



Supporting GDPR implementation through the application of BPMN Workflows

Diplomarbeit

zur Erlangung des akademischen Grades

Diplom-Ingenieur/in

eingereicht von

Richard Lechner
1610619519

im Rahmen des
Studiengangs Information Security an der Fachhochschule St. Pölten

Betreuung
Betreuer/Betreuerin: FH-Prof. Mag. Dr. Simon Tjoa

Wien, 09.08.2018

(Unterschrift Autor/Autorin)

(Unterschrift Betreuer/Betreuerin)

Ehrenwörtliche Erklärung

Ich versichere, dass

- ich diese Diplomarbeit selbständig verfasst, andere als die angegebenen Quellen und Hilfsmittel nicht benutzt und mich sonst keiner unerlaubten Hilfe bedient habe.

- ich dieses Diplomarbeitsthema bisher weder im Inland noch im Ausland einem Begutachter/einer Begutachterin zur Beurteilung oder in irgendeiner Form als Prüfungsarbeit vorgelegt habe.

- diese Arbeit mit der vom Begutachter/von der Begutachterin beurteilten Arbeit übereinstimmt.

Der Studierende/Absolvent räumt der FH St. Pölten das Recht ein, die Diplomarbeit für Lehre- und Forschungstätigkeiten zu verwenden und damit zu werben (z.B. bei der Projektevernissage, in Publikationen, auf der Homepage), wobei der Absolvent als Urheber zu nennen ist. Jegliche kommerzielle Verwertung/Nutzung bedarf einer weiteren Vereinbarung zwischen dem Studierenden/Absolventen und der FH St. Pölten.

Wien, 09.08.2018

(Unterschrift Autor/Autorin)

Zusammenfassung

Am 24 Mai 2018 trat die Datenschutzgrundverordnung auch DSGVO oder GDPR genannt in Kraft. Die Umsetzung der Bestimmungen stellt Unternehmen vor große Herausforderungen. Studien belegen das mangelnde frei-verfügbare Ressourcen einen signifikanten Anteil daran haben, dass die Einhaltung der Vorgaben nicht vollumfänglich erreichbar ist. Damit verbunden ist das potenzielle Risiko von Klagen und in deren Folge von hohen Strafzahlungen betroffen zu sein. Zur selben Zeit können Kunden keine Betroffenenrechte geltend machen, da das Unternehmen keine Umsetzungsgrundlage hat. Um Betriebe bei der Realisierung der Vorgaben zu unterstützen, ist es Ziel dieser Arbeit generische Arbeitsabläufe zu entwickeln, welche die Verwirklichung der gesetzlichen Vorgaben erleichtern. Außerdem wird die Thematik rund um das Modellieren von Geschäftsprozessen behandelt, sowie eine Marktanalyse der gängigen kostenfrei verfügbaren Software zur Prozessmodellierung durchgeführt. Als weitere unterstützende Ressource werden Beispiel Antragsformulare vorgestellt.

In den einleitenden Kapiteln der Thesis werden die Motivationsfaktoren betrachtet. Die Umsetzung der neuen Bestimmungen ist eine große Herausforderung aber auch eine große Chance für Unternehmen. Durch den hohen Strafrahmen und dem damit verbundenen Risiko hat die Umsetzung der Regulation einen hohen Stellenwert. Oftmals fehlt es Unternehmen aber an den nötigen Ressourcen, um eine schnelle Umsetzung zu gewährleisten. Diese Arbeit hat es zum Ziel, Unternehmen durch die Bereitstellung von Umsetzungshilfen in Form von Prozessen und Templates zu unterstützen.

Damit das nötige Verständnis zur Interpretation der vorgestellten Lösungen vorhanden ist, wird neben der Vorstellung von BPMN auch eine Marktanalyse zu den frei verfügbaren Prozessmodellierungsprogrammen durchgeführt. Das Ergebnis dieser Marktanalyse erlaubt es dem Anwender auf einen Blick zu entscheiden, welche Software die für seinen Anwendungsfall richtige Wahl darstellt.

