LAPIN AMK
Lapland University of Applied Sciences

APPLYING GENERAL DATA PROTECTION REGULATION IN SMALL ORGANIZATIONS

Simplified Framework and Templates for Managing a Privacy Program

Saaranen Eija

Bachelor's Thesis
School of Business and Culture
Degree Programme in Business Information Technology
Bachelor of Business Administration

2018

LAPIN AMK
Lapland University of Applied Sciences

Opinnäytetyön
tiivistelmä

Tietojenkäsittely ja tietoliikenne (ICT)
Tietojenkäsittelyn koulutusohjelma
Tradenomi (AMK)

Tekijä	Eija Saaranen	Vuosi	2018
Ohjaaja	Jari Sarja		

Työn nimi	Euroopan unionin yleisen tietosuoja-asetuksen soveltaminen käytäntöön pienissä organisaatioissa: Yksinkertaistettu viitekehys sekä mallidokumentaatio tietosuojaohjelman hallintaan
Sivu- ja liitesivumäärä	49 + 11

Euroopan unionin yleistä tietosuoja-asetusta alettiin soveltaa 25. toukokuuta 2018. Tietosuoja-asetuksen tavoitteena on luoda koko Euroopan kattava ja laillisesti sitova standardi sekä mahdollistaa tiedon vapaa liikkuvuus Euroopassa. Kaikki yritykset ja organisaatiot ovat tietosuoja-asetuksen piirissä niiden koosta huolimatta. Hallinnolliset sakot tai muut rangaistustoimenpiteet eivät ole sidoksissa organisaation kokoon. Kun otetaan edellä mainitut asiat huomioon, on todennäköistä, ettei pienillä organisaatioilla ole tehtävään ja asetuksen tuomiin muutoksiin vaadittavaa osaamista tai resursseja.

Tämä opinnäytetyö on luonteeltaan kvalitatiivinen, ja se on toteutettu sisältöanalyysin menetelmin. Lopputulos on kirjallisuuskatsaustyyppinen yhteenveto pienille organisaatioille oleellisesta tiedosta liittyen Euroopan unionin yleiseen tietosuoja-asetukseen. Työn yhteydessä luotu esimerkki dokumentaatio vastaa Euroopan unionin yleisen tietosuoja-asetuksen, Artikla 29 Tietosuoja Työryhmän, tietosuojavaltuutettujen sekä muiden asiantuntijoiden esittämiin vaatimuksiin.

Tämän opinnäytetyön tavoite käytännössä on tarjota pienille organisaatioille relevantti tieto tiiviissä ja ymmärrettävässä muodossa. Tarvittavan tiedon lisäksi, opinnäytetyön yhteydessä on työstetty yksinkertaistettu viitekehys sekä sitä tukeva esimerkkidokumentaatio pienten organisaatioiden tueksi niiden aloittaessa työnsä tietoturvaohjelmansa parissa. Esitetty viitekehys koostuu neljästä vaiheesta, ja vaiheita tukevat mallidokumentit on laadittu työn liitteeksi. Viitekehyksen vaiheet ovat määrittely, suunnittelu, dokumentointi ja toimeenpano.

Tämä opinnäytetyö tarjoaa välttämättömän tiedon pienille organisaatioille toimivan tietosuojaohjelman laatimiselle, kehittämiselle sekä ylläpitämiselle uutta asetusta noudattaen. Edellä mainittu on koottu kattavan lainsäädännön, virallisten linjausten sekä muiden asiantuntijoiden tuottaman materiaalin sisältöanalyysin tuloksena.

Avainsanat	Euroopan unionin yleinen tietosuoja-asetus, tietosuoja, rekisterinpitäjä, tietojenkäsittelijä, henkilötieto, viitekehys

LAPIN AMK
Lapland University of Applied Sciences

Abstract of Thesis

School of Business and Culture
Degree Program in Business Information Technology
Bachelor of Business Administration

Author Eija Saaranen Year 2018
Supervisor Jari Sarja
Title of Thesis Applying General Data Protection Regulation in Small Organizations: Simplified Framework and Templates for Managing a Privacy Program
Number of pages 49 + 11

The General Data Protection Regulation became effective on 25th of May 2018. The GDPR aims to create a pan-European legally enforceable data protection standard while enabling free flow of data within Europe. The GDPR will be applied to all businesses and organizations regardless of their size and the maximum punitive measures do not take into account the size of the organization. However, provided the need for changes in any organization's data protection program it is likely that small organizations will lack the knowledge and resources in ensuring their privacy program complies with the GDPR.

This thesis is qualitative in nature and more specifically content analysis was chosen as the precise research method. The end result is a material summary of the relevant information in the GDPR for small organizations and document templates that have been drafted to meet the requirements presented in the GDPR, Article 29 Data Protection Working Party, Data Protection Authorities and other expert sources.

The practical aim of this thesis is to provide the information that is relevant for small organizations in an understandable and concise manner. In addition, a simplified framework with accompanying document templates have been drafted to support the establishment of a privacy program in small organisations. The presented framework consists of four stages and documentation supporting the stages is provided. The stages are; define, plan, document and execute.

This study provides necessary information, process and document templates for small organizations to start their work on establishing, developing and maintaining a functional and GDPR compliant privacy program. The beforementioned was compiled as a result of extensive analysis of related legislation, official guidelines and materials produced by other experts.

Key words General Data Protection Regulation, data privacy, controller, processor, personal information, personal data, privacy program, framework

CONTENTS

FOREWORD

I would like to thank my fiancé for his unwavering support, even though he does not share my enthusiasm on the subject, while I have been working long days on this thesis. I am extremely grateful to my thesis supervisor, Dr. Jari Sarja, who has provided me his support, even when on his annual leave, and shared my enthusiasm.

But most of all, I want to thank my children, who give me, and this thesis, purpose.

ABBREVIATIONS

BCR	Binding Corporate Rules
CNIL	Commission Nationale de l'Informatique et des Libertés
DDoS	Distributed Denial of Service
DPO	Data Protection Officer
DPA	Data Protection Authority
DPIA	Data Privacy Impact Assessment
EEA	European Economic Area
ECHR	European Convention for the Protection of Human Rights and Fundamental Freedoms
EDPB	European Data Protection Board
ePD	ePrivacy Directive (EU) 2002/58/EC
EU	European Union
GDPR	General Data Protection Regulation (EU) 2016/679
SME	Small or Medium Enterprise
USA	United States of America
WWWF	World Wide Web Foundation

1 INTRODUCTION

As we live in a digital era where devices and cloud-based services have become a necessity to provide goods and services to consumers, the amount of data we process has increased exponentially and increased challenges in personal data protection have emerged (Tikkinen-Piri et al., 2017). Furthermore, the ever-evolving technology that enables us to provide and use smart and more efficient devices and services, requires and enables the increased collection of data.

However, the collection of data, especially personal data, brings about its own challenges. Different countries have adopted very different approaches to data privacy; the European model of one governing regulation to set foundation to all data processing activities across different fields is called the comprehensive approach. Whereas the model adopted in the United States in which industry specific requirements apply, is called sectoral approach (Swire et al., 2012; Jolly, 2017). Although, in addition to the comprehensive legislation in European Union, some sectoral laws exist.

According to Commission Nationale de l'Informatique et des Libertés (later CNIL) some level of privacy laws has been adopted in over 80 countries worldwide as can be seen in Figure 1. Despite the implementation of legislation to address privacy the World Wide Web Foundation (later WWWF) recently published The Web Index showing that 84% of countries lack in implementing appropriate legal safeguards and practices to protect the privacy of online communications. The number increased from earlier 63% despite United Nations calling the Member States to review their privacy laws and practices to ensure fundamental freedoms of individuals (WWWF, 2014).

In European Union digitalization and need for modern and uniform legislation has been addressed by passing the General Data Protection Regulation 2016/679 (later GDPR) that became effective 25th of May 2018. The aim of the GDPR is to harmonize the data protection practices in all Member States and enable organizations to operate within Europe effortlessly. The GDPR was built on The European Union Data Protection Directive (95/46/EC) specifying and adding to the requirements presented in it. Such changes include, for example,

implementing one uniform definition of personal data as opposed to each Member State developing their own under the Directive and providing data subject with right for data portability and extended transparency to processing of their personal data.

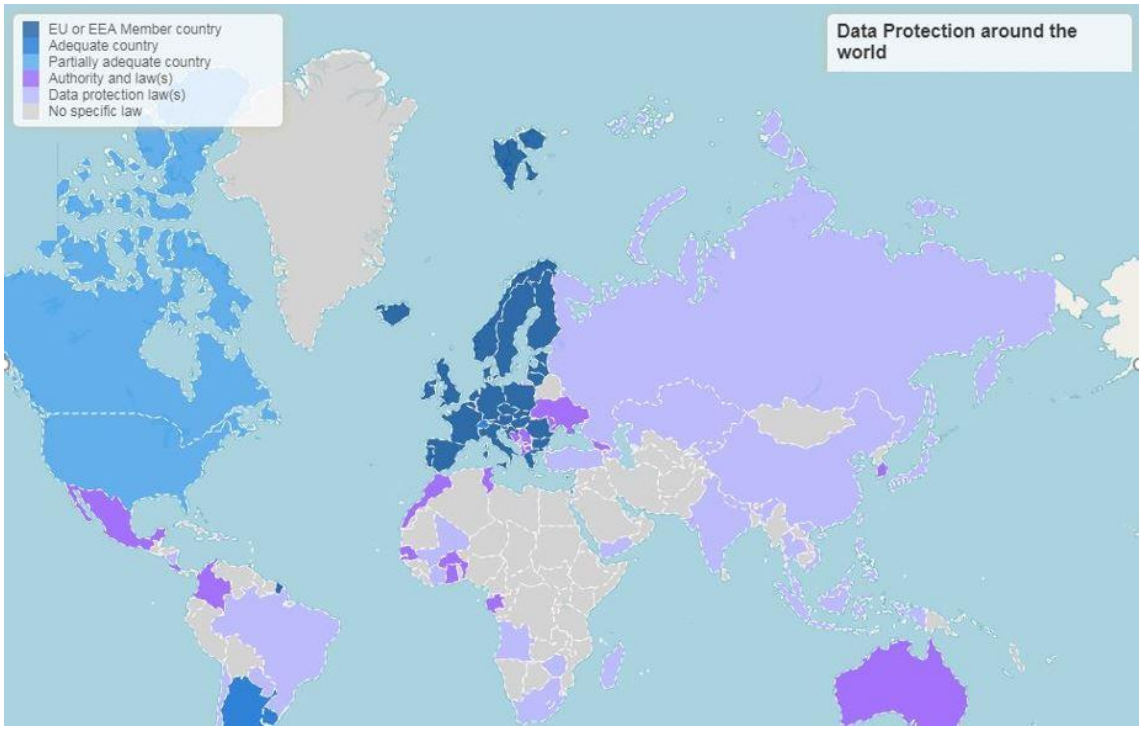


Figure 1 Adequacy of countries in term of data transfers (adopted from CNIL, 2018)

The GDPR applies to all organizations that reside within the European Union or provide services and/or monitor persons within the European Union. Citizenship is not a prerequisite for being protected by the GDPR; living within the borders of European Union is required. Additionally, it is important to note, that European companies cannot create double-standards and provide the required protection only for Europeans, but they are required to apply the same standards to all personal data processing activities. Exception to applicability of GDPR is the so called ‘household exception’. This means that private people, conducting private or household activities do not need to fulfil the requirements of the GDPR (GDPR (EU) 2016/679, Article 2:2c §.)

