Pasi Arola

Avoiding GDPR Data Breach
A guideline for SAP ERP business systems

Metropolia University of Applied Sciences
Master of Business Administration
Business Informatics
Thesis
13.2.2019
The purpose of this study was to create a handbook how to technically configure a SAP ERP system to avoid Data Breach attempts with selected non-licensed SAP-tools. This requirement of protecting the personal business data comes from the EU legalization of Global Data Protection Regulations. This is EU wide Data Protection Regulation and it came into effect 25th of May 2018. Example Company-X of this thesis is a big international IT-company, which operates in Finland and all examples concerning SAP-tools are related to its SAP department locating in Finland.

Existing knowledge was created to understand current situation about Global Data Protection readiness among of SAP customers related to Company-X, and to have understanding about Global Data Protection Regulations and SAP-tools concerning data breach. Three separated SAP tools were chosen, for this purpose. These three selected SAP-tools were not licensed products. Reason for this was, that they are available for all who have installed SAP ERP systems. Licensed products have been taken into account very shortly, and mentioned in the existing knowledge, but main focus is on the non-licensed SAP-tools. Conceptual framework tells background and version information about the SAP-tools, background information about Global Data Protection data breach regulations, and also includes current state analysis. Data for the current state analysis was collected by the survey interviews, inside of the Company-X, and for the Global Data Protection Regulations and SAP-tools existing knowledge collected by literature. Current state analysis and existing knowledge were combined together to build a framework for configuring chosen SAP-tools to avoid Data Breach attempts in SAP ERP systems.

The outcome of this study is a handbook: Instructions using SAP tools concerning Global Data Protection Regulations. Three selected SAP-tools: Read Access logging, Table Logging and Security Audit logging, were chosen to be configured. Technically instructions have been demonstrated with pictures, for each one of the tools. With instructions given in the proposal section it is possible to set those tools working, and make any SAP ERP system to be Global Data Protection Regulation compatible, concerning the data breach. Validation of the proposal has been demonstrated on Company-X demo systems as well in some live customer systems, and all given instructions have been also validated by specialist’s working with these issues. The author recommends these instructions to all who are working with Global Data Protection Regulations and data breach in SAP environments.

Keywords

SAP ERP, GDPR Data Breach, SAP-tools
## Content

1. **Context: Problem/Challenge, Objective and Outcome**
   - 1.1 Introduction
   - 1.2 Business Challenge
   - 1.3 Case Company
   - 1.4 Objective and Scope
   - 1.5 Thesis Outline
   - 1.6 Key Terms

2. **Research methods**
   - 2.1 Research Approach
   - 2.2 Research Design
   - 2.3 Data Collection and Analysis
   - 2.4 Creation process of proposal

3. **Current state analysis**
   - 3.1 SAP systems
     - 3.1.1 Finug Seminar March 2018
   - 3.2 CSA survey
     - 3.2.1 Analysing Data Breach readiness in Customers SAP environments
     - 3.2.2 Analysing GDPR Data Breach awareness by customers
     - 3.2.3 Analysing Data Breach awareness by specialists and managers
     - 3.2.4 Analysing motivation by managers and specialists
     - 3.2.5 Analysing email survey re-check
   - 3.3 GDPR project of Company-X
     - 3.3.1 Three Level System
     - 3.3.2 Minimum Level
     - 3.3.3 Modesty Level
     - 3.3.4 Maximum Level
   - 3.4 Summary

4. **Conceptual Framework**
   - 4.1 GDPR in general
     - 4.1.1 Personal Data, Data controller and Data processor
     - 4.1.2 Right of access
     - 4.1.3 Right to be forgotten
     - 4.1.4 Data Breach notification
4.1.5 Privacy by design 18
4.1.6 Penalty 19
4.2 SAP concerning GDPR 19
  4.2.1 SAP approach to Data Breach 20
  4.2.2 SAP security flaw 20
4.3 Three level security system 21
  4.3.1 Data Breach from the outside 21
  4.3.2 Data Breach from the inside 22
  4.3.3 Data Breach misusing the data 23
4.4 SAP Tools 23
  4.4.1 General description of SAP Tools 24
4.5 RAL Read Access Logging 24
  4.5.1 Availability 26
  4.5.2 RAL and Data Breach 26
4.6 Security Audit Logging 26
  4.6.1 Data Breach and Security Audit Logging 27
  4.6.2 Availability 28
4.7 Table Change Logging 28
  4.7.1 Data Breach and Table Change Logging 29
4.8 Application logging 29
4.9 Data Archiving 29
4.10 Some licensed products 29
  4.10.1 ILM 30
  4.10.2 GRC 30
4.11 SAP consultant’s role 31
5 Proposal; Instructions using SAP tools concerning GDPR 31
  5.1 Introduction 31
  5.2 Technical implementation of RAL (Read Access logging) configuration 32
    5.2.1 Authorizations to be concerned 32
    5.2.2 Enable RAL 32
    5.2.3 Creating Logging purpose 34
    5.2.4 Logging Domain 35
    5.2.5 Recording 36
    5.2.6 Recording of monitored objects 38
    5.2.7 Creating Configuration 40
    5.2.8 Configuration’s configuration 41
    5.2.9 Monitoring RAL entries 44
  5.3 Technical implementation of Table Change Logging settings 47
<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.3.1</td>
<td>Pre-requisite parameter</td>
</tr>
<tr>
<td>5.3.2</td>
<td>Listing the tables which are pre-configured to be recorded</td>
</tr>
<tr>
<td>5.3.3</td>
<td>Including tables in recording</td>
</tr>
<tr>
<td>5.3.4</td>
<td>Monitoring table change entries</td>
</tr>
<tr>
<td>5.4</td>
<td>Technical implementation of security audit logging</td>
</tr>
<tr>
<td>5.4.1</td>
<td>Profile parameters activation</td>
</tr>
<tr>
<td>5.4.2</td>
<td>Profile creation</td>
</tr>
<tr>
<td>5.4.3</td>
<td>Monitoring entries</td>
</tr>
<tr>
<td>5.5</td>
<td>Summary of the proposal</td>
</tr>
<tr>
<td>6</td>
<td>Validation of Proposal</td>
</tr>
<tr>
<td>6.1</td>
<td>Practical validation</td>
</tr>
<tr>
<td>6.2</td>
<td>Validation by system specialists</td>
</tr>
<tr>
<td>6.3</td>
<td>Validation of GDPR leading consultant</td>
</tr>
<tr>
<td>6.4</td>
<td>Validity and Reliability</td>
</tr>
<tr>
<td>7</td>
<td>Conclusions and Discussions</td>
</tr>
<tr>
<td>7.1</td>
<td>Objective and outcome</td>
</tr>
<tr>
<td>7.2</td>
<td>What did I learn about the process?</td>
</tr>
<tr>
<td>7.3</td>
<td>What would I do differently?</td>
</tr>
<tr>
<td>7.4</td>
<td>What in the future?</td>
</tr>
<tr>
<td>7.5</td>
<td>Discussions with specialists</td>
</tr>
<tr>
<td></td>
<td>References</td>
</tr>
<tr>
<td></td>
<td>Appendices</td>
</tr>
<tr>
<td></td>
<td>Appendix 1. Questions for system specialists</td>
</tr>
<tr>
<td></td>
<td>Appendix 2. Questions for GDPR group member</td>
</tr>
<tr>
<td></td>
<td>Appendix 3. Questions for managers</td>
</tr>
</tbody>
</table>
1 Context;Problem/Challenge, Objective and Outcome

1.1 Introduction

The outcome on this thesis is a handbook on how to technically configure a SAP ERP system to avoid Data Breach attempts with selected non-licensed SAP tools. The thesis also shows how to monitor possible attempts concerning critical business data especially personal data by selected SAP tools. This requirement of protecting the personal business data comes from the EU legalization of GDPR regulations.

GDPR is EU wide data protection regulation. It concerns personal data processed in any business system inside of EU area. All data, which is pointed on some person, with any indicator like address, personal id number, name, date of birth and information like that, is under the GDPR regulations. EU has specially regulated stricter data processing and controlling rules, and this demands that all companies who are processing this kind of data must be able to demonstrate, that personal data is protected like regulations say. (EUGDPR 2016)

Data breach is one part of the GDPR regulations. It is defined in GDPR regulations in following way: "'personal data breach' means 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;" (EUGDPR 2016). In this research, we concentrate on data breach area and how to cover it mainly in SAP ERP systems according of GDPR regulations. Data processors must be able to monitor systems and be able to detect if there have been any data breaches to personal data. If such a thing has happened, it must be announced to authorities, and even to person whom it concerns in 72 hours from the moment it was detected. (EUGDPR 2016) This kind of new stricter regulations, which have harder demands than earlier regulations had towards business systems. This research responds to that challenge, how to cover up personal data protection area in data breach situations in SAP systems.

1.2 Business Challenge

GDPR which is EU wide regulation concerning personal data processing in business systems. Personal data processing includes stricter data access, storing and deleting
rules. One very important issue is the data protection in the case of data breach. This raises a question: How data controllers and processors make their SAP systems to be ready for data breach situations? SAP systems have very complex structures and personal data is spread throughout SAP systems with the different elements and structures. There is also not an automatic ready protection configuration in SAP systems. That is why there is a need, to configure data protection functionalities in SAP systems, with the SAP specified tools trying to avoid and monitor possible data breach situations.

In this thesis work, focus is on avoiding personal data breach situation by SAP tools, which are included in SAP system initial-installations and those tools are not needed to be licensed differently. This in work chosen model to use non-licensed SAP tools because all customers who are using SAP ERP systems are in this way able to use those tools without extra license costs.

1.3 Case Company

In this research name Company-X is used instead of using the company’s real name. Company-X’s role is to be like an example concerning proposal configurations and seen as a service provider for the needed services, like providing help to configure needed configurations. Company-X was used also as a source for requesting data about GDPR current situation. Company-X is a big international IT-company, which works in different kind of areas in IT-business in worldwide. For this thesis work, the information is collected from Company-X SAP business locating in Finland. In Finland Company-X has a competitive SAP department and it functions as SAP service provider for many different SAP customers in different industries in Finland. When the name Company-X is used, this will refer mainly in Finland located SAP department of it because the data and examples are related to this Finnish department and its customers.

1.4 Objective and Scope

Main objective of this study is to create guidelines of how to avoid data breach and monitor possibly data breach attempts, using SAP’s offered free licensed ERP applications SAP tools. The guidelines instruct customers what kind of free licensed SAP tools they can use in their SAP environments to fulfil requirements of GDPR data protection concerning of data breach demands and which steps are needed to be taken to configure these tools be ready in their SAP ERP systems. The study focuses on possible data breach situations in customers SAP systems, especially in the SAP ERP system.
Licensed tools are intentionally left out from this thesis work, because licenses can be very big cost for the customer and purpose is to give instructions, which are applicable for all who have purchased and are using SAP ERP system without extra licensed tools.

1.5 Thesis Outline

This thesis work was done qualitative methods using interviews, questionnaires, internal documentations and participating seminar and have meetings with specialists. Literature used in this thesis is mostly official SAP documentation and GDPR legislation journals and publications from consulting companies.

