterprise includes office contacts, address and other information to get in contact with the Enterprise. General information also includes data

about people representing the Enterprise, their contact details, position and authorisation to represent the enterprise.

Organisation operation related data includes the processes, functions and daily tasks information, that is not personalised and will not be covered in more detail in this research.

Data regarding the Enterprise employees contains the majority of different categories and specific details of data that can be related to a certain person. General employee data includes the information required to sign an employment contract like name, personal identification code, bank account number etc. Employee work profile data includes information about the qualification, area of expertise, work related contacts etc. Employee human resources related data includes employee candidate CV, personality profile and the state obligatory health check results. Employee accounting related data includes information about employee salary, training, business trips, work leave and holiday and benefits compensation. Work environment and tools data includes information about work computers and phones as well as equipment used for ensuring office space security.

The mindmap displaying the Enterprise category data processed is available in Estonian in Appendix 2 – Data Processing Map – Enterprise.

4.2.2 Clients

Data about the Clients of the Enterprise includes information about the organisation, services and products, contractual and accounting related data. Within these sub-categories there are three groups of persons whose data is processed concerning a Client:

a) Contact persons;

b) Client employees involved in the service or product;

c) The Enterprise employees.

Contact persons are the people officially representing the Enterprise (contract signing authorisation), the fundamental stakeholders and sponsors, people mediating information between the Enterprise and the Client organisation departments on a daily basis and supporting functions representatives (accounting, complaints, supervision). Data about contact persons include name, e-mail, phone, position, personal identification code etc.

Client employees may not be closely tied to the service or product provided, but can be affected by the client organisation purchasing the product or service performing their tasks as an employee. For example, if a client is utilising data loss prevention service that enforces rules and controls to sending data and documents outside the client organisation, some file size, type, or other restrictions could apply to the employee who is enable to publish the data to the target audience. In that case an alert may be created for the Enterprise, or the employee may wish to contact the Enterprise to create an exception for the intended document or the target of the data. Data about client employees include name, position, network address, device ID, username, service alert etc.

The third group of people involved in Client service or product data, are the Enterprise employees delivering the service, handling the requests of Client employees, dealing with product installation or maintenance. Performing these tasks is documented for reporting and accounting purposes for the Client and relevant partners and the state. Data about Enterprise employees is limited to name, general description of tasks performed, and hours spent on the described tasks.

The mindmap displaying the Clients category data processed is available in Estonian in Appendix 3 – Data Processing Map – Clients, Marketing and Sales.

4.2.3 Marketing and Sales

Data concerning marketing and sales is connected to public performances of the Enterprise (participation on a radio show discussion) or organised by the Enterprise (conference), promotional events related data, feedback and photo galleries of events. This data is about people from client organisations, Enterprise employees, partners and contractors. Employee work profile data published refers to data already mentioned in Enterprise employee category and reused here for the purposes of sales and marketing.

The mindmap displaying the Marketing and sales category data processed, is available in Estonian in Appendix 3 – Data Processing Map – Clients, Marketing and Sales.

4.2.4 Products and Services

Data about the Enterprise products and services includes information about different lines of products and services, their development, maintenance and training. It includes also information about licencing and relevant terms, pricing, equipment and warranties. Data

about products and services is created and maintained by employees and partners, but does not contain personal data and therefore not be specified in more detail in this thesis.

4.2.5 Partners and Contractors

Data about partners and contractors includes information about vendors', distributors', service providers' companies, their contacts, contracts and accounting information. Personal data is processed regarding partners' and contractors' representatives' names, e-mails, area of expertise etc. as described in section 4.2.2 Clients.

4.3 Records of Processing Personal Data

In this section personal data processing is described as required by GDPR in records of processing activities. The Register created during this research is (in Estonian) Appendix 1 – Records of Personal Data Processing Activities, and results described with reasoning provided for coming to these results, given in this chapter.

The first component of the Register is the name and contacts of the Processor and/or Controller, their representatives and data protection officers. For the Enterprise the partners and contractors (which can be Processors, Controllers or Joint Controllers) list includes the organisations with whom more data is exchanged, the interaction has been daily, or spans over several years. State institutions, that by law require personal data, contacts, representatives and data protection officers are not included in the Register, because these are published on the institution public web page and available if required.

The structure of the rest of the results produced in the Register with this research are built up of GDPR required components. Additional information beneficial for preparation for GDPR and maintaining compliance to relevant law as described in the analysis section 4.1.2 have been added to the Register. GDPR required components (columns) are marked with GDPR requirement in the Register.

The information given for each dataset of a sub-category is divided into the following components with GDPR required information marked by asterisk:

a) Data categories*;

b) Purpose for processing*;

c) Lawful basis for processing;

d) Reference to law condition;

e) Data source;

f) Retention period*;

g) Recipients of data*;

h) Transfer to third country (business purposes): yes or no*;

i) Information system;

j) Transfer to third country (technical limitation): yes or no;

k) Role in processing: controller, processor or joint controller;

l) Controller;

m) Controllers contacts;

n) Description of security measures*;

o) Containing special categories data: yes or no;

p) Approximate amount of data subjects.

4.3.1 Personal Data Categories

Data categories are based on the data mapping described in the section 4.2 specifying the types of personal data processed, the source the data was retrieved from or created for, the special treatment the category requires. Main data categories that include personal data are *clients*, *enterprise* and *partners and contractors*. Sub-categories under these are:

a) Contact persons – official contacts of a client or a partner in performing a project or functions;

b) Representative by law – person with the authorisation to represent an organisation in specific matters (sign a contract, negotiate terms, make payments etc.);

c) Potential client – prospective client of the Enterprise approached for marketing and sales purposes, whose contacts have been obtained by a third party or in the course of a previously concluded contract;

d) Reference client – client that has given their consent to publicly refer to the completed project and organisation, and in agreed circumstances forward the contact persons information to a potential client;

e) Service participant – employee of a client involved in fulfilling the contract;

f) Service provider – employee of the Enterprise performing tasks for a client project;

g) Employee – employee of the Enterprise;

h) Accounting – data regarding the Enterprise employee's wages, training, leave or health benefits;

i) Security camera – video footage of the Enterprise office for persons and property safety.

Under the sub-categories the Register lists the dataset processed. These are described and differentiated mainly based on the purpose for data processing following the data minimisation and purpose limitation principles in GDPR (only process and transfer the data required to fulfil the specific purpose in the specific situation and client). A large portion of datasets are a person's contact data name, e-mail, phone number, position and organisation, which are processed in contact with clients, partners, contractors, representatives and employees to maintain necessary communication to complete a project, close a deal or other standard business activities. Many datasets add one or few elements to the person's contacts depending on the specific purpose and organisation the data is received from or sent to. A significant portion of datasets of the Enterprise regarding employment relations are dictated by law to be forwarded to the relevant state institutions where the dataset has been defined by law. Enterprise business functions specific datasets are defined by the practical requirement and use of data – recruitment uses candidate CVs, sales and marketing uses employee qualification and picture etc.

4.3.2 Purposes of Data Processing

Purposes of personal data processing are derived from lawful basis for data processing, business functions or obligations placed on the Enterprise. The purposes of data processing for the Enterprise are:

a) Providing a service;

b) Compliance to law;

c) Sales and marketing;

d) Human resource and Enterprise internal management;

e) Fulfilling employment contract;

f) Encouraging employee healthy lifestyle;

g) Ensuring safety and security.

4.3.3 Lawful Basis for Data Processing

Lawful basis for each data category is chosen from the list provided in GDPR as grounds for personal data processing in article 6:

a) Contract or preparation for it;

b) Existing contract;

c) Consent;

d) Legal obligation;

e) Legitimate interests;

f) Vital interests.

Reference to local law condition describes the requirement imposed or the possibility allowed to use data for the purpose given for that category or to retain it for the period specified in the law.

4.3.4 Source of Data

Source of data described for each category is data subject, Controller, Processor or a public source. This information along with lawful basis (and reference to local law condition) can be used in the context of data subject requests to fulfil their rights and identify cases where the Enterprise cannot satisfy the request due to another obligation and can inform the data subject of the situation.

4.3.5 Retention Period

Retention period is set based largely on local law condition, because many documents containing personal data are the regulated by accounting, employment, health and safety acts. Source documents for accounting that shall be retained 7 years after the financial year of their creation, employment contracts 10 years after termination of employment, employee health checks are obligatory every 3 years etc. Data retention that is not regulated by law, is defined considering the purpose for data processing and data expiration by nature. Contacts of a potential client are erased after 1 year, candidates CVs are retained 2 years after a recruitment if the candidate provides consent for it, security camera recordings are overwritten in 6 months, publicly hosted events photo gallery is available for 5 years.

4.3.6 Recipients of Data

Recipients of data are described based on the function and role they fulfil. Recipients in the Register are generalised to the level of a target group of the information where the legal basis allows it, such as state institutions, open public (events, Enterprise representative), clients (marketing) or partners and contractors. Certain service providers that are well defined and are fulfilling a specific role or participating in a specific project, are described at the level of their service – marketing, accounting, legal services with the Processor contacts listed in the Register.

4.3.7 Transfer of Data to Third Countries

Forwarding to third countries is described from two viewpoints – business need and technical limitation as described in section 4.1.2 with the addition of the information system used to process data. The information system is described by business function or the owner of the information system – accounting system, customer relationship management system, public web, office collaborative platform etc.

From IT technical perspective (like databases, network security, encryption), this revealed the argument to distinguish data transferred to a third party or an international organisation between the business motive to transfer the data or the technical precondition that the data will be transferred further by a partner or a service provider. Here are 2 examples to illustrate:

a) if there is business motive to provide a service to an organisation outside EU, then the data of people providing the service is transferred to the other organisation to establish contact people who to turn to with questions and matters regarding the service;

b) if the organisation has chosen to use an IT service provider to fulfil their business goals like accounting, the service provider may choose to host the information system used to provide the service outside the EU for better prices. Then there is no innate motive to transfer the data outside EU, but is done by the service provider for better price offering.

4.3.8 Role in Processing

Enterprise role is defined by the roles of data processing described in GDPR – Controller, Processor or Joint Controller. Controllers for each data category are defined as the Enterprise, client or partner. Reference to controllers' and processors' contacts, as described in section 4.1.2, contain references where to find the contacts. The sources are client contract and first page in the Register listing the long-term service providers, or organisations with longer history of partnership with the Enterprise.

4.3.9 Description of Security Measures

Security measures used for data protection are assigned to the data category considering the sensitivity and the risk of processing the data as discussed in section 3.8. The security measures described in the Register are:

a) Secure communication channel;

b) Secure data transfer;

c) Secure data storage;

d) Secure data sharing;

e) Data processing in secured network;

f) Data processing audit log, analysis and management;

g) Assets physical protection;

h) Data backup;

i) Secure configuration of computers;

j) Raising security awareness;

k) Information security notification and application in the organisation.

4.3.10 Special Categories of Data

Inclusion of special categories data served as a control mechanism during the creation of the Register to pay attention and determine for each category whether special categories of data is processed and why. Processing health data is compulsory in employment relations and private contacts conversations or correspondence are likely to occur using office supplies but contemplating for each data category to avoid processing special categories of data where ever possible acted as an educational tool in the process. Special categories data did not prove to be as valuable and an instrumental component for the successive continuous use of the Register, but can be used further development, audit and reassessment.

4.3.11 Amount of Data Subjects

Approximate amount of data subjects for each category is described and nearly 2/3 of categories concern 20 people as the employees of the Enterprise, because this data is processed for different purposes on different lawful basis for different periods of times. Being clear for each data set of these parameters of processing raises the awareness of the Enterprise and urges to delete or anonymise data that has fulfilled the initial processing purpose. The categories concerning the most data subjects are service participants, client contact persons and potential clients. Service participants are typically client employees that have been developing, implementing or using the Enterprise services or products,

client contact persons have been addressed client events invitations and potential clients sent marketing material of the Enterprise's services and value offering.

4.4 Activities Description by Category

This section describes the content of activities of the Register by the main data categories. The description is generalised and does not strive to list each detail of processing activities duplicating the Register, but characterises the processing performed under each category.

4.4.1 Enterprise Data

Enterprise data is the category of the largest amount and extent of personal data processing compared to other categories. Personal data is processed for all purposes included in the Register - employment relationship management, providing a service, sales and marketing, fulfilling a contract, consent, and ensuring safety and security etc. The lawful basis include all listed in the Register apart from vital interests. Reference to law condition includes accounting, occupational health and safety and employment contracts act. Data source is mainly the data subject, but some information is received from a Processor if such a service has been used (such as recruitment). Data retention period is dictated largely by state law (employment and accounting) of 7 or 10 years, the end of contract, marketing or sales related events of 5 years, or at the end of a recruitment or by the consent of the data subject for 2 years. The recipients of the data include state institutions and cover the service providers of the Enterprise – accounting, marketing, partner. The recipients are also the general public for sales and marketing purposes. Recipients of data cover most of the service providers and partners of the Enterprise, including transfer to third countries and organisations outside EU (where the partners operate). The role of the Enterprise is Controller and the contact details of the Controller are given in the Register. Security measures applied cover the whole of measures applied in the Enterprise according to the channel and tool used to process the data. Special categories of data is processed to the extent compulsory by law. The approximate amount of data subjects concerned is 20 extending to the existing employees as well as past employees, the Enterprise is obliged to retain data about.