Die auf die Marktanalyse folgenden Prozessmodelle behandeln Betroffenenrechte sowie Benachrichtigungsverpflichtungen. Insgesamt werden mehr als 10 Prozesse vorgestellt. Bei jedem Prozess wird zu Beginn auf die Vorgaben der DSGVO verwiesen, anschließend folgt eine Diskussion zu deren Bedeutung und Reichweite. Daraufhin wird der Prozessablauf, welcher unter den Vorgaben der Regulation entwickelt wurde, textuell Schritt für Schritt beschrieben, bevor er als BPMN 2.0 Modell konkretisiert dargestellt wird. Diese Prozesse können von Unternehmen beim Umsetzen der DSGVO eingesetzt werden und verringern dadurch die benötigten Ressourcen und den benötigten Aufwand.

Unterstützend zu den entwickelten Prozessmodellen werden Beispiel-Antragsformulare vorgestellt. Die Formulare dienen dem Zwecke der Kommunikation zwischen Betroffenen und dem Verantwortlichen zu vereinheitlichen und dabei die Vorgaben der DSGVO zu berücksichtigen.

Abschließend werden die Forschungsfragen beantwortet und es wird ein Fazit über die vorgestellte Arbeit gezogen sowie ein Ausblick über zukünftige Forschungsthemen und die zu erwartenden Auswirkungen der DSGVO verfasst.

Abstract

This paper discusses how generic workflows can help data controllers implement GDPR requirements. Many companies struggle to achieve compliance due to a lack of freely available resources. To support struggling entities this thesis provides both generic workflows modelled in BPMN, and request templates. The introduced material is designed to be compliant with regulatory requirements and yet generic enough to allow for customization. The work introduces the reader to the motivational factors, as well as, complimentary information regarding process modelling tools and definitions. Continuing with the discussion of data subject rights and their illustration in form of workflow models and contact templates - to be used in conjunction with the introduced workflows. Overall more than 10 such processes are presented. In the concluding chapter, a conclusion of the conducted work is drawn, and the reader is presented with an outlook of the future.

Table of Contents

1	INTRODUCTION.....	8
1.1	MOTIVATION.....	8
1.2	PROBLEM STATEMENT	10
1.3	RESEARCH QUESTION	10
1.4	THESIS OUTLINE	11
2	ESSENTIAL INFORMATION.....	12
2.1	PROCESS MODELLING NOTATIONS.....	12
2.1.1	<i>Unified Modelling Language.....</i>	12
2.1.2	<i>Flowcharts.....</i>	12
2.1.3	<i>Event-Driven Process Chain.....</i>	13
2.1.4	<i>Business Process Modelling Notation</i>	13
2.2	DEFINITIONS.....	13
2.2.1	GDPR DEFINITIONS	14
2.2.2	BPMN DEFINITIONS.....	15
2.3	LIMITATIONS	17
2.4	CONTRIBUTING LITERATURE	17
2.4.1	<i>Praxishandbuch BPMN 2.0 von Camunda.....</i>	18
2.4.2	<i>General Data Protection Regulation (EU 2016/679).....</i>	18
2.4.3	<i>The EU General Data Protection Regulation (GDPR) – A Practical Guide</i>	18
2.5	SUMMARY	18
3	BPMN 2.0 TOOL – MARKET ANALYSIS	20
3.1	RESEARCH METHODOLOGY	20
3.2	SELECTION PROCESS.....	20
3.3	RATING CRITERIA.....	20
3.4	ANALYSIS.....	21
3.4.1	<i>Camunda Modeler.....</i>	21
3.4.2	<i>Aris Express.....</i>	22
3.4.3	<i>Bonita BPM.....</i>	23
3.4.4	<i>BPMN 2 Modeler Eclipse.....</i>	24
3.4.5	<i>jBPM.....</i>	25
3.4.6	<i>Modelio.....</i>	26
3.5	COMPARISON OF RESULTS.....	27
3.6	INTERPRETATION OF RESULTS	28
3.7	SUMMARY	28
4	SUPPORTING GDPR IMPLEMENTATION THROUGH BPMN WORKFLOWS	30
4.1	WORKFLOWS – DATA SUBJECT RIGHTS	30
4.1.1	<i>Right of access by the data subject – Article 15 GDPR – Workflow</i>	31
4.1.2	<i>Right to rectification – Article 16 GDPR – Workflow.....</i>	33
4.1.3	<i>Right to erasure – Article 17 GDPR - Workflow</i>	36
4.1.4	<i>Right to restriction of processing – Article 18 GDPR – Workflow</i>	41
4.1.5	<i>Right to data portability – Article 20 GDPR - Workflow.....</i>	44
4.1.7	<i>Right to object – Article 21 GDPR - Workflow</i>	47
4.1.8	<i>Automated individual decision-making – Article 22 GDPR - Workflow.....</i>	50
4.2	WORKFLOWS – OTHER	53
4.2.1	<i>Notification obligation – Article 19 GDPR – Workflow</i>	54
4.2.2	<i>Data breach notification (supervising authority)- Article 33 GDPR – Workflow.....</i>	55

