Master's thesis

International Business Management

2018

Jukka Mast

SAP AUTHORIZATION CONCEPT RENEWAL PROJECT AND GDPR IN COMPANY X

TURKU AMK

TURKU UNIVERSITY OF APPLIED SCIENCES

MASTER'S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

International Business Management

2018 | number of pages 52

Jukka Mast

SAP AUTHORIZATION CONCEPT RENEWAL PROJECT AND GDPR IN COMPANY X

The subject of this thesis is SAP authorization concept renewal project in company X, and European Union's new General Data Protection Regulation (GDPR). The target was to create a case study about the real life planning and implementation work in company X where I am working as an IT Service Manager. This thesis is created in a close relationship with different phases in these projects in my work, document the progress, and find out which parts in these projects were successful and what we can learn about those.

This thesis includes a literature review as theoretical part and also the reviewing of practical working life. Theoretical part includes the diverse reviewing of both literature and internet sources of this subject. A lot of sources were available regarding all sections of this thesis. For SAP authorizations related sections both literature and internet sources were well available, but related to European Union's new General Data Protection Regulation only internet resources had to be utilized due to a freshness of this subject.

I believe that especially related to European Union's new General Data Protection Regulation this thesis is one of the very first theses which exist, and that increased the interest towards this work. Appropriate reference does not exist related to fulfilling the requirements of this new regulation, so we were really implementing something totally new. Therefore it is challenging to evaluate the result of this work in company X, and in real working life we will find it out only in future. However, the work did not end when the new regulation came into effect but work will still continue. This fact is disclosed in the content of this thesis as well.

The conclusion of this thesis is that it is all about the continuous change in both SAP authorization concept and European Union's new General Data Protection Regulation as well. Business and regulations are changing, and it is mandatory to be able to respond to new requirements.

KEYWORDS:

Authorizations, enterprise resource planning, information security, legal regulation

OPINNÄYTETYÖ (YAMK) | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

International Business Management

2018 | 52 sivua

Jukka Mast

SAP-KÄYTTÖOIKEUKSIENHALLINNAN UUDISTAMINEN JA GDPR YHTIÖSSÄ X

Opinnäytetyön aihe on SAP-käyttöoikeuksienhallinnan uudistaminen yhtiössä X, sekä juuri voimaan tullut Euroopan Unionin uusi tietosuojalaki (GDPR). Tavoitteena oli tehdä tapaustutkimus näiden hankkeiden käytännön suunnittelusta ja toteuttamisesta yhtiössä X, jossa työskentelen IT Palvelupäällikkönä. Tämä opinnäytetyö on tehty käsi kädessä työelämän eri hankkeiden kanssa, ja päämääränä oli dokumentoida näiden hankkeiden eri vaiheet, sekä selvittää mikä onnistui ja mitä niistä voidaan oppia.

Työhön sisältyy teoriaosuutena kirjallisuuskatsaus aihetta koskevaan materiaaliin sekä käytännön työelämän seuranta. Kirjallisuuskatsaukseen kuuluu sekä alan kirjallisten teosten että internetistä löytyvän materiaalin monipuolinen tutkiminen. Kaikkiin työn osa-alueisiin oli materiaalia hyvin saatavilla. SAP-käyttöoikeuksien hallintaan liittyvään osuuteen löytyi sekä kirjallisia teoksia että varsinkin internetissä olevaa materiaalia. Euroopan Unionin uutta tietosuojalakia koskeva osuus puolestaan on lähinnä vain internet materiaalin varassa, asian tuoreudesta johtuen.

Uskon että varsinkin Euroopan Unionin uuteen tietosuojalakiin liittyen tämä opinnäytetyö on yksi ensimmäisistä käytännön töistä kyseistä aihetta koskien, ja se osaltaan teki työn toteuttamisen mielenkiintoiseksi. Varsinaista vertailupohjaa uuden lain vaatimusten täyttämiseksi ei siis ollut, vaan oltiin todella toteuttamassa jotain täysin uutta. Siksi lopputuloksen onnistumisen arviointi on tältä osin vaikeaa, vaan se varsinaisen työelämän osalta se selviää vasta tulevaisuudessa. Työ ei kuitenkaan päättynyt vielä uuden lain voimaantulon ajankohtaan ja se jatkuu edelleen. Tämä seikka tuodaan myös tämän opinnäytetyön sisällössä ilmi.

Tämän opinnäytetyön johtopäätös on se, että sekä SAP-käyttöoikeuksienhallinnan uudistamisen, että Euroopan Unionin uuden tietosuojalain osalta kyse on jatkuvasta muutoksesta. Liiketoiminta ja lait, sekä niiden vaatimukset muuttuvat, ja muutoksiin on pystyttävä sopeutumaan.

ASIASANAT:

Käyttöoikeudet, lainsäädäntö, tietoturva, toiminnanohjausjärjestelmä

CONTENT

PICTURES

TABLES

LIST OF ABBREVIATIONS

CIA Confidentiality, Integrity and Availability (Butler etc. 2007, 10-11).

ERP Enterprise Resource Planning. System for the core processes needed to run a company: finance, HR, manufacturing, supply chain, services, procurement, and others. At its most basic level, ERP integrates these processes into a single system. (SAP SE 2018)

GDPR European Union’s new General Data Protection Regulation. “Stronger rules on data protection mean people have more control over their personal data and businesses benefit from a level playing field.” (European Commission 2018)

GRC Governance, Risk and Compliance software from SAP (SAP SE 2018).

SAP Systemanalyse und Programmentwicklung ("System Analysis and Program Development"). A German-based European multinational software corporation. (SAP SE 2018)

SAP authorization Authorization enables users to perform a particular activity in the SAP system (SAP SE 2018).

SoD Segregation of Duties. A control intended to prevent or decrease the risk of errors or irregularities, identify problems, and ensure corrective action is taken. Segregation of Duties ensure that no single individual has control over all phases of a business transaction. (SAP AG 2013)

1 INTRODUCTION

This thesis is created as a result of my MBA studies which are focused on data security and my working life as well where I am operating with similar access rights and information security related matters. There were a lot of SAP authorizations related activities ongoing in my job and also European Union’s new General Data Protection Regulation is today’s hot topic. Therefore it was quite natural to select these issues to be the subject of this MBA thesis as well.

This MBA thesis is a case study about a Finnish retail company which is operating also in several other countries, and its SAP authorization concept renewal project. Also GDPR project from SAP data security point of view is included in this thesis. SAP authorization concept renewal project and GDPR are stated in their own sections, but on the other hand, SAP authorizations and GDPR are very closely related to each other as well.

In addition of real working life related case study, this thesis includes extensive literature review part as well in order to explain all kind of terms, details and concepts so that is easier to understand the purpose of those projects which are planned and implemented in my working life and which are included in this thesis. However, I am not explaining every single different detail about every topic. In some cases we will take a look into some technical details but in most parts I am covering these issues in higher level by explaining the different processes and tools which are available in these issues.

Company X related matters are defined in higher level and I do not define for example what are the actual methods, tools and processes that are selected by company X when responding to new GDPR related needs in SAP. However, the purpose is to give a real understanding about the complexity of SAP environments, and what kind of options there are available.

Today’s business world is changing all the time. The increasing turbulence of modern life is producing several new possibilities for all of us, and at the same time it is causing a lot of new challenges and requirements for many organizations. There is a lot of sensitive data in its many forms available everywhere and it is also causing serious security risks in different systems.

This thesis includes a snapshot about this context from Company X point of view introducing the available tools in order the fulfill the needed requirements in today’s world.

The project results in chapter 3 are hidden as requested by client.

2 THEORY – SAP AUTHORIZATION CONCEPT AND INFORMATION SECURITY

The purpose of SAP authorization concept is to ensure that company's end users, information technology (IT) support, external consultants and all other parties have sufficient privileges in order to full their job duties. These SAP access rights are provided for users as a result of well-designed and functional user maintenance process. This all must be combined to a maximum security across the whole system landscape.

2.1 The purpose of SAP authorization concept

Company's business processes are widely supported by IT department. Therefore the more mature company's IT systems and processes are, the greater they impact on how people work. Normally companies are continuously reviewing and updating their organizations and established processes and, consequently, their IT systems. When SAP is deployed as a standard enterprise resource planning (ERP) software, changes to the business processes, organizations, and IT systems have to be revised, modeled and upgraded accordingly. These kind of changes always affect the SAP authorization concept as well, which in large companies reaches a complexity that cannot be maintained or developed without appropriately defined, structured and complied processes. At companies with thousands of SAP users from several countries, changes to the infrastructure of an enterprise might require projects that may take several years, where project teams must cultivate and demonstrate expertise in business processes and related organizations, but at the same time not forgetting the knowledge of IT tools and SAP technology. (IBM Business Consulting Services 2003, 11.)

In order to get authorization concept and related processes work smoothly and efficiently, good authorization concept must introduce such authorization design which meets the requirements of easy user and access rights maintenance in order to get sufficient privileges for all users that they need for fulfill their job duties, and this all must be directly combined to maximum security. A typical well maintained authorization concept also always defines all the functions that must be carried out by users in specific job positions belonging to various units which are included in Company's organization. But that kind of higher level descriptions in SAP authorization concept are not enough, as in addition of those more detail level definition and documentation about authorizations are needed as well in order to provide the needed value also for IT departments and SAP authorization specialists. Therefore the authorization concept must define the assignments of access rights in general level and also more detailed accesses as well which are needed for users in transaction, authorization object, field and field value level in order to perform their job position related duties. (SAP AG 1999)

The ultimate target in planning of well-structured procedures in SAP authorization concept and related processes is to get it work like a well-oiled machine. Nevertheless, one of the key points is that participation in organized human activity inevitably includes constraints in individual actions in a complex compilation where the goal is that each separate action should exceed the sum of its parts. Therefore control of each separate part in this concept seems to be an essential feature in organizations. According to classical management theory, control is simplistically considered as a series of different techniques in order to measure the efficiency of another management related functionalities like organizing, planning and leading, and consequently, implementing the needed corrective actions when effectiveness of concept is seen to be lacking those. It is also noticeable that control can be exercised within, between and over organizations and their members, and also resistance might occur. Control is thus closely related to power and influence as well. (Linstead etc. 2009, 321.)