4.4.2 Clients

Clients can be existing, historical or prospective clients, or based on a mutual agreement of terms, they are reference clients willing to share their experience of a project conducted or years of satisfying cooperation with the Enterprise to new and prospective clients. The purpose and legal basis for processing Client data is different for current existing clients, prospective clients and for reference clients and therefore described as different categories of client data in the Register.

The processing of client data is largely for the purpose of providing a service for the client based on a contract. The second largest purpose is sales and marketing in order to sign a contract and provide services. Lawful basis of processing due to that is contract or preparation for it. Reference to a law condition in several cases is connected to retention period of accounting source documents of 7 years. In other cases the retention period is derived from the purpose of processing – for marketing, the data is retained for 5 years of events information publishing or 1 year of potential clients. As data recipients, with client data the Processors are service providers of the Enterprise, the general public of events or other contractors and partners. Data transfers to third countries or international organisations are to partners operating outside the EU. In most cases the Controller is the Enterprise with the exception of client employees. The Processor contact information is defined in the contract and security measures applied are reflect the mostly IT technical tools used to process the data (information system). Processing special categories of data is performed in the case of preferences of the data subject for marketing and sales purposes, if the data subject has revealed such information based on consent. The approximate amount of data subjects is dependent of the specific client, contract or service details.

4.4.3 Partners and Contractors

Partners and contractors' data processing purposes are fulfilling a contract, sales and marketing, and ensuring security and safety. The lawful basis for data processing include contract or preparation for it or legitimate interests in order to fulfil the purpose of the processing. Data source is mainly the data subject or the Processor for whom the data subject is working for. Retention period is derived of the sales and marketing purposes and for 5 years in order to engage in further projects and contracts. The recipients of data are the general public and service providers of the Enterprise in order to promote the

services of the Enterprise, and a specific (potential) client interested in further details of a service. Recipients of data is dependent on the information system used to process the data, and in some cases forwarded to a third country or an international organisation of the partner if the partner is operating outside EU or using an information system ranging beyond EU. The Controller is mainly the partner as well as the Enterprise (Joint Controllers), because the partnership serves both organisations interest and goals. Contacts of the Processor are listed in the contract between the organisations and/or the Register and security measures derived from the information system and the environment the data is processed in. There is no special categories of personal data from partners and contractors processed and the amount of data subjects is directly connected to the partner organisation and contact persons disclosed.

4.5 Results Further Application

The results can be applied in the Enterprise to demonstrate GDPR compliance and to explain the manner and extent of processing personal data. The Register can be made available to the supervisory authority in electronic form and using free software tools as required by AKI.

Developing the Register the Enterprise has obtained insight into GDPR requirements and the supplemental source information to optimise its operation:

a) The enterprise has prevented allocating excessive resource in upholding more than one Register;

b) The added component of lawful basis in the Register expanded the perception of law obligating the Enterprise processing, and gathered the requirements for retaining personal data;

c) Analysing data transfer to other processors, revealed the distinction of data transfer motivation and risks, differentiating transfers for business purposes and as a result of using an IT tool;

d) Describing the processing of special categories data scrutinised the business need against the actual data processing activities and restrained from excessive data processing;

Assessing the amount of data subjects under each category enables assessing the adequacy of security measures applied in addition to reacting to data breaches

The results delivered in this research are derived of GDPR and the Enterprise context. The analysis and interpretation of requirements are applicable to organisations operating in the same industry and area of operation of the Enterprise and with modification regarding the organisation can be applied to another organisation. As can be perceived from GDPR requirements and the lack of one-size-fits-all solutions in achieving GDPR compliancy, the results application to other organisations is limited. Each solution developed to comply with GDPR requirements, by the Author's interpretation, is unique and needs to be adjusted to the specific organisation. Reusing the developed Register, should be approached considering the organisation context, but the analysis, the deliberation and the discussion, can provide insight for any organisation processing personal data. Taking into account that the full extent of purposes, lawful basis, security measures applied, and the majority of information systems used by the Enterprise, are processing personal data, any organisation employing data subjects, can reuse these categories and activities descriptions to create their Registers.

The results are more difficult to be reused in a public service provider, because the regulation affecting public services extends to numerous other state acts not reflected in this research, processing data of subjects without choice of a service provider. In those cases, a more thorough legal analysis is needed mapping of relevant regulation (obligation to process extensive data, restriction or exemption for retaining period etc).

4.6 Future Research Areas

Creating a Register numerous aspects of further research questions arose from the previously existing materials and validation of the sources and results, as well as from the Enterprise operation efficiency and choices.

Data ownership and protection responsibility is a fundamental issue in protecting personal data. Identifying who owns the data is a pressing matter in determining who is, or should be held responsible for protecting it. Different sources indicate different positions on data ownership, another layer is placed on the matter with who can and is able to protect it during processing. GDPR states the processors' responsibility which covers a significant

area for the data subject, who in many cases, is the lesser force (compared to global corporations) driving the course of data processing in the era of big data. Who owns the data and who is held responsible is a topic for further research.

With the globalisation of data processing, corporations and service providers extend their grasp to data subjects across states and local law. Business driven consumers expansion may serve the interests of the organisation, but different rules of processing personal data affect the business decisions and strategy. An organisation processing personal data most likely takes advantage of the variety of service providers across the globe, but most likely has given little deliberation of the consequences of different legal aspects accompanied by the liberties. GDPR urges to focus on this topic by inspecting the role of a Processor as a service provider. A service provider is tempted to utilize the global liberties but shall consider the contractors restrictions empowered by GDPR and fundamentally the data subject. IT service providers will have to reconsider the customers location and prepare for the data subjects' rights for limiting processing upon request, data portability and deletion. An organisation using an international service provider is responsible for adherence to GDPR and validating adherence of the Processor. If the Processor is unable to prove adherence to GDPR, losing the customer can be the result. From a Controller's perspective, choosing another, GDPR compliant service provider is a preferred choice. What are the criteria to choose a GDPR compliant service provider and how to validate adherence is a topic for further research.

The supervisory authorities across the EU, take a slightly different approach to GDPR considering local law, and assessing GDPR compliance will reflect this. Assessing compliance is a case by case tightly context driven issue. The Registers created by organisations, are strongly founded on the interpretation of GDPR requirements, and in addition to supervisory authority specific guidelines, the accredited approach will evolve in due course also based on court rulings. The assessment of Registers created, and the sufficiency of their comprehension, is yet to be determined by precedent made by the authorities. What is the sufficiently substantiated Register to aspire to, will remain a topic for further research and court rulings.

5 Summary

The General Data Protection Regulation (GDPR) of the European Union regarding personal data protection is applicable from May 25th 2018 to processing data of natural persons. Organisations processing personal data shall adhere to the requirements set in the regulation and ensure transparency in their processing activities.

The goal of this research was to create records of processing activities required by GDPR for a case study enterprise to enable displaying GDPR compliance. The research focused on analysing the steps to take to create the Register, different aspects affecting creating it, and revealing any further application opportunities and practical benefits of the Register to the Enterprise.

The research analysed documents and guidelines from a wide range of sources from the authorities of different states and the European Union to an existing Register example. The case study of the Enterprise included observing data processing activities and interviewing the Enterprise employees and service providers. Combining the insight from documents and adjusting it to the Enterprise specific context, the method for creating a Register was developed, and a Register created by the developed method.

The research described the context and background of personal data processing requirements, existing examples and guidelines, and possible alternative solutions contribution to the creation of the Register. The analysis firstly identified the steps to take in preparing for GDPR and the role of the Register in displaying compliance to GDPR. Next, the obligation of the Enterprise to create a register was established and the GDPR requirements for the Register content were analysed. The approaches to break down categories of personal data processing were analysed to create the structure of the Register, and previously existing examples of registering personal data processing were analysed to re-use and learn from insight obtained. The business consideration of data processing volume and the challenges accompanying in protecting these assets was analysed, and the motivation and design of a combined Register for business efficiency was proposed. Local state level acts and guidelines were analysed to identify if and how

these restrict or obligate personal data processing by the Enterprise, increasing the practical value of the Register and enabling transparency in personal data processing beyond GDPR. The characteristics of the Enterprise were described to better enable interpreting the content of the Register and to understand the influence of the Enterprise specifics to the content. The results of the research provided the method and consideration of developing a Register by first mapping the overall data processing and extracting personal data processing activities from that. The goal of the research was achieved by creating a Register for the Enterprise, that records personal data processing activities required by GDPR. Further work on the Register may be required after the enforcement of the local personal data protection act.

The Author believes that the research reveals the process of creating a Register, equipped the Enterprise with more than knowledge of GDPR requirements and the aspired tool for demonstrating GDPR compliance:

- Combining the Registers components, that were different for different roles of processing, enabled to ensure better efficiency in maintaining the Register;
- Describing additional components in the Register for each data category enabled to identify the underlying sources defining requirements for data processing;
- Analysis of transferring data to other organisations raised the question of reassessing the choice of service providers or IT tools used by the Enterprise;
- Listing processing of special categories of data acted as a check to keep track of and to eliminate excessive sensitive data processing;
- Assessing the amount of data subjects under each category enables assessing the adequacy of security measures applied in addition to reacting to data breaches.

Areas for further research identified include practical aspects from an organisation's point of view such as how to choose and validate a GDPR compliant service provider, and the assessment of what is a sufficient Register by a supervisory authority. On a more theoretic level, the responsibility of protecting personal data depends on who owns it. GDPR has not addressed data ownership issues, which in further research could shift the comprehension of data protection for organisations, natural persons and the authorities.

References

[1] Andmekaitse Inspektsioon. *Andmekaitsealane mõjuhinnang.* [Online]. Available at http://www.aki.ee/et/andmekaitse-reform/mis-andmekaitsealane-mojuhinnang. [Accessed 17.06.2017]

[2] Andmekaitseinspektsioon. *Delikaatsed isikuandmed.* [Online] Available at http://www.aki.ee/et/delikaatsed-isikuandmed. [Accessed 30.03.2018].

[3] Andmekaitseinspektsioon. *Don't panic. How to be compliant with the new GDPR in 5 steps.* [Online]. Available at https://e-estonia.com/how-to-be-compliant-gdpr-5-steps/. [Accessed 26.02.2018].

[4] Andmekaitseinspektsioon. *Isikuandmete töötlemine töösuhetes*. [Online] Available at http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/Isikuandmed%20t%C3%B6%C3%B6suhetes%20juhendmaterjal26%2005%202014.pdf. [Accessed 10.02.2018].

[5] Andmekaitseinspektsioon. *Isikuandmete töötlemine töösuhetes, abistav juhendmaterjal.* [Online]. Available at http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/Personal%20Data%20in%20employment%20eng.pdf. [Accessed 19.02.2018].

[6] Andmekaitseinspektsioon. *Kindlustusasutused ja krediidiasutused. Näidisvorm.* [Online]. Available at http://www.aki.ee/et/abiks-vastutavale-isikule-andmetootlusregistri-koostamisel. [Accessed 30.03.2018]

[7] Andmekaitseinspektsioon. *Sideettveõtted. Näidisvorm.* [Online]. Available at http://www.aki.ee/et/abiks-vastutavale-isikule-andmetootlusregistri-koostamisel. [Accessed 30.03.2018]

[8] Andmekaitseinspektsioon. *Turvaettevõtted, õigusabi osutajad. Näidisvorm.* [Online]. Available at http://www.aki.ee/et/abiks-vastutavale-isikule-andmetootlusregistri-koostamisel [Accessed 30.03.2018]

[9] Andmekaitse Inspektsioon. *Töötlustoimingute registreerimine.* [Online]. Available at http://www.aki.ee/et/andmekaitse-reform/tootlustoimingute-registreerimine. [Accessed 20.12.2017].

[10] Andmekaitseinspektsioon. *Töötlemistoimingute registri näidised.* [Online] Available at http://www.aki.ee/et/tootlustoimingute-registreerimine/tootlemistoimingute-registri-naidised. [Accessed 11.04.2018].

[11] Andmekaitse Inspektsioon. *Uus kohustus ettevõttele – isikuandmete töötlemise register*. [Online]. Available at http://www.aki.ee/et/uudised/pressiteated/uus-kohustus-ettevotetele-isikuandmete-tootlemise-register. [Accessed 19.03.2018].

[12] Article 29 Working Party. *Article 29 Data Protection Working Party*. [Online]. Available at http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358. [Accessed 3.02.2018]

[13] Article 29 Working Party. *Guidelines*. [Online] Available at http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1360&tpa_id=6936. [Accessed 14.03.2018].

[14] Buchel, C. Panel 1: "Who owns the data?". Presented at Tarkvõrgu konverents, Tallinn, 18.09.2017.

[15] Data Protection Commissioner. *The GDPR and You, General Data Protection Regulation.* [Online] Available at https://www.dataprotection.ie/docimages/documents/The%20GDPR%20and%20You.pdf. [Accessed 16.04.2018].

[16] Directive 95/46/EC of the European Parliament and of the Council of 24th October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. [Online]. Available at http://eur-lex.europa.eu/legal-content/ET/TXT/HTML/?uri=CELEX:31995L0046&qid=1521379872004&from=ET. [Accessed 19.01.2018].