4.2.3	<i>Data breach notification (data subject) – Article 34 GDPR – Workflow</i>	59
4.2.4	<i>Identity verification – Recital 64 GDPR – Workflow</i>	61
4.2.5	<i>Investigative Requests – Article 58 GDPR - Workflow</i>	63
4.3	CHAPTER SUMMARY.....	65
5	EXAMPLE FORMS	67
5.1	RIGHT OF ACCESS BY THE DATA SUBJECT – ARTICLE 15 GDPR – FORM.....	67
5.2	RIGHT TO RECTIFICATION – ARTICLE 16 GDPR – FORM	68
5.3	RIGHT TO ERASURE – ARTICLE 17 GDPR - FORM	69
	SOLUTION TO THE RESEARCH PROBLEM	71
6.1	SOLUTION TO RESEARCH PROBLEM 1	71
6.2	SOLUTION TO RESEARCH PROBLEM 2	71
6.3	LIMITATIONS (SOLUTION)	72
6.4	CONCLUSION	72
6.5	OUTLOOK	74
	TABLE OF FIGURES	75
	TABLE OF TABLES	76
	BIBLIOGRAPHY	77
	APPENDIX	79

Part I

Introduction & Essential Information

1 Introduction

The purpose of this chapter is to introduce you to the research paper, its objectives, and the research problem. It consists of four sections. In section one (Motivation), the factors which led to the very creation of this paper are presented. In section two, the problem statement is given, and in section three the research questions are defined. Finally, the last section presents an outline of the thesis.

1.1 Motivation

On 24 May 2016, the EU¹ General Data Protection Regulation (GDPR) came into force, two years later on 25 May 2018 it went into effect but only a fraction of organizations are fully compliant [1]. Before the consequences and thus the motivation of this paper are discussed, a short history of EU regulated data protection laws is given in order to understand the challenges that organizations face at the time. In 1995 [2] the European Union introduced the first Data Protection Directive (95/46/EC). This directive had to be implemented by the member states in national law which left room for interpretation. The key elements of this directive were the free movement of data and the individual protection in the light of data processing. The European Commission proposed an overhaul of the Directive 95/46/EC in 2012 with the goal to achieve a stronger European economy, especially in regard to IT related businesses. Furthermore, the individuals' online privacy rights should be enhanced by the proposed reform[3]. During the following years the idea of an EU-wide regulation became a reality. On 15 December 2015, the European Parliament, the European Council, and the European Commission reached an understanding [2] on the GDPR leading to its introduction on 27 April 2016. At this time, data processing regulations and applicable laws differed in many ways between member states of the EU. The new Regulation was directly applicable and there was no need to first implement it in national law, however if the law was implemented it allowed for minor changes to be made in order to fit the local needs. Institutions now had a two-year grace period to adapt to the newly introduced requirements, this came with great challenges for companies who only followed locally applicable laws up to this point.