Thesis structure is following. Questionaries’ made to stakeholders who are working tightly in different SAP customer environments. Participated to GDPR seminar and studied GDPR material concerning personal data breach. With this knowledge, current state analysis has been made. After Current state analysis, suitable SAP tools have been chosen and conceptual framework has been created together with proposal guidelines. Proposal has been finished validating it together with GDPR and system specialists. During the validation of proposal discussed topics have raised up. Some of those issues have been processed in Discussions and Conclusions chapter.

1.6 Key Terms

**Data processor** means: “‘processor’ means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;” (European Union 2016, reg.4:(8)).

**Data controller** means: “‘controller’ means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data;” (European Union 2016, reg.4:(7)).

**GDPR** means General data protection regulations and it is legislated by EU. Data breach means that someone access unlawfully your system and gets data, which is not permitted. (European Union 2016)
**Personal Data Breach** means when someone breaches unlawfully personal data which is stored in business system any business system located in EU area. (European Union 2016)

**SAP Client.** Client is the unit where in SAP users are operating with reports, transactions and other functionalities.

SAP Consultant is a specialist who works in some SAP area configuring, solving problems, installing new functionalities, creating new functionalities and consulting customer in different kind of situations.

**SAP ERP** is enterprise-planning system, which can have lot of different instances and components, and it enables to run different kind of business processes like selling, purchasing, reporting etc. (SAP Support portal 2018)

**SAP NW** means Sap NetWeaver. NetWeaver is the platform where on SAP ERP systems are based on.

**Transaction** in SAP terms means giving a transaction code and start a function, which executes wanted program this is called a transaction. Giving a transaction code and executing it makes the transaction happen.

## 2 Research methods

### 2.1 Research Approach

This study is an applied research project. Applied research project aims to solve specific problems, like Bell and Waters have written:” It is applied research, carried out by practitioners who have themselves identified a need for change or improvement, sometimes with support from outside the institution; other times not” (Bell & Waters 2014, p.19). In study this research problem itself has been identified observing changing IT-structure and its regulations legislated by EU-authorities and collecting information from the people who are working with different customer SAP systems. This study uses mainly qualitative methods, which tries to increase overall understanding of research object and topic. (Jyväskylän Yliopisto 2010)
2.2 Research Design

The research process includes following steps:

Data1: The first step includes Current State Analysis. In CSA current situation is observed with different methods. Data is collected via email inquiries, taking notes and recordings in seminar and meetings and additionally making personal discussions with specialists and managers. Data is analysed comparing answers and created notes making conclusions from them. Data1 phase will give a picture of current situation among of customers as well in the side of Company-X concerning readiness of GDPR Data Breach in SAP ERP systems. Existing knowledge of GDPR Data Breach regulations and SAP tools from the SAP support portal is used to create Conceptual Framework. Conceptual Framework describes GDPR regulations concerning data breach and explains features of selected SAP tools. In Conceptual framework there is also included in security aspect of SAP systems and at the end also some information about licensed tools. All this knowledge together creates Conceptual Framework.

Data2: Second phase Data2 which includes building a proposal: technical configuration guide lines for selected non-licenced SAP tools. Guidelines will be included in the proposal chapter. The proposal covers up Data Breach regulations demanded by GDPR regulations set by European Union. Proposal has been constructed mainly from the existing knowledge of the SAP documentation and best practices based on Company-X's SAP technical team. Company-X has lot of different SAP customers and all configurations, which are instructed in the proposal, have been tested either in some of customers environment or in some demo system owned by Company-X.
Data 3: Validation of the proposal. When the proposal has been constructed, there have been final meetings and discussions about it with GDPR and System specialists. Specialists and leading GDPR project member have gone through the proposal and validated it. Notes have been written about their feedback. There have been two separated validation sessions, first with system specialists and other one with leading GDPR specialist. Discussion, which have been made in these sessions, have been noted and important comments taken in Discussion and Conclusion chapter. The final proposal can be found under the chapter 5 in this thesis work.

2.3 Data Collection and Analysis

Purpose for the data collection of current state analysis is to create evidences for it. It has been collected from the managers and GDPR project members and system specialists. Collection of data has happened via email queries and questionnaires made by Google Forms. All these questions and queries were sent to receivers, three groups of people via email. After some months, re-checking questions have been sent to few of managers and one GDPR specialist to recheck the current situation among of the SAP customers. Data collection process is illustrated in Table 1 below.
<table>
<thead>
<tr>
<th>Phase</th>
<th>Data Type</th>
<th>Source</th>
<th>Year/Month</th>
<th>Approach</th>
<th>Data collection method</th>
</tr>
</thead>
<tbody>
<tr>
<td>(DATA 1) Current State Analysis</td>
<td>Questionnaire</td>
<td>Technical specialist</td>
<td>2018/2</td>
<td>Google forms</td>
<td>Questionnaire online</td>
</tr>
<tr>
<td></td>
<td>Questionnaire</td>
<td>GDPR project group</td>
<td>2018/2</td>
<td>Google forms</td>
<td>Questionnaire online</td>
</tr>
<tr>
<td></td>
<td>Questionnaire</td>
<td>Manager</td>
<td>2018/2</td>
<td>Google forms</td>
<td>Questionnaire online</td>
</tr>
<tr>
<td></td>
<td>Observer</td>
<td>GDPR Meeting project group</td>
<td>2018/3</td>
<td>Meeting/presentation</td>
<td>Recording, notes</td>
</tr>
<tr>
<td>(DATA1) Current State Analysis</td>
<td>Observer</td>
<td>Finug GDPR seminar</td>
<td>2018/3</td>
<td>Meeting/lessons</td>
<td>Recording, notes</td>
</tr>
<tr>
<td>(DATA1) Current State Analysis</td>
<td>Email inquiry</td>
<td>managers</td>
<td>2018/12</td>
<td>Email</td>
<td>Written answers</td>
</tr>
<tr>
<td>(DATA1) Current State Analysis</td>
<td>Email inquiry</td>
<td>specialist</td>
<td>2018/12</td>
<td>Email</td>
<td>Email answers</td>
</tr>
<tr>
<td>(DATA 2) Building proposal</td>
<td>Existing knowledge</td>
<td>SAP documents</td>
<td>2019/01</td>
<td>Literature</td>
<td>notes</td>
</tr>
<tr>
<td>(DATA 2) Building proposal</td>
<td>Company-X best practices</td>
<td>Demo Systems</td>
<td>2019/01</td>
<td>Practical work</td>
<td>Screen shots</td>
</tr>
<tr>
<td>Validation</td>
<td>discussion</td>
<td>specialists</td>
<td>2019/01</td>
<td>meeting</td>
<td>notes</td>
</tr>
<tr>
<td>Validation</td>
<td>discussion</td>
<td>GDPR leading specialist</td>
<td>2019/01</td>
<td>meeting</td>
<td>notes</td>
</tr>
</tbody>
</table>

Table 1. Data Collection plan

During the data collection process there have been also some meetings and discussion in those meetings when data is collected observing the topic with notes and recordings. One seminar has been participated, which concerned GDPR issues and was organized by Finug, which is well known SAP customers organization in Finland. Analyzing all this data together has given reliable sources to build up current state analysis.

The proposal is based strongly on SAP documentations and best practices in Company-X together with the SAP tools used in the proposal. The proposal is created for the situation, which comes from current state analysis and can be achieved with selected non-licensed SAP tools described in the proposal.
Validation of the thesis work has been in two stages. First stage was to collect data and existing knowledge, where all groups mentioned earlier participated to data collecting process via questionnaires. Second stage has been done after proposal creation, proposal has been discussed through with GDPR and system specialist has and validated with them. Questions of the questionnaires will be gone through later in current state analysis Chapter 3 and all questions and questionnaires will be found in Appendices at the end of this work.

2.4 Creation process of proposal

Creation of the proposal is strongly based on SAP documentation, which can be found from their Support Portal references marked as SAP help portal 2018. General there do not exist many references in this thesis work, besides of SAP help portal documentation, because of the tight SAP specified nature of the issue dealt with in this thesis work. It was not easy to find multiple sources telling about SAP data breach nowhere else than from officially SAP documents. This is the reason why this thesis work mostly rely on the fact, that SAP knows their own products best and they are the best direction for the documentation to tell what must be done with their products. For this reason theoretic background of the proposal mainly comes from the SAP documentation. Best practices of the Company-X have been also one source used to create the proposal technically, this means all configurations mentioned in the proposal have been tested on Company-X's own demo systems and discovered to work. The best practices in Company-X and SAP documentation have given the direction which SAP tools should be chosen. One criterion was to have non-licensed tools and second criterion was to have tools which really are compatible to cover requirements coming from the GDPR regulations. Collecting existing knowledge and comparing it to current state analysis and making conclusions of the situation three non-licensed SAP tools have been chosen. These tools have been tested either on demo systems of Company-X or in some real customer environment. All the information, which is, recorded when tools have been used for demo purposes regarding this thesis work and are copied onto this work and could expose some personal or detailed information of any user, system or something similar, has been masked in the example figures. Only personal information, which can be seen in the proposal chapter's example figures, is the information concerning author of this thesis work. This information has not been seen critical because the name of the author is unclassified and can be found on the cover page and information area of this thesis work. All the examples in proposal concerning configuration of the SAP tools are authentic and
have been tested in real life systems. All the example information in the proposal collected and copied onto this work is authentic from the real life SAP systems. There are no assumptions in the proposal, all what have been demonstrated, have been tested in real life systems. This is very crucial thing, which validates the proposal. When the proposal was created and it was ready, it has been validated with GDPR and system specialists. Proposal has been demonstrated to them and they have given feedback of it and validated it to be valid in real life scenarios. Some of these discussions and comments are included in Validation, Discussions and Conclusions chapters.

3 Current state analysis

Current states analysis was made from the following elements: Questionnaire data which was collected by Google form questionnaires, email queries, notes and observations collected by participating to seminar, meetings and personal interviews with specialists. Specialist have very deep knowledge what is going on in customers SAP systems and that’s why information got from them is very valuable concerning current state analysis. Meaning for the current state analysis is to get data about the situation of the current state concerning GDPR data breach awareness among of customers and those who are working tightly with customers. Google form questionnaires can be found from the appendices and they are grouped in those three different groups. Email queries are told in Analysing email survey in chapter 3.2.5.

3.1 SAP systems

Situation concerning SAP systems does not differ much from the other systems. Many of the customers have their own processes how they process their current data and it can be that partly it already covers GDPR regulations. In SAP system’s general, there are some functions, which are implemented since the system is installed. There is some reporting, security, monitoring functions, which are normally set on when the system is installed. GDPR brings now much more detailed, and stricter requirements for data processing.