[17] *Draft Cyber Security Act*. [Online]. Available at https://eelnoud.valitsus.ee/main/mount/docList/775b7e36-09e2-480f-9217-81fb79ed293b. [Accessed 9.03.2018].

[18] Eelnõude infosüsteem. *Isikuandmete kaitse seaduse eelnõu*. [Online]. Available at http://eelnoud.valitsus.ee/main/mount/docList/1909e111-ca98-4d1b-830a-ee49dea64a97#BKGJmJCo. [Accessed 26.02.2018].

[19] *Electronic Communications Act*. [Online]. Available at https://www.riigiteataja.ee/en/eli/521082017008/consolide. [Accessed 11.03.2018].

[20] *Employment Contracts Act*. [Online]. Available at https://www.riigiteataja.ee/en/eli/518122017004/consolide#para59. [Accessed 12.02.2018].

[21] European Commission. *It's your data – take control - data protection in the EU*. [Online] Available at https://ec.europa.eu/commission/sites/beta-political/files/data-protection-overview-citizens_en.pdf. [Accessed 17.04.2018].

[22] Government of Estonia. *The system of security measures for information systems*. Regulation. [Online]. Available at https://www.ria.ee/public/ISKE/Regulation-the-system-of-security-measures-for-information-systems-2007-12-20.pdf. [Accessed 10.03.2018].

[23] *Handbook on European Data protection law*. European Union Agency for Fundamental Rights, Council of Europe and Registry of the European Court of Human Rights. 2013. [Online]. Available at https://rm.coe.int/16806b294a. [Accessed 11.02.2017].

[24] Information Commissioner's Office. *Documentation template for controllers.* [Online] Available at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/documentation/. [Accessed 28.03.2018].

[25] Information Commissioner's Office. *Documentation template for processors.* [Online] Available at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/documentation/. [Accessed 28.03.2018].

[26] Information Commissioner's Office. *How do we document our processing activities*. [Online] Available at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/documentation/how-do-we-document-our-processing-activities/. [Accessed 28.03.2018].

[27] Information Security Forum Limited. *Preparing for the General Data Protection Regulation: Implementation Guide.* [Online]. Available at https://www.securityforum.org/research/preparing-for-thementation-guide/. [Accessed 10.02.2018].

[28] Justiitsministeerium. *Isikuandmete kaitse seaduse rakendamise seaduse eelnõu*. [Online] Available at https://eelnoud.valitsus.ee/main/mount/docList/f73f1d4e-17b8-4408-9112-6c10d337aaeb [Accessed 15.03.2018].

[29] Majandus- ja Kommunikatsiooniministeerium. *Kübervaldkonna seaduse väljatöötamise kavatsus*. 2017. [Online]. Available at https://eelnoud.valitsus.ee/main/mount/docList/e7ff643b-8b72-4a70-8f3e-dab03f9ca79f. [Accessed 11.03.2018].

[30] Riigi Infosüsteemide Amet. *Infosüsteemide kolmaeastmelise etalonturbe süstemi ISKE rakendusjuhend.* [Online]. Available at https://www.ria.ee/public/ISKE/ISKE_rakendusjuhend.pdf. [Accessed 10.03.2018].

[31] Riigi Infosüsteemide Amet. *Infosüsteemide turvameetmete süsteem.* [Online]. Available at https://www.riigiteataja.ee/akt/13125331. [Accessed 6.03.2018].

[32] *Occupational Health and Safety Act*. [Online]. Available at https://www.riigiteataja.ee/en/eli/505052017007/consolide#para14 [Accessed 12.02.2018].

[33] *Personal Data Protection Act*. [Online]. Available at https://www.riigiteataja.ee/en/eli/507032016001/consolide#para14. [Accessed 12.02.2018].

[34] Pild, M. "Triniti hommikuseminar – Andmekaitsemäärusest ettevõtjale," Triniti Estonia, Tallinn, 14.03.2018.

[35] PricewaterhouseCoopers. "Isikuandmete kaitse üldmäärus – kas oled valmis?" Presented in Atea Hommikuseminar, Tallinn, 30.05.2017.

[36] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and of the free movement of such data, and repealing directive

95/46/EC. [Online]. Available at http://eur-lex.europa.eu/legal-content/ET/TXT/HTML/?uri=CELEX:32016R0679&from=ET. [Accessed 11.05.2017].

[37] Roessing, R.v. *Implementing the General Data Protection Regulation*. ISACA, 2018. [Online] Available at http://www.isaca.org/Knowledge-Center/Pages/default.aspx. [Accessed 26.03.2018]

[38] Sallinen, J. "What does GDPR mean to: Companies, Organizations and Management?". Presented in Conf. Infoturbe Summit, Tallinn, 10.05.2017.

[39] *Security Act.* [Online]. Available at https://www.riigiteataja.ee/en/eli/521062017007/consolide. [Accessed 19.02.2018].

[40] Security Software. *Enterprise introduction.* Published for prospective contractors and clients.

[41] Security Software. *Kontatkid.* [Online]. Available at https://secsoft.ee/kontakt/. [Accessed 18.12.2017].

[42] Tietosuojavaltuutetun toimisto. *Mallipohja rekisterinpitäjälle: selosta käsittelytoimista.* [Online] Available at http://www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltutetuntoimisto/lomakkeet/T9VSTMX2N/Mallipohja_rekisterinpitajalle.xlsx. [Accessed 30.03.2018].

[43] Äripäev AS. *Firmast.* [Online]. Available at http://firma.aripaev.ee/firmast/?kmi=mmKRTZr2xjPT69eaX83L5xKft00%3D. [Accessed 11.04.2018].

[44] Äripäev AS. *Äripäev AS Töötlemistoimingute register.* [Online] Available at https://www.aripaev.ee/materjalid/Tootlemistoimingute_register_Aripaev.pdf. [Accessed 6.04.2018].

Appendix 1 – Records of Personal Data Processing Activities

Ettevõte

Nimi	Security Software OÜ
Aadress	Pärnu mnt 139f, 11317 Tallinn
Telefon	+372 669 9707
E-mail	info@securitysoftware.ee
Esindaja	*konfidentsiaalne*
Andmekaitsespetsialist	*konfidentsiaalne*

Volitatud töötlejad, koostööpartnerid

Raamatupidamisteenuse osutaja

Nimi	*konfidentsiaalne*
Aadress	*konfidentsiaalne*
Telefon	*konfidentsiaalne*
E-mail	*konfidentsiaalne*
Esindaja	*konfidentsiaalne*
Andmekaitsespetsialist	*konfidentsiaalne*

Sideteenuse osutaja

Nimi	*konfidentsiaalne*
Aadress	*konfidentsiaalne*
Telefon	*konfidentsiaalne*
E-mail	*konfidentsiaalne*
Esindaja	*konfidentsiaalne*
Andmekaitsespetsialist	*konfidentsiaalne*

Turundusteenuse osutaja

Nimi	*konfidentsiaalne*
Aadress	*konfidentsiaalne*
Telefon	*konfidentsiaalne*
E-mail	*konfidentsiaalne*
Esindaja	*konfidentsiaalne*
Andmekaitsespetsialist	*konfidentsiaalne*

Kontoriruumi haldusteenuse osutaja

Nimi	*konfidentsiaalne*
Aadress	*konfidentsiaalne*
Telefon	*konfidentsiaalne*
E-mail	*konfidentsiaalne*
Esindaja	*konfidentsiaalne*
Andmekaitsespetsialist	*konfidentsiaalne*

Koostööpartner

Nimi	*konfidentsiaalne*
Aadress	*konfidentsiaalne*
Telefon	*konfidentsiaalne*
E-mail	*konfidentsiaalne*
Esindaja	*konfidentsiaalne*
Andmekaitsespetsialist	*konfidentsiaalne*

Personaliteenuse osutaja

Nimi	*konfidentsiaalne*
Aadress	*konfidentsiaalne*
Telefon	*konfidentsiaalne*
E-mail	*konfidentsiaalne*
Esindaja	*konfidentsiaalne*
Andmekaitsespetsialist	*konfidentsiaalne*

Juriidilise teenuse osutaja

Nimi	*konfidentsiaalne*
Aadress	*konfidentsiaalne*
Telefon	*konfidentsiaalne*
E-mail	*konfidentsiaalne*
Esindaja	*konfidentsiaalne*
Andmekaitsespetsialist	*konfidentsiaalne*

Tervishoiuteenuse osutaja

Nimi	*konfidentsiaalne*
Aadress	*konfidentsiaalne*
Telefon	*konfidentsiaalne*
E-mail	*konfidentsiaalne*
Esindaja	*konfidentsiaalne*
Andmekaitsespetsialist	*konfidentsiaalne*

GDPR nõue	GDPR nõue		GDPR nõue				GDPR nõue	GDPR nõue	GDPR nõue					GDPR nõue	GDPR nõue		
Kategooria	Alamkategooria	Andmed	Eesmärk	Õiguslik alus	Õigusakti viide	Andmeallikas	(Säilitamis-tähtaeg)	Volitatud töötlejad ja andmete edastamine 3 osapoolele (kontaktid kättesaadavad registri esilehelt)	3 riikidesse edastamine (äriline vajadus)	Infosüsteem	3 riikidesse edastamine (tehniline piirang)	Ettevõtte roll	Vastutav töötleja	Vastutava töötleja kontaktid	(Turvameetmete kirjeldus)	Eriliigiliste / tundlike andmete sisaldumise võimalus	Andme-subjektide hulk (ligikaudne suurusjärk)
Kliendid	Seaduslik esindaja	Nimi, positsioon, isikukood	Teenuse osutamine	Leping või ettevalmistamine	KMS §36 arvete säilitamine 7 a	Vastutav töötleja	7 a peale lepingu lõppu	Juriidilise teenuse osutaja Raamatupidamisteenuse osutaja	Ei	Raamatupidamissüsteem	Ei	Volitatud töötleja	Klient	Kliendilepingus Töötleja kontaktide lehel registris	Turvaline andmeedastus/vahetus Turvaline andmete ühiskasutus Andmete kasutamise kontrolljälgede salvestamine, analüüs ja reageerimine Organisatsiooni varade füüsiline turve Turvaline tööjaamade ja serverite häälestus	Ei	*konfidentsiaalne*
Kliendid	Kontaktisikud	Nimi, e-post, telefon, organisatsioon, positsioon	Teenuse osutamine	Leping või ettevalmistamine	KMS §36 arvete säilitamine 7 a	Vastutav töötleja	7 a peale lepingu lõppu	Juriidilise teenuse osutaja Raamatupidamisteenuse osutaja Koostööpatner	Jah	Raamatupidamissüsteem CRM Partneri infosüsteem	Jah	Volitatud töötleja	Klient	Kliendilepingus Töötleja kontaktide lehel registris	Turvaline andmete ühiskasutus Varukoopiate turvaline salvestus Turvaline tööjaamade ja serverite häälestus	Ei	*konfidentsiaalne*
Kliendid	Kontaktisikud	Üritusel osalemine, fotogalerii	Turundus ja müük	Õigustatud huvi		Andmesubjekt	5 a	Avalikkus Turundusteenuse osutaja Kliendid Koostööpartner	Jah	Välisveeb Kontoritarkvara	Jah	Vastutav töötleja	Ettevõte	Töötleja kontaktide lehel registris	Turvaline andmete ühiskasutus Andmete kasutamise kontrolljälgede salvestamine, analüüs ja reageerimine Varukoopiate turvaline salvestus Turvaline tööjaamade ja serverite häälestus	Ei	u 300
Kliendid	Kontaktisikud	Ürituse tagasiside, tagasiside andja kontaktid, organisatsioon	Teenuse osutamine	Õigustatud huvi		Andmesubjekt	5 a	Turundusteenuse osutaja Koostööpartner	Jah	Kontoritarkvara	Jah	Vastutav töötleja	Ettevõte	Töötleja kontaktide lehel registris	Turvaline andmesalvestus Turvaline andmete ühiskasutus Andmete kasutamise kontrolljälgede salvestamine, analüüs ja reageerimine Turvaline tööjaamade ja serverite häälestus	Ei	*konfidentsiaalne*
Kliendid	Kontaktisikud	Avalik võti krüpteerimiseks	Turvalisuse tagamine	Õigustatud huvi		Vastutav töötleja	3 a peale lepingu lõppu	-	Ei	Raamatupidamissüsteem	Ei	Vastutav töötleja	Ettevõte	Kliendilepingus Töötleja kontaktide lehel registris	Turvaline andmeedastus/vahetus Turvaline andmesalvestus Turvaline tööjaamade ja serverite häälestus	Ei	u 20
Kliendid	Kontaktisikud	Nimi, e-post, telefon, organisatsioon, positsioon	Turundus ja müük	Nõusolek	ESS §103 pr 1 lubatud olemasoleva kliendile sarnase teenuse pakkumisel (kui on iga kord võimalik keelduda)	Vastutav töötleja	7 a peale lepingu lõppu	Turundusteenuse osutaja	Ei	Raamatupidamissüsteem CRM	Jah	Vastutav töötleja	Ettevõte	Töötleja kontaktide lehel registris	Turvaline andmete ühiskasutus Varukoopiate turvaline salvestus Turvaline tööjaamade ja serverite häälestus	Ei	*konfidentsiaalne*
Kliendid	Kontaktisikud	Isiklikud eelistused	Turundus ja müük	Nõusolek		Andmesubjekt	3 a peale lepingu lõppu	-	Ei	Raamatupidamissüsteem CRM	Jah	Vastutav töötleja	Ettevõte	Töötleja kontaktide lehel registris	Turvaline andmeedastus/vahetus Turvaline andmesalvestus Turvaline andmete ühiskasutus Andmete kasutamise kontrolljälgede salvestamine, analüüs ja reageerimine Varukoopiate turvaline salvestus Turvaline tööjaamade ja serverite häälestus	Jah	*konfidentsiaalne*
Kliendid	Potentsiaalne klient	Nimi, e-post, telefon, organisatsioon, positsioon	Turundus ja müük	Leping või ettevalmistamine		Vastutav töötleja	1 a	Turundusteenuse osutaja	Ei	Teenusepakkuja keskkond	Jah	Kaasvastutav töötleja	Ettevõte	Töötleja kontaktide lehel registris	Turvaline andmesalvestus Turvaline andmete ühiskasutus Andmete kasutamise kontrolljälgede salvestamine, analüüs ja reageerimine Turvaline tööjaamade ja serverite häälestus	Ei	*konfidentsiaalne*
Kliendid	Referentsklient	Nimi, e-post, telefon, organisatsioon	Turundus ja müük	Nõusolek		Vastutav töötleja	5 a peale lepingu lõppu või vastavalt kokkuleppele kliendiga	Avalikkus Turundusteenuse osutaja Kliendid Koostööpartner	Jah	Välisveeb Kontoritarkvara	Jah	Vastutav töötleja	Ettevõte	Töötleja kontaktide lehel registris	Turvaline andmete ühiskasutus Andmete kasutamise kontrolljälgede salvestamine, analüüs ja reageerimine Turvaline tööjaamade ja serverite häälestus Turvateadlikkuse tõstmine Infoturbe teadvustamine ja rakendamine kogu organisatsiooni tasemel	Ei	u 20