All organizations to which the GDPR will be applied to need to take steps to ensure compliance as the GDPR brings about the possibility for Data Protection

Authorities (later DPAs) to impose administrative fines up to 20 million euros or 4 % of annual global turnover, whichever is higher in addition to other punitive measures (GDPR (EU) 2016/679, Article 83 §.)

The purpose of this thesis is to provide simplified framework with basic set of general instructions and tools for small organizations, that may not have the required resources themselves or to outsource the task, to become compliant and show compliance should they be audited. Size of the organization is not a factor when considering if the GDPR will be applied to an organization nor is it a factor when considering the amount of administrative fine. However, as stated in Article 83 in the GDPR, the efforts to be compliant and the intentionality of or negligence resulting in infringements or incidents are a factor when deciding on the appropriate administrative fine and other punitive measures, such as suspension of processing activities (GDPR (EU) 2016/679, Article 5 §.)

The following pages will first provide historical background for data privacy, introduce used research methods, an overview of the GDPR and, finally, present the framework for small organizations to start the work on compliance including examples of documentation needed to ensure that their operations are in line with the GDPR.

1.1 Historical Background

The history of privacy extends further back than many of us expect; already in 1890 Samuel Warren and Louis Brandeis published “The Right to Privacy” in the Harvard Law Review. In their essay they defined privacy as the *“right to be left alone*”. Dating even further back, the Jewish law recognizes the freedom not to be watched. Since then several other definitions have been proposed, but the foundation for the modern data protection was laid by the General Assembly of the United Nations in 1948 when the Universal Declaration of Human Rights was adopted (Swire et al., 2012).

In Europe the European Convention for the Protection of Human Rights and Fundamental Freedoms (later ECHR) was established by the Council of Europe in 1950. ECHR started building on the foundation laid by the Universal Declaration of Human Rights and stated that “*everyone has the right to respect*

for his private and family life, his home and his correspondence" (Charter of Fundamental Rights (EU) 2012/C 326/02, Article 8 §)

European Union's first attempt in harmonizing the data protection legislation within its Member States came in 1995 when The European Union Data Protection Directive (95/46/EC) was adopted (later Directive). As a directive it was not enforceable as is, but it required national laws to be passed by the Member States to become enforceable. Despite the effort, the Directive was unevenly interpreted and applied in Member States and it did not provide equal rights to everyone living in the European Union.

Determined to harmonize and create a pan-European, legally enforceable standard for data protection, the European Union started the preparation of the new regulation in 2009 (Tikkinen-Piri et al., 2017). After the law preparation process the European Commission adopted the GDPR on 25th of May 2016. Adoption of the regulation was followed by a two-year transfer period during which companies were able to take actions to ensure compliance. The GDPR became effective on 25th of May 2018 by which time all organizations that process personal information should have been compliant and furthermore, must be able to demonstrate that compliance.

1.2 Research Methods

This thesis can be considered to be qualitative in nature which is described by the University of Utah (2018) to concentrate on the 'why' rather than the 'what'. As Shank (2002) has defined qualitative study as "a form of systematic empirical inquiry into meaning" opposed to quantitative study that is concerned with measurements and numbers (University of Utah, 2018.) From among the several analysis methods that may be used in qualitative study, content analysis is best suited for the purposes of this thesis.

Content analysis is a method where documents and other materials are studied to answer specific questions. As the subject field of this thesis is wide and the scope of bachelor's thesis is limited, the main research question was set to be:

- *How to apply General Data Protection Regulation in small organizations that may lack awareness and/or resources?*

Supporting questions to help answer the main research question are:

- *What documentation is essential to demonstrate compliance?*
- *What information is relevant to small organizations?*

The internet plays a central role in searching for materials for this thesis as European Commission and other officials whose publications have relevance to this thesis, have materials available online. Table 1 shows examples of the search phrases used.

Table 1 Examples of search phrases used in the course of this thesis

Examples of search phrases
General Data Protection Regulation
Data Protection officer or DPO
Data Privacy Impact Analysis or DPIA
Privacy policy and privacy statement
Data Privacy Management
Data Security Management
Data controller and data processor
Right to be forgotten
Right for data portability

Consideration is given to materials made available by such expert organizations as International Association of Privacy Professionals (IAPP) and research foundations. Such materials can be considered as secondary sources of information.

Materials drafted or provided by businesses endorsing their own services or expertise are excluded from the scope of this thesis as they serve commercial purpose and are, more often than not, limited in their scope.

The above mentioned materials are considered to be qualitative in which case, it is necessary to evaluate the publishing time, credibility of the source and the applicability to the scope of this thesis.

Furthermore, it should be noted that spelling and style for this thesis are adapted, where appropriate, from the European Union's Interinstitutional Style Guide: House Rules for the Preparation of Text, which dictates, for example, that Member States shall be capitalized when referring to EU Member States (European Union, 2018).

Legal praxis has not been established at the time of drafting this thesis, therefore the subject matter of this thesis is based on the regulation, interpretations provided by the Article 29 Data Protection Working Party and other materials and templates drafted by The European Commission, data protection authorities and legal advisors. Special attention has been paid to studies and guidelines created by professional organizations and legal advisors, specifically on studies and other material examining the implications of the GDPR and measures that are required to ensure compliance. These materials can be considered as primary sources of information.

This thesis is intended as material summary to serve as an overview of the topic for small organizations. Produced and compiled materials together with the relevant information create an easy-to-understand framework intended to be used by small organizations to ensure their compliance and to serve as a starting point for comprehensive privacy program. It should be noted, however, that it is not intended to serve as or replace legal counsel.

2 REQUIREMENTS PRESENTED IN THE GENERAL DATA PROTECTION REGULATION

The General Data Protection Regulation was approved and adopted by European Parliament on 25th of May 2016. The two-year transition period ended in May 2018 when the GDPR became effective. As a regulation rather than a directive, the GDPR became effective as it is, without the need to pass national legislation by the Member States. However, the GDPR does leave some room for national changes, such as the age limit for parental consent is set to be 16 years of age in the GDPR but Member States can lower it to 13 (GDPR (EU) 2016/679, Article 8:1 §) and the possibility to exempt public bodies from administrative fines (GDPR (EU) 2016/679, Article 83:7 §).

The GDPR imposes requirements for any organization regardless of its geographical location or function, that processes identified or identifiable information of natural persons who are citizens or reside within the European Union. GDPR also states that principles of processing must be the same for all data subjects whose information is processed by any organization regardless of the data subject's location, thus preventing European organizations in creating a double-standard (GDPR (EU) 2016/679, Article 3:1 §)

Furthermore, the GDPR applies to all organizations regardless of the type of the organization; charities and other non-profit organizations are under GDPR similar to businesses or sports clubs.

To meet the requirements presented in the GDPR, as shown in Figure 2, all organizations must take the appropriate technical and organizational measures. The GDPR in itself is vague on what counts as appropriate technical and organizational measures foreseeing the rapid development of modern technology, but it does provide instruction to take into account the state of the art and cost of implementation, which is relevant for small organizations that may not have the same financial resources at their disposal as larger organizations.

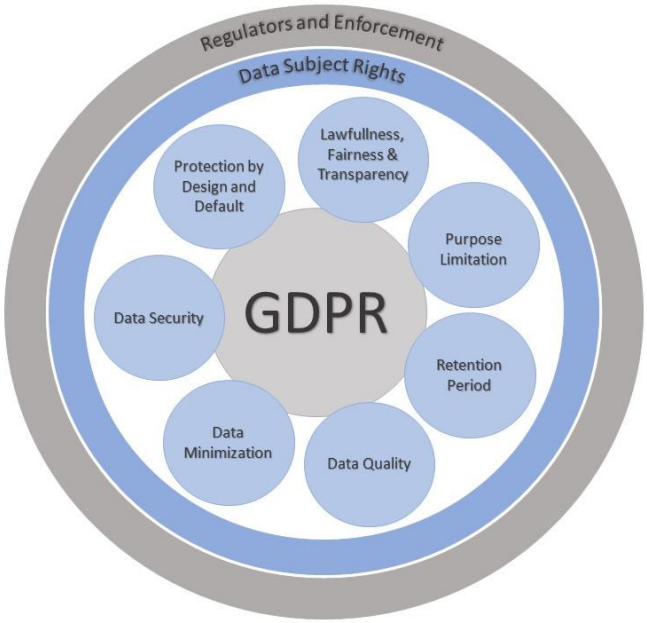


Figure 2 GDPR in a nutshell (adopted from Eccenca, 2018)

2.1 Personal Data and Processing Personal Data

Article 4:1 of the GDPR (EU 2016/679) defines personal data as follows:

"'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;"

Because of the digitalizing world the definition of personal data has been extended to mean such data that has not been previously classified as personal data. European Commission (2018c) provides the following examples when describing personal data:

- a name and surname
- a home address
- an email address such as name.surname@company.com

- an identification card number
- location data (for example to location data function on a mobile phone)
- an Internet Protocol (IP) address
- a cookie ID
- the advertising identifier of your phone

European commission (2018c) does note that some of the above items are governed by specific sectoral legislation regulating for instance the use of cookies; ePrivacy Directive (ePD) or more precisely; Privacy and Electronic Communications Directive (EU) 2002/58/EC. The existing sectoral law is not covered in this thesis, but it is good to keep their existence in mind when planning for your organization's privacy program.