3.1.1 Finug Seminar March 2018

According of FINUG GDPR seminar, which was held in Helsinki end of the March 2018, the issue was risen up, that many customers understand GDPR demands, but only some
have done some concrete plans how their SAP systems should be configured and most of the customers are still thinking what they should do. (Halonen 2018)

3.2 CSA survey

The purpose of the CSA survey was to collect data, about the current situation from the persons who are tightly connected with customers. This data will give evidences about the current situation concerning GDPR data breach in customer systems, and general awareness of it, among those who are working with customers. There were made Google forms questionnaire in the end of February 2018 for three different groups: system specialists, managers and GDPR group members. Managers group were chosen 5 people, system specialists 5 people and GDPR group members 4 people. Response percentage of system specialists was 80 % this means four of the responded, in GDPR percentage was also 80 % four of five responded and in managers group percentage was 60 %, 3 of 5 answered. All over percentage of responses was 71 %, this means 10 of 14 people answered so, those answers are enough to get good picture about situation in different customer environments. What validates also the answers, is the fact, that most of the responders are working more than 3 different customers. This gives enough broad picture, about the current situation, among of the SAP customers and makes the knowledge of it wide enough to create current state analyse of it. It should be also clarified, that GDPR group members are working as well as system specialists in their SAP area, we can call them as well system specialists, but for the sake of clarity they will be called GDPR group members. Questions were asked for the purpose to get an answer: What is the current situation among of customers concerning GDPR in SAP environments? Questions were made by Google Forms, and sent via email link to all target groups. Answers were copied into Word document and summaries taken out from each group, so that these could be compared with each other’s. Questions were formed quite in similar way, for system specialist’s and GDPR group members and all questions can be found in appendices section in the end of this thesis work grouped by names Questions for Specialists (Appendix 1 p.1-2), GDPR project members (Appendix 2 p.1-2) and Managers (Appendix 3 p.1-2). Managers received little bit shorter questionnaire form, but idea was quite the same in those questions. Questionnaire was formed in this way, that we could get whole picture what these group members knows about GDPR Data Breach readiness among themselves and among of the customers with whom they are working with.
3.2.1 Analysing Data Breach readiness in Customers SAP environments

According of questionnaire made in Company-X in spring 2018, which were made among of people who work tightly with different SAP customers (see Appendices 1–3). Analysing all the questionnaire answers, the readiness status of customers SAP systems seems to be lightly. It seems that customers are somehow aware of GDPR, and its regulations, and they have some information about what Data Breach means, but they are very slowly establishing their own GDPR projects and preparing themselves towards it concerning SAP systems. We need also remind, that there are lot of other systems as well, not only SAP systems, which these GDPR regulations are concerning for. Questionnaire were made separated in three different groups: technical specialists, managers and GDPR project group, people who have been working with GDPR concerning SAP environments. All these groups have answered, that there have been some discussions with customers and some preparations work has been done, but not very concrete things. What comes to data breach itself, it seems to be more such a situation, which is still open what to do to it in concrete way. SAP systems include certain readiness for Data Breach, but it seems, that most of the customers do not have yet clear idea what must be configured and set, so that their SAP systems are in Data Breach readiness according of GDPR rules. Those who are working with this issue in system level including all these three groups: system specialists, GDPR project persons and managers, need still more understanding and education what GDPR Data Breach demands mean in real life concerning customers SAP systems. This creates a situation at spring 2018 where information still increases around of GDPR regulations and actions and different ways to handle this takes still a form, so there is a progress going on around this topic.

3.2.2 Analysing GDPR Data Breach awareness by customers

System specialists and GDPR group were asked what the situation in your customers SAP environments is concerning GDPR Data Breach? (Appendix 2 p.1) For system specialist’s, that question was formed little bit broader than only GDPR, it was formed in that way that it concerns information security in general in customers SAP systems where they are working for (Appendix 1 p.1). System specialist could choose more than one answer, there were two answers which got 75 % it means those two answers were answered by 75 % of them, those were: Something is dealt with and something is not dealt
with, concerning security and there is still a lot of weaknesses. There was also one answer from the group of system specialist’s: I could not be less interested. GDPR group members answering to this question concerning GDPR awareness by their customers (Appendix 2 p.1). Results were following: 33 % of them have been dealing this issue with the customers and 66 % of them have been actively bringing them to customer. Managers answer to this question was 75 % says customer needs more information about it and 25 % answered they have too less information about it (Appendix 3 p.1). Conclusion is, there is information and some sort of awareness, but there should be done more that customers get real understanding and can prepare their systems to be fully GDPR Data Breach compatible. We can also analyse system specialists’ answers with understanding it concerns not only data breach, but also general security situation. It must also be kept in mind, that SAP systems include lot of different functionalities, where there is demand for very specific security settings, and we cannot have all of them under one person’s control, this could explain the “feeling” that someone says, it could not interest me or there are lot of weaknesses. (Appendix 1 p.1)

3.2.3 Analysing Data Breach awareness by specialists and managers

For example, question concerning: How well you are aware of GDPR Data Breach regulations, was asked from system specialist’s (Appendix 1 p.1), and GDPR group members (Appendix 2/1). System specialist’s 50 % answered, that they know what GDPR and Data Breach means, and 50 % of them answered that they have heard about it, but they don’t know enough about the topic. GDPR group members answered to similar question that 100 % of them knows, what Data Breach means concerning of GDPR regulations (Appendix 2 p.1). This is quite clear because they have been involved in project to deal with GDPR issues, so awareness of GDPR issues is much higher among of them. Manager group was asked similar kind of questions but formed little bit different. The question about awareness of GDPR data breach was formed in a way: Do you know those customers SAP systems at where you are working protected against data breaches? (Appendix 3 p.1). From the manager group 66 % answered, that systems are partly protected and 33 % answered, that they cannot say are system’s protected. Conclusion of all these answers is similar, as the big picture shows, that awareness of GDPR reflects also readiness, that there is some readiness, but not fully. There is lot of information and some preparations, but not all fully done yet. Also, we can make a conclusion about those who are working with the systems, that they have some sort of readiness, but they need still more education and information about the things and also real-life
working experiences more to fulfil their duties concerning GDPR Data Breach regulations.

3.2.4 Analysing motivation by managers and specialists

From system, specialists there was an extra question are they willingly to learn more about GDPR (Appendix 1 p.2). It was answered 100 % with an answer: I am willingly to learn more about it. This helps us to cross check question where one answer was: I could not care less. Therefore, we could close out in our conclusions, that someone is not motivated concerning this issue, but maybe frustrated because of huge data flow and information, which comes with these new regulations, and actions belonging to it. GDPR (Appendix 2 p.2) and Manager questions (Appendix 3 p.2) are reflecting the same idea, that all those group members are willingly to learn and bring more information to customers. Conclusion of this is, that all persons participating to these questionnaires were well motivated and have answered honestly so, the picture given is credible.

3.2.5 Analysing email survey re-check

Keeping the data reliable, it has been important to do a recheck about current situation from the stakeholders. There were sent questions via email about current situation to three managers working in Company-X and to one GDPR project group member, who is leading GDPR specialist in December 2018. Purpose was to recheck the current situation again, was there any changes compared to beginning of the 2018 when questionnaires were sent to three different groups. Regulations came in power in May 2018 so there are few months now when the GDPR regulations have been in power and earlier questions were about two months earlier than GDPR came in power. Questions were answered by three people, two managers, and by one GDPR leading specialist. One manager did not respond. Questions were in very short form and asked in following order from managers: First question was: Has there occurred anything-new concerning customers you are involved with regarding SAP GDPR regulations and if something what? Second question was: In which customers are you involved in or you can give number of customers? Third question was: Have customers started to work with GDPR things in SAP environments, or do they have still similar status than before GDPR regulations came on power 28th of May 2018? Fourth question was: Is there anything else to com-
ment on GDPR? First question was obvious, there has not occurred new things concerning GDPR, and both answers confirmed this. What comes to customers these two managers are working with several customers, so they have view of some different SAP environments. Third question was like additional question-to-question number one and both answered that situation is similar like earlier. Last question was answered by one of them, that the current situation is still like in waiting mode. Questions which were sent to GDPR leading specialist, were same than those which were sent to managers. First questions response answered by GDPR specialist was: There are several customers with whom this specialist has been involved with and there is going on evaluation of the GDPR needs. Second questions response answered by GDPR specialist was: This specialist is working with several customers, no clear number of customers told. Third questions response answered by GDPR specialist was: Customers are more aware about GDPR than earlier in the spring. Such a GDPR solutions have been brought forward, and implemented, which are technically possible, and where does not come more additionally license or project costs. Fourth question was not answered by this GDPR specialist at all.

3.3 GDPR project of Company-X

GDPR project gives for the CSA good background information about the current situation what is going on in service provider level and also about the situation what is going on by customers side, because all of its members are working tightly with this issue and have connections to different customers. As a service provider Company-X has to be able to respond to this GDPR challenge, that is why, it has established a project group. To this project group belongs several different SAP specialists and a project leader. This group is gathering together periodically with in GDPR meetings and changing the information about GDPR. There have been also some customer presentations about GDPR, which this project has proceed. SAP has provided some education about GDPR and about their tools. Project members have taken part of those trainings. Part of the GDPR project this research has helped to cover data breach area and given tools to cover GDPR regulations concerning data breaches.

3.3.1 Three Level System

Purpose of these three levels is to offer customers three different ways to implement their security. It does not mean that they could not have from all of them something, but these levels are created in the purpose of having at least minimum and then very strong
security. It is always up to customer how much they have resources to invest on those solutions.

3.3.2 Minimum Level

When we think GDPR as a whole, it means lot of more than only a data breach regulation. In this research even if we concentrate on that particular area, we need to understand that in discussion with customers there is need to take also in talk these other requirements as well.

Our project group has developed three level system to approach GDPR requirements. First level is minimum which means we talk with customer about their GDPR needs and try to help them to evaluate what they need. If customer sees that they do not want some extra costs and they can survive with their current solutions, we offer this minimum level support. It means we consult them what all is possible to do in concern of their systems and what possibilities are there and we tell them also what GDPR says that they are aware of those regulations. However, at the end we do not do any other actions than consulting, because if they want to live with current situation as it is, it goes at their own risk.

3.3.3 Modesty Level

Second manner of approach is to offer customer modesty level. Modesty level means customer wants to have some solutions and maybe some of them from SAP tools, and some of them customized. Because some of the tools are license based it is also question of the costs. Some of the regulations can be covered with already existing SAP functions, but if customer wants to have sophisticated and exactly tailored tools for example for data deleting and masking, they should choose SAP provided tools for it. This is of course question of negotiations and how customer sees their current situation. This modesty model leaves the door open for further extensions in the future.

3.3.4 Maximum Level

This level means full implementation of SAP solutions, or both SAP and customized solutions. Customer is willingly to invest money to fulfil those regulations, which EU has legislated. This means all those important regulations concerning of personal data will
be covered. This costs more money, but it also gives better tools for the business to
govern their data and be prepared for all possible threats coming towards to their SAP
business systems.

3.4 Summary

Outcome from the current situation is, that situation currently seems to be good business
opportunity for service providers like Company-X. Different customers seems to be
aware of it, what they supposed to do concerning GDPR data breach regulations, this
means to get more information and education from the service providers like Company-
X and set some projects to fulfil GDPR regulations concerning Data Breach in SAP sys-
tems. There is increasingly lot of information (books, videos, websites) and seminars
which will give opportunities for customers to think about their systems and give ideas
how to develop them further concerning GDPR regulations general. Of course, we need
to see, that all this concerns lot of systems, which are, not SAP ones and this thesis does
not focus on that situation but concerns of SAP systems. It could be in many other IT-
sections and IT-systems they have already very far away brought GDPR projects and
implementations, but at least these customers who are dealt with Company-X and its
provided SAP environments concerning GDPR Data Breach readiness situation is like
described in here. This situation demands from the service provider like Company-X lot
of research more and very active attitude to bring up these GDPR Data Breach regulation
needs to customer known, as well generally GDPR regulations, because there is no clear
answer to that what all kind of things must be set and what is enough to do. (Halonen
2018) This creates a current challenge: first to educate own personnel to be readier,
so that they can give right information further for the customers. This is also very good pos-
sibility for the business to create some new models or even working products to help
customers to fulfil GDPR Data Breach regulations. Even if it seems that situation is still
in progress and readiness is in many ways not yet what it should be, with good co-oper-
ation and trying to find out ways to do this in right way, there are very good business
opportunities which can develop customers security in many levels as well. This thesis
work gives an answer to this need concerning GDPR Data Breach and it can be found
in proposal section.