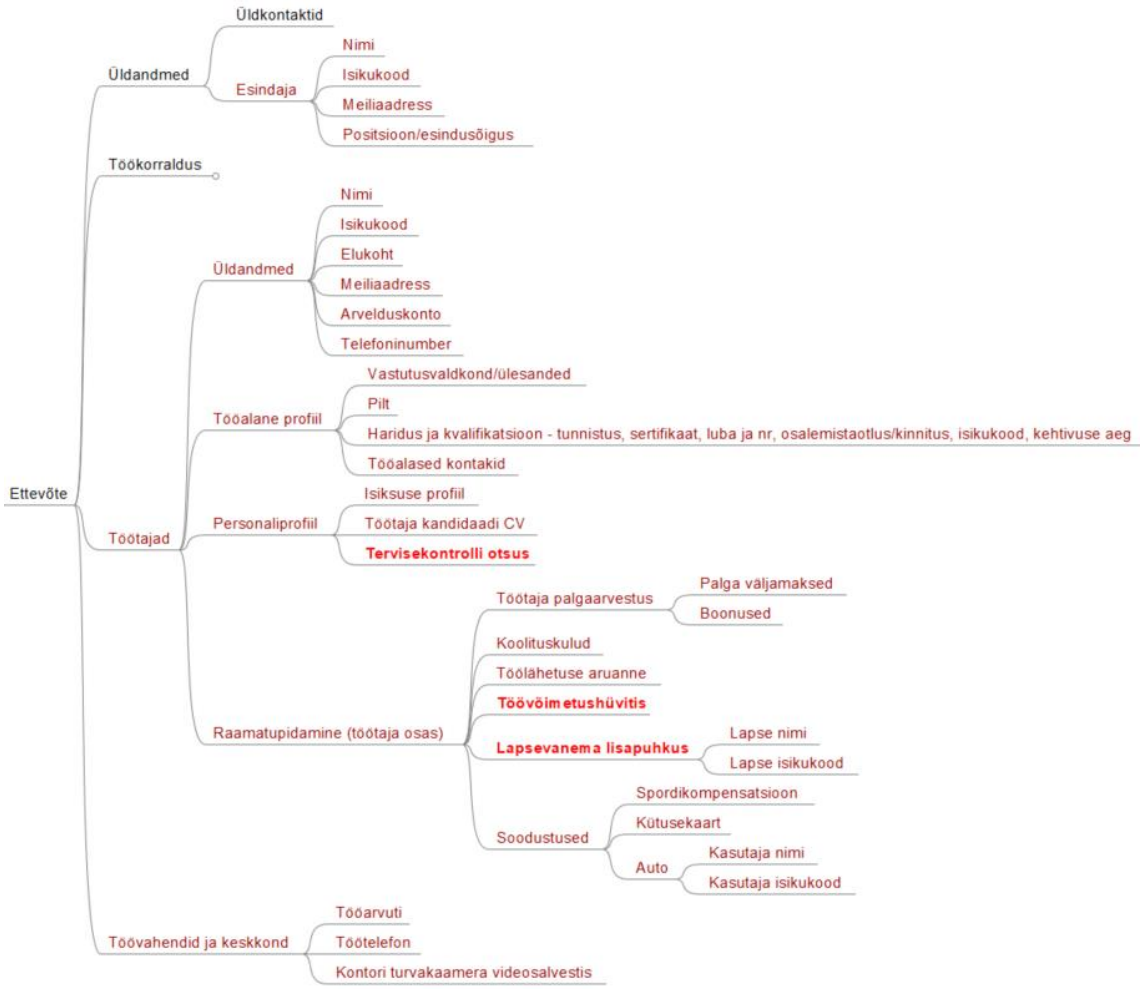
Kliendid	Töödes osaleja	Nimi, organisatsioon, positsioon, e-post, telefon, võrguaadress, kasutajanimi, seadme nimi, teenuse sündmus	Teenuse osutamine	Leping või ettevalmistamine		Vastutav töötleja	1 a peale lepingu lõppu või vastavalt kokkuleppele kliendiga	-	Ei	Grupitöö keskkond Toote halduskeskkond	Jah	Volitatud töötleja	Klient	Kliendilepingus	Turvalise andmesidekanali kasutamine Turvaline andmeedastus/vahetus Turvaline andmesalvestus Turvaline andmete ühiskasutus Andmete kasutamine organisatsiooni sisevõrgus Andmete kasutamise kontrolljälgede salvestamine, analüüs ja reageerimine Organisatsiooni varade füüsiline turve Varukoopiate turvaline salvestus Turvaline tööjaamade ja serverite häälestus Turvateadlikkuse tõstmine Infoturbe teadvustamine ja rakendamine kogu organisatsiooni tasemel	Ei	*konfidentsiaalne*
Kliendid	Töö teostaja	Nimi, e-post, töötundide maht, tööde kirjeldus	Teenuse osutamine	Seadus	RPS §12 lg 1 tööaja arvestus, palgalehed, lähetuskorraldused jms raamatupidamise algdokumentide säilitamine 7 a	Vastutav töötleja	7 a	Raamatupidamisteenuse osutaja	Ei	Raamatupidamissüsteem	Jah	Vastutav töötleja	Ettevõte	Töötleja kontaktide lehel registris	Turvaline andmeedastus/vahetus Turvaline andmesalvestus Turvaline andmete ühiskasutus Andmete kasutamise kontrolljälgede salvestamine, analüüs ja reageerimine Varukoopiate turvaline salvestus Turvaline tööjaamade ja serverite häälestus	Ei	u 20
Kliendid	Töö teostaja	Nimi, e-post, töötundide maht, tööde kirjeldus	Teenuse osutamine	Leping või ettevalmistamine		Vastutav töötleja	7 a	Raamatupidamisteenuse osutaja	Ei	Kontoritarkvara Grupitöö keskkond Raamatupidamissüsteem Toote halduskeskkond	Ei	Vastutav töötleja	Ettevõte	Töötleja kontaktide lehel registris	Turvalise andmesidekanali kasutamine Turvaline andmeedastus/vahetus Turvaline andmesalvestus Turvaline andmete ühiskasutus Andmete kasutamine organisatsiooni sisevõrgus Andmete kasutamise kontrolljälgede salvestamine, analüüs ja reageerimine Organisatsiooni varade füüsiline turve Varukoopiate turvaline salvestus Turvaline tööjaamade ja serverite häälestus Turvateadlikkuse tõstmine Infoturbe teadvustamine ja rakendamine kogu organisatsiooni tasemel	Ei	*konfidentsiaalne*
Kliendid	Töö teostaja	Avalik või krüpteerimiseks	Turvalisuse tagamine	Õigustatud huvi		Andmesubjekt	7 a	-	Jah	Raamatupidamissüsteem	Ei	Vastutav töötleja	Ettevõte	Töötleja kontaktide lehel registris	Turvaline andmeedastus/vahetus Turvaline andmesalvestus Turvaline tööjaamade ja serverite häälestus	Ei	u 20
Ettevõte	Esindaja	Nimi, e-post, isikukood, esindusõigus	Teenuse osutamine	Leping või ettevalmistamine		Vastutav töötleja	7 a peale esindusõiguse lõppu	Asjakohased riigiasutused Kliendid Koostööpartner Turundusteenuse osutaja Raamatupidamisteenuse osutaja Juriidilise teenuse osutaja Personaliteenuse osutaja	Jah	Raamatupidamissüsteem Partneri infosüsteem Kontoritarkvara	Jah	Vastutav töötleja	Ettevõte	Töötleja kontaktide lehel registris	Turvaline andmeedastus/vahetus Turvaline andmesalvestus Andmete kasutamise kontrolljälgede salvestamine, analüüs ja reageerimine Varukoopiate turvaline salvestus Turvaline tööjaamade ja serverite häälestus	Ei	u 5
Ettevõte	Esindaja	Nimi, e-post, isikukood	Seaduse täitmine	Seadus	RPS §12 lg 2 Raamatupidamislike aruannete säilitamine 7 a	Vastutav töötleja	7 a peale esindusõiguse lõppu	Asjakohased riigiasutused	Ei	Kontoritarkvara	Jah	Vastutav töötleja	Ettevõte	Töötleja kontaktide lehel registris	Turvaline andmeedastus/vahetus Turvaline tööjaamade ja serverite häälestus	Ei	u 5
Ettevõte	Töötajad	Nimi, isikukood, elukoht, eraisiku e-post, arvelduskonto	Töölepingu täitmine	Leping või ettevalmistamine	TLS §5 lg5 töölepingu säilitamine 10 a	Andmesubjekt	10 a peale lepingu lõppu	Asjakohased riigiasutused	Ei	Raamatupidamissüsteem Kontoritarkvara	Jah	Vastutav töötleja	Ettevõte	Töötleja kontaktide lehel registris	Turvaline andmeedastus/vahetus Turvaline andmesalvestus Turvaline andmete ühiskasutus Andmete kasutamise kontrolljälgede salvestamine, analüüs ja reageerimine Varukoopiate turvaline salvestus Turvaline tööjaamade ja serverite häälestus	Ei	u 20
Ettevõte	Töötajad	Nimi, isikukood	Seaduse täitmine	Seadus	TLS §5 lg5 töölepingu säilitamine 10 a	Andmesubjekt	10 a peale lepingu lõppu	Asjakohased riigiasutused	Ei	Raamatupidamissüsteem Kontoritarkvara	Jah	Vastutav töötleja	Ettevõte	Töötleja kontaktide lehel registris	Turvaline andmeedastus/vahetus Turvaline tööjaamade ja serverite häälestus	Ei	u 20