Using Germany as an example to showcase the struggles organizations face, a representative survey of over 500 companies unveils major shortcomings. More than two thirds [4] of all survey participants will not be able to meet all GDPR requirements. At the same time roughly 40% depend on personal information, and in some cases, their business model depends on it. Looking at a broader spectrum including the USA², EU, and UK³, a huge gap in the understanding of the GDPR can be found. While two thirds of the European IT specialists are informed about the impact on their business and are in favor of the new terms, only 19% [5] of US IT⁴ Professionals are knowledgeable of the impact on their business and only about one third are welcoming the new regulations. Companies located in the UK are leading in the full fulfillment of the new Data Protection requirements with about half of them meeting the new regulations when they came into force on May 25th 2018. Due to the law being applicable to all Institutions, processing information of EU residents the *BREXIT* won't affect the liability of UK based corporations. Shifting the focus onto why companies struggle to meet the regulation, a survey conducted by Spiceworks [5] identifies seven shortcomings. Across the board more time and resources are required to implement the necessary changes than are available to the IT department, many times the budget does not allow for a quick implementation of the requirements. Another two top reasons for falling short on the implementation are simply the lack of understanding of the requirements in the first place and where to find support. In Germany, [6] 40% claim that the lack of supporting resources is one of the biggest factors on why they struggle to comply with the GDPR. The cost of trying to

¹ EU – European Union

² USA – United States of America

³ UK – United Kingdom

⁴ IT – Information Technology

achieve compliance just for the UK FTSE⁵ and the US Fortune 500 companies amounts to \$9 billion USD [7], this number reflects the spending for the implementation as well as expenses for legal counsel. Especially for small to medium sized businesses, freeing the necessary resources to comply [8] with the new specifications can be a struggle. But not only businesses are affected by the new regulations also clubs, unions or associations have to comply with the new law.

Data processing as a whole needs to be approached under new circumstances. Companies need to ask themselves if the gathering and processing of personal information is business critical and for how long the information needs to be stored. In fact, the GDPR calls for a valid consent by the data subject or legal permission for any data processing to be conducted [9]. As an example, it is no longer allowed to package the consent of the terms and conditions of a webpage with a newsletter subscription. Special restrictions apply to the processing of so called sensitive categories regarding personal information. Additionally, specific special rules apply when processing the information of minors. This circumstance forces even big corporations to raise the minimum required age to use their services to above 16 years of age [10]. Right now, if we take a look at the approach *WhatsApp* has taken, it is unclear if and how this age limit will be enforced as it is only implemented by a change in the usage terms of the service.

With this new regulation a set of opportunities arise which should be taken. Since many companies face massive changes to their data processing processes, a more flexible approach to data protection can be implemented [11]. Also, new and innovative business approaches can be developed to cope with more restricted access to personal information[12]. The new rules allow for a chance to regain the trust of customers as headlines in the daily news about the misuse of personal information or the manipulation of masses took a toll on faith [13]. As data is the company's most important asset, it can yield a high return in the future to implement processes now which ensure a compliant handling of personal data. In addition it will be necessary to introduce new documentation such as processing purposes, data retention or with whom which data is shared [14].

The risk involved with not meeting the requirements is great. A breach of the law is punishable with fines of up to 20 million EUR or up to 4% of [15] the worldwide turnover per year; whichever is greater. The enforcement of this law doesn't stop at the EU borders [16]. If data of EU individuals is processed the conducting entity must appoint an EU-stationed agent. However, at this time no rulings have been made, how strict and efficient the enforcement of the law can be conducted remains open. The fines are administered by the supervisory authorities of each member state[17]. The severity and thus the amount of the fine is determined by defined criteria some of which are:

- Intention
- Nature of infringement
- Preventative Measures
- History

While this list is not exhaustive, it is intended to show how mitigating nonconformities and actively improving processes can allow the creation of a so-called "defensible position" in case of a lawsuit [18].

To support these struggling entities, this paper strives to provide useful resources to the IT professionals, process architects and process engineers and whom it may concern. The intended outcome is to provide a set of usable information regarding workflows and their improvement to achieve compliance with GDPR requirements. In addition to these generic workflows, example forms shall be provided to further help taking the first steps towards full compliance.

⁵ FTSE – Financial Times Stock Exchange

1.2 Problem Statement

According to a *Bitcom* survey almost half of all corporations struggle to implement the GDPR requirements due to the lack of supporting material [4]. The reasons as to why this is can be discussed, however there are factors such as a lack of freely accessible material to help integrate the given requirements in the company's environment.