As we can see, that current situation according of CSA survey email survey can be sum-
marized to be pending at the moment. From customers side it seems, they need to have
more information and they have not yet very actively done some special settings in SAP
environments, this gives good opportunity to tell them about security tools which are
mentioned in the proposal. From the perspective of the service provider Company-X there are activities going on, for example GDPR project group. Some the project group members are quite well aware of what is going on with GDPR regulations regarding data breach. Company-X’s project with three level approach shows, that readiness in service providers side is quite good, and there is progress going on and there has been taken activates respond to this challenge. According of questionnaires there were people from Company-X side who wanted to have more information and education about GDPR and data breach in SAP environments. This shows that the attitude towards GDPR regulations concerning SAP systems is in state willing to learn more. Conclusion all of this is, that this GDPR is quite new thing at the moment and that, there is need for the clear instructions like this thesis work’s proposal. The proposal of this thesis will respond to this need to learn more and help customers to protect their systems like it is required in GDPR data breach regulations.

4 Conceptual Framework

Conceptual framework is created from the existing knowledge of SAP documentation and GDPR regulations. It includes information about important GDPR regulation concerning Data Breach, how these regulations concern SAP systems, Security aspects of SAP systems and SAP tools, which will be used to protect system against data breach.

4.1 GDPR in general

GDPR enforcement date has been 25th of May 2018. This is biggest change to personal data regulations EU wide since 1995. (European Data Protection Supervisor n.d) One of the big changes is, that these regulations apply to all companies who are processing personal data residing in the EU, despite company’s location. It will also apply to those companies who locate outside of EU, but who are offering products and services to EU citizen inside of EU. (EUGDPR 2016) GDPR concerns all those companies who work inside of EU or outside of EU, if they have some businesses inside of EU. This means hundreds of thousands of companies all over the globe. SAP’s estimation is that 48 % of businesses inside of EU were not ready yet in October 2017. (Pickering 2017) Most of the companies are doing their own evaluations what could this mean for their businesses. There is also very much legally information, which must be sorted out and researched. We need to understand as well that many companies have lot of different kind of systems
where the data is processed. SAP systems are in some cases only part of those system chains. Customer needs to take care of all their IT-systems, not only SAP systems.

4.1.1 Personal Data, Data controller and Data processor

Personal Data means any information, which can be identified, and pointed to a natural person. Natural person is anyone who is identified directly or indirectly by reference like a name, an identification number, a location data, a home address, an email address or any similar factor. Data controller means public authority, legal person, agency or other that kind of body who determines the purposes and means processing of personal data. Processor of the data means a legal or natural person, public authority, agency or other that kind of body who processes the data on behalf of the controller. (European Union 2016)

4.1.2 Right of access

Data object whom personal data is processed by the data processor, has right to have information what kind of data and where, when and what purpose it has been processed. Data object has right to obtain that kind of information from the data controller and get confirmation of it. Data controller is also responsible to provide free of charge copy of the personal data, in a electronic format. (European Union 2016, reg.15)

4.1.3 Right to be forgotten

Data object has right to demand data to be erased concerning his/her personal data. Data, which can be erased, is explained more in details in GDPR regulations article 17 generally, it means data, which is not anymore relevant or needed to any original purposes for processing. (European Union 2016, reg.17)

4.1.4 Data Breach notification

Under GDPR regulations breach notification is mandatory in all EU member states. Notification of the data breach, when it has become aware, must be done in next 72 hours. Data processor is obligated to inform customers without delay when they have become aware of the data breach. (European Union 2016, reg.33(1))

4.1.5 Privacy by design
Article 25 calls data controllers to design their systems so that they are compliance with GDPR regulations: “The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed.” (European Union 2016, reg.25(1)).

4.1.6 Penalty

GDPR regulations charge penalty up to 4% of annual global turnover or 20 million euros in the case of GDPR regulation breach. These regulations apply those who control the data and those who process the data. (European Union 2016, reg.83(6))

4.2 SAP concerning GDPR

SAP has expressed many times, that they cannot give a ready package for the customers how to fulfil all required enforcements in customer’s environments: “This all must be done in good co-operation with customers and try to search best possible solutions for every customer differently. It is also said that a service- or a hardware provider cannot give ready solution to any customer, they must decide themselves what they going to do” (Pickering 2017). In Article 33 EU GDPR regulations define about Data Breach following: “In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.” (European Union 2016, reg.33:(1)).

When personal data is focused, the main entity who controls the data must be able to monitor data. The data must be monitored in such a way, when any attempts takes a place and data breach occurs, the controller must be able to have detailed information: What kind of data was breached? Whom it concerns? And When did it happen? To have such a mechanism in SAP systems, there is need to use SAP tools and configurations, which are told later in following chapters of this thesis work. However, conclusion of these regulations is following: We need to know where the attack came from? How it came? And, who possibly was behind of it? Proposal of this thesis work will give possibility to cover all of those questions.
4.2.1 SAP approach to Data Breach

SAP systems are generally very complex and there are a lot of different security settings and functionalities. Some of those are licensed and some are free licensed. Approach, which SAP speaks about GDPR concept, is the inductive approach. Inductive approach means: “Inductive reasoning makes broad generalizations from specific observations. Basically, when there is data, then conclusions are drawn from the data, makes broad generalization from specific observations” (Bradford 2017). In SAP environment’s according of SAP and GDPR book concept will be following: “Our approach, however, is exactly the opposite: the truth lies in the data. We therefore assume that stocktaking in the system at the level of real data is objectively necessary! Furthermore, this approach allows us to reach our goal much faster and to record the actual data situation much more accurately. The inductive approach therefore starts from the current status to determine which purpose are actually pursued in data processing” (Cristoph et al., 2018 p.114-115). That is why this security concept in this thesis is based on this same approach: we look at the current data details and build up security recommendations concerning GDPR from that perspective. It means we are using SAP tools described later in this section with purpose to use them to fulfil Data Breach rules written in GDPR regulations:

“‘personal data breach’ means 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;” (European Union 2016, reg.4(12)).

4.2.2 SAP security flaw

It has been researched, that SAP security breaches will come mostly because of too old configuration settings. Pierluigi Paganini, who is member of the ENISA (European Union Agency for Network and Information Security) refers to this issue on his blog saying: “According to the security firm Onapsis, 90 percent SAP systems were impacted by the vulnerability that affects SAP Netweaver and that can be exploited by a remote unauthenticated attacker who has network access to the system.” (Paganini 2018). This shows how important it is to have current security configuration up to date and configured in reasonable way that it is possible to recognize possible data breach attempts.
4.3 Three level security system

With the approach mentioned in section 4.2.1 and understanding how important it is to keep the systems security settings up to date, in this thesis work is used a three-level system which concern on those security points told earlier. Three level system description picture covers security risks in following way described in Figure 3 below:

![Three level security risks](image)

Figure 3. Three level security risks

4.3.1 Data Breach from the outside

Outside breach means, that someone breaches to personal data from outside of the system. This can happen either trying to breach through the network trying to use some programs or functions or trying to steal user information and abuse the system with illegal access to the SAP system. We cannot explain all possible methods what can be used, but main purpose is to understand that outside from the system means attack through all those security layers, which protect the system. Picture 4 describes outside coming attacks.
Like we can see in the Picture 4, that there are many layers to go through and SAP has also its own security layers inside the application, nevertheless this is one possible way try to breach personal data. This can happen accidentally or unlawfully and is needed to be monitored and traced.

4.3.2 Data Breach from the inside

Data breach from the inside can also be a attack from the outside first, if it is done first breaking the security outside, this means those layers in Picture 4, firewall, network and SAP’s application level security, after that attacker can be able to use some user inside to continue the attack. Inside Data Breach can mean also someone who has authority to do it, so it is unlawful attack. Someone is user authorization in illegal way and altering, destroying or stealing the personal data.
4.3.3 Data Breach misusing the data

Third level in this approach is abusing the data inside the system. This means either there is illegal use of the data or someone has achieved to breach inside the system and is using unlawfully someone other’s user who has right to access that data which attacker wants to access. Other possibility is that some user is unlawfully accessing data, which is not mentioned to be accessed by that person. There are also possibilities that someone has a role to access data, but partly there is information, which is masked, and there is no access with roles used, and someone for some way gets an authorization role to access data, which is not mentioned to be seen by that person. This kind of misbehaving is a data breach.

4.4 SAP Tools

Sap tools are functionalities made by SAP to take care of certain functions in the system. These functionalities need to be maintained first and after that, they can be used for
those purposes for which they were made. Sap tools include security-based functionalities, and purpose of this chapter is to describe, some of those tools which are valuable, for this task concerning the issue dealt with in this thesis work.

4.4.1 General description of SAP Tools

SAP has created inside the SAP systems lot of different tools, so that customer can use them to cover their needs using SAP system with them. Because GDPR regulations concerns large amount of data and SAP tools which are provided for these purposes are mostly license based and this means more costs for the customers, the idea is to find solution to find non-licensed basic tools, included in basic system license without extra cost for the customer. Customers have also possibilities to develop such a tools by their own developers. Nevertheless, initial installed SAP systems includes tools, which are included in basic license prices, and these tools are ready for the use after some initial configuration and customizing settings.

SAP includes many different modules, which have thousands of tables and all kind of structures and all these structures includes lot of data and in the data contains lot of personal data. This is reason why this framework is limited to deal with chosen SAP tools and their general use and not to go very special detailed table or data level. In this thesis work very customer tailored solutions are not handled but presenting general recommended solutions by chosen not licensed SAP tools, which can be used mostly in all SAP environments.

4.5 RAL Read Access Logging

Read access logging (RAL) is a tool, which helps to monitor and audit sensitive data, in this scenario personal data. This tool comes along with SAP software and it has been developed to work in certain support package levels. SAP says on their support web pages: “Read Access Logging (RAL) is used to monitor and log read access to sensitive data. This data may be categorized as sensitive by law, by external company policy, or by internal company policy” (SAP help portal 2018). Read access logging can be used to monitor for example following issues:

- Who accessed transaction and data which fields were used?
- Who accessed personal data?
- What kind of data was queried, was it personal data?
- Was the data only read or also changed?
Read access logging is based on logging purpose that you can freely define according of your organizations data privacy rules. You can choose most sensitive transactions and include critical fields to be monitored (SAP help portal 2018). There is configuring interface which enables you to define different kind of logging scenarios and monitoring interface which allows you to monitor accessed transactions and data. Read access logging writes all pre-defined information in Read access logging system log where you can go and read it either immediately or later. (SAP help portal 2018)

In a RAL configuration will be specified following elements:

a) Log context

This is what SAP says on their Support portal about log context:” A log context is the key field that other fields displayed within the logging session are related to. When read access is logged and the log context changes, previous values displayed for all other dependent fields are deleted from the memory and new values are logged together with the log context. For example, the log context of a configuration for a HR application may be the employee number. As soon as a new employee number is entered, values for all other fields such as religion, salary, and so on no longer belong to the employee previously displayed. Using the log context, the values for the religion and salary fields are always logged with the correct employee number.” (SAP support portal 2018). In Log Context there is relation to Logging domain. SAP describes meaning of the Logging Domain in following way:” Within an application, the data to be logged must be defined on a semantic level, before the actual fields and rules are defined. This is done by creating log domains as semantic descriptions of semantically identical or related fields that have different technical representations” (SAP support portal 2018). This is like a title for all information to be logged under certain title.

b) One or more log groups

SAP describes on their support portal about log groups:” A log group is a collection of fields that are displayed in the same log entry (based on the logging purpose). For example, in Web services, the fields are elements of the underlying Web service message;
in Web Dynpro, the fields are UI elements of Web Dynpro applications.” (SAP support portal 2018).

c) Conditions

SAP says on their support portal about conditions: “Conditions are the rules you define to specify when the fields in the log group are logged. For detailed information about how to use the log context in your configurations” (SAP support portal 2018). Conditions are optional to use but recommended.