Processing is defined in Article 4:2 in the GDPR (EU 2016/679) as follows:

"'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;"

In other words, from the perspective of the GDPR, processing means anything and everything from collection, storage, encryption, usage and modification of data to its eventual destruction. It is important to note that in this context 'processing' does not require activity from the controller or processor to be taken towards the data; just the storage or archiving the data qualifies as processing.

All organizations process some personal data; at the very least employee data must be processed. But it is likely that some data of customers, members, affiliates or other natural persons is processed. Even in a situation where organizations only co-operate with each other, contact information of the representatives of that organization must be processes. As stated by the

European Commission (2018c); this data is to be considered personal data as well.

Furthermore, European Commission (2018d) and Article 5 of the GDPR (EU 2016/679) present guidelines on what data we can process and under which conditions. These guidelines state that personal data can only be processed for specific purposes (purpose limitation) and only as much personal data can be processed as necessary to fill the purpose (data minimization). All processing activities must be lawful and transparent, and data can not be stored longer than necessary. Recital 39 additionally states that personal data should only be processed if the purpose cannot reasonably be fulfilled in another way.

2.1.1 Data Controller's and Processor's Obligations

As defined by Article 29 Data Protection Working Party (2010); data controller is the natural or legal person, public authority, agency or any other body defining the means and purposes of data processing. Whereas a processor is required to be a separate legal entity from the controller but who is processing personal data on the controller's behalf. What may cause confusion is that an organization can function as a controller and a processor in respect to different sets of data.

Additionally, it is possible to decide on 'how' and 'why' personal data will be processed jointly with another controller, in which case that organization would be a joint controller. In such case, it is important to define each controller's role and to communicate the situation to the data subjects (European Commission, 2018).

If a processor decides to make an independent choice about data processing activities without consulting the controller, the processor will be considered the controller of that data set. In other words; all the responsibilities and liability of a controller will be with the processor (Article 29 Data Protection Working Party, 2010).

The GDPR extends liability not only to the controller, but to the processor as well. In any case the processor is not exempted from administrative fine, damages to data subject or other punitive measures. Compliance and documentation

requirements are extended to the processor in the same manner (GDPR (EU) 2016/679, Recital 146 §)

2.2 Protecting Personal Data

In Europe the issue of privacy is approached from human rights perspective and the European Union Charter of Fundamental Rights (2012) stipulates that all EU citizens have the right to protection of their personal data.

The GDPR, adopted in 2016, protects personal data of natural persons and aims to improve free movement of such data within the EU. Although Europe's approach to data privacy is considered to be comprehensive in nature, some sectoral laws apply in addition; the 'Cookie Directive' or more specifically ePrivacy Directive (EU 2002/58/EC) and Data Protection Directive on Police Matters (EU 2016/680) that governs the protection of personal data in regards of such data being processed in connection with criminal offences or the execution of criminal penalties (European Commission, 2018e).

The GDPR states that appropriate organizational and technical measures must be employed to protect all personal data. This includes protection against unlawful or unauthorized processing as well as protection against accidental loss, destruction or damage (GDPR (EU) 2016/679, Article 5:1 §) Even though the GDPR is not specific on such measures ~~it~~, and Article 29 Data Protection Working Party have provided views on some methods such as pseudonymization and possibility of anonymization of personal data. The GDPR does introduce the concept of privacy by design and default and requires the state of the art, cost of implementation and the nature, scope, context and purposes of processing as well as the related risks to be considered when deciding on appropriate measures (GDPR (EU) 2016/679, Article 25 §)

To supervise and advise on data protection related matters, supervisory organization within EU has been re-organized and clarified. Most of the functions have existed before GDPR but as mentioned, their roles have been clarified.

Each Member State has its own Data Protection Authority who acts as the first point of contact for natural persons or organizations seeking advice, notifying of

a breach or complaining of a breach of the GDPR. Furthermore, they have the power to decide on any punitive measures on organizations in breach of the GDPR. Their work is carried out in accordance with Article 8:3 of the Charter of Fundamental Rights of the EU (2012).

On 25th of May 2018 the Article 29 Data Protection Working Party was replaced by the European Data Protection Board (later EDBP) which is the highest data protection authority in EU. They give advice and guidance on the GDPR to the national data protection authorities as well as determine disputes with them (European Commission, 2018e).

2.2.1 Anonymization

Anonymized data is not considered personal information and the GDPR (GDPR (EU) 2016/679, Recital 26 §) will not be applied to the data that has been processed irreversibly to prevent identification of the data subject (Article 29 Data Protection Working Party, 2014). Article 29 Data Protection Working Party (2014) identify two main anonymization techniques as randomization and generalization, they also note that different techniques may be advisable to be combined to truly anonymize the data. However, pseudonymization is not an anonymization technique and pseudonymizing an attribute of a data subject does not qualify as anonymization. Pseudonymization is explained in more detail in paragraph 2.2.2 Pseudonymization.

However, it may not be possible to render all data anonymous by simply removing the name of the data subject, which may present its own challenges to anonymization as it must be considered if identification is possible by the controller or any other third party by, for example, combining data sets to identify the data subjects. One such example is genetic data which in itself may be unique enough, especially when compared to available genealogy registers (Article 29 Data Protection Working Party, 2014).

Anonymization may be worth considering when, for example, research data is needed as then data protection laws will no longer be applied to it. However, it must be noted, that anonymization needs to be re-evaluated and improved when

necessary during the life cycle of the data (Article 29 Data Protection Working Party, 2014).

2.2.2 Pseudonymization

Unlike anonymization, pseudonymization of data does not qualify it not to be considered personal data (GDPR (EU) 2016/679, Recital 26 §). It is intended as an additional protection measure and only reduces the linkability of a data set with the data subject (Article 29 Data Protection Working Party, 2014).

Pseudonymization means that some unique identifying attribute or attributes of the data subject are replaced by another i.e. a pseudonym such as generated numerical or alphanumerical string. The pseudonym used can be independent from the original attribute or attributes if it is, for example, a randomly generated string. Another option is to use a hash function or an encryption key to create the unique identifiers (Article 29 Data Protection Working Party, 2014).

2.3 Documentation

Documentation is a key requirement stated in the GDPR and it even goes as far as naming some of the required documents and they are necessary for demonstrating compliance in case of a complaint, incident or audit.

The regulation states that the data controller must be able to demonstrate such items as consent given by the data subject (GDPR (EU) 2016/679, Recital 42 §), data processing activity log (GDPR (EU) 2016/679, Article 30 §) and execution of the data privacy impact assessment (later DPIA) to name a few. However, it should be noted that there are conditions that need to be fulfilled before conducting a DPIA or creating BCRs, for example, becomes mandatory.

The required documentation may be executed in electronic form or with the help of privacy software, which may be a cost-effective way to fulfill the requirements of GDPR for small organization (Tikkinen-Piri, et al., 2017.) Recently increasing amounts of specialized software for mapping personal data, consent management tools have been developed and brought to market.

2.3.1 Data Processing Log

Article 30 (GDPR (EU) 2016/679) specifies the requirement of keeping a data processing log and what it is required to contain. Specifically named items to be included in said log are:

- Controller, joint controller, other representative and/or DPO name and contact information
- Purposes of processing
- Categories of data and categories of data subjects
- Recipients of the data
- Information on transfers to third countries and reference to appropriate safeguards or specific situations
- Retention period
- General description of organizational and technical measures taken to protect the data

As any other documentation, the log needs to be kept up to date and evaluated regularly.

2.3.2 Transparency Principle and Informing the Data Subject

As stated in the GDPR all processing activities must be legitimate and transparent to the data subjects whose personal information is being processed. This includes that information on collection, storage and all other processing activities must be easily accessible and presented in plain language for the data subject. Additionally, the data subjects must be made aware of the risks, rules, safeguards, retention periods and their rights in relation to the processed data (GDPR (EU) 2016/679, Article 12 §)

Before GDPR several countries had laws with very specific requirements on privacy statement and its contents. One such example is Finland where a

separate statement had to be made for each data register. However, Finnish DPA recently stated on their webpage that GDPR does not impose as strict rules on separate statements or the exact content of the statement. Informing data subjects is necessary and some minimum requirements are presented, but only one statement to cover all data processing activities will suffice (Office of the Data Protection Ombudsman, 2018).

2.3.3 Data Breach Notification Obligation

A personal data breach is defined in the GDPR Article 4:12 (EU 2016/679) as follows:

"*...a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*."

The definition provided by the GDPR covers both accidental and intentional cases of data breach and the notification obligation extends to even accidental deletion or corruption of a data set in addition to the more obvious theft, misuse, interception and so forth. However, Article 31:3 (GDPR (EU) 2016/679) states that "situations that are unlikely to result in a risk to rights and freedoms of natural persons" do not require a notification to DPA.

In case of an incident such as data breach, authorities must be notified by the controller within 72 hours of becoming aware of the breach. Additionally, the affected data subjects must be notified if the incident is considered to be high risk to the privacy of the data subject. The obligation to notify authorities lies with the data controller. Data processors should notify the data controller who, in turn, will notify the authorities. The processor is required to notify the controller without undue delay, but no specific time limit is defined in the GDPR (Article 29 Data Protection Working Party, 2017).

According to Article 33:3 (GDPR (EU) 2016/679), at the very least a breach notification is required to contain the following information:

- Controller's name, address and contact information

- Controller representatives name and contact information
- When the incident took place
- How the incident was discovered
- What categories of data was breached
- Estimation of how many data subjects and records are affected
- Evaluation on is the incident likely to cause significant risk to the privacy or rights of the data subject
- What actions have been taken or will be taken to mitigate the breach

In addition to being responsible for notifying the authorities, both the controller and processor, are required to maintain an incident log as per Article 33:5 of the GDPR. This log should contain details of the breach, it's effects and remedial actions taken (GDPR (EU) 2016/679, Article 33:5 §).

2.4 Legitimacy of Data Processing

With the GDPR all organizations must be able to identify and inform data subject of the legitimate reason they are processing the data on. This information should be available in the privacy statement that is easily available to the data subject.

Article 6 and Recital 112 of the GDPR (EU 2016/679) provide the lawful reasons for processing personal data which are as follows:

- Data subject has given his/hers consent
- Performance of a contract the data subject is a party to
- Legal obligation of the controller
- Public interest
- Official authority
- Legitimate interests of the controller or third party

- Vital interest of the data subject or another person

For the purposes of this thesis it is noted that the likely reasons for lawfully processing personal data for average organization in usual circumstances are contractual obligation and consent. These two items will be described in more detail in paragraphs 2.4.1 Contractual Obligation and 2.4.2 Consent. However, it should be noted that the legitimate interests of the data controller or a third party do, in some cases, provide a legitimate reason for such activities as marketing (Data Commissioner's Office, 2018.)