In general the risk management is the most crucial part of information security and the most important task of risk management is decrease the amount and rating of risks. In practice it means that the possibility of risk realization must be decreased to an acceptable level. Nevertheless, it is important to remember that it is not possible to totally remove all existing risks – it would mean that company should end all its operations in order to get into such level where any risks do not exist. Instead of that company’s business and risk management departments must together decide and define what is the acceptable level of risks that company and its business is able to tolerate and still efficiently continue its operative business in a safe way. However, as business and IT worlds are under constant change and development all different risk scenarios cannot not be taken into account. But proper risk management is the key to get as accurate view of predictable future risks as possible and make the needed corrective actions early enough. The identification of possible risks requires the definition of these four basic elements: what are the real threats, what are the possible consequences of realized threats, how often threat might occur and how possible it is that threat come true. (Krutz & Vines 2003, 15)

Risk management and related processes themselves must be appropriately evaluated, controlled and maintained as well. The purpose of this information security governance is to closely examine the internal control structures in order to ensure that all needed controls are correctly in place and working efficiently. These kind of governance requirements are increasing continuously in today's demanding business world where organizations and companies are competing against rivals in the global marketplace where many kind of best practices, guidelines and laws must be followed. Due to this today's business world related facts and requirements many companies have understood themselves or are forced by laws or other mandatory requirements that it is worthwhile to invest in such IT processes which provide direct benefits security and risk management. Nowadays IT department is no longer only a back-office department for the most of the companies or businesses, instead of that it is an integrated part of company's core business. This kind of dependency between company's IT and business departments ensures the proper visibility and understanding of risks and risk management to the business enabling both departments to understand each other and their needs.

The other way round, poorly managed IT and risk management processes may cause a severe risk to companies' reputations – companies must be able transparently demonstrate and prove the reliability of their IT systems, processes and governance models in order to achieve the trust from all relevant parties like partners, shareholders, employees and, the first priority, consumers. After all the well-defined and implemented governance model for all risk management and information security related processes is the key mechanism for the board of directors and management to have the appropriate control of risk management to the company and keep the risks at an acceptable level. This is a mandatory element for example to keep reliability of reporting in a good level and of course to earn the trust form the customers. (Krause & Tipton 2007, 16)

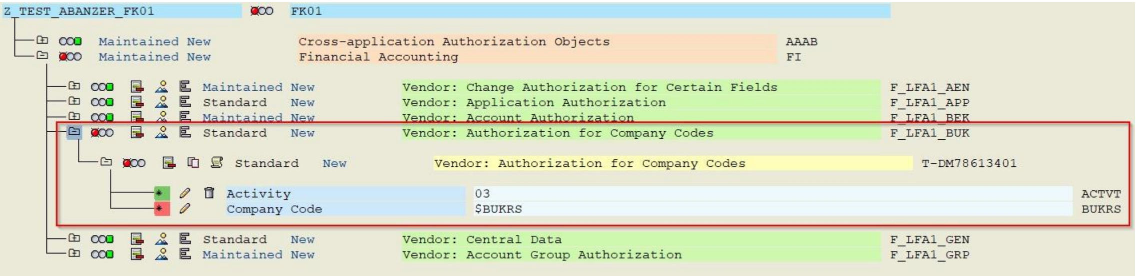
IT security risks are often very extensive and widespread. Security risks may be even fatal enough to get whole company on its knees. Despite that such organizations still exist which do not have any comprehensive and systematic way to handle the IT security risks. The reason might be that the biggest risks for companies are their products and customers – faulty or purposeless products may ruin the company whereas customer who do not pay their bills or otherwise abandon the company can cause huge financial losses as well. But IT risks are crucially in the loop as well and today the well-working IT security processes are actually the whole world for many companies. The amount of this kind of companies who just cannot operate without proper IT processes is increasing all the time because the fact is that huge amount of vital information such as customer registers and product specifications are in digital form in company's databases. This sort of information must be secured. (Jordan & Silcock 2005, 10-11)

2.2 SAP authorizations

Companies must to protect their sensitive business data based on separate laws, regulations and agreements. There is a need to fulfill certain legal requirements based on company's country of operation. These requirements are related to for example different data protection laws or employee protection. Companies must be also able to follow the agreements with and requirements of their customers, vendors and other partners.

There are a large number of possible threats and it is impossible to ensure a perfect security against all of those. Therefore companies should concentrate on such areas in which a clear benefits can be realized through expenditures caused by well defined, planned and implemented authorizations. It is also disadvantageous if authorizations are implemented in such was that almost every function that users are trying to perform leads to an error message caused by the missing authorizations. That kind of situation is not favorable for the companies' business processes and may even lead to a situation where it would be cheaper to replace the financial losses caused by some human error by user with too wide authorizations, than to protect the data and all functionalities in SAP at great expense. (SAP AG 2006, 6-7)

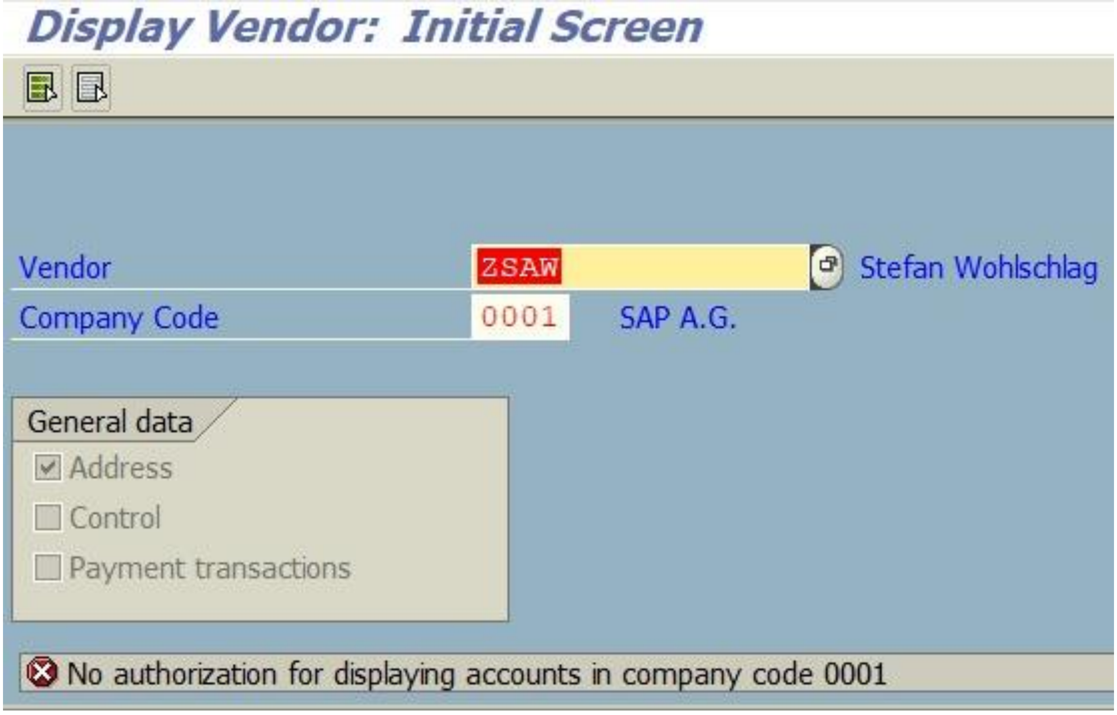
In technical level there are many components in SAP authorizations. In higher level SAP authorizations consist of single roles and composite roles, which may include one or many single roles. Single roles can include for example different transaction codes, services, programs, authorization objects, activities, field values and organizational data. This below stated picture shows some possible content in authorizations in SAP role.



```
Z_TEST_ABANZER_FK01          FK01
  Maintained New          Cross-application Authorization Objects            AAAB
  Maintained New          Financial Accounting                               FI
     Maintained New           Vendor: Change Authorization for Certain Fields     F_LFA1_AEN
     Standard   New           Vendor: Application Authorization                   F_LFA1_APP
     Maintained New           Vendor: Account Authorization                       F_LFA1_BEK
     Standard   New           Vendor: Authorization for Company Codes             F_LFA1_BUK
        Standard   New           Vendor: Authorization for Company Codes             T-DM78613401
           Activity              03                                                     ACTVT
           Company Code          $BUKRS                                                 BUKRS
     Standard   New           Vendor: Central Data                                F_LFA1_GEN
     Maintained New           Vendor: Account Group Authorization                 F_LFA1_GRP
```

Picture 1. SAP authorizations - role, object and field values (Banzer 2017).

If user is trying to access some data in SAP where user does not have an authorization, authorization error will occur and access is denied. The next picture includes an example of SAP authorization error.



Display Vendor: Initial Screen

Vendor: ZSAW Stefan Wohlschlag

Company Code: 0001 SAP A.G.