All these elements belong to process implementing RAL configuration. When these elements are configured and specified SAP system will be ready for using the RAL functionality. Technical configuration of these elements will be described in chapter 5.

4.5.1 Availability

Read access logging is available for following versions onward: NW 7.01 sp15, NW 7.02 sp15, NW 7.11 sp13, NW 7.30 sp11, NW 7.31 sp9 and NW 7.40 sp0 – sp4 (sp3 with automatic transport of configurations and sp4 shipment of Webdynpro query logging, Dynpro+ALV Grid channel) (SAP Product Management Security 2015, p.15-16).

4.5.2 RAL and Data Breach

Read Access Logging (RAL) is tool used to monitor if someone has breached or tried to do it unlawfully. It will write entries who did it, which transaction was used, which data was tried to be accessed and when did it happen. You can get quite detailed information about unlawful data breach. Auditing data is stored in database level and it is not overwritten or deleted automatically so, it is possible to go so long back in the history as data is stored in database level. This helps to fulfil GDPR’s demands to be able to solve data breaches which have happened in the past.

4.6 Security Audit Logging

Security audit log gives a detailed view what happens inside of the sap system. “By activating the audit log, you keep a record of those activities you consider relevant for auditing” (SAP help portal 2018). Beside of the RAL functionality (section 5.6) using security audit log is very powerful tool to keep records what is happening inside the system. It
writes logging files in file system level, which can be stored either in their current location so long as customer wants, or files can be removed or archived to different location. Security audit logging can be used to record following data according of SAP:

The main objective of the audit log is to record the following information:

- Security-related changes to the SAP system environment (for example, changes to user master records)
- Information that provides a higher level of transparency (for example, successful and unsuccessful logon attempts)
- Information that enables the reconstruction of a series of events (for example, successful or unsuccessful transaction starts) (SAP Support portal 2018).

SAP says also that in special cases there is possibility to record following information: successful and unsuccessful dialog logon attempts, rfc logon attempts, RFC calls to function modules, successful and unsuccessful transaction and report starts, master data change, changes to audit configuration and other events like: file downloads, internet communications, use of digital signatures performed by the system etc. (SAP support portal 2018)

Security audit log is activated via technical transactions, this is explained in the Proposal chapter section 6.4. In activation process there are filters, which are defined, what kind of information will be recorded. Selection is quite wide and there are many selections for example client, user, transaction name, program name etc. It is possible to form security audit logging in such away which responses to customer’s needs.

In Security audit logging configuration there are following elements:

a) Preparing Security audit log with needed system parameters and restart the SAP system (section 5.4.1)

b) Set either dynamic or statistic profiles and configure filters (section 5.4.2), in this thesis work we will concentrate only on statistic profile.

4.6.1 Data Breach and Security Audit Logging
From the perspective of the data breach Security Audit logging gives a powerful tool to record what is happening inside the SAP system. In the case of data breach Security Audit Logging is able to give detailed information who was doing what, in which transaction, which program was used, from which application server was used or which terminal, what dialog process was used etc. It is possible to go back in the history so long as Security Audit Logging files have been stored and are accessible. Security Audit Logging helps to monitor important events inside of the system and that's why as an tool it helps to fulfil requirements of the GDPR Data Breach demands.

4.6.2 Availability

Security Audit Logging is available in all SAP versions and can be activated and configured in all supported SAP ERP versions.

4.7 Table Change Logging

Table change logging is functionality which is created inside of every SAP ERP system. Main purpose of the Change Logging is to record customized object changes, of course there are also SAP standard tables which can be set in logging mode. Change Logging happens in the database table level. Every change in the table either it is insert, update or delete, will be logged in certain table logs, which can be evaluated with certain transaction afterwards. Table logs are stored in the database and those logs can be deleted or archived afterwards if needed. Data controller can check out, if someone has done some changes and what was done and when it was done to those logged tables. Table Change Logging is configured and activated by system level via technical transactions like shown in the Proposal chapter section 6.3. Activation and configuration follow following main lines:

a) Customer lists all business-critical tables which must be logged for the changes
b) When the list has been done table recording will be set active via technical transaction like explained in the Proposal Chapter in section 5.3.1
c) After the table logging has been set active all changes can be monitored via technical transactions like described in the Proposal Chapter in section 5.3.2

Steps listed above tells the main steps how to implement the Table Change Logging.

(SAP support portal 2018)
4.7.1 Data Breach and Table Change Logging

Table Change Logging responds the need to monitor what happens to business-critical data in table level. What has been changed and by whom? It helps to get information in data level and gives very clear signs what kind of data was accessed like described in the Proposal chapter section 6.3.2.

4.8 Application logging

“Application logging records the progress of the execution of an application so that you can reconstruct it later if necessary” (SAP help portal 2018). Even if the application logging is not included in the proposal of this thesis work, it has been mentioned because of it’s character to offer very valuable information about what is going on in the system. Meaning of application logging is to be able to have logging entries from all kind of actions made in application level. This helps afterwards to trace what has happened? Who has done what? Which application was active in that certain moment? Application logging can be also used to trace error situations and to see what kind of problems there occurs. In GDPR view application logging can be used to trace which application has done what, which user was doing it and what kind of actions were taken with that application in the certain moment. Application Logging is automatically configured and set to be on since the installation of the SAP system.

4.9 Data Archiving

Data archiving is part of the functionality where data is either directly deleted or during the archiving process it is processed to be deleted. Data Archiving is not also part of the proposal process of this thesis work, but it can be used for example to reduce logging data which comes from the tools mentioned in the proposal and this is the reason why it is mentioned here. Archiving could be integrated to ILM tool (licensed product) or it can be used without any licensed tools using SAP ERP integrated archiving functions. In archiving process data which will be archived with certain rules towards archiving objects which will define when and where the data to be archived will be stored. In GDPR archived data must be handled concerning user data regulations, so that personal data is possible to be deleted from the archived data as well. ILM gives some SAP created tools for that purpose. (SAP help portal 2018)

4.10 Some licensed products
Even if this thesis work does not focus on licensed products, two of these tools will be taken as an example to this work in this tool’s description section. This helps to give us broader picture about possibilities to use SAP system functionalities and helps to give understanding that there are more possibilities if customer is willingly to invest more to this area. There are of course lot of more tools than these two, but for the sake of bigger picture of SAP tools, these two examples represent possibilities to extend SAP systems in this area with subject to charge tools.

4.10.1 ILM

SAP Information lifecycle management is a SAP tool which enables to manage the lifecycle of live and archived data. ILM is based on rules which you can pre-define and according of those rules data will be processed in the system. ILM includes also masking optionality which enables data to be covered from unauthorized use or views. (SAP help portal 2018)

4.10.2 GRC

GRC which means: Governance, Risk and Compliance. It has many different modules: SAP access control, SAP Emergency Access management, SAP Risk management, SAP process control, SAP Global Trade Services and Financial risk.

SAP access control helps customer to monitor all user access coming and going from the system. It gives to tool to monitor given user rights and profiles and what happens inside of the system with those rights.

SAP Emergency Access Management is used to perform some of the duties that users are not normally privileged to do, but with appropriate approvals users can carry out some business transactions for a specified period (Asokkumar, Rajen Iyer & Sudhalkar 2014, p. 147). Emergency Access Management tracks this kind of special situations and minimizes risk that something unlawful happens. It can be also used in normal situation to restrict and debug authorizations in production environment.

SAP Risk Management: The Access Risk Analysis tool is an automated security audit and segregation of duties (SoD) analysis application that is used to identify, analyse, and
resolve all SoD and audit issues relating to regulatory compliance in your IT landscape, especially in an SAP ERP environment. (Asokkumar, Rajen Iyer & Sudhalkar 2014, p. 169)

*SAP Process control* helps customer to build up a structure inside the system which bunches together demanded regulations from different authorities and informs affected employees about them. SAP describes it in following way: “SAP Process Control helps inform affected employees of regulatory requirements and obligations, documents employees’ acceptance, and even tests their understanding and awareness” (Asokkumar, Rajen Iyer & Sudhalkar 2014, p. 342).

*SAP Global Trade Services and Financial risk*, SAP describes it in following way “SAP GTS provides reporting features, especially for audits, that enable you to handle changing import/export requirements and controls” (Asokkumar, Rajen Iyer & Sudhalkar 2014, p. 583).

### 4.11 SAP consultant’s role

SAP consultants in different areas are very important. There are technical level consultants who could be called administrators as well. There are application level consultants who manage different areas of the application levels for example HR, BW, FICO, SD, SCM etc. All these consultants are needed to be defining and tailoring GDPR solutions for the customers. SAP tools mentioned in this section can be implemented technically, but if the rules are not clear what to audit and which definitions are important to be set, data cannot be protected properly. That is the reason why SAP consultants are involved very tightly into pre-define work and implementation work of the GDPR tools in SAP systems.

### 5 Proposal; Instructions using SAP tools concerning GDPR

#### 5.1 Introduction

In this proposal we will approach GDPR Data Breach regulations with three different SAP tools described in chapter 4: Read Access Logging, Table Change logging and Security Audit logging. These three SAP tools are non-licensed tools and they come together with initial installation of SAP ERP system. This makes them to be available for all customers
who have installed SAP ERP. Like in Chapter 4.3 there has been described about three level security, we have used similar kind of approach in this proposal using three level system with three different SAP tools. These tools fulfils minimum requirements of GDPR Data Breach regulations in SAP systems. These three SAP tools use some similar functionalities and, in some points, they cross over each other, but this makes the solution only much more secure, because all those three SAP tools are like three level buffer avoiding any kind of data breaches. The structure of the proposal will be following: first will come technical part how to configure those tools and after it a short summary about implementation of the tools. What must be also considered is, that we cannot give a ready template how the system must be defined. Customers responsibility will be define business critical transactions, tables and fields. In this proposal there is told how to make configuration functional and addition to that customers responsibility is always to provide template and tables for the business-critical data. This all will be monitored according of GDPR rules with these SAP tools. In this proposal there are no customer specified templates or recommendations which data or tables should be monitored or configured with these SAP tools, that will be always an project to to do. All examples in this proposal are only for the purpose to show how SAP system can be configured to fulfil technically GDPR Data Breach requirements.