If no legitimate reason for data processing can be shown by the controller or processor, the processing is considered illegitimate in which case the data subject can exercise their right to restrict (GDPR (EU) 2016/679, Article 18 §) the use of their data or complain to data privacy authority. It is the DPAs discretion if and when punitive measures are applied.

2.4.1 Contractual Obligation

One legitimate ground for processing is fulfillment of a contract or taking steps before entering the contract to which the data subject is a party to (GDPR (EU) 2016/679, Article 6:1b §) This means that an organization that sells goods or services to data subjects does not need any other legitimate grounds for processing the data required to fulfill the contractual obligation. Such necessary information may be, for example, delivery address, billing information and contact information.

However, it is important to distinguish the purposes the data is used for. As stated in Article 5:1b (GDPR (EU) 2016/679) data can only be collected for specified and explicit purposes, on the principle of purpose limitation. To continue the above example; if the same service provider would also like to use the information for other purposes than filling the contractual obligation, a consent is required for that activity. Such example could be sending a newsletter to customer in which case consent for marketing would be needed. The consent must be explicit and separate from the service contract (GDPR (EU) 2016/679, Article 7:2 §) It is also advisable to mention that the consent is not required to be provided to use the

service. In other words; the data subject has the right to withdraw his/hers consent at any time (GDPR (EU) 2016/679, Article 7:3 §.)

2.4.2 Consent

As listed in paragraph 2.4 Legitimacy of Data Processing, most of the reasons are very specific in nature and for example marketing purposes is not listed in itself. This will lead to a situation where consent will have a significant role in data processing activities in the future.

Consent must be freely given and informed. Data subject must give the permission without duress and be able to withdraw his or hers consent at any time without repercussion for it to be considered freely given (GDPR (EU) 2016/679, Article 7 §)

The GDPR does identify certain situations in which the consent may not be considered freely given (GDPR (EU) 2016/679, Recital 43 §). One example of such situation is the employer-employee relationship in which the parties cannot be considered equal.

Additionally, in a case where children's personal data is to be collected, reasonable effort must be made to ensure parental consent. In the context of GDPR, a person under 16 years of age is considered to be a child. However, Member States have the option to lower this limit to 13 years of age (GDPR (EU) 2016/679, Article 8:1 §)

Furthermore, processing of special categories of data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic or biometric data, health data or data relating to sex life and sexual orientation is prohibited unless there is another legitimate reason for processing or express consent is given by the data subject (GDPR (EU) 2016/679, Article 9 §).

2.5 Appointment of Data Protection Officer

In some cases, a Data Protection Officer must be appointed, but the Article 29 Data Protection Working Party (2016) does encourage organizations to appoint

a DPO voluntarily. A DPO can have another simultaneous role in the organization, which is reasonable in smaller organizations. Benefit of voluntarily appointing a DPO or similar function is assigning responsibility of the privacy program to someone in the company. This way the execution of privacy related tasks will be coordinated and there will be an established point of contact in the organization.

The appointment of a Data Protection Officer is mandatory by public authorities, organizations that engage in large scale systematic monitoring and organizations that engage in large scale processing of sensitive personal data (GDPR (EU) 2016/679, Article 37 §)

As stated by the Article 29 Data Protection Working Party (2016); the controller is responsible for providing adequate resources to perform the tasks of data protection officer and must enable the maintenance of the DPO's expertise.

It is possible to out-source the role of DPO, which may be a reasonable option for small organizations to get expert guidance in privacy related matters at lower cost (Article 29 Data Protection Working Party, 2016).

2.6 Data Subject's Rights

With the GDPR, as defined in Chapter III, the data subjects will have extended rights to their own data. This includes the right to object or limit to the use of data (GDPR (EU) 2016/679, Articles 18; 21 §), right to access all data (GDPR (EU) 2016/679, Article 15 §), right for rectification (GDPR (EU) 2016/679, Article 16 §), data portability (GDPR (EU) 2016/679, Article 20 §) and the right to be forgotten (GDPR (EU) 2016/679, Article 17 §). However, these rights are not absolute (GDPR (EU) 2016/679, Recital 4 §) and the GDPR defines exceptions in which the data controller's or processor's rights and obligations resulting from another law or official authority, national security, defence, public security, judicial independence, criminal investigation and equivalent items will supersede the data subject's rights (GDPR (EU) 2016/679, Article 23 §). For example, a data subject cannot exercise his/hers right to be forgotten in terms of a criminal record or in a situation where they have entered a contract but have not fulfilled their obligations, such as paying for the goods or service, towards it. However, it is

important to distinguish the role of the reason used for the lawful processing of personal data; for example, if data is processed on data subjects' consent, the consent is only considered to be freely given if the data subject has the right to withdraw it at any time (GDPR (EU) 2016/679, Article 7 §).

Articles 13 and 14 (GDPR (EU) 2016/679) discuss the data subjects' right to information of the data processing and what information must be provided to the data subject at the time of collecting the data. Paragraph 2.3.2 Transparency Principle and Informing the Data Subject of this thesis describes the privacy statement and its contents as well as the notion of transparency presented in the GDPR in more detail.

When data subject expresses his or her wish to exercise any of the above rights the reply must be provided without undue delay but always within one month of receiving the request. Extension of up to two months is available for the processor in case the one-month limit cannot be met, for example, due to high quantity of requests (GDPR (EU) 2016/679, Article 12:3 §) Even if no action is required and data subject cannot exercise their right, a reply with a reason for rejecting the request must be provided within one month of receiving the request. The reply is, however, required to contain information on the data subjects right to complain to supervisory authority (GDPR (EU) 2016/679, Article 12:4 §.)

2.7 Cross-Border Data Transfers

By addressing the cross-border data transfers the GDPR aims to limit the risks towards personal data of European citizens. Some countries are considered to be adequate as they are and no additional safeguards such as the BCRs or Standard Contractual Clauses are required for data transfers to these countries (GDPR (EU) 2016/679, Recital 108 §). Naturally this covers European Union Member States, European Economic Area (later EEA) countries (Norway, Iceland & Liechtenstein). On 25.7.2018 the adequacy decision has been made on; Andorra, Argentina, Canada (commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay and a United States of America (limited to the Privacy Shield framework) (European Commission, 2018f).

However, new adequacy decisions will likely be made in the future, for example on Japan as publicized by the European Commission (2018g) and South Korea, but it should also be noted that European Commission reserves the right to maintain, amend or withdraw adequacy decisions and the status should always be confirmed before any data transfers (European Commission, 2018f).

Furthermore, due to United Kingdom's intention to leave the European Union, it would be considered a third country after 30th of March 2019 00:00h CET (European Commission, 2018b).

The GDPR does encourage the establishment of certification mechanisms and data protection seals and marks that would allow organizations to demonstrate their compliance (GDPR (EU) 2016/679, Article 42; Recital 100 §) and lays an extensive groundwork for the application of such mechanisms seals and marks in demonstrating compliance in Recitals 77, 81, 166 and Articles 24, 25, 28 and 30 (GDPR (EU) 2016/679). Article 46f (GDPR (EU) 2016/679) states that existence of such certification may indicate adequacy of an organization in third country. However, no such mechanisms, seals or marks were available yet at the time of writing this thesis.

2.7.1 Binding Corporate Rules

This paragraph is intended as a brief overview rather than a detailed instruction as the target audience for this thesis are small organizations that are unlikely to be multinational and, therefore, have a need to draft Binding Corporate Rules.

Binding Corporate Rules is a concept originally introduced in the Directive, but GDPR continues to recognize the BCR as a way to enable international organizations to transfer data across borders for their organizations use. To clarify; the existence of BCR does not provide for data transfers to third parties but solely internally within the organization which has the BCR in effect (GDPR (EU) 2016/679, Article 47a §)

The BCR are required to be legally binding in nature (GDPR (EU) 2016/679, Article 47c §) and reflect the principles presented in the GDPR, tools for

effectiveness and an element proving that the rules are binding (European Commission, 2018h.)

The BCRs would need to be approved by competent supervisory authority. The first step of the approval procedure is to designate the lead data protection authority for the approval process. The decision is based on relevant criteria such as where is the European headquarters of the organization located, where is the data protection function of the organization located and the EU country from which most of the transfers outside EEA would take place. The organizations decision must be communicated to the intended lead DPA (European Commission, 2018h).

The next step is to draft the binding corporate rules according to requirements presents by Article 29 Data Protection Working Party in WP 153 (2010). After this the BCRs will be circulated among relevant DPAs for commenting. The procedure is closed when the receipt of the BCRs has been acknowledged and it is considered that they comply with Article 29 Data Protection Working Party in WP 153 (2010). A decision will be provided within one month of the receipt of the BCR and other documentation (European Commission, 2018h).

2.7.2 Standard Contractual Clauses

Standard contractual clauses are to be used when transferring data to a party outside your organization in a third country as opposed to BCRs that are intended for internal transfers for multinational organizations (GDPR (EU) 2016/679, Recital 168 §) These clauses cannot be negotiated or altered but must be accepted and signed as set forth by the European Commission (European Commission, 2018i).

So far, the European commission has issued two sets of standard contractual clauses; for data transfers from data controllers in the EU or EEA to controllers outside the EU or EEA and for data transfers from controllers in the EU or EEA to data processors outside the EU or EEA. The standard contractual clauses are freely available in European Commission website (European Commission, 2018i).

2.8 Role of National Legislation

As has been stated previously, the aim of the GDPR is to harmonize data privacy and bring forth a legally enforceable standard for processing of personal information. However, the GDPR does allow some decisions to be made nationally in part, because of Member States' constitutions addressing the issue or the issues fall out of European Union's legal competence (Gabel & Hickman, 2016). For example, Article 8:1 (GDPR (EU) 2016/679) allows for Member States to lower the age of a data subject adequate to give consent for the use of their data down to 13 years of age, even though the Article 8 states it is 16 years of age and Article 83:7 (GDPR (EU) 2016/679) states that Member States have the right to decide if and to what extent administrative fines can be imposed on public bodies.

However, not all the Member States have passed laws accommodating the issues GDPR leaves for the Member States to decide or clarify as seen in Figure 3, which is a concern when creating a privacy program for an organization.

Figure 3 Status of GDPR related national legislation by country (adopted from Bird & Bird, 2018)

Of course, it must be noted, that in addition to different laws from one Member State to the next cause additional headaches, but ~~furthermore~~, third countries may have laws on data protection (i.e. USAs sectoral approach to data protection) which need to be considered when planning for data transfers or providing of goods and services to other countries, including the EU and EEA members.