General data

☑ Address

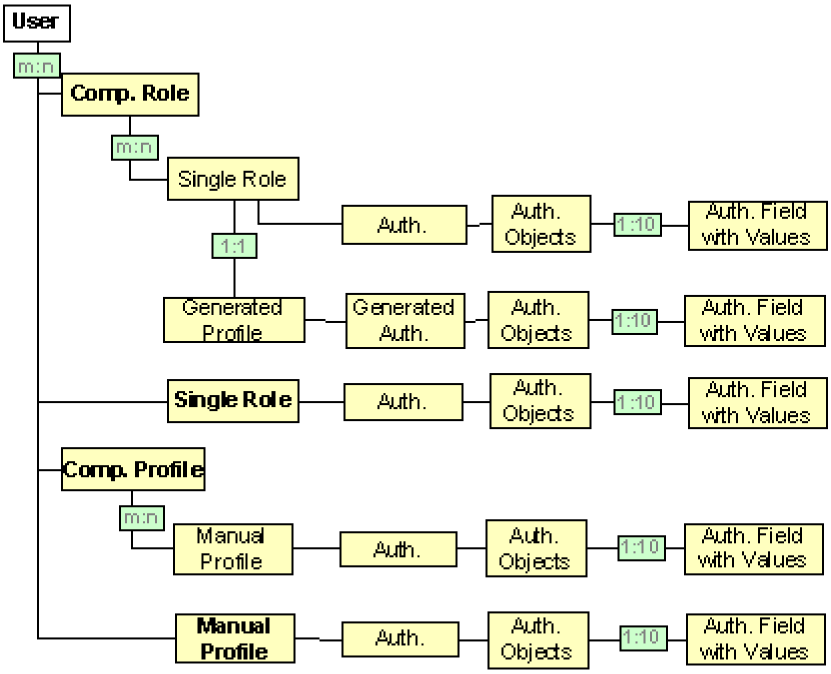
□ Control

□ Payment transactions

No authorization for displaying accounts in company code 0001

Picture 2. SAP authorization error (Banzer 2017).

Composite and or single roles are assigned for users, and the authorizations that users have in SAP systems are collected from the generated profiles of all single roles which are assigned to users directly or via composite roles altogether. The authorization components and their relationships are introduced in next picture.



Picture 3. The authorization components and their relationships (SAP SE 2015).

2.3 The CIA triad

Even though SAP authorization concept and it details are very complicated, in general level its targets go hand in hand in common with IT security universally. In “IT Security Interviews Exposed” the authors very well define the fundamental objectives of information and cyber security. The three main objectives are confidentiality, integrity and availability, also known as the CIA triad. These security aspects can be easily compared to corresponding physical security related matters which exist in world around us. For example various alarms, locked doors, locked windows and another physical and protective items reflect the functionality of passwords, authorizations and intrusion detection methods in IT systems. When transferring these security related concepts and matters from the physical world to the IT world, it is important to always define the real business needs and the terminology first in order to make these IT security versions of those physical world’s security items to really protect the business and its data. (Butler etc. 2007, 10-11)

2.3.1 Confidentiality

Butler et al. write that first of those main security objects is confidentiality which purpose is to protect information from unauthorized exposure. The prerequisite for this to make it work correctly is to understand the content and purpose of the data that must be protected and who are the users who should have authorization to it (Butler etc. 2007, 170). I personally agree with this. In addition, my opinion is that it is not necessarily mandatory to understand and know all such users beforehand who should not have authorization to it. I justify this statement by following my understanding and perspective to basis of information security: the default authorization for all users is no authorization and all authorization requests must be separately requested, justified, validated and approved by nominated approvers. This way it is not necessarily to spend time and resources to trying to understand and define the mass of users who should not have authorization to some certain data.

Another very important aspect when planning a security concept is to understand the primal goal and keep in crystal clear in mind: information systems must do actions what we want, how we want and when we want. Those actions must be also performed in as secure way as possible without any unnecessary risks – the fact is that IT systems are tools for business to work smoothly in a secure way, but IT systems are not business owners. Therefore the first of the above stated three main objectives, confidentiality, is about protecting information system and its data from unauthorized access and usage. In order to fulfill this requirement it is crucial to be aware of the content of data which needs protective controls. When the data what should be protected and who should have access into it are known, it is easier to define how to protect it.

2.3.2 Integrity

The second information security main objective, integrity, is about securing the information system and its data from unauthorized modification.

In his blog, IT Security community blog - Confidentiality, Integrity, Availability: The three components of the CIA Triad, Terry Chia states that information is valuable only if its content is valid and correct. If information is somehow modified and changed, it may prove costly. For example, if some payment run transaction for 500 € is performed but its data is changed in such a way that you actually sent 50,000 €, it might prove to be a very costly for user. Along with data confidentiality, different cryptography methods play a very important role in ensuring data integrity. Commonly used methods to secure data integrity are for example hashing the data that user is receiving and comparing it with the hash of the original data in the message that has been sent. In practice it means that the hash included in the original data must be provided to user in a protected way. (Chia 2012)

2.3.3 Availability

Finally the third objective availability refers to ensuring that information system and its data is accessible to such users who really need it and whenever they need it. And when thinking it vice versa, it must be ensured that users who should not have access really are not authorized for that. (Butler etc. 2007, 170-171)

My personal mindset says that in SAP system landscape the default authorization is always "No authorization" and the really needed authorizations must be always separately requested and approved. So this is the opposite approach to a logic or solution where all users have very wide access rights in order to ensure that all users are allowed to perform many functionalities to avoid situations where possible authorization errors might prevent or at least slow down the core business and the needed activities in SAP systems.

2.3.4 The CIA sub-attributes

Along with the main objects, there also three sub-attributes in CIA triad which are closely involved into main objects: authenticity, accountability and non-repudiation.

In information security it is always mandatory to validate that all elements in the data are authentic. The other aspect of authenticity is to ensure that all involved parties are genuine and who they claim to be. In some data security systems also authentication tools like "digital signatures" are used, which duty is to prove that the information is original and real, and it was sent by someone who really owns the appropriate signing key. These are the key points in first CIA sub-attribute, authenticity. (Hanis 2014)

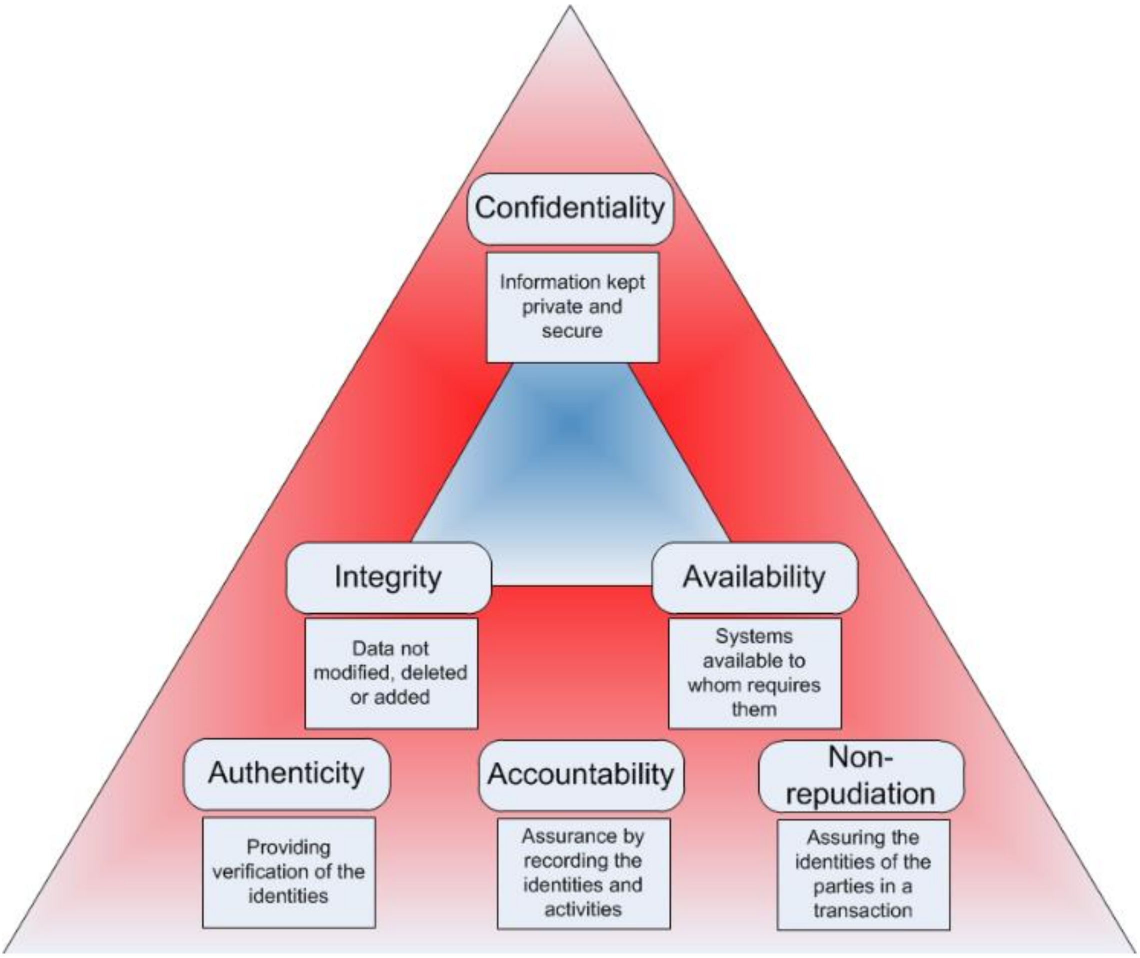
The second CIA sub-attribute, accountability is about ensuring that the identity of the involved users and their activities in the information system can be traced. That is to say, accountability means the action where the identity of a user who performed some action, the time when action happened, method, and the level of access to a system and the details of performed actions are possible to record (Information security handbook 2009). The third CIA sub-attribute, Non-repudiation refers to the capability to prove the occurrence of any action in a way that the particular action is not possible to be repudiated afterwards later on. (Kamkarhaghighi M. etc. 2016)

2.3.5 The conclusion

After all and returning to those three information security main objects, the result is that all those three items merge to each other. Both confidentiality and availability heavily contribute to integrity as denying unauthorized accesses and on the other hand allowing legit and authorized accesses to the needed information are standard ways to maintain the integrity of the information system and included data. Sometimes the integrity failures still happens even though all the needed security controls are adequately defined and also implemented. One reason for this is the fact that the people we trust are still not necessarily worth of trust. Sometimes we are forced to trust some people we actually know very little about. This kind of users can be for example third-party business partners, consultants, summer trainees or some other temporary workers.