Ettevõte	Töötajad	Nimi, positsioon, vastutusvaldkond, pilt	Turundus ja müük	Õigustatud huvi		Andmesubjekt	Lepingu lõpp	Avalikkus Turundusteenuse osutaja Kliendid Koostööpartner	Jah	Välisveeb Kontoritarkvara	Jah	Vastutav töötleja	Ettevõte	Töötleja kontaktide lehel registris	Turvalise andmesidekanali kasutamine Turvaline andmeedastus/vahetus Turvaline andmete ühiskasutus Varukoopiate turvaline salvestus Turvaline tööjaamade ja serverite häälestus	Ei	u 20
Ettevõte	Töötajad	Üritusel osalemine, fotogalerii	Turundus ja müük	Õigustatud huvi		Andmesubjekt	5 a	Avalikkus Turundusteenuse osutaja Kliendid Koostööpartner	Jah	Välisveeb Kontoritarkvara	Jah	Vastutav töötleja	Ettevõte	Töötleja kontaktide lehel registris	Turvaline andmete ühiskasutus Andmete kasutamise kontrolljälgede salvestamine, analüüs ja reageerimine Varukoopiate turvaline salvestus Turvaline tööjaamade ja serverite häälestus	Ei	u 20
Ettevõte	Töötajad	Nimi, positsioon, kvalifikatsioon ja haridus, kontaktandmed	Teenuse osutamine	Õigustatud huvi		Volitatud töötleja	10 a peale lepingu lõppu	Kliendid Koostööpartner Turundusteenuse osutaja Raamatupidamisteenuse osutaja	Jah	Raamatupidamissüsteem Partneri infosüsteem	Jah	Vastutav töötleja	Ettevõte	Töötleja kontaktide lehel registris	Turvaline andmesalvestus Turvaline andmete ühiskasutus Andmete kasutamise kontrolljälgede salvestamine, analüüs ja reageerimine Varukoopiate turvaline salvestus Turvateadlikkuse tõstmine Infoturbe teadvustamine ja rakendamine kogu organisatsiooni tasemel	Ei	u 20
Ettevõte	Töötajad	Personaliprofiil	Töökorraldus ja personali juhtimine	Õigustatud huvi		Volitatud töötleja	2 a peale töölepingu lõppu	Personaliteenuse osutaja	Ei	Kontoritarkvara	Jah	Vastutav töötleja	Ettevõte	Töötleja kontaktide lehel registris	Turvaline tööjaamade ja serverite häälestus	Ei	u 20
Ettevõte	Töötajad	Töötaja kandidaadi CV	Töökorraldus ja personali juhtimine	Leping või ettevalmistamine		Andmesubjekt	Värbamise lõpp	Personaliteenuse osutaja	Ei	Kontoritarkvara	Jah	Vastutav töötleja	Ettevõte	Töötleja kontaktide lehel registris	Turvaline andmeedastus/vahetus Turvaline andmesalvestus Turvaline andmete ühiskasutus Andmete kasutamine organisatsiooni sisevõrgus Andmete kasutamise kontrolljälgede salvestamine, analüüs ja reageerimine Turvaline tööjaamade ja serverite häälestus	Ei	u 20
Ettevõte	Töötajad	Töötaja kandidaadi CV	Töökorraldus ja personali juhtimine	Nõusolek		Andmesubjekt	2 a peale värbamist	Personaliteenuse osutaja	Ei	Kontoritarkvara	Jah	Vastutav töötleja	Ettevõte	Töötleja kontaktide lehel registris	Turvaline andmeedastus/vahetus Turvaline andmesalvestus Turvaline andmete ühiskasutus Andmete kasutamine organisatsiooni sisevõrgus Andmete kasutamise kontrolljälgede salvestamine, analüüs ja reageerimine Turvaline tööjaamade ja serverite häälestus	Ei	u 20
Ettevõte	Töötajad	Tervisekontrolli otsus, tööõnnetused, kutsehaigused	Seaduse täitmine	Seadus	TTOS §13 lg 1 p 7 kohustus viia läbi tervisekontroll, §22 tööõnnetusest teavitamine, §23 kutsehaiguse kontrollimise ja diagnoosimise kohustus	Volitatud töötleja	3 a	Asjakohased riigiasutused Tervishoiuteenuse osutaja	Ei	-	Ei	Vastutav töötleja	Ettevõte	Töötleja kontaktide lehel registris	Turvalise andmesidekanali kasutamine Turvaline andmeedastus/vahetus Turvaline andmesalvestus Organisatsiooni varade füüsiline turve Turvaline tööjaamade ja serverite häälestus	Jah	u 20
Ettevõte	Töötajad	Sportimise kulud	Töötaja terviseedendus	Seadus	TMS par 48 lg 5 prim 5 Võimalus hüvitada tervise ja spordiga seotud kulutusi	Andmesubjekt	7 a	Raamatupidamisteenuse osutaja	Ei	Raamatupidamissüsteem	Ei	Vastutav töötleja	Ettevõte	Töötleja kontaktide lehel registris	Turvalise andmesidekanali kasutamine Turvaline andmeedastus/vahetus Turvaline andmesalvestus Turvaline andmete ühiskasutus Andmete kasutamise kontrolljälgede salvestamine, analüüs ja reageerimine Varukoopiate turvaline salvestus Turvaline tööjaamade ja serverite häälestus	Ei	u 20
Ettevõte	Töötajad	Töövahendid	Töökorraldus ja personali juhtimine	Leping		Andmesubjekt	Lepingu lõpp	Koostööpartnerid Raamatupidamisteenuse osutaja	Ei	Raamatupidamissüsteem Toote halduskeskkond Teenusepakkuja keskkond	Ei	Vastutav töötleja	Ettevõte	Töötleja kontaktide lehel registris	Turvalise andmesidekanali kasutamine Turvaline andmesalvestus Andmete kasutamise kontrolljälgede salvestamine, analüüs ja reageerimine Varukoopiate turvaline salvestus Turvaline tööjaamade ja serverite häälestus	Ei	u 20

Ettevõte	Töötajad	Töötelefon	Töökorraldu se ja personali juhtimine	Õigustatud huvi		Andmesubjekt	Lepingu lõpp	Raamatupidamisteenu se osutaja Sideteenuse osutaja	Jah	Raamatupidamis süsteem Teenusepakkuja keskkond	Jah	Vastutav töötleja	Ettevõte	Töötleja kontaktide lehel registris	Turvalise andmesidekanali kasutamine Turvaline andmesalvestus Andmete kasutamise kontrolljälgede salvestamine, analüüs ja reageerimine Varukoopiate turvaline salvestus Turvaline tööjaamade ja serverite häälestus	Jah	u 20
Ettevõte	Töötajad	Töölähetuse aruanne	Töökorraldu se ja personali juhtimine	Seadus		Andmesubjekt	7 a	Koostööpartnerid Raamatupidamisteenu se osutaja Asjassepuutuvad riigiasutused	Ei	Raamatupidamis süsteem Kontoritarkvara	Jah	Vastutav töötleja	Ettevõte	Töötleja kontaktide lehel registris	Turvalise andmesidekanali kasutamine Turvaline andmeedastus/vahetus Turvaline andmesalvestus Turvaline andmete ühiskasutus Andmete kasutamise kontrolljälgede salvestamine, analüüs ja reageerimine Varukoopiate turvaline salvestus Turvaline tööjaamade ja serverite häälestus	Ei	u 20
Ettevõte	Raamatupidamine	Haigestumine, lisapuhkuse andmise aluseks olevad andmed	Töökorraldu se ja personali juhtimine	Seadus	TLS § 15 p 1 lg 10 ajutisest töövõimest tavitamine, § 19 p 2 ajutisest töövõimetusest tulenevalt töö tegemisest keeldumine TLS §38 keskmise töötasu maksmise kohustus tööandjal TTOS § 12 pr 1 haigushüvitise välja maksmine RPS §12 lg 1 raamatupidamise algdokumendid 7 a	Andmesubjekt	7 a	Asjakohased riigiasutused Raamatupidamisteenu se osutaja	Ei	Raamatupidamis süsteem	Ei	Vastutav töötleja	Ettevõte	Töötleja kontaktide lehel registris	Turvalise andmesidekanali kasutamine Turvaline andmeedastus/vahetus Turvaline andmesalvestus Turvaline andmete ühiskasutus Turvaline tööjaamade ja serverite häälestus	Jah	u 20
Ettevõte	Raamatupidamine	Töötaja palgaarvestus, väljamaksed ja boonused	Seaduse täitmine	Seadus	RPS § 12 lg 1 raamatupidamise algdokumendid 7 a	Vastutav töötleja	7 a	Asjakohased riigiasutused Raamatupidamisteenu se osutaja	Ei	Raamatupidamis süsteem	Ei	Vastutav töötleja	Ettevõte	Töötleja kontaktide lehel registris	Turvalise andmesidekanali kasutamine Turvaline andmeedastus/vahetus Turvaline andmesalvestus Turvaline andmete ühiskasutus Andmete kasutamise kontrolljälgede salvestamine, analüüs ja reageerimine Varukoopiate turvaline salvestus Turvaline tööjaamade ja serverite häälestus	Ei	u 20
Ettevõte	Raamatupidamine	Koolituskulud	Töökorraldu se ja personali juhtimine	Seadus	RPS § 12 lg 1 raamatupidamise algdokumendid 7 a	Vastutav töötleja	7 a	Asjakohased riigiasutused Raamatupidamisteenu se osutaja	Ei	Raamatupidamis süsteem	Ei	Vastutav töötleja	Ettevõte	Töötleja kontaktide lehel registris	Turvalise andmesidekanali kasutamine Turvaline andmeedastus/vahetus Turvaline andmesalvestus Turvaline andmete ühiskasutus Andmete kasutamise kontrolljälgede salvestamine, analüüs ja reageerimine Varukoopiate turvaline salvestus Turvaline tööjaamade ja serverite häälestus	Ei	u 20
Ettevõte	Turvakaamera	Videosalvestis	Turvalisuse tagamine	Õigustatud huvi	IKS §14 lg 3 isikute või vara kaitseks jälgimisseadmestiku kasutamine lubatud ilma nõusolekuta	Vastutav töötleja	6 kuud	-	Ei	-	Ei	Vastutav töötleja	Ettevõte	Töötleja kontaktide lehel registris	Turvaline andmesalvestus Turvaline andmete ühiskasutus Andmete kasutamine organisatsiooni sisevõrgus Andmete kasutamise kontrolljälgede salvestamine, analüüs ja reageerimine Organisatsiooni varade füüsiline turve Turvaline tööjaamade ja serverite häälestus	Ei	*konfidentsiaalne*
Koostööpartner	Kontaktisikud	Avalik või krüpteerimiseks	Turvalisuse tagamine	Õigustatud huvi		Andmesubjekt	5 a peale lepingu lõppu	-	Ei	Kontoritarkvara	Jah	Volitatud töötleja	Koostööpa	Kliendilepingus Töötleja kontaktide lehel registris	Turvaline andmeedastus/vahetus Turvaline andmesalvestus Turvaline tööjaamade ja serverite häälestus	Ei	*konfidentsiaalne*
Koostööpartner	Kontaktisikud	Nimi, e-post, telefon, organisatsioon, positsioon	Teenuse osutamine	Leping või ettevalmista mine		Vastutav töötleja	5 a peale lepingu lõppu	Konkreetne klient Turundusteenuse osutaja	Ei	Kontoritarkvara	Jah	Kaasvastutav töötleja	Koostööpa	Kliendilepingus Töötleja kontaktide lehel registris	Turvaline andmete ühiskasutus Trvaline tööjaamade ja serverite häälestus	Ei	*konfidentsiaalne*

Koostööpartner	Kontaktisikud	Üritusel osalemine, fotogalerii	Teenuse osutamine	Leping või ettevalmistamine		Andmesubjekt	5 a	Avalikkus Turundusteenuse osutaja Kliendid Koostööpartner	Jah	Välisveeb Kontoritarkvara	Jah	Vastutav töötleja	Ettevõte	Kliendilepingus Töötleja kontaktide lehel registris	Turvaline andmete ühiskasutus Andmete kasutamise kontrolljälgede salvestamine, analüüs ja reageerimine Varukoopiate turvaline salvestus Turvaline tööjaamade ja serverite häälestus	Ei	*konfidentsiaalne*
Koostööpartner	Kontaktisikud	Üritusel osalemine, fotogalerii	Turundus ja müük	Õigustatud huvi		Andmesubjekt	5 a	Avalikkus Turundusteenuse osutaja Kliendid Koostööpartner	Jah	Välisveeb Kontoritarkvara	Jah	Kaasvastutav töötleja	Koostööpa	Kliendilepingus Töötleja kontaktide lehel registris	Turvaline andmete ühiskasutus Andmete kasutamise kontrolljälgede salvestamine, analüüs ja reageerimine Varukoopiate turvaline salvestus Turvaline tööjaamade ja serverite häälestus	Ei	*konfidentsiaalne*

Appendix 2 – Data Processing Map – Enterprise



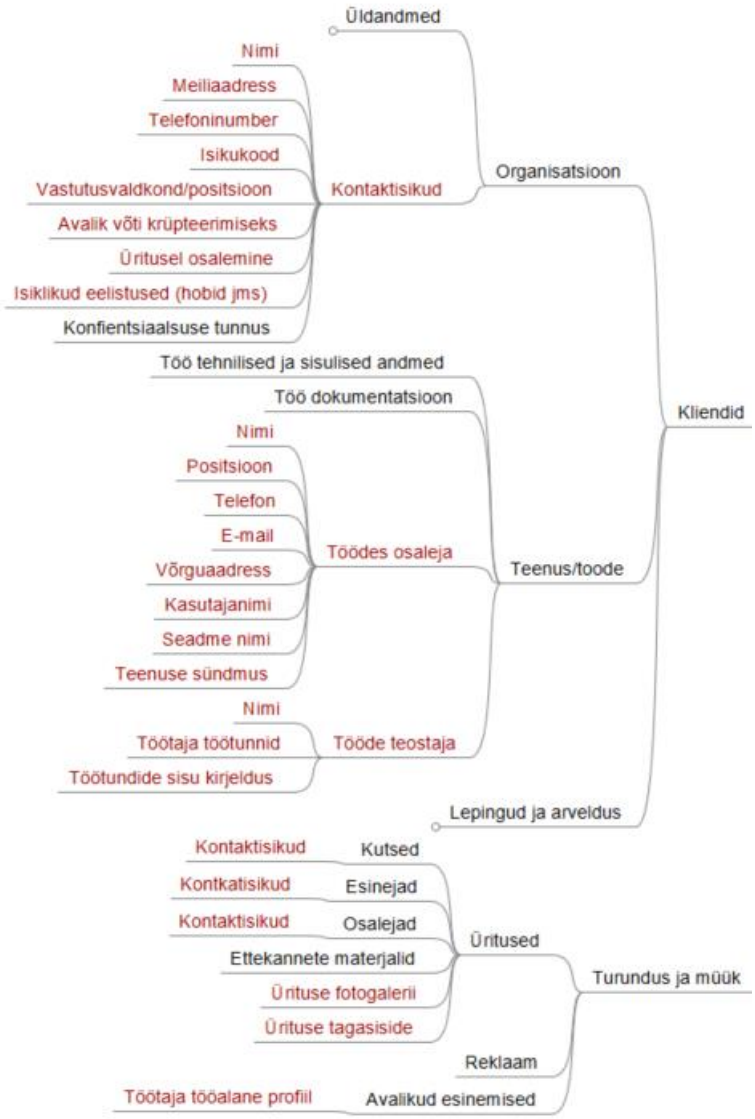
Colour scheme:

Red bold – special categories of personal data, or sensitive data with specific focus by GDPR (personal data of children);

Maroon – personal data;

Black – data that does not contain personal data of natural persons.