In order to comply with the law clear policies on how personal information is handled need to be defined. In addition, it is necessary to have structured processes in place to conform with data subject rights. These processes consist of clear steps to be taken and are supported by documentation. The supporting documentation consists of policies, forms and a record of the current cycle⁶.

This thesis strives to provide generic workflows in accordance with GDPR requirements which are adaptable to any business' needs and to give a review of the tools needed to conduct such an adjustment. Furthermore, a set of sample forms will be attached to processes which can also be adapted to individual requirements. In addition to a visual workflow representation, a source code⁷ will be attached.

1.3 Research Question

In order to fulfil the EU GDPR, corporations need to make adjustments in their processing of personal information. With the introduction of data subject rights new processes need to be implemented. These processes need to fulfil the given specifications and at the same time should integrate with already existing infrastructure. BPMN 2.0⁸ is a standardized process modelling notation which is widely used.

There is a wide variety of tools available to create diagrams with BPMN notation, however many of them differ in functionality. In order to make an informed decision on which tool to choose to create own processes in with BPMN 2.0 and to adjust the generic processes provided a market analysis is conducted. The first research problem is:

Which cost-free specialized tools are available on the market to create BPMN 2.0 diagrams and how do they differ in their functionality?

The main focus of this thesis is, however, the creation of generic workflows which support the implementation of GDPR requirements. Notably the rights of the data subject. Therefore, the second research problem is:

How can generic workflows support the implementation process of GDPR requirements?

⁶ Each request and the effort to fulfill the request have to be documented

⁷ XML code representation of workflow

⁸ BPMN – Business Process Modelling Notation

1.4 Thesis Outline

In Chapter 1 of this thesis, a general introduction is given. This introduction consists of section 1.1 in which the motivation for this paper is discussed. In section 1.2 the problem statement is given as to why it is important to conduct this research. Section 1.3 covers the two research problems and gives a short overview of what is to be accomplished. In this section – section 1.4 the thesis is outlined, and a short description of each part and its sections is given. Chapter 2 provides essential information needed to understand the further paper. First, process modelling notations are examined in section 2.1. Thereafter, in section 2.2 definitions are set. The known limitations of this research paper are provided in section 2.3. The most significant contributing literature is presented in chapter 2.4. A short summary of chapter 1+2 can be found in section 2.5 concluding Part 1 of this paper

A market analysis regarding BPMN tools is conducted in chapter 3, this chapter can be skipped if a comparison between available tool options is not of interest. After a short Introduction section 3.1 displays the chosen methodology to conduct the analysis. A selection process is introduced in section 3.2 and a rating criterion is outlined in section 3.3. The main section of this chapter is section 3.4 where the analysis of the different tools is conducted. In section 3.5 the results are integrated and presented while in section 3.6 the results are interpreted. Section 3.7 concludes both chapter 3 and Part 2 of this thesis with a short summary.

Part 3 of this paper is not only the middle part but also the focus point. In section 4.1 applicable⁹ GDPR requirements are presented. The scope of this section is Data Subject Rights. Further workflows regarding notifications, verification of identity or communication with the supervising authority can be found in section 4.2. Within section 4.3 a summary of the chapter can be found.

Part 4 of this introduces sample forms to help the data controller with the implementation of GDPR compliant contact points.

In part 5 of the thesis contains the solution to the research problem and concludes the thesis. Section 6.1 and 6.2 contains the answers to the research problem. Section 6.3 is about limitations regarding the answers to the research problem. Section 6.4 Conclusion and section 6.5 Future Work and Outlook.

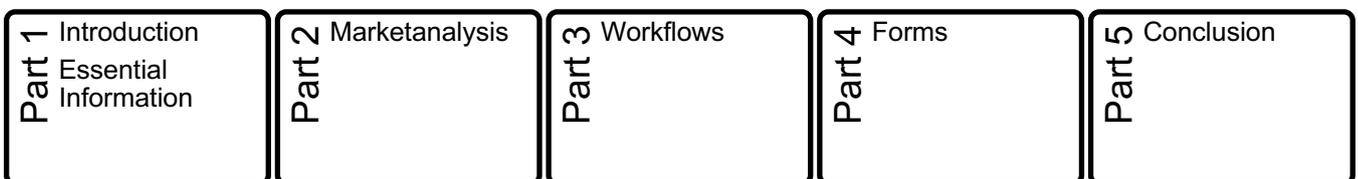


Figure 1. Thesis Outline

⁹ Requirements for which a generic process will be presented in this thesis

2 Essential Information

This chapter provides information regarding different process modelling notations and why BPMN was chosen to model the workflows. It also defines what certain GDPR roles are and gives a short introduction on BPMN symbols, semantics, and syntax. Section 2.4 within this chapter introduces supporting literature.