The profit driven core business urgently demands us to provide the authorizations for the users in order to avoid any breaks in the production cycle and keep the income rate continuously in high level. Therefore the integrity and security controls must go further from simple “who” definitions and find the answer to “what” question: as access rights are granted for users, what are the functionalities that they are able to perform in information systems? This kind of very important question must be taken into account. That is the key question when planning, defining and implementing the restrictions to authorizations and access rights in information systems. In a well-planned and secured information system all users have job-role based authorizations which allows users to perform their duties but nothing else. (Butler etc. 2007, 171)

In GeraintW Online blog CIA & InfoSec, author Geraint Williams presents and summarizes the CIA triad and related sub-attributes very well in next picture.


Confidentiality
Information kept private and secure
Integrity
Data not modified, deleted or added
Availability
Systems available to whom requires them
Authenticity
Providing verification of the identities
Accountability
Assurance by recording the identities and activities
Non-repudiation
Assuring the identities of the parties in a transaction

Picture 4. The CIA triad and sub-attributes (GeraintW Online Blog 2012).

2.4 The Russian customer data act

The background for new Russian data protection law was that the Russian data protection authority, Roscomnadzor, did have a number of meetings with separate Russian business associations in order to respond to the increased amount of questions which were asked related to the interpretation and application of Russia's personal data localization law. The final outcome was that the new data protection law, which entered into force on September 1, 2015, requires that any operator who is in way or another collecting some personal data from individuals, ensures that the storage, recording, systematization, accumulation, rectification meaning any update or change in data and extraction of Russian citizens' personal data are using databases which are physically located in Russia. Any databases locating in any other country that in Russia were not allowed anymore. However, this act addressed some concerns as well related to questions whether data stored in Russia could also be transported outside from Russia, and the reach of the law’s jurisdiction. (Shaftan, V. 2015)

Russian data protection law is valid for all data operators and third parties who are operating under the authorization of data operators. Russian data protection law does not include such separate concepts like "data processor" or "data controller". Nevertheless, the Personal Data Protection Act still refers to the concept of "data operator". A data operator can be a state or municipal organ, legal or physical individual who organizes or performs the processing of personal data, or determines the purposes of personal data processing, the content of any kind of personal data, and the actions which are related to personal data. The data processing can be transferred to a third party, subject to the data subject's approval, who will be acting under the authorization of the data operator based on the appropriate agreement, or by operation of the special state or municipal act. (Medvedev, S. 2017)

The data protection law also states that, if the personal data is shared with third parties like business partners or service providers, it is a mandatory task for data operators to explain the actions they take in order to protect the individuals’ personal privacy data. The policy of data operators should also inform that the data operators enter into contracts with third party recipients in order to protect the individuals’ privacy data. In addition, the policy must be also able to state the reason for that kind of privacy data sharing, the actual amount of personal data which is going to be shared, the data usage limitations, including confidentiality obligations, and the existing and used security related actions in both organizational and technical level. Eventually, the data protection law and its policy must inform both names and addresses of all third party recipients of personal data. (Hogan Lovells 2017)

2.5 The General Data Protection Regulation - GDPR

“The EU General Data Protection Regulation (GDPR) is the most important change in data privacy regulation in 20 years - we're here to make sure you're prepared.” This is how GDPR Portal’s main page summarizes the impact of this European Union’s new data protection law. The purpose of GDPR Portal is to educate all of us about the main elements of new General Data Protection Regulation. (EU GDPR Portal 2017)

This new data protection law was approved by the European Union Parliament on 14 April 2016. The actual enforcement date is May 25th 2018. At that date those organizations who have not planned and implemented the needed actions, are non-compliance for this new law and there they will face heavy fines. GDPR replaces the former Data Protection Directive 95/46/EC and it was planned to harmonize the existing separate data privacy laws across all over the Europe. The purpose of this new regulation is to secure and empower the privacy data of all EU citizens and to reform the existing procedures how organizations in EU area are interpreting and applying the privacy data. (EU GDPR Portal 2017)

Perhaps the right to erasure or in other words the right to be forgotten is one of the key items of GDPR. It means that data subject, meaning all of us individuals, has the right to obtain from the data controller in any organization the erasure of any personal data concerning individual without unreasonable delay and the controller must erase personal data without undue delay. (Intersoft consulting 2018)

3 SAP AUTHORIZATION CONCEPT RENEWAL PROJECT

Results of the project are confidential.

3.1 Audit findings

Results of the project are confidential.

3.2 GRC

Results of the project are confidential.

3.3 Authorizations and user accounts

Results of the project are confidential.

3.4 Access rights management

Results of the project are confidential.

3.5 Project results

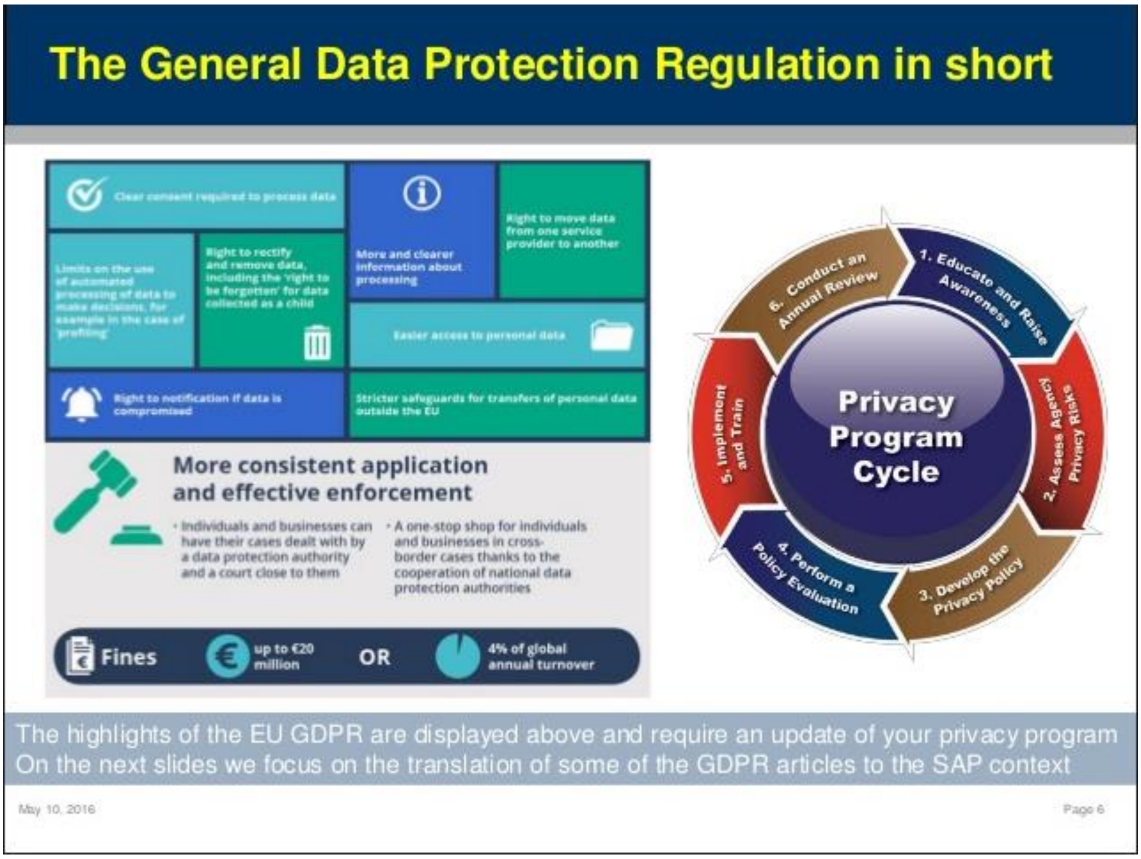
Results of the project are confidential.

3.6 Russia Data Act project

Results of the project are confidential.

4 GDPR PROJECT

The EU General Data Protection Regulation (GDPR) project in company X, or at least my role in it as a SAP authorizations representative, started on the beginning of year 2017. The requirements of GDPR includes a lot of actions from many various aspects, processes, systems and applications from both business and IT. SAP authorization concept is also heavily involved into it and therefore I'm also participating to this project. In general GDPR is a massive change which has effect on many systems and processes but in this chapter I'm focusing on SAP, authorizations and access risk management part only. The next picture summarizes the General Data Protection Regulation in short.



The General Data Protection Regulation in short

Clear consent required to process data

More and clearer information about processing

Right to move data from one service provider to another

Limits on the use of automated processing of data to make decisions, for example in the case of 'profiling'

Right to rectify and remove data, including the 'right to be forgotten' for data collected as a child

Easier access to personal data

Right to notification if data is compromised

Stricter safeguards for transfers of personal data outside the EU

More consistent application and effective enforcement

- Individuals and businesses can have their cases dealt with by a data protection authority and a court close to them
- A one-stop shop for individuals and businesses in cross-border cases thanks to the cooperation of national data protection authorities

Fines up to €20 million OR 4% of global annual turnover

The highlights of the EU GDPR are displayed above and require an update of your privacy program
On the next slides we focus on the translation of some of the GDPR articles to the SAP context

May 10, 2016

Page 6

Privacy Program Cycle
1. Educate and Raise Awareness
2. Assess Agency Privacy Risks
3. Develop the Privacy Policy
4. Perform a Policy Evaluation
5. Implement and Train
6. Conduct an Annual Review

Picture 5. The General Data Protection Regulation in short. (Kuijper 2016)

4.1 GDPR compliance in SAP

GDPR is one of the most extensive regulations ever implemented in the European Union. Its purpose is to give citizens decide and control how their personal data is stored and used. This law takes effect on May 25, 2018. The consequences of non-compliance with GDPR are high: a fine of up to 20 million euro or 4% of company's global revenue, whichever is higher. Even if the company is not registered in Europe, the law may still be valid if company process data which belong to data subjects in the EU, for example by offering them goods or services or monitoring their activities. (SAP SE 2018)

As already stated in this thesis, company X already has an authorization concept which has been updated to meet the today's requirements. Therefore we are not planning or implementing something totally new from scratch because of GDPR. Instead of that, we are utilizing, reviewing, modifying and validating our existing SAP authorization concept in order to include the relevant and required GDPR relevant specification there. In order to fulfill the GDPR requirements in SAP authorizations area, company X has selected a partner to complete these tasks. This partner is an external company oriented SAP authorizations and GRC. SAP authorizations related work in company X together with our partner will be split into 3 streams: Content definition, risk determination and processes.