Appendix 3 – Data Processing Map – Clients, Marketing and Sales



Colour scheme:

Maroon – personal data;

Black – data that does not contain personal data of natural person

Appendix 4 – Records of Processing Activities of Äripäev

ÄRIPÄEV AS Töötlemistoimignute register

Siit leiad detailse info sellest kuidas, millisel alusel ja miks Sinu isikuandmeid töödeldakse

Äripäev

Vastutusala	Töötlemise eesmärgid	Andmesubjektide kategooriad	Andmetüübid	Vastuvõtjad	Mis alusel me midagi teeme?	Säilitamise tähtajad	Volitatud töötleja
Äripäev AS klienditeenindus							
Vastutav isik töötlemistoimingute registri eest:	**Erika Truuverk**						
Andmekaitseametnik:	**Toomas Jõgi**						
Klienditeenindus	Kliendi tellimuste vastuvõtmine ja täitmine	Kliendid, tellijad	Klientide kontaktandmed, kliendi tellimuste info		Lepingu sõlmimiseks ja täitmiseks vajalik - GDPR 6b	Andmeid säilitatakse tähtajatult	Uptime OÜ
Klienditeenindus	Arvete väljastamine	Kliendid, tellijad	Klientide kontaktandmed, kliendi tellimuste info	E-Arvete puhul pangad	Lepingu täitmiseks vajalik - GDPR 6b	Andmeid säilitatakse tähtajatult	Uptime OÜ, pangad
Klienditeenindus	Toodete/tellimuste väljastamine, kojukanne	Kliendid, tellijad	Klientide kontaktandmed, kliendi tellimuste info	Express Post, Omniva	Lepingu täitmiseks vajalik - GDPR 6b	Lepinguliste nõuete aegumise tähtajani	Uptime OÜ, Express Post AS, Omniva AS
Klienditeenindus	Üritustele registreerimine	Kliendid, tellijad	Klientide kontaktandmed, info üritusel osalemise kohta		Lepingu täitmiseks vajalik - GDPR 6b kui üritusele registreerimine on seotud lepinguga. Õigustatud huvi - GDPR 6f, kui üritusele registreerimine ei ole seotud otseselt lepingu täitmisega.	Andmeid säilitatakse tähtajatult	Uptime OÜ
Klienditeenindus	Lepingute lõpetamine ja tühistamine	Kliendid, tellijad	Klientide kontaktandmed, kliendi tellimuste info		Lepingu täitmiseks vajalik - GDPR 6b	Lepinguliste nõuete aegumise tähtajani	Uptime OÜ
Klienditeenindus	Meeldetuletuste saatmine tellimuste lõppemise kohta	Kliendid, tellijad	Klientide kontaktandmed, kliendi tellimuste info		Lepingu täitmiseks vajalik - GDPR 6b näiteks kui lepingus norm, mis viitab automaatsele pikenemisele/lõppemisele kui kumbki pool ei teavita teisiti. Kui lepingus vastav kokkulepe puudub, siis õigustatud huvi GDPR 6f	Lepinguliste nõuete aegumise tähtajani	Uptime OÜ
Klienditeenindus	Maksekäitumise info (vastav märge, kui klient on võlgu)	Kliendid, tellijad	Klientide kontaktandmed, kliendi maksekäitumise info		Lepingu täitmiseks vajalik - GDPR 6b	Lepinguliste nõuete aegumise tähtajani	Uptime OÜ
Klienditeenindus	Raamatuklubi liikmete igakuine sms-iga teavitamine uutest raamatutest	Kliendid, tellijad	Klientide kontaktandmed, kliendi tellimuste info		Nõusolek - GDPR 6a, kui andmesubjekt on tellnud vastava teavituse Lepingu Täitmiseks vajalik - GDPR 6b, kui on on raamatuid telliv klient Õigustatud huvi - lubatud otseturundus, kuni klient sellest ei keeldu - seda vastavalt GDPR preambula punktile 47	Lepinguliste nõuete aegumise tähtajani	Uptime OÜ
Klienditeenindus	Pretensioonide lahendamine	Kliendid, tellijad	Klientide kontaktandmed, kliendi tellimuste info		Lepingu täitmiseks vajalik - GDPR 6b	Lepinguliste nõuete aegumise tähtajani	Uptime OÜ, Omniva, Express Post
Klienditeenindus	Teavitused SSOst ja e-poest (tehingu kinnitused, õiguste andmine, jagamine ja eemaldamine)	Kliendid, tellijad	Klientide kontaktandmed, kliendi tellimuste info		Lepingu täitmiseks vajalik - GDPR 6b	Lepinguliste nõuete aegumise tähtajani	Uptime OÜ
Klienditeenindus	Klienditeeninduse kõnede salvestamine	Kliendid, tellijad	Klientide telefonikõned	IP Kõnekeskuste OÜ	Vajalik lepingu sõlmimiseks - GDPR 6b VÕS sätestatud kinnituste nõuete täitmiseks kui lepingu sõlmimise eesmärk. Õigustatud huvi - GDPR 6f osas, mis on vajalik kvaliteedi tagamiseks	Lepinguliste nõuete aegumise tähtajani	IP Kõnekeskuste OÜ
Äripäev AS telemarketing							
Vastutav isik töötlemistoimingute registri eest:	**Erika Truuverk**						
Andmekaitseametnik:	**Toomas Jõgi**						
Telemarketing	Telefoni teel müügipakkumiste tegemine	Kliendid, tellijad	Kliendi kontaktandmed, varasemaid tehingud, seosed ettevõtetega, profiil, helistamiste logi		Õigustatud huvi - GDPR 6f	Andmeid säilitatakse tähtajatult või kuni andmesubjekti teistsuguse soovini	Uptime OÜ
Telemarketing	E-maili teel müügipakkumiste tegemine	Kliendid, tellijad	Kliendi kontaktandmed, varasemaid tehingud, seosed ettevõtetega, profiil, helistamiste logi		Õigustatud huvi (GDPR 6f) kui on sarnast toodet/teenust varem tellinud Nõusolek (GDPR 6a) kui ei ole Äripäev AS klient olnud, sarnast toodet tellinud	Andmeid säilitatakse tähtajatult või kuni andmesubjekti teistsuguse soovini	Uptime OÜ
Telemarketing	Tehingute registreerimine telefoni teel, müügiarvete väljastamine	Kliendid, tellijad	Klientide kontaktandmed, kliendi tellimuste info		Lepingu täitmiseks vajalik - GDPR 6b -VÕS nõuete täitmine	Lepinguliste nõuete aegumise tähtajani	Uptime OÜ
Telemarketing	Müügikõnede salvestamine	Kliendid, tellijad	Kliendi andmed ja kõne salvestus		Nõusolek (GDPR6a). Lepingu sõlmimiseks vajalik (GDPR 6b), kui müügikõne kaudu säilitatakse lepingu sõlmimise soov VÕS nõuete täitmiseks. Õigustatud huvi osas, mis on vajalik kvaliteedi tagamiseks ning lepingu sõlmimiseks / täitmiseks (GDPR 6b) vajalikkus kinnituste alles hoidmiseks.	Andmeid säilitatakse tähtajatult, lepinguliste nõuete aegumise lõpuni või kuni andmesubjekti teistsuguse soovini	Elisa Eesti AS ja Uptime OÜ

Telemarketing	Kampaaniate tehingute registreerimine (märge kliendi juures, et tuli läbi mingi kampaania)	Kliendid, tellijad	Kliendi andmed		Õigustatud huvi- GDPR 6f	Andmeid säilitatakse tähtajatult või kuni andmesubjekti teistsuguse soovini	Uptime OÜ
Äripäev AS Andmetöötlus							
Vastutav isik töötlemistoimingute registri eest:	**Liis Rush**						
Andmekaitseametnik:	**Toomas Jõgi**						
Andmetöötlus	Helistamisnimekirjade koostamine	Kliendid, tellijad, juriidilised isikud ja nende kontaktisikud Infopangast või avalikest allikatest	Klientide kontaktandmed, kliendi tellimuste info		Õigustatud huvi (GDPR 6f) Lepingu täitmine (GDPR 6b). Nõusolek (GDPR 6a) osas, mis ei ole seotud lepingu täitmisega ega õigustatud huvi alusel töötlusega	Andmeid säilitatakse tähtajatult või kuni andmesubjekti teistsuguse soovini	Uptime OÜ
Andmetöötlus	Postitusnimekirjade koostamine (tunnused - kasutusstatistika, professionaalne profiil, ostuajalugu, tuletatud segmendid)	Kliendid, tellijad, juriidilised isikud ja nende kontaktisikud Infopangast või avalikest allikatest	Klientide kontaktandmed	Sendsmaily OÜ	Õigustatud huvi (GDPR 6f) Lepingu täitmine (GDPR 6b). Nõusolek (GDPR 6a) osas, mis ei ole seotud lepingu täitmisega ega õigustatud huvi alusel töötlusega	Andmeid säilitatakse tähtajatult või kuni andmesubjekti teistsuguse soovini	Uptime OÜ, Sendsmaily OÜ
Andmetöötlus	Opt-in opt-out haldus	Praegused või endised tellijad, juriidilised isikud ja nende kontaktisikud	Klientide kontaktandmed	Sendsmaily OÜ	Õigustatud huvi (GDPR 6f) või nõusolek (GDPR 6a). Otseturunduslike tegevuste puhul on kliendil olema alati võimalus loobuda.	Andmeid säilitatakse tähtajatult või kuni andmesubjekti teistsuguse soovini	Uptime OÜ, Sendsmaily OÜ
Andmetöötlus	Aruandlus	Kliendid, tellijad, juriidilised isikud ja nende kontaktisikud Infopangast või avalikest allikatest	Klientide kontaktandmed		Lepingu täitmine (GDPR 6b) Õigustatud huvi (GDPR 6f) äritegevuse toetamiseks: müügiprotsessi jälgimiseks või müügipotentsiaali otsimiseks.	Andmeid säilitatakse tähtajatult või kuni andmesubjekti teistsuguse soovini	Uptime OÜ, Infovara OÜ
Andmetöötlus	Juriidiliste isikute andmete importimine infopangast	Juriidiliste isikute andmed ja nende kontaktisikute andmed	Klientide kontaktandmed		Suuremas osas ei lange füüsiliste isikute andmete alla, muus osas õigustatud huvi - GDPR 6f	Andmeid säilitatakse tähtajatult või kuni andmesubjekti teistsuguse soovini	Uptime OÜ
Äripäev AS Kasutusandmete kogumine ja turundusautomaatika							
Vastutav isik töötlemistoimingute registri eest:	**Liis Rush**						
Andmekaitseametnik:	**Toomas Jõgi**						
Digiturunduse osakond	Kasutajaaktiivsuse monitooring, digiturundustegevuste mõõtmine ja planeerimine	Kliendid, veebilehtede külastajad	Kliendiandmed, isikustatud ja anonüümne kasutusstatistika	Google Analytics, Kissmetrics, Uptime OÜ, AWS	Õigustatud huvi GDPR 6f.	Andmeid säilitatakse tähtajatult või kuni andmesubjekti teistsuguse soovini	Uptime OÜ, Google Analytics, Kissmetrics, Uptime OÜ, AWS
Digiturunduse osakond	Kliendile selgelt sihitud automaatsete teavituste ja pakkumiste edastamine on-site või e-posti teel	Kliendid, veebilehtede külastajad	Kliendiandmed	Sendsmaily OÜ	Õigustatud huvi praegustele ja endistele tellijatele teavituste edastamiseks ja turundusliku sisu edastamiseks sarnaste toodete/teenuste osas (GDPR 6f).	Andmeid säilitatakse tähtajatult	Uptime OÜ, Sendsmaily OÜ
Äripäev AS Reklaami müük							
Vastutav isik töötlemistoimingute registri eest:	**Asso Laido**						
Andmekaitseametnik:	**Toomas Jõgi**						
Reklaam	Reklaamitellijate esindajate kontaktinfo hoidmine, tellimuste ja suhtluse ajaloo säilitamine	Reklaamiklientide esindajad	Reklaamiklientide esindajate kontaktandmed ja suhtlemise ajalugu		Lepingu täitmine (GDPR 6b) ja õigustatud huvi (GDPR 6f).	Andmeid säilitatakse tähtajatult	Uptime OÜ
Äripäev AS Finants ja personalihaldus							
Vastutav isik töötlemistoimingute registri eest:	**Toomas Truuverk**						
Andmekaitseametnik:	**Toomas Jõgi**						
Finants, Personal, IT	Tööle kanditeerijate CV-des olevate isikuandmete kogumine ja säilitamine	Töötajad	Tööle kanditeerijate isikuandmed		Õigustatud huvi- GDPR 6f (tagatud on töötjaateteavitus läbi tööpakkumise)	2 aastat	
Finants, Personal, IT	Tööle kanditeerijate kohta taustauuringu teostamine ning säilitamine	Töötajad	Tööle kanditeerijate isikuandmed		Õigustatud huvi- GDPR 6f (tagatud on töötajateteavitus läbi tööpakkumise) ning taustauuringu osas nõusolek läbi CV saatmise	2 aastat	
Äripäev AS Infopank							
Vastutav isik töötlemistoimingute registri eest:	**Toomas Truuverk**						
Andmekaitseametnik:	**Toomas Jõgi**						
Infopank	Turundusnimekirjade koostamine ja väljavõtete tegemine infopanga kasutajatele, ettevõtete kontaktinfo	Ettevõtted	Ettevõtte aadressiandmed, registriandmed, kontaktid, ettevõtete finantsandmed	Infopanga lepingulised kliendid	Kasutus on ettevõtete põhiandmete kaudu, seega GDPR ei kohaldu. Ulatuses, milles ettevõtte põhikontaktina on esitatud isikuandmed, on töötluse aluseks õigustatud huvi (osas, milles andmebaasi ja inforegistri tegevuspõhimõtted sisaldavad endas info visualiseerimist, sortimist ja filtreerimist ja andmebaaside koostamist)	Andmeid säilitatakse tähtajatult	Uptime OÜ, infopanga kliendid