Nevertheless, local legislation and the data processor's policy on data processing and/or BCRs must be evaluated before the processing has begun and all processing activity must meet the requirements of the above.

3 THE GENERAL DATA PROTECTION REGULATION IN PRACTICE

The purpose of this thesis is to provide basic information and tools for small organizations in understanding and implementing the requirements presented in the GDPR. The following sub-chapters will provide practical explanation and easy-to-understand examples for small organizations. To support the instructions provided below a binder set with templates for the basic mandatory documentation can be found in APPENDICES. The binder set comprises of templates prepared in the course of this thesis to align with the GDPR (GDPR (EU) 2016/679) and have been filled with examples to help any organization to get started with their privacy program.

The documentation provided together with the process presented in Figure 4 and explained in detail in following sub-chapters, form a framework for privacy program for a small organization to follow.

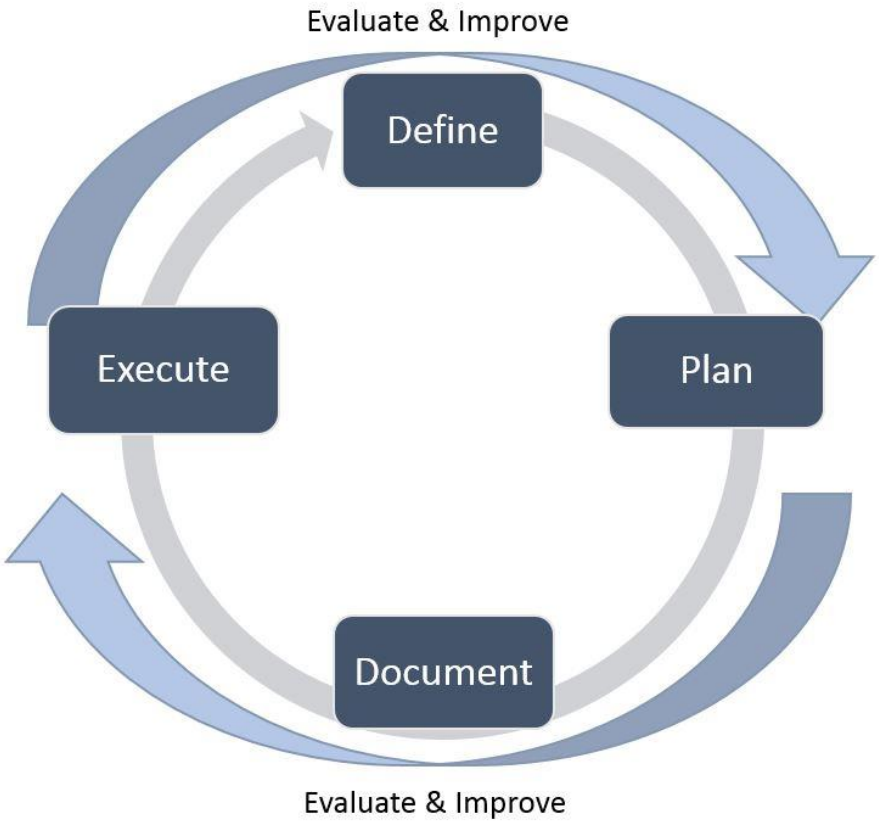


Figure 4 Process for Privacy Program

3.1 Define

Helpful questions to consider during defining phase:

- What are you planning to do?
- What data is the minimum requirement to achieve the desired outcome?
- What is the justification for processing activities?

The first step in establishing compliant data processing activity is to define the roles and responsibilities of your organization as the responsibilities are dependent on the role of controller and processor. However, it is likely that companies have both roles in which case tasks relating to each role must be identified and separated. An organization may have a different role in respect to each separate set of data. The purposes for processing and your organization's role in the processing must be clearly identified and documented separately. Your organization may want to use Appendices 2 and 3, as seen in Figures 5 and 6, as supporting materials to properly structure your processing activities.

PROCESSING LOG OF PERSONAL DATA FOR CONTROLLER							
Purpose of processing	**Name of other parties processing the data and description of their role**	**Description of data subjects**	**Description of personal data**	**Recipients of personal data including cross-border transfers**	**Reference to contract governing the processing**	**Retention period or description of how it will be determined**	**Description of organizational and technical protection measures**
[e.g. salary payment]	[e.g. accounting, processor of data]	[e.g. employees]	[e.g. name, contact information, employment and health information]	[e.g. accounting, tax office	[e.g. employment contract, contractual obligations of the employer]	[e.g. retention period of employment and salary information is governed by law]	[e.g. encryption, access management]

Figure 5 Processing Log of Personal Data for Controllers, Appendix 2

PROCESSING LOG OF PERSONAL DATA FOR PROCESSOR							
Purpose of processing	**Name of other parties processing the data and description of their role**	**Description of data subjects**	**Description of personal data**	**Recipients of personal data including cross-border transfers**	**Reference to contract governing the processing**	**Retention period or description of how it will be determined**	**Description of organizational and technical protection measures**
[e.g. salary payment]	[e.g. Company A, data controller]	[e.g. employees]	[e.g. name, contact information, employment and health information]	[e.g. tax office]	[e.g. service contract]	[e.g. retention period of employment and salary information is governed by law]	[e.g. encryption, access management]

Figure 6 Processing Log of Personal Data for Processors, Appendix 3

At the very least every company will act as a data controller in terms of their own employee's personal data as they are the party deciding on processing of that data. But the other role of your organization could be, for example, a cloud service provider for other companies that store their employee and customer data in the cloud service? In such a situation the organization will act as a data processor and your customers are the controllers of their respective sets of data. As the processor, your organization should always follow the rules for data processing set forth by the controller of that specific set of data.

It is important to differentiate the roles as the responsibilities and liability varies between the roles. In a case where a data processor does an independent decision regarding the data processing activities without the knowledge or consent from the data controller, the processor may be considered to be a data controller in terms of that activity and set of data. Naturally this entails that the responsibilities and liability of the controller will be transferred to the processor.

The next item to determine is the minimum amount of personal data needed to achieve what you are planning. As the GDPR forbids the use of personal data if the same result can reasonably be achieved without the use of personal data, consideration should be given to performing the task without it, for example, by using anonymized data.

Finally, the legitimate reason or justification for the processing activity must be determined as described in paragraph 2.4 Legitimacy of Data Processing.

As a result of the defining phase you should have listed the purpose you are processing the data for, your organization's role in the data processing activity, types of personal data needed and the legitimate reason for the planned activity. For the purpose of this thesis and to provide an example, let's say we have decided on selling clothes to consumers in an online store, our role is the role of a processor, we will need name, delivery address and billing information and we are processing the data to fulfill the orders our customers have made i.e. contractual obligation.

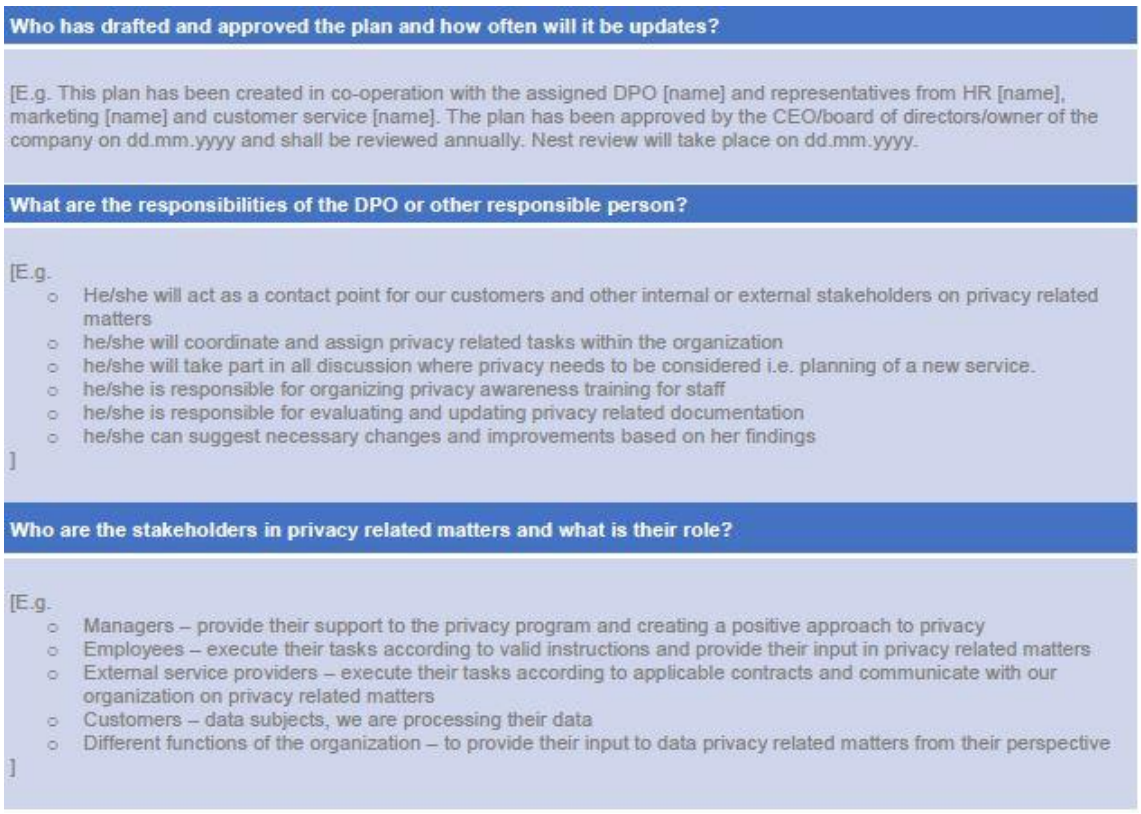
3.2 Plan

Helpful questions to consider during planning phase:

- How will the data be collected?
- Where the data will be stored?
- How will the data subject be informed of the processing activity?
- How will the collected data be protected?
- How will the data subject's rights be ensured?
- Are there national laws to consider?

The target of the planning phase is to design in detail the technical and organizational measures needed for executing the planned activity in a compliant manner.

When planning the personal data processing activities, privacy by design and default should be any organization's leading thought. The GDPR emphasizes privacy by design and default which should be considered the foundation of all personal data processing activities. The GDPR does not give precise set of requirements, especially for technical measures, but requires controllers to consider the state of the art and cost of implementation. This leaves room for the rapid development of technologies. The GDPR does state that continuing improvement is necessary, and it should be noted that after the performance of activities described in this thesis, data controllers and processor should evaluate and improve upon them as a part of their processes (Tikkinen-Piri et al., 2017). To help with continuous improvement a Data Privacy Plan should be drafted. Template for the plan can be found in Appendix 7 and seen in Figure 7.