The content definition part means in practise the definition of GDPR relevant data objects, like transaction codes, tables, authorization objects and other GDPR relevant details in SAP authorizations. In addition, GDPR risk library must be defined based on our partner's best practice. Also our existing and recently renewed authorisation concept must be re-structured and updated with the GDPR relevant content.

In risk determination phase the existing GDPR relevant risks must be identified and analysed based on the above stated risk library, and the risk levels must be agreed and approved by company X business and IT representatives. Finally also processes must be updated so that all new GDPR specifications are adapted into company X's SAP authorization and user access management processes, roles and responsibilities are clearly defined, GDPR ways of working fit smoothly in our concept and the needed additional GDPR approval steps and approvers are updated there as well.

4.2 GDPR risks and role design

GDPR risks in company X roles and users must be identified and analysed first before it is possible to perform any further risk management related decisions and clean-up work. Therefore the initial risk measurement must be implemented in order to discover the actual and present GDPR risk level in our SAP systems. Company X has a large number of SAP ERP environments and it is not reasonable to try to cover all existing SAP environments within this first phase. Therefore we decided take five biggest and most business critical SAP ERP systems from finance and logistics side into loop into first phase of company X GDPR SAP authorization project.

The initial GDPR risk measurements happen into those five SAP ERP systems the measurement results are uploaded into our partner's service portal. This service portal is the place where company X responsible person from both IT and business side will review and analyse our GDPR risks, and decide the further actions. This very first initial measurement activity includes SAP standard transaction codes and related authorizations only, the dedicated custom authorizations which exist in company X SAP environments only are not included in this GDPR project's phase one.

As said, the results of these initial measurements in our five SAP systems will be reported by using a service portal provided by our partner. Those results should enable us to proceed further with the needed activities and changes which are needed in order keep all company X SAP environments GDPR compliant in future. That service portal and its data should give us an appropriate understanding of changes which will be needed for designing and implementing the mandatory authorization changes in SAP roles, removing the access rights from users, developing remediation actions as a part of GDPR risk management, defining the needed authorization concept changes, updating approval processes by for example adding the new mandatory approval steps for such roles which are confirmed to include GDPR relevant risky authorizations, etc. In this first phase of our GDPR project's SAP authorization stream the main focus will be in concept, processes and documentation side, but of course in case of any critical findings in our initial GDPR risk measurements, the needed clean-up actions will happen immediately in order to decrease the amount of critical GDPR risks.

Based on the initial measurement results our partner will provide an action plan for the needed technical authorization changes regarding SAP roles and / or user access rights, which should take place in company X GDPR project's SAP authorization stream phase 2. This phase 2 is optional and company X will make the Go or No-Go decision based on the finding in phase 1. In practice the phase 2 would mean more massive and systematic authorization changes in big amount of roles in all company X SAP environments. The target for these massive authorization changes is of course get all of our SAP systems into more GDP compliant level. But the possible need of optional phase 2 will be clarified later on once phase 1 is first completed.

So the key items which phase 1 should provide us are the needed updates to company X SAP authorization concept so that it is compliant with GDPR requirements, GDPR relevant updates to all processes which are in the scope, roles and responsibilities related to GDPR are agreed, maintenance process for authorisation concept is agreed in order to enable adaptions of the applications of the law, the most critical technical level SAP authorization findings are solved, and detailed action plan, targets and costs for optional and possible phase 2 is clearly agreed.

4.3 GDPR – the other methods

In addition of SAP authorizations related changes, GDPR causes many other requirements as well. I am not too deeply all of those, but many of them touch upon my job as well more or less. Here I introduce some of those.

4.3.1 Read Access Logging – RAL

Read Access Logging (RAL) can be used to log and monitor read accesses to many kind of sensitive data in SAP systems. The data which is monitored and logged with RAL can be categorized as sensitive for example by internal or external company policy or for example by law. The typical reasons for Read Access Logging usage might be for example these kind of questions:

- Who has accessed to some sensitive data, for example a bank account?

- Who has accessed to some personal data, concerning for example some business partner related data?

- Are there such employees who have accessed to some personal information, concerning for example employees’ religions?

- Are some employees searched and accessed some privacy data, for example, concerning for example any kind of individuals’ health care related information?

- Which business partners or accounts or were accessed by some company employees or some other users?

It is possible to answer this kind of questions by using information about who accessed particular data within some certain specified time period. The prerequisite is that all related remote infrastructures that access the data, must be enabled for logging.

The normal reason for Read Access Logging usage is to comply with some legal regulations or public standards such as data privacy. Data privacy is about securing and limiting certain accesses to some personal data. In such situations where any kind of data access log or monitoring is not performed, it is extremely difficult to track any data leaks to the outside world. Read Access Logging is used in order to get that information.

Read Access Logging is must be based on some purpose that is defined according to certain requirements of a company, like data privacy. Therefore this kind of logging is assigned to several log entries as attributes, which enable the log data to be defined, organized and classified according to the logging purpose. For example, reporting or archiving related rules can be planned and implemented based on the actual and dedicated logging purposes.

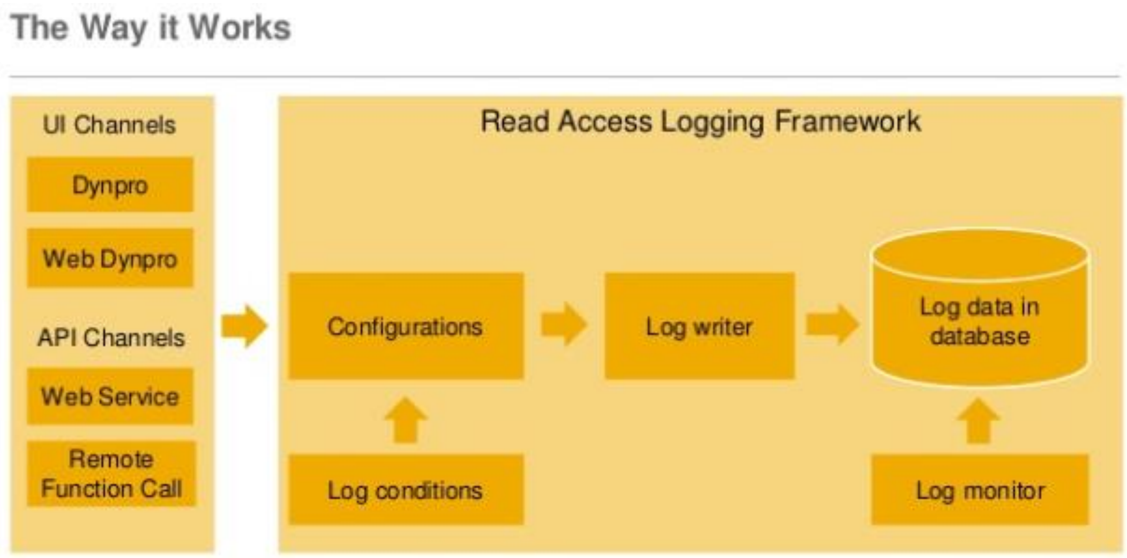
The Read Access Logging framework can thus be used to meet some legal or other pre-defined regulations, to detect any frauds or data thefts, for internal or external auditing purposes, or for any other appropriate purpose. Therefore Read Access Logging can be considered to be a very relevant tool for GDPR requirements as well.

There are of course technical requirements for Read Access Logging as well. However, when any SAP system is created and application is started, the Read Access Logging is initially turned “On” and its configuration is read. It indicates whether the valid and allowed remote function modules, Web service operations, or Web Dynpro UI elements are log-relevant and to what extent. One of the main questions is that should only accesses themselves be logged, or the content of the accesses as well? It is possible to structure the log entries based on the various needs.

Different SAP systems may contain some predefined configurations in Read Access Logging. But usually company administrators must adapt them in order to meet the different and specified needs to fulfill the needed legal requirements in organization - requirements that are not necessarily related to SAP at all. It is also possible that companies create their own Read Access Logging configurations.

One very important key element in all logging is that the need to log data must be in balance with the workload that logging will cause on the performance of SAP system. The SAP system performance will depend upon the amount of data which is logged and also the complexity of the rules and conditions that are specified for which data is logged. (SAP AG 2013)

Therefore it is perhaps not wise to try to log and monitor every possible details in SAP systems because of the workload. The other reason is that too large amount of logs are not readable anymore to. So too much is too much in Read Access Logging as well. In next picture the Read Access Logging Framework is described in higher level without drilling down into technical details.