2.1 Process Modelling Notations

BPMN 2.0 is a flexible standardized notation which strives to enable corporations to not only better understand their processes, but also to achieve such detailed modelled processes that they can be imported into an BPE¹⁰ and thus be executed to automate the process which has been designed in accordance with the before determined requirements [19]. Before BPMN and its advantages are examined, a short introduction to alternatively used techniques and notations is given.

2.1.1 Unified Modelling Language

One of the most commonly used diagrams in software engineering are described by the UML¹¹. There are currently 13 different diagram types in the UML 2.0 standard [20], [21]. These types are grouped into two categories:

Table 1 UML Diagram types

Structural UML Diagrams	Behavioral UML Diagrams
Class diagram	Activity diagram
Object diagram	Use case diagram
Package diagram	Timing diagram
Component diagram	Sequence diagram
Deployment diagram	State diagram
Composite structure diagram	Communication diagram
	Interaction overview diagram

While discussing each individual type is out of scope for this thesis the diagrams in the right section of table 1 are of interest. This type is used to model activities such as which have to be conducted. This procedure is similar to process modelling. While UML was created with software modelling in mind, the use of the diagrams has spread beyond that use case. Anyhow, a simple conversion between the UML notation and BPMN is not possible. Many symbols are exclusive to UML, especially regarding software processes [22].

2.1.2 Flowcharts

The usage of flowcharts as way to document a process dates back to the early 1920s where they have been introduced by Lillian and Frank Gilbreth [23]. A flowchart represents a successive order of activities or events. Contrary to a BPMN process, a flowchart only supports a sequential flow and no parallel activities. Another drawback is the lack of standardization. Without clearly defined rules and symbols, a flowchart only allows a [24] high-level perspective on a process. However, this can be useful to start a discussion among affected parties and can serve as a rough draft for the later development of a BPMN modelled process. There are four different kinds of flowcharts, namely the document flowchart, the data flowchart, the system flowchart, and the program flowchart.

¹⁰ BPE – Business Process Engine

¹¹ UML – Unified Modelling Language

2.1.3 Event-Driven Process Chain

Developed in 1992, the EPC¹² became widely adopted as the toolkit ARIS¹³ was released. The tight integration of ARIS with ERP¹⁴ software developed by the German enterprise software developer SAP¹⁵ further helped the acceptance and application of the EPC notation [22], [25]. However, in recent years, BPMN is becoming the notation of choice and many businesses switched or consider switching to BPMN [26]. Even the ARIS tool kit which once was the go-to design tool for designing processes in EPC has now the BPMN notation as an alternative implemented. Fortunately, it is possible to convert processes from EPC to BPMN with minor changes. There are however multiple things to consider if such a conversion is planned. Processes designed in EPC do not differentiate between when an event occurs such as *start*, *intermediate*, *end* and is also missing types like *message* or *time* [22]. Especially in the context of process automation, BPMN is in a clear advantage over EPC, as BPMN was designed with automation in mind.

2.1.4 Business Process Modelling Notation

In 1989, the Object Management Group was formed [27], this institution maintains since a merger with the Business Process Management Initiative; the BPMN standard. BPMN is graphical notation that is widely used to design processes. The notation may be used to create new processes, document existing processes or improve processes. A great advantage of BPMN in version 2.0 is the capability to execute the process model in a business process engine. This in conjunction with a standardized approach allows for flexibility when choosing a software to design processes and creates the opportunity to seize synergies with external partners who also use BPMN. The standard provides a set of symbols and a ruleset on how they can interact with each other. Additionally, a defined meaning of those symbols is provided. Together both syntax and semantics allow for a predictable interpretation of the process and thus the automation of it. The Symbol library of BPMN allows for artifacts, these artifacts allow the process analyst to create symbols individually in order to better adjust the design to business needs. There are 6 groups of symbols – Gateways, Activities, Participants, Artefacts, Data, and Events. These groups are connected using so-called sequence flows.