Who has drafted and approved the plan and how often will it be updates?

[E.g. This plan has been created in co-operation with the assigned DPO [name] and representatives from HR [name], marketing [name] and customer service [name]. The plan has been approved by the CEO/board of directors/owner of the company on dd.mm.yyyy and shall be reviewed annually. Nest review will take place on dd.mm.yyyy.

What are the responsibilities of the DPO or other responsible person?

[E.g.
- He/she will act as a contact point for our customers and other internal or external stakeholders on privacy related matters
- he/she will coordinate and assign privacy related tasks within the organization
- he/she will take part in all discussion where privacy needs to be considered i.e. planning of a new service.
- he/she is responsible for organizing privacy awareness training for staff
- he/she is responsible for evaluating and updating privacy related documentation
- he/she can suggest necessary changes and improvements based on her findings

]

Who are the stakeholders in privacy related matters and what is their role?

[E.g.
- Managers – provide their support to the privacy program and creating a positive approach to privacy
- Employees – execute their tasks according to valid instructions and provide their input in privacy related matters
- External service providers – execute their tasks according to applicable contracts and communicate with our organization on privacy related matters
- Customers – data subjects, we are processing their data
- Different functions of the organization – to provide their input to data privacy related matters from their perspective

]

Figure 7 Excerpt from Privacy Program Plan, Appendix 7

As we established during the first phase; we will be selling clothes to consumers in an online store, our role is the role of a processor, we will need name, delivery address and billing information and we are processing the data to fulfill the orders our customers have made i.e. contractual obligation. To continue on this example; when selling clothing to consumers on a webstore, a delivery address is required to fulfill the contractual obligation of delivering the goods the data subject has purchased. However social security number is not needed if the customer has decided on debit or other form of payment before delivery of goods. But the social security information may be needed to perform a credit check in a case where the consumer has requested to be invoiced after the delivery of goods. In such a case, consent is not required to be provided separately, but the privacy statement must, nevertheless, be easily accessible to the customer as explained in more detail in paragraph 2.3.2 Transparency Principle and Informing the Data Subject. A link to the statement should be readily available on the site. It could be located, for example, in the menu-bar of the webpage and additionally a link may be provided on the order form itself to ensure the customer is aware and is provided the opportunity to peruse the privacy statement before providing

their personal data. In the context of a web-based clothing store it should never be needed to collect medical, ethnic or other sensitive information from the data subject.

It is noteworthy that organizations can identify several purposes for processing data. In this example the service provider may wish to use the collected data for marketing purposes as well. If this is the case, a separate consent is required as the data will be used for another purpose. Appropriate way to collect the information would be to add an opt-in (an empty tick-box, where the data subject must take the action to tick the box to demonstrate consent) possibility to receive marketing communications from the service provider and possibly their partners as well. Inactivity does not constitute as consent as in opt-out approach where activity is required to decline rather than approve the use of personal data for marketing purposes. Such approach to informing the data subject of secondary purpose to collect their personal data and to collect the consent can be considered privacy by design.

It has been established above that name and delivery information such as address is required to be collected for the processor to perform its contractual obligations. The next task is to identify and assess the flow of personal information. Determining the flow of information will help the controller in identifying the physical and logical storage locations of the data, employees who require access to the personal information to perform the work assigned to them, will help determine if the data will be transferred across borders at any stage and will help determining retention period of the data.

As the GDPR states; the impact and risk related to processing of data must be evaluated before the processing starts. This includes conducting Data Privacy Impact Analysis (later DPIA) where necessary. However, it is only recommended to be done unless new technology is used, or processing is likely to result in a high risk to the rights and freedoms of the data subject. DPIA will not be covered in this thesis in detail.

3.2.1 Organizational Measures

Organizational and technical measures are required to be described in data processing logs. All the protective measures must be considered prior to processing and when considering facilitating the processing. Facilitating processing lawfully requires such organizational measures to be adopted as policies, staff training and awareness, contractual measures such as standard contractual clauses, due diligence before choosing partners and data processors and creating a positive culture around privacy related issues. The mentioned items must be considered and formalized prior to the start of processing activities. The beforementioned measures should be included in your organizations Data Protection Plan (Appendix 7).

At this stage, local legislation as well as the legislation of any third country to which the data may be transferred as part of the processing activities should be taken into consideration. Additional organizational measures may be needed to address the differences in legislation.

Organizational measures from other frameworks such as service management could well be applied when considering data processing activities; these frameworks provide best practice guidance in, for example, vendor vetting and information management.

3.2.2 Technical Measures

Technical measures entail the technologies employed to protect the data. However, the cost must be proportionate to the nature of processed data and the purpose the data is processed for. For small organizations out-sourcing and using cloud services are valuable options as choosing such service providers will lower the cost. Additionally, choosing trusted service providers will provide added expertise in protecting the personal data.

Even if services are outsourced it must be kept in mind that responsibilities are not. For example, in a situation where email services are outsourced, and the data is processed on the service provider’s platform and facilities, the responsibilities of the controller are not transferred to the service provider. The

service provider will become a processor for your organization’s data and they will only process the data in accordance with valid service contracts and the controller’s instructions.

Even though data security and data privacy are two separate terms that have different meaning, data privacy cannot exist without data security. Data security relates to the protection of all data regardless of the nature of it, whereas data privacy refers to a subset of data, personal information, and relates to the protection of it.

Furthermore, it should be noted that especially the technical measures needed to ensure the protection of personal data are, for the most part, the same as used to ensure data security. Such measures include but are not limited to:

- password policies and management
- physical integrity of the office(s) and devices used to process personal data
- encryption of hard drives on computers and mobile devices
- hardening of devices and services
- encryption of external medias if used (cloud computing should be preferred to ensure accessibility and portability)
- antivirus software on all company devices including mobile devices
- Employing available technologies to ensure security of the organizations network. For example, firewalls and network segmentation.

The technical measures used should be included in your organization’s Data Protection Plan as well.

3.3 Document

Helpful questions to consider during documentation phase:

- How will a log of processing activities be kept up to date?

- What kind of privacy statement is required?

Documenting the intended activities should begin even during planning of the coming data processing activities and updated throughout the process.

For the ease of understanding your roles with regards to different data sets, two templates are provided; Processing Log of Personal Data for Controllers (Appendix 2) and Processing Log of Personal Data for Processors (Appendix 3). Organization Information Sheet (Appendix 1) is intended as inseparable part of the other documentation you will be compiling in your organization's binder. Questions found on this template will help you understand the data flows and give you an overview of stakeholders in terms of personal data. Filling of the template documentation will help you in identifying the data you are processing and your role in it.

The term privacy policy and privacy statement are often used synonymously even though their meaning is very different. All organizations do need to have both in documented form to prove compliance when necessary. Privacy policy is the internal set of rules and principles for handling personal information whereas privacy statement is the external communication that is generally publicly available, for example, on a company's web page. The information collected with table found under Appendices 1, 2 and 3 should then be used as basis for privacy statement, keeping in mind what information must be made public without compromising other data subject's rights or the security of the data. A template for privacy statement can be found in Appendix 4 and excerpt is shown in Figure 8.

Last two templates provided in this framework are Incident Log (Appendix 5) for keeping record of all data breaches as defined in the GDPR and explained in more detail in paragraph 2.2.3 Notification Obligation. Of each breach an Incident Notification (Appendix 6) should be filled and it can be provided as it is to your local DPA. After all these phases have been completed you can start to execute your data processing activities but the processes and protective measures must be evaluated and improved regularly according to your Data Privacy Plan (Appendix 7).

Data Controller			
Organization's information		[DPO or other point of contact, specify]	
Name		Name	
Company ID		Position	
Address		Address	
Email		Email	
Phone number		Phone number	

Why are we processing your personal information?

[Here you should describe all the processing purposes identified in your organization. It is important to be detailed but keeping in mind that this document is public and should be easily accessible to data subjects. E.g.as a sports club, we process our members information for invoicing, club management and tournament purposes.]

What information are we collecting and processing?

[Clearly specify all the information collected and difference between required information and possible additional information. Processing purposes (e.g. membership and marketing) should be explained and specified what is done under contractual obligation (e.g. membership agreement) and what is done under other legitimate reasons (e.g. consent was collected during enrolling to provide you with personalized marketing in related events and products.)

E.g. When signing up to the sports club we will request you to provide your name, address, email and phone number. Additionally, your social security number is required for insurance and licensing. Membership, payment and tournament information will be added to your data as it accumulates during your membership.

When visiting our website your IP-address may be collected. However, it is not stored or connected to your data.]

Who are we giving your information to?

[E.g. We insure all our club members and therefore we provide your personal data to insurance company. You can find their privacy statement here. (Always add a link to the third party's privacy statement.)

Furthermore, the club purchases annual license for each player annually. Club does this for you to ensure no-one is excluded from a tournament due to non-valid license. When purchasing the license, your information is given to the [name of administering association]. You can find their privacy statement here. (Always add a link to the third party's privacy statement.)

Figure 8 Excerpt from Privacy Statement, Appendix 4

3.4 Execute

After careful planning and documenting the data processing activities can now be executed. Execute any data privacy related tasks first as processing activity should only start after all necessary steps have been taken. Although, as GDPR has only recently become effective, if the privacy program is established only now for already ongoing activities, the needed steps will only be taken after processing has already started. Nevertheless, they need to be taken to show compliance.

In small organizations it may be reasonable to appoint one person to coordinate data security and data privacy related task due to the overlapping and relatively small environment to manage. However, following a structured framework and making sure staff training, data subject requests, evaluation, updates and so forth are planned and documented, will help create the required organizational measures for your company.

To help with execution and continuous improvement of the privacy program, a plan should be created. Appendix 7 will provide a structured form to do this and help establish a process to continue with proper privacy program management.

4 DISCUSSION

The objective of this thesis was to provide concise and easy-to-understand information on GDPR and a simplified framework to function as basis for more comprehensive work on privacy in small organizations. Understanding privacy and requirements around it is essential for any organization in digitalizing world. Raising awareness and providing information and tools in a compact package is essential for the target group, small organizations, which may lack awareness and resources and therefore, unintentionally neglect their responsibilities when it comes to privacy.