The Way it Works

UI Channels

Dynpro

Web Dynpro

API Channels

Web Service

Remote Function Call

Read Access Logging Framework

Configurations

Log writer

Log data in database

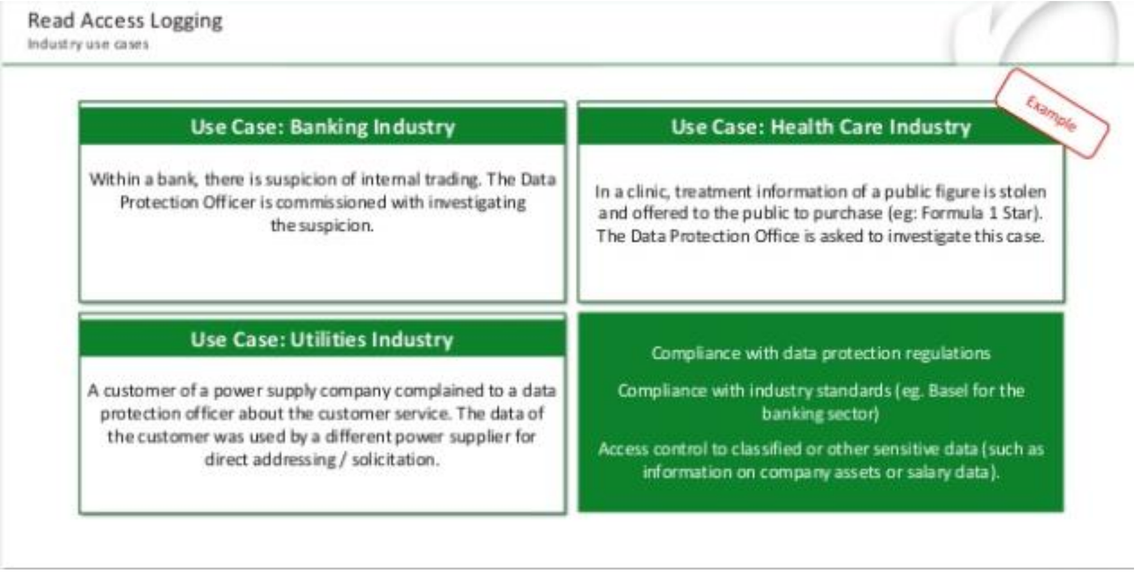
Log conditions

Log monitor

Picture 6. Read Access Logging Framework (SAP AG 2013).

So in summary, Read Access Logging can be utilized to log and monitor sensitive accesses to different fields in different data in SAP systems. It is possible to perform logging and monitoring on various input channels and levels. Logging and monitoring is enabled in function and program calls –level and in user interfaces as well, and the monitoring in detailed field level is possible. The monitoring results can be viewed in the function view, but the usage of in further applications related to customized threat detection or dedicated alarm mechanisms and evaluations can be used as well. (Dahse 2017)

Below stated picture shows some examples of possible Read Access Logging usage.



Read Access Logging

Industry use cases

Example

Use Case: Banking Industry

Within a bank, there is suspicion of internal trading. The Data Protection Officer is commissioned with investigating the suspicion.

Use Case: Health Care Industry

In a clinic, treatment information of a public figure is stolen and offered to the public to purchase (eg: Formula 1 Star). The Data Protection Office is asked to investigate this case.

Use Case: Utilities Industry

A customer of a power supply company complained to a data protection officer about the customer service. The data of the customer was used by a different power supplier for direct addressing / solicitation.

Compliance with data protection regulations

Compliance with industry standards (eg. Basel for the banking sector)

Access control to classified or other sensitive data (such as information on company assets or salary data).

Picture 7. Read Access Logging - Industry use cases (Dahse 2017).

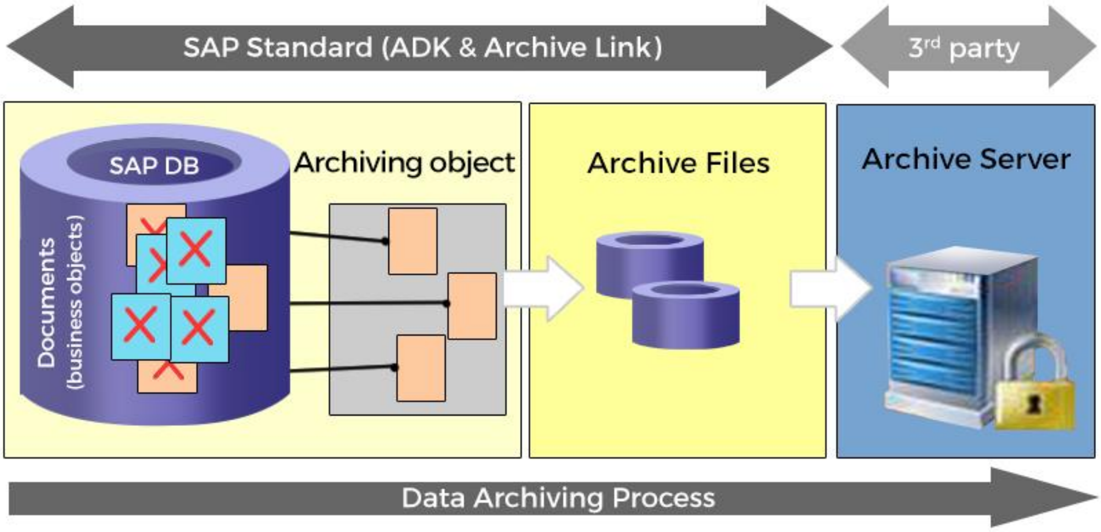
4.3.2 Data archiving in SAP

Data archiving is used to remove the big masses of data from the SAP databases are no longer needed in the system but which must remain in a such format that can be analyzed when needed.

Archiving is required in SAP systems because of the continuous growth of SAP data bases. Growing has an effect for example to servers, hard disks, backup devices and servers. It means that the performance of SAP servers will degrade and SAP system response times will increase. In other words it means that SAP systems are getting slower.

GDPR and data archiving in SAP are tied together when thinking it from legal regulation point of view. One reason for GDPR is to support data subject rights. Many SAP products include various functionalities which help organizations to identify and report different sensitive data, for example personal privacy data. In addition, functionalities related to the deletion of available data help organizations to achieve the GDPR requirements of personal data deletion, blocking or minimization (SAP SE 2017).

So data archiving in SAP is definitely linked to this legal requirement when simply deletion of data is not a valid option due to retention requirements, so therefore the most reasonable solution is data archiving. (Avaali 2015). The next picture reveals the main concept of SAP Data Archiving Process.



Picture 8. SAP Data Archiving Process (Avaali 2015).

In SAP data archiving functionality all SAP archiving objects are supported including an automated media management for different archive files on hard disc, optical libraries or for example on tape. SAP data archiving ensures transparent processing, high performance and scalability, and the archiving results can be displayed directly via the SAP Graphical User Interface (SAP GUI). For most of the archiving objects, the SAP data archiving concept is based on the Archive Development Kit (ADK). This functionality also has a support for the SAP Archive Information System (SAP AS).

There are several benefits of data archiving in SAP. For all SAP users, including business end users, system administrators and all other users, the increased SAP performance is always a good news. So as SAP data archiving reduces the growth of the SAP data bases and actually making the data bases smaller, the system performance is increased. Data archiving also enables the faster backups and also aster data base recoveries, which are handled by SAP system administrators. The increased throughput of the SAP systems is one benefit as well. Also when SAP data archiving functionality is implemented and in use, it normally reduces the extra investments for some additional hardware and less efforts from system administrators are needed for various maintenance and administration tasks.

There are remarkable advantages especially for all SAP end users as well. SAP data archiving can be utilized when optimizing different business processes. Data archiving also allows SAP systems to provide better response times to various customer inquiries performed by end users. It is also remarkable that when some archived information is needed even after many years, it is available instantly. That is something that I personally appreciate very much as in my SAP authorizations related tasks I sometimes got requirements where some very old information is needed urgently.

4.3.3 Data anonymization

Data anonymization is a process which either encrypts or removes any personally identifiable information from data sets so that individuals whom the data describes remain anonymous. Data anonymization irreversibly prevents all possibilities of identifying the data subject. In other words it means that anonymization is the destruction of the identifiable data.

There are different methods in data anonymization:

- Data suppression: Suppress the data by replacing a value with some place holder. For example, instead of value “age 35,” the value is set to be “X.” Another method is the generalizing the data. Instead of “age 35,” the input is “between 30 and 40.”

- Data encryption: Replaces any sensitive data with some encrypted data. Data encryption method provides effective data confidentiality and in addition it transforms the data into an unreadable format.

- Data substitution: Any sensitive information values of the original data context are replaced with some other parameters.

- Data aggregation: In order to make some sensitive data not to be singled out, a data subject is grouped or merged with some other data subjects which share some or all sensitive personal data, for example their age and gender.

- Noise addition: Means that some impreciseness is added into the original sensitive data.

In each of above stated methods the main target for anonymization is to create such data sets which are still available for analysis needs but without identifying any individual persons. Another target is to protect some sensitive data in organizations. If organizations contribute information into some certain data sets, but do not want any person to identify their actual valid data. In this case, the organizations themselves are the actual individuals and those are then the data subjects which must be protected. The typical use cases for these kind of scenarios are benchmarking within industries. Choosing the corrected and the needed method usually depends on the organizations' privacy requirements or laws and used data sets. The final decision and approval on the method and the parameters usually must be done by organizations' data privacy officers. (SAP SE 2018) Below stated table includes some fictional example of Data Anonymization.

Name	Birth	City	Weight	Illness
Paul	07-1975	Walldorf	82 kg	AIDS
Martin	10-1975	Hamburg	110 kg	Lung Cancer
Nils	01-1975	Munich	70 kg	Flu
Annika	09-1970	Berlin	58 kg	MS

Table 1. Data Anonymization (SAP SE 2018).

4.3.4 Data pseudonymization

Data pseudonymization substitutes the identity of some certain data subjects so that the data subjects cannot be directly identified anymore. In order to re-identify the data subjects, additional information would be required. In pseudonymization method some identifiable data is substituted with consistent and reversible values. However, in pseudonym method it might be possible to identify the data subjects by analyzing some other underlying or related data.

Data Pseudonymization methods can be basically split into two groups:

- Hash functions: Hashes are popular and commonly used as those can be computed quickly. Those are normally used for example to map any data of any size to some certain codes of a fixed size. For example some persons' first and last names can be simply hashed to be values “01”, “02”, and “03”. The length of first and last names do not matter as the hash values are always two digits.

- Tokenization: Tokenization is a method where some specified data elements are substituted with some non-sensitive equivalents. Those equivalents are called as tokens.

The tokens do not have any identifiable values, but it those act as identifiers for some certain data subjects. Those are the reference values which can be utilized in order to trace back into the original data. Tokenization is a nonmathematical method which is used to protect some sensitive data but preserving the data type and its length. An example of Data Pseudonymization with fictional content is stated in this next table.