5.2 Technical implementation of RAL (Read Access logging) configuration

5.2.1 Authorizations to be concerned

Before there can be any activities taken right roles needs to be added to users who going to do this configuration work within RAL. Following authorizations: SAP_BC_RAL_ADMIN_BIZ role, a template for business administrators doing the configuring and monitoring. SAP_BC_RAL_ADMIN_TEC role, for technical administrators responsible for archiving, disabling client and monitoring administrative log.
SAP_BC_RAL_ANALYZER role, a template role for Read Access Logging analyser,
SAP_BC_RAL_SUPPORTER role, a template for Read Access Logging support engineer (SAP Product Management Security 2015, p.14) We don’t consider which other roles should be added to user’s and administrator’s, but with those roles mentioned above it is possible to be able to configure RAL successfully with examples told in this chapter 5 concerning RAL configurations.

5.2.2 Enable RAL
RAL configuration must be first enabled in the SAP client where it will be used for. First SRALMANAGER transaction must be accessed, which launches RAL administration window like shown in Figure 6 below. On that RAL main menu there are all options to be needed for configuration and administrating RAL functions.

![Read Access Logging (S4H/700)](image)

**Figure 6.** RAL admin menu.

From the Read Access logging Administration menu there will be chosen Enabling in client which open’s a configuration screen like (Figure 7)
Above the Client specific settings, enable RAL setting in change mode, clicking on edit (pencil icon) and after that choose Enabled in the right down corner and checkmark it, so that there will be checkmark under the Enabled text. This same setting can be done with profile parameter (sec/ral_enabled_for_rfc) setting should be set to be 1. It is recommended to set this parameter permanently.

5.2.3 Creating Logging purpose

In the RAL administration menu (Figure 6) and choose Logging Purposes clicking up on it and create suitable title for the logging purpose, clicking on Logging Purposes link on Admin menu and there will appear a screen where logging purpose can be created by clicking create button like shown in Figure 8.
After logging purpose is created it will be listed on the search list from the Logging purpose main screen and this can be searched from the existing Logging Purpose list if needed.

5.2.4 Logging Domain

Logging Domain will be created next. Logging domain is not mandatory, but in this example, it will be created. Logging domain can be let out or included in the configuration if needed. On the Admin menu (Figure 6) Logging Domain link will be clicked and Logging Domain screen will appear like in Figure 9 below.
Pushing the create bottom and giving the name and Business area and some description Logging Domain will be created and it will exist on the Log Domain list in the main screen of Logging Domains and can be searched by search criteria afterwards.

5.2.5 Recording

Next phase is to record what is needed to be monitored. Monitored fields and transactions will be defined by the customer and this thesis work does not give instructions which kind of business-critical transactions should be monitored. In Admin menu (Figure 6) recordings will be chosen clicking the recordings link. The screen will appear like shown in Figure 10 below.
Figure 10. Create recording.

Obligatory channel type has to be chosen (in this example will be used DynPro channel type) as well recording name, description is optional but recommended. After definitions have been set, push the create button. After these settings Recording starts and the recording can be found on the recording list like in Figure 11 below.
Like we can see in the Figure 11 Actions status has two different kind of icons: glasses and stop button, which means recording is running. Running status can also be seen in the State column. When recording is not running the State will change to finished and in Actions column there will be glasses and green triangle (play) icons like in Figure 12 example below.

![Figure 12. Actions Icons in Recording.](image)

5.2.6 Recording of monitored objects

Now when recording is actively running, wanted object’s: transactions or fields can be recorded in the SAP system and are included in RAL configuration. In another session open wanted transaction and wanted fields, which should be included in configuration. Recording of wanted fields can be selected with menu which open’s with clicking the right mouse button. Like in Figure 13 has been shown field must be chosen and after it Record field option. This should be reminded that when recording has been set in running status all transactions which are accessed during the recording are included in RAL configuration which is currently running. This makes it possible to have different kind of recordings and configurations.
When transaction is recorded it is included in RAL configuration and all changes which are concerned to chosen field in that transaction are included now in monitoring configuration like Figure 14 shows. To see what recording now includes go back to Admin menu and choose again recording and reviewing, clicking upon glasses icon. We can recognize that chosen field (DATE_TO) is included in this recording configuration. After all wanted transactions and fields are included. When recording is completed push the stop button.

Figure 13. Recording transaction.

Figure 14. Viewing recording content.
5.2.7 Creating Configuration

Locating your recording by selecting Configuration from the Admin menu (Figure 6). Configuration administration appears like in Figure 15 is shown. Channel Dynpro will be chosen and Recording name will be given and search executed.

Figure 15. Configuration.

When recording is found from the list, it must be created as configuration, it will be created by pushing the create button like in Figure 16 below:

Figure 16. Create configuration.
After this configuration is ready to be configured and certain definitions added to it.

5.2.8 Configuration’s configuration

Selecting Configuration in the Admin menu (Figure 6) opens a search where wanted just created Recording (watch section 5.2.6) can be located from the Configuration list. When the right Recording is found in Actions column pencil icon should be clicked so, that configuration screen appears like in Figure 17 below shown:

![Configuration Screen](image)

Figure 17. Configuration

Like in Figure 17 there are Four different definitions have to be configured. Each definition has a creation button and deletion button under the title of it. By this create button will be created wanted configuration.

**Log context:** Like in Figure 18 we can see the Log context below. Log context defines the title how the entries will be found in the system monitoring. This is the title which has been defined in section 5.2.3 earlier in this chapter describing Logging Purposes. This purpose is a title for all those configurations which are included in this particular configuration. This enables easier access to collect all certain entries under one title. In Figure 18 we can see that in this example purpose which was created earlier in section 5.2.3 was used to be Log context in this configuration.
Log Groups: Log groups configuration includes all those fields which are chosen to be logged in groups. Values of these fields are dragged together with chosen Fields Channel definition in Field list (Figure 19). Like in Figure 20 below we can see, that there are many columns which comes together with chosen definitions like: Field Labels, Sample Values, Log Domain, Logging Type, Exclude if Initial, Field Type Path type, Effective Path and Field.

When wanted fields like RSYSLOG which refers to system log transaction which was used as an example (section 5.2.6) it will be dragged and dropped from the field list.
(Figure 19) and after it all those mentioned definitions columns can be configured with wanted values.

![Figure 20. Details of Log Group](image)

We can take a one example Username Field in Figure 21 below. This row was dropped and dragged from the Field list (Figure 19), and there are few possibilities to change values which are allowed or wanted to be in the configuration. In this example Field type column describes what kind of entries will be logged: Output, Input or Both. Input is logging entries made by user. Output is logging changes or new values. Both is recording Output and Input.

![Figure 21. Logging Fields](image)
Conditions: Condition is created with create button (Figure 17 in section 5.2.8.). This setting defines conditions for our earlier chosen transaction in section 5.2.6. In this example we have chosen system log transaction (transaction code sm21) and in there Date To field, which will be monitored with this configuration. We can choose system level conditions which can be dragged and dropped from the field list (Figure 19). In this example we have only one transaction system log, which gives us possibility to create a system level condition for following values Username, Screen Title and Transaction code (Figure 22). Sign column value can be chosen inclusive or exclusive and Option to it would be equal, greater, less than etc., with similar values. The purpose of this example is to use only one named user whose usage of transaction sm21 will be logged. Configuration is set to be equal to this username. Screen title and transaction code are empty which means they can be whatever values together with the defined username.

<table>
<thead>
<tr>
<th>Path Type</th>
<th>Field</th>
<th>Sign</th>
<th>Option</th>
<th>Low/High Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fully Specified</td>
<td>User Name</td>
<td>Inclusive</td>
<td>Equals</td>
<td>FPASAROL</td>
</tr>
<tr>
<td>Fully Specified</td>
<td>Screen Title</td>
<td>Inclusive</td>
<td>Equals</td>
<td></td>
</tr>
<tr>
<td>Fully Specified</td>
<td>Transaction code</td>
<td>Inclusive</td>
<td>Equals</td>
<td></td>
</tr>
</tbody>
</table>

Figure 22. System level Conditions

When all these steps have been completed configuration needs to be saved and activated which will happen with Save as Activate button (Figure 23).

Figure 23. Save as Active

5.2.9 Monitoring RAL entries

When this configuration is active, and someone is using the transactions defined in our RAL monitoring configuration, then we are able to check out entries occurring in the system. In this example we have one transaction system log (transaction code sm21) which is monitored by one named user. This user has been accessing this transaction
and date to field in there after the configuration has been activated. First what we need to do is to go to RAL monitoring. Monitoring will be found in RAL transaction SRAL-MANAGER and when we launch it, there will popup RAL admin menu where we can choose monitoring like shown in Figure 24 below. Choose the Monitor tab and click under it locating link: Read Access Log.

![Read Access Logging (S4H/700)](image)

Figure 24. Read Access Logging monitoring

When we have clicked the Read Access Log link under the Monitor tab, we will come on the monitor screen where we can choose to find according of our definitions wanted entries if they exist. Like in Figure 25 below, we can see certain options to be chosen. In this scenario we choose Source Raw Database, other option would be Extended Database, but it is not covered in this proposal. Search criteria will be: This week.

![Read Access Logging: Monitor (S4H/700)](image)

Figure 25. Read Access monitoring Search
After those chosen search criteria’s we can start to search with pushing search button. In search results we will choose View as Extended. Now like we can see in Figure 26 below, there are lot of different information existing according of the named user defined in the configuration earlier. We can already see (Figure 26) very valuable entries, even if it does not show all existing values. Those values can be found when the transaction screen is extended with a lower beam to the right in result screen. Those other values which are not seen (Figure 26) are: Correlation ID, Application Component, Software Component, Legal Entity Value, App.Server, Configuration ID, Log ID. All these values can be seen in monitoring view extending the screen with lower beam in results screen.

<table>
<thead>
<tr>
<th>View</th>
<th>Extended</th>
<th>Hits</th>
<th>15</th>
</tr>
</thead>
<tbody>
<tr>
<td>Created</td>
<td>File Name</td>
<td>Local Time</td>
<td>User Name</td>
</tr>
<tr>
<td>28.12.2018 12:21:00</td>
<td>FIPASAROL</td>
<td>Output</td>
<td>EXAMPLE FOR THESIS</td>
</tr>
<tr>
<td>28.12.2018 12:22:00</td>
<td>FIPASAROL</td>
<td>Output</td>
<td>EXAMPLE FOR THESIS</td>
</tr>
</tbody>
</table>

Figure 26. Monitoring results

There is also possibility to go deeper in results and see better details of the results. Like in Figure 27 below, we can see detailed information of the records choosing first details tab and under of it clicking upon certain monitoring record, we can see now detailed information (Figure 27) shows. In detailed information we can see output which was defined in the configurations in system condition and in field definition. Output value of the field value (Figure 27) is 20181229 and user value is named user output, which was used in this example. Those values which were chosen to be monitored and recorded have been accessed and the example shows we can find the information about it what has happened in that certain transaction. We can also recognize that there is our Logging
purpose used and if we extend the results more to the right, we can see different values listed earlier coming up to the screen.

Figure 27. Monitoring results details

5.3 Technical implementation of Table Change Logging settings

Table Change Logging setting is included in all SAP system automatically. In SAP technical table settings there is automatically settings which will allow or disallow this functionality to certain tables.