By following the 4-step framework and preparing the provided documentation, the small organizations will, firstly, become compliant with the GDPR and secondly gain awareness on the changing privacy related issues. As it has been stated in this thesis, some items that have previously not been considered to be personal data, now are, which may play a role in understanding the topic.

Small organizations could start their work on becoming compliant of privacy regulations by planning their processing activities using the provided templates. The templates will be used as a visual aid throughout the planning and defining phases. The use of the templates will help the organization to ask the right questions and account for items they might not have previous knowledge of. The third phase concentrates on finalizing the documentation in addition to considering if any other documentation, such as Standard Contractual Clauses, are needed before the processing activity can commence. The final phase is continuous in nature. It does concentrate on executing the planned activities, but it also holds in it the principles of continuous improvement that are established in the documented Privacy Plan. It should be noted that the phases are not restrictive in nature and you can, and it is recommended that you do, go back to each phase as necessary, therefore continuously improving on your previous work.

As the GDPR has become enforceable very recently and legal praxis has not been established yet, it poses its own challenges on writing a thesis on the matter. Another challenge is, of course, the fact that data privacy and management of it,

is a vast subject whereas a bachelor's thesis is relatively restricted in scope. However as one of the supporting questions of this thesis concentrates on the relevancy of the data to the subject group, small organizations, some items that are clearly aimed for larger corporations have been left out.

As the future application of the provided framework does require the steps to be taken before the start of processing activities, the initial work, now that GDPR has become enforceable**,** is more complicated. Firstly; since processing activities are already ongoing and may not be understood thoroughly which increases the time needed for mapping these activities. Secondly; no privacy program may have been established in small organizations and review of old documentation may not be possible.

Providing a universal framework to follow when establishing a privacy program is difficult as every organization has different aspects to it, that cannot be accounted for in a generalized model. Nevertheless, as stated in the beginning of this thesis, the aim was to provide simple and easy-to-understand instructions and framework to work as basis for more comprehensive work on privacy, in which this thesis has succeeded.

5 CONCLUSION

This study provides necessary information, process and document templates for small organizations to start their work on establishing, developing and maintaining a functional and GDPR compliant privacy program. Extensive content analysis of documentation prepared by European Commission, Article 29 Data Protection Working Party, Data Protection Authorities and other experts were conducted to provide a concise and easy-to-understand information package and framework for small organizations. The practical aim is to provide the needed information and tools for such organizations that may not otherwise have the needed resources to become compliant. However, as the GDPR only became effective recently and, therefore, legal praxis has not been established at the time of writing this thesis, the current developments should be considered when executing privacy program with the knowledge and documentation provided in this thesis.

BIBLIOGRAPHY

Article 29 Data Protection Working Party. 2008. Working Document setting up the table with the elements and principles to be found in Binding Corporate Rules. Accessed on 25 July 2018 http://collections.internetmemory.org/haeu/20180322140344/http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp153_en.pdf

Article 29 Data Protection Working Party 2010. Opinion 1/2010 on the concepts of "controller" and "processor". Accessed on 22 July 2018 http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf

Article 29 Data Protection Working Party. 2014. Opinion 05/2014 on Anonymisation Techniques. Accessed on 23 July 2018 http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

Article 29 Data Protection Working Party. 2016. Guidelines on Data Protection Officers ('DPOs'). Accessed on 25 July 2018 https://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf

Article 29 Data Protection Working Party. 2017. Guidelines on Personal data breach notification under Regulation 2016/679 (wp250rev.01). Accessed on 22 July 2018 http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052

Bird & Bird. 2018. GDPR Tracker. Accessed on 29 July 2018 https://www.twobirds.com/en/in-focus/general-data-protection-regulation/gdpr-tracker

Charter of Fundamental Rights (EU) 2012/C 326/02

Commission Nationale de l'Informatique et des Libertés. 2018. Data protection around the world. Accessed on 21 July 2018 https://www.cnil.fr/en/data-protection-around-the-world

Data Protection Directive (EU) 95/46/EC

Data Protection Directive on Police Matters (EU) 2016/680

Densmore, R. 2013. Privacy Program Management – Tools for Managing Privacy Within Your Organization. International Association of Privacy Professionals; United States of America.

Eccenca, 2018. Comply with GDPR. Accessed on 17 May 2018 https://www.eccenca.com/en/solutions/comply-with-gdpr.html

European Commission 2018a. What is a data controller or a data processor?. Accessed on 22 July 2018 https://ec.europa.eu/info/law/law-topic/data-

protection/reform/rules-business-and-organisations/obligations/controller-processor/what-data-controller-or-data-processor_en

European Commission. 2018b. Notice to Stakeholders – Withdrawal of the United Kingdom from the Union and EU Rules in the Field of Data Protection. Accessed on 22 July 2018 http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=611943

European Commission. 2018c. What is personal data?. Accessed on 22 July 2018 https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en

European Commission 2018d. What data can we process and under which conditions?. Accessed on 24 July 2018 https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr/what-data-can-we-process-and-under-which-conditions_en

European Commission. 2018e. Data protection in the EU. Accessed on 24 July 2018 https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en

European Commission. 2018f. Adequacy of the protection of personal data in non-EU countries. Accessed on 25 July 2018 https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en

European Commission. 2018g. The European Union and Japan agreed to create the world's largest area of safe data flows. Accessed on 25 July 2018 https://ec.europa.eu/cyprus/news/20180717_en

European Commission. 2018h. Binding Corporate Rules. Accessed on 25 July 2018 https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/binding-corporate-rules_en

European Commission. 2018i. Model Contracts for the Transfer of Personal Data to Third Countries. Accessed on 26 July 2018 https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en

European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR). 1950. Accessed on 4 August 2018 https://www.echr.coe.int/Documents/Convention_ENG.pdf

European Union. (2018). Interinstitutional Style Guide: House Rules for the Preparation of text. Accessed on 6 August 2018 http://publications.europa.eu/code/en/en-4100000.htm

Gabel, D. & Hickman, T. (2016). Chapter 17: Issues subject to national law – Unlocking the EU General Data Protection Regulation | White & Case LLP International Law Firm, Global Law Practice. Accessed on 29 July 2018 https://www.whitecase.com/publications/article/chapter-17-issues-subject-national-law-unlocking-eu-general-data-protection

General Data Protection Regulation (GDPR) (EU) 2016/679

Information Commissioner's Office. 2018. When can we rely on legitimate interests?. Accessed on 5 August 2018 https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/when-can-we-rely-on-legitimate-interests/

Jolly, I. 2017. Data Protection In the United States: overview Accessed on 22 July 2018 https://content.next.westlaw.com/Document/I02064fbd1cb611e38578f7ccc38dcbee/View/FullText.html?contextData=(sc.Default)&transitionType=Default&firstPage=true&bhcp=1

Office of the Data Protection Ombudsman. 2018. Tietosuoja-asetus ei edellytä entisen kaltaista rekisteri- tai tietosuojaselostetta. Accessed on 22 July 2018 https://tietosuoja.fi/artikkeli/-/asset_publisher/tietosuoja-asetus-ei-edellyta-entisen-kaltaista-rekisteri-tai-tietosuojaselostetta

Privacy and Electronic Communications Directive (ePrivacy Directive) (EU) 2002/58/EC

Shank, G. 2002. Qualitative Research. A Personal Skills Approach. New Jersey: Merril Prentice Hall.

Statistics Finland. 2018. Pienet ja keskisuuret yritykset. Accessed on 22 July 2018 https://www.stat.fi/meta/kas/pienet_ja_keski.html

Swire, P. Ahmad, K. & McQuay, T. 2012. Foundations of Information Privacy and Data Protection – A Survey of Global Concepts, Laws and Practices. International Association of Privacy Professionals: United States of America.

Tikkinen-Piri, C., Rohunen, A. & Markkula, J. 2017. EU General Data Protection Regulation: Changes and implications for personal data collecting companies. Computer Law & Security Review: The International Journal of Technology Law and Practice. doi: 10.1016/j.clsr.2017.05.015

University of Utah. 2018. What is Qualitative Research?. Accessed on 5 August 2018 https://nursing.utah.edu/research/qualitative-research/what-is-qualitative-research.php

Warren, S., & Brandeis, L. (1890). The Right to Privacy. Harvard Law Review, 4(5), 193-220. doi:10.2307/1321160

World Wide Web Foundation. 2014. The Web Index. Accessed on 21 July 2018 http://thewebindex.org/report/

APPENDICES

ORGANIZATION INFORMATION SHEET

Updated on: [ddmmyyyy]	By: [Name]

Organization Information sheet is intended to answer basic questions relevant to data privacy and processing activities. It will help you to identify related issues and stakeholders. This sheet will be the first item in your company's privacy binder. Please fill it carefully and review and update regularly.

Data Controller			
Organization's information		DPO or other point of contact	
Name		Name	
Company ID		Position	
Address		Address	
Email		Email	
Phone number		Phone number	

Location of HQ	[City, Country]
Location of other offices	[City, Country] [City, Country] [City, Country]
Line of Business	
Number of Employees	
Number of subsidiaries if any?	
Purposes of data processing in your company?	[e.g. Use log in APPENDIX 2 for guidance. List all the identified purposes here.]
Legitimacy of data processing?	[e.g. Use log in APPENDIX 2 for guidance. List all the identified legitimate reasons here.]
Is data transferred to third countries by your company? If yes, where?	
Have you outsourced services? If yes, what?	[e.g. accounting, IT-services]
Have you established policies to protect privacy, map personal data?	[e.g. Yes, process description can be found in xxxx]
Have you established process to manage consent and privacy preferences?	[e.g. No, evaluation of possibilities on-going]

Have you established a process to answer data subject requests?	[e.g. Not formalized, improvement on-going]
Are you acting as a data processor as part of your business?	[e.g. cloud service provider, accountant, consultant]

Processing Log of personal data is intended as a tool to identify purposes, legitimacy and stakeholders to your organizations processing activities. It will help you to keep a record of processing activities, but also to map governing contracts and plan for future improvements. The template has been drafted in accordance with Article 30 of the GDPR (GDPR (EU) 2016/679) *and should always be attached to the Company and Business Information Sheet.*