Name	Birth	City	Weight	Illness
0c4a67	07-1975	Walldorf	82 kg	AIDS
df89aa	10-1975	Hamburg	110 kg	Lung Cancer
305be2	01-1975	Munich	70 kg	Flu
7422c2	09-1970	Berlin	58 kg	MS

Table 2. Data Pseudonymization (SAP SE 2018).

4.3.5 Data masking

Data User Interface masking in SAP is an active form of suppressing display of sensitive data in SAP Graphical User Interface (SAP GUI) for business and technical transactions. It means that the needed sensitive data is masked in SAP GUI transactions from all unauthorized users. Data masking can be also utilized for logging of requests from users which try to access to configured data fields. Data masking does happen in the User Interface (UI) level, and therefore it does not include database-level functionality like encrypting. For example many important table view transactions can be protected with data masking.

Data masking in SAP works requires certain tasks in order to make it work. First there is a need to define which data fields are sensitive and how those should be masked. After that the defined field can be technically masked by using screen variants and transaction variants. Those roles and / or users must be also defined and configured who should be authorized to see unmasked data. Then those specified users can be assigned to certain role which allows users to see unmasked values for the applicable fields.

So by default all the defined sensitive data is masked from all SAP users, but users who should be able to see it, must defined separately and assigned with certain authorizations which allows that access. In other in this phase we are basically talking about data encryption, which means such keys or algorithms that allows only certain specified users with the right access rights to see the data – all data or some parts of it (Baird

2013).Tracking of requests for any sensitive data by users (who, when, what, IP address) is also possible, and tracking generates also audit trail for possible audit purposes later on.

The key benefits of data masking are:

- Minimal on system performance, or no impact at all.

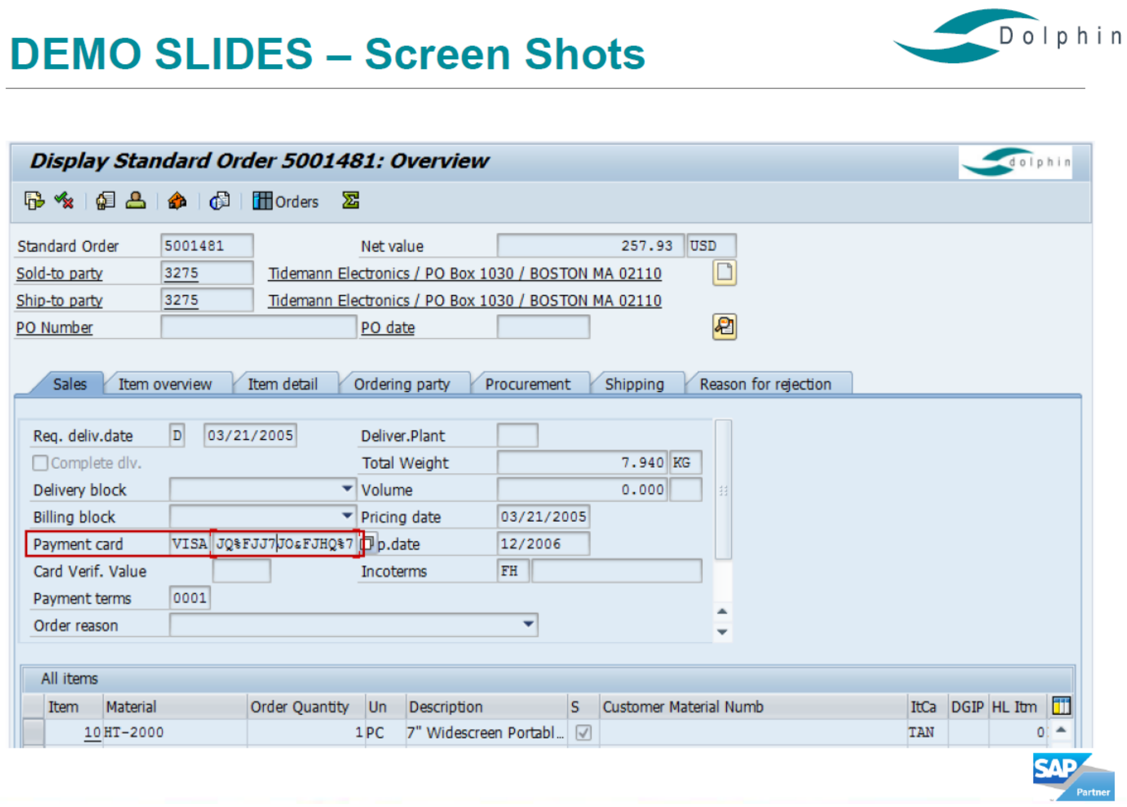
- Data masking enables archiving functionality for the tracking file.

- Masking can also be utilized for data downloads and printouts, protecting the data, avoiding the data damaging and costly cases of data loss.

- It Increases the transparency of accesses to any sensitive data including audit trail on field levels.

- Data masking ensures compliance within various data privacy regulations – such as GDPR.

The next picture shows some possible Data masking case in SAP.



DEMO SLIDES – Screen Shots

Display Standard Order 5001481: Overview

Standard Order	5001481	Net value	257.93 USD
Sold-to party	3275	Tidemann Electronics / PO Box 1030 / BOSTON MA 02110	
Ship-to party	3275	Tidemann Electronics / PO Box 1030 / BOSTON MA 02110	
PO Number		PO date	

Sales | Item overview | Item detail | Ordering party | Procurement | Shipping | Reason for rejection

Req. deliv.date	D 03/21/2005	Deliver.Plant	
□ Complete dlv.		Total Weight	7.940 KG
Delivery block		Volume	0.000
Billing block		Pricing date	03/21/2005
Payment card	VISA JQ%FJJ7JO&FJHQ%7	p.date	12/2006
Card Verif. Value		Incoterms	FH
Payment terms	0001		
Order reason			

All items

Item	Material	Order Quantity	Un	Description	S	Customer Material Numb	ItCa	DGIP	HL Itm
10	HT-2000	1	PC	7" Widescreen Portabl...	✓		TAN		0

Picture 9. Data masking in SAP (Baird 2013).

4.3.6 SAP Identity Lifecycle Management - ILM

SAP Identity Lifecycle Management (ILM) enable organizations to comply with regulations such as GDPR for data retention procedures with information lifecycle management. With ILM it is possible to improve system performance and availability by archiving data into easily accessible storage. ILM may also help organizations to streamline the IT infrastructures by revoking the legacy systems and automating the data retention processes based on the customized rules that organizations can define also minimizing risk of losing the data control at the same time.

With SAP Identity Lifecycle Management it is possible to archive the obsolete data in order to reduce the database size, reduce the administration costs and also enhance the system performance significantly. Also IT management costs will be usually reduced with ILM by the effect of consolidating systems and revoking their legacy systems.

ILM supports the data retention procedures by creating dedicated archives for various data lifetimes based on the actual need in each case separately. Therefore Identity Lifecycle Management is a potential tool in order to conserve the compliance auditing and reporting capabilities in revoked systems, reduce the costs and risks related to legal discoveries by automating data collection for possible legal requirements. (SAP SE 2018)

4.3.7 Summary and the actual plan

As stated above, GDPR is definitely not a one-man show. There are a lot of options to select but there is not a single person to tell what is the absolute correct way to proceed in order to achieve the guaranteed data security and safety related to SAP, authorizations and GDPR. Therefore the plan is to select various ways of working from different perspectives and formulate a suck plan and concept from different pieces and various tools which together help us to achieve what is needed. SAP authorizations will be definitely included.

In practice this all means that there will be a tool box which includes a lot of different tools and processes from different teams in order to cover everything which is required. In addition of that, this all means a lot of paper work and documentation. And even more documentation after documentation. The point is that companies must be able show that they themselves know where they store different kind of sensitive data and for what purposes. Then the current amount of sensitive data must be documented, and validate who have the accesses into that data. That kind of information must be available and appropriately documented. If some kind of leaks are noticed when doing this validation and documentation work, those must be of course corrected immediately.

I will not go into details that what are the very detail level actual actions that company X is performing in order to achieve the new GDPR requirements. However, SAP authorizations are very relevant part of GDPR project, and work is ongoing. All relevant accesses are under review and a lot of various documentation work is done in that area as well.

5 CONCLUSIONS

Why authorizations and authorization concept exist? Sometimes the missing authorizations cause frustration and even anger towards authorization concept and its responsible persons. The users who face missing authorizations when performing their job duties may feel like company – or its authorization concept – do not give them the needed accesses in order help the company to exercise its core business and produce maximum returns. I have personally came across the countless number of situations with users where authorizations are missing, the urgency is in critical level or company will lose significant amount of money. But yet again, I trust that authorization concept is very important keystone for companies' information security and it must be followed.

Some security risks in SAP system landscape are undoubtedly only theoretical threats. It would need a very high level expertise to perform some certain critical tasks in SAP which would cause some serious consequences. But again, SAP authorizations exist in order to rule out the possible theoretical security risks as well. It is not allowed to drive companies' core businesses into a such situation where all users have all possible accesses in SAP environments – in SAP world this is known as authorization profile called SAP_ALL – and rely on their goodwill and trust that every possible action by every single user is always performed bona fide. And even if users do not mean to perform any illegal activities or broke anything in SAP system, the possibility of human errors must be always taken into account as well. I have heard a rumor about a junior SAP consultant who was curious to know whether SAP Basis side transaction code called "SCC5 – Delete client", really does what it says – delete SAP system client – which means that particular SAP system cannot be used anymore by anyone. Well, the consultant tried it and it worked very well. The result was that the system client was deleted causing a huge damage to company's core business and devastating losses in profits. This is only a one practical example but I think it very well demonstrates why SAP authorization concept is justified and why authorizations must be well-defined and implemented. In a good SAP authorization concept this kind of user never has an authorization to such transaction which can cause this kind of consequences.