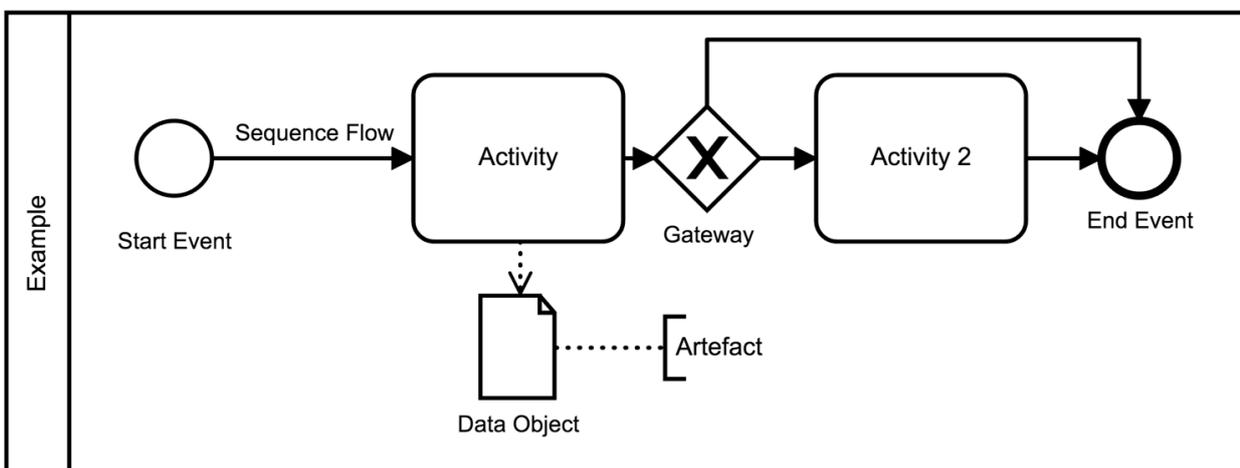


Figure 2 BPMN Symbols Example

2.2 Definitions

¹² EPC – Event Driven Process Chain

¹³ ARIS – Architecture of Integrated Information Systems

¹⁴ ERP – Enterprise Resource Planning

¹⁵ SAP – Systems, Applications and Products in Data Processing

Due to the fact that many roles, responsibilities, and concepts will be used continuously throughout this thesis, a set of definitions is introduced to guarantee a common understanding of the introduced ideas.

2.2.1 GDPR Definitions

To understand the given instructions as intended it is critical to be familiar with the following key terms and their definition. These definitions have their origin in Article 4 of the GDPR.

Considering the GDPR only applies to personal data one might agree that defining what “personal data” truly means is of critical importance, personal data is defined as follows:

“personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person” [28, p. 33]

The term data processing can be used to describe any kind of activities relating to data, such as recording data, altering data, storing data etc. concerning the GDPR processing as defined by the regulation as:

“processing’ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction” [28, p. 33]

The obligations one faces with regard to the GDPR are primarily put on the controller and the processor [29]. Both share the primary responsibility to comply with the regulation, the role of a controller is defined as:

“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; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law” [28, p. 33]

A controller can contract an external partner to process data on his behalf, however if the controller is processing such information the same strict rules apply and the processor has the obligation to comply with the law. A processor is defined as:

“processor’ means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller” [28, p. 33]

A third option is to contract a third party as an entity who processes data. A third party is defined as:

“third party’ means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorized to process personal data” [28, p. 33]

Any data subject needs to consent before his data can legally processed if not necessary to comply with other applicable laws. Once the consent is granted data can be processed by both the controller or any

applicable processor. In order for a given consent to be valid it needs to meet the following criteria of how a consent is defined:

“consent” of the data subject means any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her” [28, p. 34]

If an unauthorized access to stored data occurs the data subject has to be informed about the so called ‘data breach’. A data breach is defined as:

“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” [28, p. 33]

The storage of personal data regardless of used technology is defined as a “filing system” if it meets the following criteria:

The storage of personal data regardless of used technology is defined as a “filing system” if it meets the following criteria:

If “sensitive information” is processed special restriction apply. Types of sensitive information are defined as personal data containing political opinions, racial or ethnic origin, trade union membership, genetic data, religious beliefs, philosophical beliefs, sexual orientation, health data or genetic data [28], [30].