PROCESSING LOG OF PERSONAL DATA FOR CONTROLLER

Purpose of processing	Name of other parties processing the data and description of their role	Description of data subjects	Description of personal data	Recipients of personal data including cross-border transfers	Reference to contract governing the processing	Retention period or description of how it will be determined	Description of organizational and technical protection measures
[e.g. salary payment]	[e.g. accounting, processor of data]	[e.g. employees]	[e.g. name, contact information, employment and health information]	[e.g. accounting, tax office	[e.g. employment contract, contractual obligations of the employer]	[e.g. retention period of employment and salary information is governed by law]	[e.g. encryption, access management]
[e.g. sales]	[e.g. logistics partner]	[e.g. customers]	[e.g. name, contact and delivery information]	[e.g. not transferred, services provided locally]	[e.g. service contract and its terms and conditions]	[e.g. for two years after last order]	[e.g. encryption, access management]

Processing Log of personal data is intended as a tool to identify purposes, legitimacy and stakeholders to your businesses processing activities. It will help you to keep a record of processing activities, but also to map governing contracts and plan for future improvements. The template has been drafted in accordance with Article 30 of the GDPR (GDPR (EU) 2016/679) *and should always be attached to the Company and Business Information Sheet.*

PROCESSING LOG OF PERSONAL DATA FOR PROCESSOR

Purpose of processing	Name of other parties processing the data and description of their role	Description of data subjects	Description of personal data	Recipients of personal data including cross-border transfers	Reference to contract governing the processing	Retention period or description of how it will be determined	Description of organizational and technical protection measures
[e.g. salary payment]	[e.g. Company A, data controller]	[e.g. employees]	[e.g. name, contact information, employment and health information]	[e.g. tax office]	[e.g. service contract]	[e.g. retention period of employment and salary information is governed by law]	[e.g. encryption, access management]

PRIVACY STATEMENT

Updated on: [ddmmyyyy]

Privacy Statement is a public document intended to be easily accessible to data subjects to inform them of your organizations data processing activities and principles. Please fill the form carefully in plain and easily understandable language. The template has been drafted in accordance with Articles 12, 13 and 14 of the GDPR (GDPR (EU) 2016/679).

Data Controller			
Organization's information		[DPO or other point of contact, specify]	
Name		Name	
Company ID		Position	
Address		Address	
Email		Email	
Phone number		Phone number	

Why are we processing your personal information?

[Here you should describe all the processing purposes identified in your organization. It is important to be detailed but keeping in mind that this document is public and should be easily accessible to data subjects. E.g.as a sports club, we process our members information for invoicing, club management and tournament purposes.]

What information are we collecting and processing?

[Clearly specify all the information collected and difference between required information and possible additional information. Processing purposes (e.g. membership and marketing) should be explained and specified what is done under contractual obligation (e.g. membership agreement) and what is done under other legitimate reasons (e.g. consent was collected during enrolling to provide you with personalized marketing in related events and products.)

E.g. When signing up to the sports club we will request you to provide your name, address, email and phone number. Additionally, your social security number is required for insurance and licensing. Membership, payment and tournament information will be added to your data as it accumulates during your membership.

When visiting our website your IP-address may be collected. However, it is not stored or connected to your data.]

Who are we giving your information to?

[E.g. We insure all our club members and therefore we provide your personal data to insurance company. You can find their privacy statement here. (Always add a link to the third party's privacy statement.)

Furthermore, the club purchases annual license for each player. Club does this for you to ensure no-one is excluded from a tournament due to non-valid license. When purchasing the license, your information is given to the [name of administering association]. You can find their privacy statement here. (Always add a link to the third party's privacy statement.)

The club will enroll the teams in tournaments and relevant information of all players will be provided to the organizer. Organizers vary, please contact our office if you have questions of a specific tournament.]

Are we transferring your data to other countries?

[E,g. Currently we are not as our club only participates in tournaments locally. Our service providers for accounting and IT-services are located within the European Union.]

How long will you store my data?

[Describe the retention period and/or the factors determining it. Some retention periods are governed by law, such as financial records and employment information. Check your local legislation. Others you must define in your organization.]

What are my rights?

[Here you should describe all the rights the data subject has and how to exercise them.

List of data subjects' rights:

- right to access
- right to object
- right to restrict
- right to be forgotten
- right for data portability
- right to withdraw consent when processing is based on data subjects' consent (e.g. additional newsletters and other marketing)
- right to complain to Data Protection Authority and contact information of your local DPA

It is advisable to mention conditions that may restrict exercising of data subject's rights and advise how quickly the data subject will receive a reply from you.]

Are you using my data for profiling or automated decision making?

[It is important to note that profiling is sometimes used as a tool in marketing. Include other parties you are buying services from (e.g. Facebook Ads, Google Analytics) and provide links to their privacy statements.]

What if I can't find the answer I am looking for in your Privacy Statement?

[Provide clear instructions and contact point for the data subjects for additional inquiries. Update your statement based on feedback received from the data subjects and other stakeholders.]

Incident Log is an overview of recorded incidents that is required to be maintained under the GDPR. Additional information can be stored in the form of the notification and possible reports and other information received from third parties. Gathered information can then be used in evaluating and improving data privacy program. The template has been drafted in accordance with Article 33 of the GDPR (GDPR (EU) 2016/679) *and should always be attached to the Company and Business Information Sheet.*

INCIDENT LOG

Date and time of incident	Date and time DPA was notified	Date and time data subjects were notified	Are other stakeholders affected and when they were notified	Description of incident	Type of affected data	Number of affected data subjects	Corrective actions

INCIDENT NOTIFICATION

Created on: [ddmmyyyy]

Incident Notification is intended to serve as a template when informing your local DPA of a data breach. Internally it is a useful tool to record incidents and use them when evaluating your privacy program. Some local DPAs offer the option to fill out an electronic form on their website. The template has been drafted in accordance with Article 33:3 of the GDPR (GDPR (EU) 2016/679).

Data Controller			
Organization's information		[DPO or other point of contact, specify]	
Name		Name	
Company ID		Position	
Address		Address	
Email		Email	
Phone number		Phone number	

Line of business	[E.g. banking, IT service provider]
Date and time the incident started	[dd/mm/yyyy hh:mm]
Date and time the incident ended	[dd/mm/yyyy hh:mm]
Date and time the incident was noticed	[dd/mm/yyyy hh:mm]
If you were notified by a processor, when?	[dd/mm/yyyy hh:mm]
How was the incident discovered?	[E.g. User notified of a lost device, processor notified of anomalies during routine network scan]
Other affected parties	[E. g. co-controller or processors. Specify affected party's names and contact information]
Description of the incident	[E.g. Employees luggage was stolen in Luxembourg Airport. The luggage contained a company laptop and mobile device that both have company information on them and access to shared resources.]
Methods used by the breaching party?	[E.g. Theft or DDoS attack]
Was the breach caused directly or indirectly by negligence or intentionality? Please elaborate.	[E.g. Yes, disgruntled employee copied customer database and took it with him/her.]
What types of data are affected?	[E.g. names, addresses, phone numbers, salary information, health information]

Was special categories data affected?	[E.g. Yes, union membership and criminal background information]
What categories of data subjects were affected?	[E.g. customers, employees, patients]
Estimated number of affected data subjects?	
How the breach my affect data subjects?	[E.g. Possibility of identity theft, other unauthorized use of data]
Does the breach result in high risk to the privacy and rights of the data subject?	[E.g. No, as the information did not contain sensitive or special categories of information and device was remotely erased.]
Have the affected data subjects been notified?	[E.g. No, as the incident does not result in high risk./Yes, the data subjects will be notified within the next 24 hours.]
Actions taken after the breach?	[E.g. Device was remotely wiped, police were notified and lost external media was returned, network security and additional protection measures have been implemented i.e. firewall rules]
Is it necessary to notify other European DPAs, third countries data privacy officials or any other officials?	[E.g. Yes, multiple data subjects who were affected live elsewhere (name authorities)]

PRIVACY PROGRAM PLAN

Updated on: [ddmmyyyy]

Privacy Program Plan is intended to describe the activities and steps your organization is taking to ensure a functioning privacy program. By following the plan, you will ensure the Privacy Program is evaluated regularly.

Data Controller			
Organization's information		[DPO or other point of contact, specify]	
Name		Name	
Company ID		Position	
Address		Address	
Email		Email	
Phone number		Phone number	

Who has drafted and approved the plan and how often will it be updates?

[E.g. This plan has been created in co-operation with the assigned DPO [name] and representatives from HR [name], marketing [name] and customer service [name]. The plan has been approved by the CEO/board of directors/owner of the company on dd.mm.yyyy and shall be reviewed annually. Nest review will take place on dd.mm.yyyy.

What are the responsibilities of the DPO or other responsible person?

[E.g.
- He/she will act as a contact point for our customers and other internal or external stakeholders on privacy related matters
- he/she will coordinate and assign privacy related tasks within the organization
- he/she will take part in all discussion where privacy needs to be considered i.e. planning of a new service.
- he/she is responsible for organizing privacy awareness training for staff
- he/she is responsible for evaluating and updating privacy related documentation
- he/she can suggest necessary changes and improvements based on her findings

]

Who are the stakeholders in privacy related matters and what is their role?

[E.g.
- Managers – provide their support to the privacy program and creating a positive approach to privacy
- Employees – execute their tasks according to valid instructions and provide their input in privacy related matters
- External service providers – execute their tasks according to applicable contracts and communicate with our organization on privacy related matters
- Customers – data subjects, we are processing their data
- Different functions of the organization – to provide their input to data privacy related matters from their perspective

]

Describe the organizational measures used to ensure privacy?

[E.g. Per this plan we have:
- assigned responsibility of the program
- evaluated our actions
- created the necessary documentation
- policies to ensure best protection practices are applied
- provided privacy awareness training for all employees
- planned for additional training on internal processes
- involved internal stakeholders from all levels to ensure a comprehensive privacy program

]

Describe the technical measures used to ensure privacy?

[E.g. Per this plan we have:
- Access management – everyone has access to only that data which is required to perform their work
- Encrypting - medias used in the company
- Firewall management – default deny rules
- Network segmenting

]

How are the organizational and technical measures evaluated?

[E. g. The evaluation is continuous and as feedback is received from stakeholders, improvements are considered. Additionally, if breaches happen they are evaluated and improvements to prevent future incidents of the same nature are implemented.

External audit is being planned to map the need for improvements.]

Describe the baseline of privacy/last period?

[List changes in data processing activities when compared to last period, analyze incidents and so on. Visual aids, such as graphs, to see developments in amounts of breaches, data subject request and so forth are a valid tool to establish and follow up on the baseline.]

Describe the planned actions/improvements for the next period?

[Consider the baseline and agree on areas to improve on coming year. Even if there would be no evident issues, actions such as establish a new process or improve on onboarding/offboarding of new employees can be added to ensure continuous improvement. Set goals that are realistic when considering the available resources.]