Infopank	Turundusnimekirjade koostamine ja väljavõtete tegemine infopanga kasutajatele, isikute kontaktinfo	Ettevõtted, isikud	Ettevõtetega seotud isikute kontaktid, ettevõtete finantsandmed	Infopanga lepingulised kliendid	Nõusolek (GDPR 6a) Õigustatud huvi (GDPR 6f) (osas, milles andmebaasi ja inforegistri tegevuspõhimõtted sisaldavad endas info visualiseerimist, sortimist ja filtreerimist ja andmebaaside koostamist)	Andmeid säilitatakse tähtajatult	Uptime OÜ, infopanga kliendid
Infopank	Ettevõtete ja ettevõtetega seotud võtmeisikute andmete kogumine ja süstematiseerimine ehk hoiame infot enda poolt tehtava ajakirjanduse tarbeks	Ettevõtted, isikud	Ettevõtete kontaktid, isikute kontakrid, isikute elulooline info, isikute ajaloolised seosed ettevõtetega, ettevõtete finantsandmed, ettevõtete maksekäitumise info	Äripäeva töötajad	Ajakirjanduslik erand (Eesti IKS, GDPR 85, preambula p 153) Õigustatud huvi (GDPR 6f) (osas, milles andmebaasi ja inforegistri tegevuspõhimõtted sisaldavad endas info visualiseerimist, sortimist ja filtreerimist ja andmebaaside koostamist)	Andmeid säilitatakse tähtajatult	Uptime OÜ
Infopank	Telmoses olevate ettevõtete andmete kontroll ja uuendamine	Ettevõtted, isikud	Ettevõtete konaktid, ettevõtetega seotud isikud, isikute kontaktid	Infosüsteem Telmos ettevõtte siseselt	Õigustatud huvi (GDPR 6f) (osas, milles andmebaasi ja inforegistri tegevuspõhimõtted sisaldavad endas info visualiseerimist, sortimist ja filtreerimist ja andmebaaside koostamist)	Andmeid säilitatakse tähtajatult	Uptime OÜ
Infopank	Ettevõtete ja ettevõtjate edetabelite koostamine ajakirjanduslikul eesmärgil	Ettevõtted, isikud	Ettevõtete finantsandmed, Ettevõttega seotud isikud		Ajakirjanduslik erand (Eesti IKS, GDPR art 85, prembula p 153)	Andmeid säilitatakse tähtajatult	Uptime OÜ
Infopank	Ettevõtete tausatinfo ja finantsnäitajate süstematiseerimine ja ülevaatlikult esitamine infopanga klientidele ettevõtete krediidivõimekuse hindamise eesmärgil	Ettevõtted, isikud	Ettevõtete finantsandmed, ettevõtete võlaandmed, ettevõtetega seotud isikud, seotud isikute ajaloolised seosed ettevõtetega	Infopanga kliendid	Õigustatud huvi (GDPR 6f) (osas, milles andmebaasi ja inforegistri tegevuspõhimõtted sisaldavad endas info visualiseerimist, sortimist ja filtreerimist ja andmebaaside koostamist)	Andmeid säilitatakse tähtajatult	Uptime OÜ, infopanga kliendid
Infopank	Ettevõtete tausatinfo ja finantsnäitajate süstematiseerimine ja ülevaatlikult esitamine Äripäeva siseseks kasutamiseks klientide krediidivõimekuse hindamise eesmärgil	Ettevõtted, isikud	Ettevõtete finantsandmed, ettevõtete võlaandmed, ettevõtetega seotud isikud, seotud isikute ajaloolised seosed ettevõtetega	Äripäeva sisesed kasutajad	Õigustatud huvi (GDPR 6f) (osas, milles andmebaasi ja inforegistri tegevuspõhimõtted sisaldavad endas info visualiseerimist, sortimist ja filtreerimist ja andmebaaside koostamist)	Andmeid säilitatakse tähtajatult	Uptime OÜ
Infopank	Elulooliste andmete kogumine ja avaldamine ajakirjanduslikul eesmärgil (leksikonide koostamine)	Isikud	Isikute seosed ettevõtetega, isikute elulooline info	Infopanga kliendid Äripäeva sisesed kasutajad	Nõusolek (GDPR 6a)	Andmeid säilitatakse tähtajatult	Uptime OÜ
Infopank	Ettevõtete kataloogi hoidmine ettevõtete kontaktinfo leidmise lihtsustamise eesmärgil	Ettevõtted	Ettevõtete kontaktinfo	Infopanga kliendid Üripäeva sisesed kasutajad Infopanga teenuse lepinguta kasutajad	Õigustatud huvi (GDPR 6f) (osas, milles andmebaasi ja inforegistri tegevuspõhimõtted sisaldavad endas info visualiseerimist, sortimist ja filtreerimist ja andmebaaside koostamist)	Andmeid säilitatakse tähtajatult	Uptime OÜ, infopanga kliendid
Äripäev AS IT koolitus							
Vastutav isik töötlemisto/mingute registri eest:	**Martin Palm**						
Andmekaitseametnik:	**Toomas Jõgi**						
IT koolitus	Uudiskirja saatmine uudiskirja tellinud klientidele	kliendid	klientide e-maili aadressid		Nõusolek (GDPR 6a)	Andmeid säilitatakse tähtajatult või kuni andmesubjekti teistsuguse soovini	
IT koolitus	Spetsiifiliste koolituste suunatud pakkumiste saatmine endistele klientidele	endised kliendid	klientide e-maili aadressid		Õigustatud huvi (GDPR 6f)	Andmeid säilitatakse tähtajatult või kuni andmesubjekti teistsuguse soovini	
IT koolitus	Klientide koolitustele registreerimine	kliendid	klientide kontaktandmed, isikukood	Juhul, kui koolitust viib läbi kolmas isik, siis edastatakse koolitusel osalejate isikuandmed koolituse läbiviijale. Riigihankena tehtud koolituste puhul osalejate andmete edastamine Töötukassale või MKM-ile	Lepingu täitmine (GDPR 6b)	Lepinguliste nõuete aegumise tähtajani	Koolituse läbiviija juhul, kui koolitust viib läbi kolmas isik: Koolituse tellija (MKM, Töötukassa jms.)
IT koolitus	Klientide eksamitele registreerimine	kliendid	klientide kontaktandmed, isikukood	Andmed edastatakse eksami läbiviijale	Lepingu täitmine (GDPR 6b)	Lepinguliste nõuete aegumise tähtajani	eksami läbiviija
IT koolitus	Tunnistuste väljastamine ja tunnistuste registreerimine andmebaasis	kliendid	klientide kontaktandmed, isikukood	Kui koolituse tellija on kolmas isik, siis edastatakse tunnistuste andmed sellele kolmandale isikule	Lepingu täitmine (GDPR 6b), õigusaktidest tulenev kohustus (GDPR 6c)	Andmeid säilitatakse tähtajatult või kuni andmesubjekti teistsuguse soovini	koolituste tellija

IT koolitus	Arvete väljastamine	kliendid	Klientide kontaktandmed		Lepingu täitmine (GDPR 6b)	Lepinguliste nõuete aegumise tähtajani	Uptime OÜ
Äripäev AS Akadeemia							
Vastutav isik töötlemistoimingute registri eest:							
Andmekaitseametnik:	**Toomas Jõgi**						
Akadeemia (koolitused)	Telefoni teel klientidele müügipakkumiste tegemine	Kliendid	klientide kontaktandmed		Õigustatud huvi (GDPR 6f)	Andmeid säilitatakse tähtajatult või kuni andmesubjekti teistsuguse soovini	Uptime OÜ
Akadeemia (koolitused)	Koolitusel osalejate kontaktandmete avaldamine teistele koolitusel osalejatele	Kliendid	klientide kontaktandmed	Teised koolitusel osalejad	Nõusoleku alusel (GDPR 6a)	Toimingu lõpuleviimiseni	
Akadeemia (koolitused)	Klientide koolitustele registreerimine, e-maili saatmine registreerumise kinnitusega	kliendid	klientide nimed, kontaktandmed, isikukood	Juhul, kui koolitust viib läbi kolmas isik, siis edastatakse koolitusel osalejate isikuandmed koolituse läbiviijale. Riigihankena tehtud koolituste puhul osalejate andmete edastamine Töötukassale või MKM-ile	Lepingu täitmine (GDPR 6b)	Lepinguliste nõuete aegumsie tähtajani	Koolituse läbiviija juhul, kui koolitust viib läbi kolmas isik: Koolituse tellija (MKM, Töötukassa jms.)
Akadeemia (koolitused)	Tunnistuste väljastamine ja tunnistuste registreerimine andmebaasis ning tunnistuste failide säilitamine	kliendid	klientide nimed, kontaktandmed, isikukood	Kui koolituse tellija on kolmas isik, siis edastatakse tunnistuste andmed sellele kolmandale isikule	Lepingu täitmine (GDPR 6b), õigusaktidest tulenev kohustus (GDPR 6c)	Andmeid säilitatakse tähtajatult või kuni andmesubjekti teistsuguse soovini	koolituste tellija
Akadeemia (koolitused)	Tagasiside küsimine koolitusel osalejatelt koolituse kohta	kliendid	klientide nimed		Õigustatud huvi (GDPR 6f)	Lepinguliste nõuete aegumise tähtajani	
Akadeemia (koolitused)	Koolitusel osalejate info edastamine koolitajale	kliendid	klientide nimed		Õigustatud huvi (GDPR 6f)	Toimingu lõpuleviimiseni	
Akadeemia (koolitused)	Koolitajate kontaktinfo andmebaasi pidamine	koolitajad, koostööpartnerid	Koolitajate nimed ja kontaktinfo		Lepingu täitmine (GDPR 6b), õigustatud huvi (GDPR 6f) tagamaks ettevõtte kollektiivne teadmine koolitajatest	Andmeid säilitatakse tähtajatult või kuni andmesubjekti teistsuguse soovini	
Akadeemia (koolitused)	Arvete väljastamine	Kliendid	Klientide kontaktandmed		Lepingu täitmine (GDPR 6b	Lepinguliste nõuete aegumise tähtajani	Uptime OÜ
Äripäev AS Konverentsid							
Vastutav isik töötlemistoimingute registri eest:							
Andmekaitseametnik:	**Toomas Jõgi**						
ÄP konverentsid	E-maili teel klientidele müügipakumiste tegemine	Kliendid	klientide kontaktandmed		Õigustatud huvi - GDPR 6f	Andmeid säilitatakse tähtajatult või kuni andmesubjekti teistsuguse soovini	Uptime OÜ
ÄP konverentsid	Telefoni teel klientidele müügipakumiste tegemine	Kliendid	klientide kontaktandmed		Õigustatud huvi (GDPR 6f) kui on andmesubjekt osalenud sarnastel koolitustel Nõusolek (GDPR 6a).	Andmeid säilitatakse tähtajatult või kuni andmesubjekti teistsuguse soovini	Uptime OÜ
ÄP konverentsid	Tehingute registreerimine/osalejate registreerimine ütritustele ja arvete väljastamine	Kliendid	klientide kontaktandmed		Lepingu täitmine (GDPR 6b)	Lepinguliste nõuete aegumise tähtajani	Uptime OÜ
ÄP konverentsid	Klientidele meeldetuletuste edastamine üituste toimumise kohta	Kliendid	klientide kontaktandmed		Lepingu täitmine (GDPR 6b)	Lepinguliste nõuete aegumise tähtajani	Uptime OÜ
ÄP konverentsid	Üritustel osalejate nimekirjade hoidmine	Kliendid	klientide kontaktandmed		Lepingu täitmine (GDPR 6b)	Lepinguliste nõuete aegumise tähtajani	Uptime OÜ
ÄP konverentsid	Tänukirja ja tagasisiside küsimise edastamine klientidele	Kliendid	klientide kontaktandmed		Õigustatud huvi - GDPR 6f	Andmeid säilitatakse tähtajatult või kuni andmesubjekti teistsuguse soovini	Uptime OÜ

Appendix 5 – ICO Example of Records of Processing Activities – Processor

Processor					
Name and contact details		**Data Protection Officer (if applicable)**		**Representative (if applicable)**	
Name	Example processor	**Name**	Example DPO	**Name**	N/A
Address	Street, city, postcode	**Address**	Street, city, postcode	**Address**	N/A
Email	Email address	**Email**	Email address	**Email**	N/A
Telephone	Tel. number	**Telephone**	Tel. number	**Telephone**	N/A

Article 30 Record of Processing Activities						
Link to contract with controller	**Name and contact details of controller**	**Name and contact details of controller's representative (if applicable)**	**Categories of processing**	**Names of third countries or international organsations that personal data are transferred to (if applicable)**	**Safeguards for exceptional transfers of personal data to third countries or international organisations (if applicable)**	**General description of technical and organisational security measures (if possible)**
Link	Controller A - Address,	N/A	Payroll	N/A	N/A	Encrypted storage
Link	Controller B - Address,	N/A	Payroll	N/A	N/A	Encrypted storage
Link	Controller B - Address,	N/A	Bookkeeping	N/A	N/A	Encrypted storage
Link	Controller B - Address, Email, Tel. Number	N/A	Cloud storage	Canada	N/A	Encrypted storage, access controls

Colour scheme:

Green background – required components in by GDPR and UK Data Protection Bill;

Blue background – components not required by GDPR and UK Data Protection Bill.