When I'm writing this particular section, GDPR is already valid. A lot of various preparation work has been done in past days, weeks, months and even years, and even more work is still ahead us. The long-awaited and even feared magical GDPR date May

25th 2018 arrived and now it is already part of history. However, new regulation is now here and we all must be able to comply with it. New legal requirements are here but the business must still run on daily basis as usual, despite GDPR. There are just more details and procedures which must be taken into account in every day job. Because after all, it is still all about business and IT must still fulfill its requirements.

I think that in general both SAP authorization concept renewal and European Union's new General Data Protection Regulation projects were planned and implemented well. A lot of work has been done, but even more work will follow in future as the fact is that both of these subjects are under continuous change. Certain projects may have their end dates and project teams are dissolved, but the work itself continues.

The most successful parts in these projects are the amount of new information that I was able to acquire as a mandatory part of these new requirements. There is a lot of new very clear and detail level documentation now available which did not exist before these projects. For example new GDPR requirements enforced to jump into such areas where I had not been working earlier, and that kind of way of working has teached me a lot of new things.

However, in my opinion GDPR is also some kind of huge set of very high level requirements, and when drilling down into the details in grass roots level of SAP authorizations, it not so clear anymore that which kind of changes are actually needed. The fact is that SAP AG headquarters has never provided any kind of clear instructions about what authorizations related details are in the scope, where we need to pay attention and which parts in this huge context are actually not so relevant. I personally see it so that the reason for the missing detail level instructions is this simple fact: no one knows what is actually needed in order to properly meet the GDPR requirements in SAP authorizations. Any kind of precedents do not exist yet as GDPR came into force only a very short time ago. That is the reason why there is not a single person even in legislators' side who is able to confidently state that by doing these or those changes in your processes, you are in safe. No, even legislators do not know it yet that what kind of cases there will be in future.

I assume that GDPR related audits will start in near future, and the auditors will hit first for example to hospitals or other similar organizations which contain a lot of very sensitive personal data. After that they will extend the audits into companies in all other areas as well. Only then, in form of results of those first waves of audits, we are able to see what is actually required from companies in order to be on the safe side. I assume that some warnings will be given as well in such cases where some companies have not been careful enough in their GDPR related matters. I also assume that the actual fines, 4 percent of companies' annual revenue or 20 million euros, will happen only in such cases were companies have not done any kind of corrective actions despite the several warnings.

So because of the lack of actual detail level instructions, we had to make our own decisions on those. It means that a lot of documentation related work has been done so far so that we are to see what kind of access rights we have in our systems. And I believe that we have chosen the correct way to proceed.

There are of course also areas to improve as well. One of those is the roles and responsibilities which may have been planned and implemented better in GDPR project. Now in some cases there have been some misunderstandings about the responsibilities in certain tasks which have caused unnecessary delay. Therefore I recommend all other organizations who are dealing with GDPR related issues to make very detail level plans about everything which is in the scope, and also prepare the roles and responsibilities in as accurate level as possible. In that way everyone knows what is expected from them. And finally, careful documentation about all accesses to any kind of sensitive data is the key to success. In that way companies are aware themselves what are the most critical weak points which must be fixed without any delay.

REFERENCES

Avaali Solutions Pvt Ltd. 2015. Cited: 29.4.2018. http://www.avaali.com/ecm-soluitons-for-sap-archiving-software/

Baird, J. 2013. Can you Continue to Ignore Data Encryption in SAP? Dolphin. Cited: 29.4.2018. https://www.isaca.org/chapters3/Atlanta/AboutOurChapter/Documents/SAP%20Data%20Encyption.pdf

Banzer, A. 2017. Comparison of SAP Role Design Concepts. Cited: 29.4.2018. https://xiting.us/blog/comparison-sap-role-design-concepts/

Butler, C., Cameron, R., Ferratt, M., Fuller, E., Hurley, C., Kirouac, B., Miles, G. & Rogers, R. 2007. IT Security Interviews Exposed. Indianapolis: Wiley Publishing, Inc.

Chia, T. 2012. IT Security community blog - Confidentiality, Integrity, Availability: The three components of the CIA Triad. Cited: 12.11.2017. http://security.blogoverflow.com/2012/08/confidentiality-integrity-availability-the-three-components-of-the-cia-triad/

Cohen, B., Gulyaeva, N. & Sedykh, M. 2017. Hogan Lovells: Chronicle of Data Protection, Privacy & Information Security News & Trends - Russian Data Protection Authority Publishes Privacy Policy Guidance. Cited: 26.11.2017. https://www.hldataprotection.com/2017/08/articles/international-eu-privacy/russian-data-protection-authority-publishes-privacy-policy-guidance/

Dahse, P. 2017. Data Security and Data Privacy Natuvion Webcast (8) – SAP RAL - Read Access Logging Natuvion GmbH. Cited: 29.4.2017. https://www.slideshare.net/pdahse/webcast-security-no-8-read-access-logging-ral

EU GDPR Portal 2017. Cited: 26.11.2017. https://www.eugdpr.org/

European Commission 2018. 2018 reform of EU data protection rules. Cited: 27.5.2018. https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en

Hanis, G. 2014. Security IDs. Cited: 12.11.2017. https://www.slideshare.net/GregTampa/security-ids

IBM Business Consulting Services 2003. SAP Authorization System. Design and Implementation of Authorization Concepts for SAP R/3 and SAP Enterprise Portal. Bonn: SAP Press.

Information security handbook 2009. Cited: 12.11.2017. http://ishandbook.bsewall.com/risk/glossary.html#accountability

Intersoft consulting services AG. General Data Protection Regulation (GDPR). Cited: 27.5.2018. https://gdpr-info.eu/art-17-gdpr/

Jordan E. & Silcock L. 2006. Strateginen IT-riskien hallinta. Helsinki: Edita Publishing Oy.

Kamkarhaghighi M., Moghaddasi H. and Sajjadi S. 2016. The Open Medical Informatics Journal - Reasons in Support of Data Security and Data Security Management as Two Independent Concepts: A New Model. Cited: 12.11.2017. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5090776/

Krause, M. & Tipton, H. F. 2007. Information Security Management Handbook Sixth Edition. Boca Raton: Auerbach Publications.

Krutz, R. L., & Vines, R. D. 2003. Tietoturvasertifikaatti – CISSP. Helsinki: IT Press.

Kuijper, N. J. W. 2016. Materializing dataprivacy in SAP - How? Cited: 29.4.2018. https://www.slideshare.net/nicokuijper11/materializing-dataprivacy-in-sap-how-61895340

Linstead, S., Fulop, L. & Lilley S. 2009. Management & Organization. A critical text. 2nd Edition. Hampshire: Palgrave Macmillan.

Medvedev, S. 2017. Data protection in Russian Federation: overview. Cited: 12.11.2017. https://uk.practicallaw.thomsonreuters.com/2-502-2227?transitionType=Default&contextData=(sc.Default)&firstPage=true&bhcp=1

SAP AG 1999. Authorizations Made Easy – Generating Authorization Profiles. Palo Alto: SAP Labs, Inc.

SAP AG 2006. ADM940 – SAP Authorization Concept.

SAP AG 2013. Application Link Enabling (ALE). Cited: 12.11.2017. https://help.sap.com/erp_hcm_ias_2012_03/helpdata/en/4a/a93aac05e24458e10000000a42189b/frameset.htm

SAP AG 2013. Read Access Logging (RAL) for SAP NetWeaver Overview. Cited: 28.4.2018. https://www.slideshare.net/SAPTechnology/read-accessloggingoverview

SAP AG 2013. Segregation of Duties. Cited: 27.5.2018. https://help.sap.com/doc/saphelp_grcac10/10.0/en-US/17/76b1e9bb29435582eb8ef3366112c6/frameset.htm

SAP SE 2015. SAP Authorization Concept. Cited: 29.4.2018. https://help.sap.com/doc/saphelp_dm40/4.0/en-US/52/671285439b11d1896f0000e8322d00/frameset.htm

SAP SE 2017. Data Protection and Privacy at SAP - Getting Ready for May 25, 2018, Part 2: Product and Services Compliance. Cited: 29.4.2018. https://www.sap.com/documents/2017/08/9a35c37d-cc7c-0010-82c7-eda71af511fa.html

SAP SE 2018. SAP: A 46-year history of success - Building on a track record of innovation. Cited: 27.5.2018. https://www.sap.com/corporate/en/company/history.html

SAP SE 2018. Comply with regulations for data retention with information lifecycle management. Cited: 27.5.2018. https://www.sap.com/products/information-lifecycle-management.html

SAP SE 2018. Cybersecurity and Governance, Risk, and Compliance (GRC). Cited: 27.5.2018. https://www.sap.com/products/financial-management/grc.html

SAP SE 2018. GDPR Compliance and SAP ERP. Cited: 7.4.1018. https://www.sap.com/documents/2017/11/e48dd993-df7c-0010-82c7-eda71af511fa.html

SAP SE 2018. SAP Data Anonymization – FAQ. Cited: 29.4.2018. https://www.sap.com/documents/2017/11/0406aa8b-de7c-0010-82c7-eda71af511fa.html

SAP SE 2018. User and Role Administration of Application Server ABAP - ABAP Authorization Concept. Cited: 27.5.2018. https://help.sap.com/viewer/c6e6d078ab99452db94ed7b3b7bbcccf/7.5.9/en-US/4f4decf806b02892e10000000a42189b.html

SAP SE 2018. What is ERP? Cited: 27.5.2018. https://www.sap.com/products/what-is-erp.html

Shaftan, V. 2015. Data Protection Report - Russian data protection authority explains data localization law; says cross-border transfer still permitted. Cited: 12.11.2017.

https://www.dataprotectionreport.com/2015/08/russian-data-protection-authority-explains-data-localization-law-says-cross-border-transfer-still-permitted/

Williams, G. 2012. GeraintW Online Blog – CIA & InfoSec. Cited: 12.11.2017. http://geraintw.blogspot.fi/2012/09/cia-infosec.html