5.3.1 Pre-requisite parameter

There is only one parameter which must be set on to define that recordings will be done on the wanted client. This parameter is rec/client and it must be either to be set to value ALL which means all possible client or then it must be defined to be one certain client for example client 999. When this parameter value is set to be OFF it means this recording functionality is not on and there will not happen any recording off changes. This parameter should be set in the profile parameter and it becomes valid after the restart of the SAP system in next time.
5.3.2 Listing the tables which are pre-configured to be recorded

In transaction SCU3 all tables which SAP has pre-defined can be listed. With this same transaction SCU3 it is possible to analyse all table change logs. This happens choosing SCU3 transaction and clicking List of Logged tables tab (Figure 28).

![Figure 28. Change log tables listed.](image)

5.3.3 Including tables in recording

According of customers need’s concerning business critical tables and data in them, tables can be added to Table change logging. This happens either in transaction se11 Abap dictionary maintenance or directly with transaction se13. In this proposal, we will use transaction se13 directly. Choosing first transaction se13 and writing the name of the wanted table in the table/view box like shown in the Figure 29.
Figure 29. Transaction se13.

After the transaction se13 opens and the table has been set in the table/view box and after it clicking change button, there will open settings area where table recording can be set on (Figure 30). As it can be seen (Figure 30) there is a check mark in the box below where locates the text: Log Data Changes, this entry is highlighted with yellow colour (Figure 30). When the check mark is in the box locating beside the text Log Data Changes, it means the table logging has been activated for the table and table is logged for the changes. If the check mark is missing from the box, it must be check marked and after it change logging is active for the table. When the table change logging is activated, the client where the change will take a place must be set in change mode and all changes must be allowed. Otherwise system will not accept table change logging to be activated for the table. The client can be set in change mode in transactions SCC4 and SE06, but it demands administration rights, so there could be a need to ask administrator to set those settings before actual table change activation.
5.3.4 Monitoring table change entries

After the table is set in table change recording mode all changes in the table are monitored. In the same transaction SCU3 which was mentioned in the beginning of chapter 5.3.2. all tables can be monitored, and changes find out. Going to transaction SCU3 and choosing the tab Analysing logs like shown in Figure 28 and clicking upon it, there will open the analysing screen, where it is possible to choose the table, which ones analysing logs should be analysed (Figure 31). There is option to choose tables, which means SAP standard tables or customizing objects, which means customers own created tables. In this proposal as an example there will be used a standard object T000, which is client setting table.
When wanted table is set in the table/view box and wanted analysis period is chosen, it is possible to choose also output options with ALV Grid Display and Only Actual Changes options. We will choose both in this example. After that pushing the execute button, which is green checkmark button in the left-up corner. Now we have a result according of our chosen timeframe and we will see all the changes made in the T000 (client settings) table shown in Figure 32.

Figure 31. Analyzing change logs.
Like we can see (Figure 32) there has been some textual changes, the text Testi has been changed to Testi Muutos and afterwards it has been changed back to be in previous state Testi. We can see in the user field who was responsible for this change. We can also see, that there has been changes in other settings deleting values 2 and 3 in Columns Corr.Sys and NoCrsCli. Afterwards at 19:38:11 we will see that those same values have been changed back again. It is possible also to choose: Only Actual Changes value in the analysing screen (Figure 31). If we choose only that option and we will leave the ALV GRID option away and output will be following screen output like in the Figure 33.
5.4 Technical implementation of security audit logging

Security audit logging can be used statistically and dynamically. Dynamically means, it is possible to define configuration which is valid until next SAP system restart. In restart the configuration must be defined again. Statistically configuration will be set permanently to be valid and it will be on after the system restart as well. In this proposal we will focus on statistic one.

5.4.1 Profile parameters activation

There are several parameters which must be set before we can start to using statistic security audit logging. Parameters are can set in following way like illustrated in Figure 34.
<table>
<thead>
<tr>
<th>Profile parameter name</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>rsau/enable</td>
<td>1</td>
<td>Enables the use of statistic profiles for the security audit logging</td>
</tr>
<tr>
<td>rsau/max_diskspace_local</td>
<td>numeric value with suffix k or m</td>
<td>Defines how big will be one system log file be on the filesystem level. This can be defined with kilos (k) or megabytes (m)</td>
</tr>
<tr>
<td>rsau/selection_slots</td>
<td>numeric value example: 3</td>
<td>Number of configuration slots</td>
</tr>
</tbody>
</table>

There are also some optional parameters which can be selected if needed: rsaus/max_diskspace/per_file, rsau/max_diskspace/per_day, rsau/user_selection, but these values are not necessary for our purpose. After the parameters are set the system must be restarted that all those parameters becomes valid.

### 5.4.2 Profile creation

Before security audit log can be used security audit profile must be created. Creation of this profile happens in transaction sm19. In transaction sm19 like in Figure 35 is shown, happens creation of the audit profile. Create a profile and give name for it.

Figure 34. Parameter values of security audit log

Figure 35 Audit profile creation
When audit profile name is set there will come filter (slots) selection, what kind of values will be recorded like in Figure 36.

![Filter options](image)

Figure 36. Filter options

It is possible to choose client number or set asterix which means all possible entries. Recommendation is to choose all values and check mark all Audit classes and choose all Events in this example because we want to have all possible values to be recorded. Filters can be selected for the different purposes and that’s why there is possibility to choose different number of filters if needed. Filters are called as well slots and can be defined statistically by parameter (Figure 34) rsau/selection_slots, which defines how many filter tabs will be used. Filter values can be chosen differently for different kind of event monitoring or even some special event monitoring. After chosen selections configuration should be saved and it will be active together with parameters (section 5.4.1) after the next restart of the system.

5.4.3 Monitoring entries

After the configuration is valid and system is restarted because of parameter changes to become valid, system will start monitoring all entries happening in application level. Entries can be found using transaction SM20.
Like in Figure 37 above, we can see that transaction sm20 opens a view where we can choose date and time frame and user, client on events tab. We can also use Statistics tab where we can choose following options like in Figure 38 below:

Or we can choose Extras as well Format tabs shown at pictures 36 and 37 below:
Figure 39. Format selections

Figure 40. Extras selections

With these selections there is possible to select and filter certain information. In this proposal we will use the Event tab and select all possible entries. After the selections when we push the button of Reread Audit Log (Figure 37) we will get following results according of our selections
There we can see application server name (Name), date and time, username, terminal where the connection came from, transaction code what was used, program what was used etc., lot of information what was happening in the system and application level.

5.5 Summary of the proposal

It has been demonstrated in this proposal chapter, that with these three mentioned SAP tools it is possible to create a configuration which responses to GDPR Data Breach requirements. When those three tools are configured and activated in a way described in the proposal chapter 5, customers system will be technically in GDPR Data Breach readiness and customer is ready to monitor and record business critical events in SAP systems. Like mentioned earlier these settings will not cover up which tables and which transactions do have detailed personal data and that is reason why this proposal gives only technical readiness for the customer. Together with this proposal, customers are able to establish a project where is defined detailed tables and transactions and trans-
action fields to be monitored. This proposal of course gives a possibility to monitor unlawful accesses and other transaction and function accesses happening in the system without defining any detailed tables or transactions. When we still go through, what has been set, we can come to following outcome with this proposal: Read Access Logging is gathering information from business-critical transactions and fields, Table Change Logging records events in table level and shows what kind of changes has happened on the focused tables and Security Audit Logging records all events happening in system and application level. With these three tools, we can cover the demand of GDPR Data Breach regulation and fulfil described three level system security risks described in the Chapter 4 in section 4.3. We can monitor what is going on in database level and in transaction level, targeting business critical tables and transactions, especially those who include personal data. It is possible afterwards to go and check out what kind of users and programs have been actively changing, deleting, or updating the data, and in the case of data breach to find out root cause and possible responsible entities for the data breach. At least it is possible later on find out which kind of users or programs were used for the data breach or what kind of data was accessed when the data breach took a place. It must be mentioned as well, that customers can also additionally use licensed products, some of them introduced in chapter 4 and there in section 4.10 forward. When using licensed tools together with license free programs described in this proposal, extends protection level and makes the data breach readiness more widely than mentioned in this thesis work. What should be also mentioned, that examples focus have not been to show certain tables including personal data or transactions, even if the GDPR speaks precisely about personal data breach, but to show how it is possible to configure with the help of those three SAP tools protection against unlawfully use of personal data breach. This proposal gives general guidelines how to use those tools in towards personal data tables and transactions.
6 Validation of Proposal

6.1 Practical validation

Validations have been done with with different levels. One validation level has been to demonstrate all given examples on already existing SAP systems. This makes all proposal examples to be reliable because they are practically tested. Practical testing has been executed on Company-X’s demo SAP systems and on some customers SAP systems. As an conclusion we can say, that all what is proposed in proposal section have been tested and validated in real life systems and recognized that those configurations are functional.

6.2 Validation by system specialists

There has been arranged meeting for the validation of the proposal in January 2019. Three system specialists who have senior level skills technically in SAP systems have been invited to participate this validation session. First it has been demonstrated what the thesis work includes and after it demonstrated the proposal itself. Proposal has been gone through from the beginning till the end. At the same time when proposal has been demonstrated system specialists have been commenting freely the proposal. Some of the comments were written in the Conclusions and Comments chapter. All specialists
agreed that with these instructions it is possible to implement those SAP tools and they can be used for the purpose which is demonstrated in the proposal.

6.3 Validation of GDPR leading consultant

There was arranged a meeting with leading GDPR consultant who is working with SAP systems. Validation agenda was similar as with technical system specialists earlier. Thesis work’s business challenge and object was gone through and after it focused on the proposal. Leading GDPR consultant has been working with customers SAP systems concerning GDPR configurations. GDPR consultant agreed that with proposals instructions those tools can be implemented and GDPR data breach regulations be covered. It was also mentioned that these instructions together with customers other activities with GDPR will help them to increase security level of their SAP systems without extra license costs.

6.4 Validity and Reliability

In order to have confidence the worth, validity and reliability of the data, you need to consider the following questions for each archival source. 1. Who collected the data? 2. When was it collected? 3. What was collected? 4. Why was it collected? (Coghlan, Brannick, 2014, p. 91). Validity of this research data is reliable because it has been shown who has collected the data. There is data plan, which shows when, and what was collected, and purpose of the collection has been shown in this research. So, all criteriums of the validity and reliability of the data will be proven to be consistent. Reliability of the data will be proven also in the way the data has been collected: it was taken from several sources from the people who are specialists and stakeholders in this area, and they know SAP system field very well with many years’ experience. Data collection has followed also well-known data collection methods: interviews, observations, inquiries and questions. Existing knowledge data which has been used in this research is also reliable and easy to access and validate afterwards. Reliability of it supports the fact, that it is produced by SAP which is one of the leading ERP expertise companies in the world and knows best how the of its own created applications should be used in the best manner. Proposal was created based on existing knowledge of SAP official documentation, which has been proved to be very reliable source. The proposal has been validated with professionals who have high level knowledge and education about SAP products. They also have capability to see what kind of solutions are working and what kind of solutions won’t
work in different SAP environments. Also, all demonstrated examples have been validated by practical way in real SAP systems, testing them practically and proving them to work. Statement out of this all could be similar like in the book Doing Action research in your organization has been said: “the narrative needs to be sufficiently comprehensive and transparent so that the reader can arrive at the end of it able to judge for themselves the validity of the research, its claims to creation of knowledge and any claims for its extrapolation. This form of presentation presents the evidence in a factual and neutral manner” (Coghlan, Brannick, 2014, p. 169). All what was previously described makes the contents of this research reliable.