Appendix 6 – ICO Example of Records of Processing Activities – Controller

Controller					
Name and contact		**Data Protection Officer (if**		**Representative (if applicable)**	
Name	Example controller	**Name**	Example DPO	**Name**	N/A
Address	Street, city, postcode	**Address**	Street, city, postcode	**Address**	N/A
Email	Email address	**Email**	Email address	**Email**	N/A
Telephone	Tel. number	**Telephone**	Tel. number	**Telephone**	N/A

Article 30 Record of Processing Activities											Privacy Notices			
Business function	**Purpose of processing**	**Name and contact details of joint controller (if applicable)**	**Categories of individuals**	**Categories of personal data**	**Categories of recipients**	**Link to contract with processor**	**Names of third countries or international organsations that personal data are transferred to (if applicable)**	**Safeguards for exceptional transfers of personal data to third countries or international organisations (if applicable)**	**Retention schedule (if possible)**	**General description of technical and organisational security measures (if possible)**	**Article 6 lawful basis for processing personal data**	**Article 9 basis for processing special category data**	**Legitimate interests for the processing (if applicable)**	**Link to record of legitimate interests assessment (if applicable)**
Finance	Payroll	N/A	Employees	Contact details	HMRC	N/A	N/A	N/A	5 years post-employment	Encrypted storage and transfer	Article 6(1)(c) - legal obligation	N/A	N/A	N/A
Finance	Payroll	N/A	Employees	Bank details	HMRC	N/A	N/A	N/A	3 years post-employment	Encrypted storage and transfer	Article 6(1)(c) - legal obligation	N/A	N/A	N/A
Finance	Payroll	N/A	Employees	Pension details	HMRC	N/A	N/A	N/A	75 years post-employment	Encrypted storage and transfer	Article 6(1)(c) - legal obligation	N/A	N/A	N/A
Finance	Payroll	N/A	Employees	Tax details	HMRC	N/A	N/A	N/A	6 years post-employment	Encrypted storage and transfer	Article 6(1)(c) - legal obligation	N/A	N/A	N/A
Human Resources	Personel file	N/A	Employees	Contact details	N/A	N/A	N/A	N/A	6 years post-employment	Encrypted storage	Article 6(1)(b) - contract	N/A	N/A	N/A
Human Resources	Personel file	N/A	Employees	Pay details	N/A	N/A	N/A	N/A	6 years post-employment	Encrypted storage, access controls	Article 6(1)(b) - contract	N/A	N/A	N/A
Human Resources	Personel file	N/A	Employees	Annual leave details	N/A	N/A	N/A	N/A	6 years post-employment	Encrypted storage, access controls	Article 6(1)(b) - contract	N/A	N/A	N/A
Human Resources	Personel file	N/A	Employees	Sick leave details	N/A	N/A	N/A	N/A	6 years post-employment	Encrypted storage, access controls	Article 6(1)(b) - contract	Article 9(2)(b) - employment	N/A	N/A
Human Resources	Personel file	N/A	Employees	Performance details	N/A	N/A	N/A	N/A	6 years post-employment	Encrypted storage, access controls	Article 6(1)(b) - contract	N/A	N/A	N/A
Human Resources	Recruitment	N/A	Successful candidates	Contact details	Referee	N/A	N/A	N/A	6 years post-employment	Encrypted storage and transfer	Article 6(1)(b) - contract	N/A	N/A	N/A
Human Resources	Recruitment	N/A	Successful candidates	Qualifications	N/A	N/A	N/A	N/A	6 years post-employment	Encrypted storage, access controls	Article 6(1)(b) - contract	N/A	N/A	N/A
Human Resources	Recruitment	N/A	Successful candidates	Employment history	N/A	N/A	N/A	N/A	6 years post-employment	Encrypted storage, access controls	Article 6(1)(b) - contract	N/A	N/A	N/A
Human Resources	Recruitment	N/A	Successful candidates	Ethnicity	N/A	N/A	N/A	N/A	6 years post-employment	Encrypted storage, access controls	Article 6(1)(b) - contract	Article 9(2)(b) - employment	N/A	N/A
Human Resources	Recruitment	N/A	Successful candidates	Disiability details	N/A	N/A	N/A	N/A	6 years post-employment	Encrypted storage, access controls	Article 6(1)(b) - contract	Article 9(2)(b) - employment	N/A	N/A
Human Resources	Recruitment	N/A	Unsuccessful candidates	Contact details	N/A	N/A	N/A	N/A	6 months post-campaign	Encrypted storage, access controls	Article 6(1)(b) - contract	N/A	N/A	N/A
Human Resources	Recruitment	N/A	Unsuccessful candidates	Qualifications	N/A	N/A	N/A	N/A	6 months post-campaign	Encrypted storage, access controls	Article 6(1)(b) - contract	N/A	N/A	N/A
Human Resources	Recruitment	N/A	Unsuccessful candidates	Employment history	N/A	N/A	N/A	N/A	6 months post-campaign	Encrypted storage, access controls	Article 6(1)(b) - contract	N/A	N/A	N/A
Human Resources	Recruitment	N/A	Unsuccessful candidates	Ethnicity	N/A	N/A	N/A	N/A	6 months post-campaign	Encrypted storage, access controls	Article 6(1)(b) - contract	Article 9(2)(b) - employment	N/A	N/A
Human Resources	Recruitment	N/A	Unsuccessful candidates	Disiability details	N/A	N/A	N/A	N/A	6 months post-campaign	Encrypted storage, access controls	Article 6(1)(b) - contract	Article 9(2)(b) - employment	N/A	
Sales	Direct marketing	N/A	Existing customers	Contact details	Processor - marketing co.	Link	N/A	N/A	End of customer	Encrypted storage and transfer	Article 6(1)(a) - consent	N/A	N/A	N/A
Sales	Direct marketing	N/A	Existing customers	Purchase history	Processor - marketing co.	Link	N/A	N/A	End of customer	Encrypted storage and transfer	Article 6(1)(a) - consent	N/A	N/A	N/A
Sales	Direct marketing	N/A	Potential customers	Contact details	Processor - marketing co.	Link	N/A	N/A	1 year post-campaign	Encrypted storage and transfer	Article 6(1)(a) - consent	N/A	N/A	N/A
Sales	Direct marketing	N/A	Potential customers	Lifestyle information	Processor - marketing co.	Link	N/A	N/A	1 year post-campaign	Encrypted storage and transfer	Article 6(1)(a) - consent	N/A	N/A	N/A

			Consent	Access Requests	Data Protection Impact Assessments			Personal Data Breaches		Data Protection Bill - Special Category or Criminal Conviction and Offence data				
Rights available to individuals	Existence of automated decision-making, including profiling (if applicable)	The source of the personl data (if applicable)	Link to record of consent	Location of personal data	Data Protection Impact Assessment required?	Data Protection Impact Assessment progress	Link to Data Protection Impact Assessment	Has a personal data breach occurred?	Link to record of personal data breach	Data Protection Bill Schedule Condition for processing	GDPR Article 6 lawful basis for processing	Link to retention and erasure policy document	Is personal data retained and erased in accordance with the policy document?	Reasons for not adhering to policy document (if applicable)
Access and rectification	No	Data subject	N/A	Finance payroll system	No	N/A	N/A	No	N/A	N/A	N/A	N/A	N/A	N/A
Access and rectification	No	Data subject	N/A	Finance payroll system	No	N/A	N/A	No	N/A	N/A	N/A	N/A	N/A	N/A
Access and rectification	No	Controller	N/A	Finance pension system	No	N/A	N/A	No	N/A	N/A	N/A	N/A	N/A	N/A
Access and rectification	No	Controller	N/A	Finance payroll system	No	N/A	N/A	No	N/A	N/A	N/A	N/A	N/A	N/A
Access, data portability, rectification	No	Data subject	N/A	HR personel system	No	N/A	N/A	No	N/A	N/A	N/A	N/A	N/A	N/A
Access, data portability, rectification	No	Controller	N/A	HR personel system	No	N/A	N/A	No	N/A	N/A	N/A	N/A	N/A	N/A
Access, data portability, rectification	No	Data subject	N/A	HR personel system	No	N/A	N/A	No	N/A	N/A	N/A	N/A	N/A	N/A
Access, data portability, rectification	No	Data subject	N/A	HR personel system	No	N/A	N/A	No	N/A	Sch.1, Pt.1, 1 - Employment	Article 6(1)(b) - contract	Link	Yes	N/A
Access, data portability, rectification	No	Controller	N/A	HR personel system	No	N/A	N/A	No	N/A	N/A	N/A	N/A	N/A	N/A
Access, data portability, rectification	Yes	Data subject	N/A	HR Recrtuiment system	Yes	Completed	Link	No	N/A	N/A	N/A	N/A	N/A	N/A
Access, data portability, rectification	Yes	Data subject	N/A	HR Recrtuiment system	Yes	Completed	Link	No	N/A	N/A	N/A	N/A	N/A	N/A
Access, data portability, rectification	Yes	Data subject	N/A	HR Recrtuiment system	Yes	Completed	Link	No	N/A	N/A	N/A	N/A	N/A	N/A
Access, data portability, rectification	No	Data subject	N/A	HR Recrtuiment system	No	N/A	N/A	No	N/A	Sch.1, Pt.1, 1 - Employment	Article 6(1)(b) - contract	Link	Yes	N/A
Access, data portability, rectification	No	Data subject	N/A	HR Recrtuiment system	No	N/A	N/A	No	N/A	Sch.1, Pt.1, 1 - Employment	Article 6(1)(b) - contract	Link	Yes	N/A
Access, data portability, rectification	Yes	Data subject	N/A	HR Recrtuiment system	Yes	Completed	Link	No	N/A	N/A	N/A	N/A	N/A	N/A
Access, data portability, rectification	Yes	Data subject	N/A	HR Recrtuiment system	Yes	Completed	Link	No	N/A	N/A	N/A	N/A	N/A	N/A
Access, data portability, rectification	Yes	Data subject	N/A	HR Recrtuiment system	Yes	Completed	Link	No	N/A	N/A	N/A	N/A	N/A	N/A
Access, data portability, rectification	No	Data subject	N/A	HR Recrtuiment system	No	N/A	N/A	No	N/A	Sch.1, Pt.1, 1 - Employment	Article 6(1)(b) - contract	Link	Yes	N/A
Access, data portability, rectification	No	Data subject	N/A	HR Recrtuiment system	No	N/A	N/A	No	N/A	Sch.1, Pt.1, 1 - Employment	Article 6(1)(b) - contract	Link	Yes	N/A
Access, data portability, rectification, objection, erasure	Yes	Data subject	Link	Sales system, data processor	Yes	Completed	Link	No	N/A	N/A	N/A	N/A	N/A	N/A
Access, data portability, rectification, objection, erasure	Yes	Data subject	Link	Sales system, data processor	Yes	Completed	Link	No	N/A	N/A	N/A	N/A	N/A	N/A
Access, data portability, rectification, objection, erasure	Yes	Data broker co.	Link	Sales system, data processor	Yes	Completed	Link	No	N/A	N/A	N/A	N/A	N/A	N/A
Access, data portability, rectification, objection, erasure	Yes	Data broker co.	Link	Sales system, data processor	Yes	Completed	Link	No	N/A	N/A	N/A	N/A	N/A	N/A