7 Conclusions and Discussions

In this chapter I going to summarize what was objective and what was the outcome of it. What was promised to do, and what did I do and analysing the process itself by personal perspective.

7.1 Objective and outcome

In the beginning, business challenge was GDPR data breach and how it concerns SAP ERP systems. The promise was to find out solution to fulfil regulation requirements with SAP tools, which do not cost extra costs for the customer. The idea of finding tools was not very difficult because SAP has been ERP provider several decades and they have lot of solutions and selections of tools for different purposes. Of course, challenge is always to have solution, which does not have extra license costs. When the idea was born what would be the object of this research, I already knew what kind of tools I would use in the proposal. Next thing was to plan how to collect data about current situation. The idea was already there to have it from those professionals who are very tightly doing SAP work with different kind of customers. There was also just created GDPR SAP project, which started in 2017. I had an idea to do surveys for these people because they would have most updated information and knowledge about these things. Surveys were sent in March 2018. Existing knowledge about SAP has been around of me already years, because I work all the time with SAP, and it is almost daily to search some sort of new knowledge. I have had also opportunity to work with many different customers in different SAP environments so; I had very good possibility to get practical experiences about tools and about the topic itself. What comes to GDPR regulations they are easily found in EU parliament’s web sites, so to read those regulations was not a problem, of
course it took a time to understand what will be demanded and for this I got support from our company’s professionals as well from the outside sources like seminar which I participated. With these elements I started to work with this issue. There have been some timely challenges of course, but I got all that what was promised to be done. Proposal itself in my opinion is very practical and helps for sure those who are willingly to use it implementing those security tools. As an summary what was objected in the beginning and promised has been done through this thesis work.

7.2 What did I learn about the process?

What did I learn through this process? A lot, first of all what I have learnt to appreciate very much are clear instructions, what must be done and how with very examples. In this kind of applied research project there could be many kinds of opinions and theories what should be done next and how it should be done but making things simple and explained with examples helps a lot. Other thing which I have learnt to appreciate is to discuss about your thesis work with other people and tutors as much as you need, it will give more perspective what is maybe going in wrong way and what could be done better. There is always a danger to stick some topic and not to get over it, discussing about it with others will help. One key word what could be mentioned here is an attitude. To have an attitude go further and not giving up that’s the engine of the whole work. Many times, when it feels that this will not go forward, and I don’t know what to do the key is: start to do it! Very often we are ready to give up too early and too easily, this kind of research demands patient and durability. I think this is one of the fruits which will be picked up to learn that things can go longer but they will become ready if you are patient enough to work for it. Working with thesis teaches as well systematic thinking which I think is one the main purposes to do such a research. You will learn certain way to perceive the things and put them in certain order. This I see one of the very big benefits of this kind of process.

7.3 What would I do differently?

I would choose much easier topic. Even if I am professional in SAP technical issues, I found this nevertheless quite challenging to do. Even if the materials and data was quite easily available for this kind of topic, rather there are not lot of information than out of SAP’s own sources. This whole topic concerns challenging environments and you can
not only do it, you need to know what you are doing. Someone might say that you need always to know what you are doing as your thesis work, yes indeed! But there are topic’s which are much more easily to write than other topics. Working itself with this topic I would not do differently, because doing the research with given instructions has been working quite well. Time plan is only thing what I would change maybe little bit. This thesis work was supposed to be started as earlier as possible, I understand some people have target to be graduated with minimum time frame. For me it is not a problem to work, learn and do other things at the same time, but sometimes it starts to be too challenging. I would start to do this kind of work first after all courses, benefit of course to start it earlier is to have some kind of body of the work already when the time comes go for it with full gas. Nevertheless, I have recognized that for me the best method is to carry out all other things first and then afterwards concentrate to graduate thesis work. This is maybe one of the biggest issues what I would have been done differently, not to have such a stress about this research so early.

7.4 What in the future?

Security issues are there to stay. World changes and cyber attacks as well. Data breach is one of the future topics and it will form itself. Definitely I will learn more about these kinds of thing concerning SAP and other IT-infrastructures. Artificial intelligence is the hot topic all over. Cloud services and how they affect SAP environments. There are lot of things to learn and be aware of. There are lot of things to do and learn and in fact learning is part of our daily working life till the end, so we are never smart of well educated enough to stop learning something new.

7.5 Discussions with specialists

In discussions there has come up several issues from system specialists regarding of the proposal. One question was: What about version levels concerning RAL? It has been shown, that this issue is dealt with in Conceptual Framework chapter. Version recommendations have been listed in chapter 4.6.2. This question was excellent because many times tools provided by SAP are version level depended. Chosen tools in the proposal are chosen also in that perspective, that most of the supported SAP versions will support usage of them. Other issue, which was discussed, that how large is the actual background information which concerns these configurations and what all belongs to it. Even if in the proposal there are three different tools describe, but that what lays behind of the
GDPR regulation and actual use of those tools is much more than only those three tools. There is a whole security concept and all what includes in it. There are lot of detailed information, which should be concerned, and it demands from customer’s side quite a lot effort to establish working set of security concerning GDPR. What was also discussed with leading GDPR consultant was that it demands lot of co-operation between different professionals to create working GDPR security concept and settings. This is reason why this thesis work gives a good ground to go forward with such a plans. It was also discussed with technical system specialists about retention time of the information, which is gathered with these tools. This would be follow-up work for this thesis work. Archiving and deleting security data and set retention times and making proposal how to achieve that all would be for sure the next step after creating in the proposal mentioned configurations first. One of the technical specialists commented on Security Audit Logging functionality and told a story about how it was used in some customer tracing a kind of data misuse. It was commented that this tool has been quite a long around, but not all customers use it. It was discussed generally how wide area security itself is. There are many kinds of data breaches and those entities who are doing such a unlawfully actions are using very different channels and tools. If the data breach takes a place and SAP system is attacked, it means they have gone already through many security layers before it. This does not mean that nothing should be done because mostly SAP systems locate behind many security layers. However, it means that we need to understand complexity of the security and different applications working with each other as well SAP systems. Conclusion of all these very valuable discussions was that security is very important aspect and SAP gives very good tools for it. What comes to GDPR itself it gives of course very clear directions what should be done to avoid such a situation where data breach to personal data can take a place. Nevertheless, there are lot of to do for such a thing’s and this thesis work is an example, which shows very clearly, what can be done in SAP environments.
References


12 Paganini, P. 2018. 90 % of the SAP customers exposed to hack due to 13 Year-Old configuration flaw. Available from: https://securityaffairs.co/wordpress/71908/security/sap-configuration-flaw.html


16 Lähdetieto Lähdetieto Lähdetieto Lähdetieto Lähdetieto Lähdetieto Lähdetieto Lähdetieto Lähdetieto Lähdetieto Lähdetieto Lähdetieto Lähdetieto.
APPENDIX 1

Questions for system specialists:

1. How many customers you are working with?
2. Awareness of GDPR (you can comment yourself to other field if you want)
   a) I am aware of GDPR and GDPR data breach regulations
   b) I have heard about it but I don’t know clearly
   c) I don’t know anything about it
   d) Other
3. System security in your customers SAP systems
   a) Is very well and all Sap’s recommended settings have been set
   b) Something has been done, something not
   c) Lot of lacking security issues
   d) Customer is not interested about the security of their system
   e) It does not matter to me
   f) Other
4. Do you know that in your customer’s roadmap concerning SAP systems GDPR
   and data breach is concerned somehow?
   a) I don’t have any kind of information about it
   b) We have been discussing about it
   c) It has been in plans and also done
   d) It is under the progress
   e) Other
5. Awareness in your customers landscape about GDPR
   a) Customer with whom I am working for knows GDPR and data breach
   b) I don’t know what they know
   c) Some of the customers know, some of them not
   d) Difficult to say but I will try to find out
   e) This all belongs to manager who will take care of it
   f) Other
6. Are you yourself ready to get more information and education about the GDPR and data breach concerning SAP systems? And are you ready to bring this information forward to your customers?
   a) It does not belong to me in any way
   b) I am ready to get more information and education about it
   c) I am not interested at all
   d) I see that it is more service managers or some other managers duty than mine
   e) Other

7. Your own attitude towards GDPR and data breach
   a) I could not care less about it
   b) I am interested in, but I know too less about it, I need to have more information about it first
   c) I know about it and I want to be involved in developing it
   d) Other
APPENDIX 2

Questions for GDPR project group:

1. How well do you know about GDPR regulations?
   a) I have some knowledge of it
   b) I have explored it for example reading about it or participating seminars etc.
   c) I am not familiar with it
   d) I am not interested about it

2. Do you know what data breach regulations means concerning GDPR?
   a) I know what data breach is, but I don’t know what it has to do with GDPR
   b) I know what data breach is and what it has to do with GDPR
   c) I am not really familiar with it
   d) I am not interested

3. Customers
   a) I am working with 1 – 2 customers
   b) I am working with 2 – 4 customers
   c) I am working with more than 4 customers

4. Customers and GDPR
   a) I have been discussing about GDPR with my customers
   b) We have not been discussing with GDPR with my customers
   c) The thing has been somehow around but not directly discussed
   d) I have been working with GDPR in several customers
   e) Other

5. Data breach and customers SAP systems: Are you aware of it that your customers systems are protected against data breaches?
   a) Systems are protected just like they should be
   b) Systems can be partly protected
   c) I can not say are they or not
   d) Other
6. Which of the following things describes your customers situation concerning GDPR and data breach? (multiple choice)

a) Customer knows about GDPR regulations
b) Customer knows about GDPR data breach regulations
c) By my customer there have own GDPR project
d) Customers technical basis team is aware of GDPR things
e) My Customer does not know lot of GDPR regulations
f) I think there is lot of lacking things by my customer concerning it
g) It is very difficult to say anything to this
APPENDIX 3

Questions for managers:

1. Are you personally aware of GDPR regulations?
   a) I know it exists, but I don’t know about it much
   b) I am familiar with it and I know something about it
   c) I am very familiar with it
   d) I don’t know anything else than the title GDPR

2. Do you know what data breach means concerning GDPR regulations?
   a) I know what data breach is, but I don’t know how it is related to GDPR
   b) I know what it means and how it is related to GDPR
   c) I don’t know anything about it
   d) I have heard it been mentioned, but I don’t know about it

3. Customers
   a) I am working with 1 – 2 customers
   b) I am working with 3- 4 customers
   c) I am working with more than 4 customers

4. Customers and GDPR
   a) I have been discussing about GDPR with the customer
   b) We have not been discussing about it
   c) GDPR has been somehow around, but not discussed seriously
   d) Other

5. GDPR and data breach protection: Are you aware of protection of your customers SAP systems against data breach?
   a) Systems are protected just like they should be
   b) Systems are partly protected
   c) I don’t know are they protected
   d) Other
6. What of the following statements describe the best the current situation in your customers SAP environments concerning GDPR and data breach? (multiple choices)

a) My customer knows very well what is required from them concerning GDPR

b) My customer is aware of GDPR data breach regulations

c) My customer does not know about GDPR regulations

d) By my customer there is a need for more information about it

e) I think my customer is willingly to order more consultation concerning it

f) My customer thinks, it does not concern them

g) I don’t going to bring it forward

h) I think this is good opportunity to sell more consultation

i) This whole thing is in vain