Mentioned definitions are key phrases used within this thesis but do not reflect a full collection of definitions presented by the GDPR. However, it can be assumed that if a definition by the GDPR for a term is in place, that this definition applies to the mention term here within.

2.2.2 BPMN Definitions

The Business Process Modelling Notation describes a visual representation of a sequence of activities. This notation consists of clearly defined types of symbols. Activities can be grouped into 4 categories (see Figure 3 BPMN Activity Types).

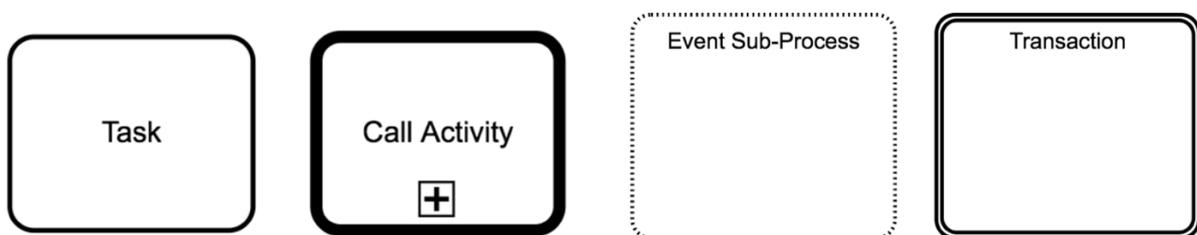


Figure 3 BPMN Activity Types

- The Task activity is an atomic activity of a workflow [31]. It describes work which has to be conducted.
- The Call Activity will call a subprocess which is a globally defined task. The plus symbol marks a collapsed subprocess.
- The Event Sub-Process is a process which can only be triggered by an event, it “may be interrupting or non-interrupting” [32].
- A transaction is a subprocess which succeeds only if all parts of work are completed successfully

All activities can be assigned to types of activities such as sending, receiving, service etc. in addition to an assigned type for which activities may be marked. Marking activities is used to describe the execution behavior.

Gateways are used to control the process flow. There are 5 types (see Figure 4 BPMN Gateways).

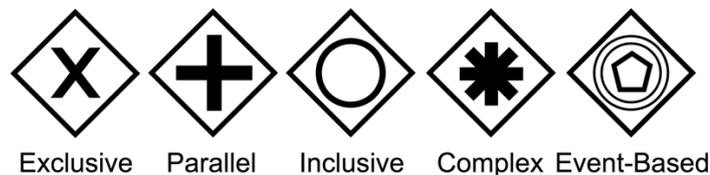


Figure 4 BPMN Gateways

If the gateway is used to split the flow the gateway behaves as follows:

- An exclusive gateway directs the flow to only one applicable exit.
- A parallel gateway splits the flow and multiple exits are activated.
- An inclusive gateway is condition-based and can activate one or more flows.
- A complex gateway behaves as defined by the user.
- An event-based gateway directs the flow to the connected event which becomes true first.

If the gateway is used to consolidate the flow the gateway behaves as follows:

- An exclusive gateway waits for the first input flow before it passes on the flow.
- A parallel gateway waits for all input flows before it puts the flow through.
- An inclusive gateway is condition-based and can synchronize one or more inputs before it activates the flow.
- A complex gateway behaves as defined by the user.
- An event-based gateway directs the flow to the connected event which becomes true first.

Pools and lanes are used represent participants and responsibilities. A pool or a lane can be a role, an organization, or a system. Arrows with a dashed line represent the information flow between pools. BPMN also supports data objects. Data objects are representative of information items such as E-Mails or documents flowing through the process. A sequence flow is marked by an arrow with an uninterrupted line and it represents the flow of the process. Sequence flows can switch between lanes but never cross the pool border.

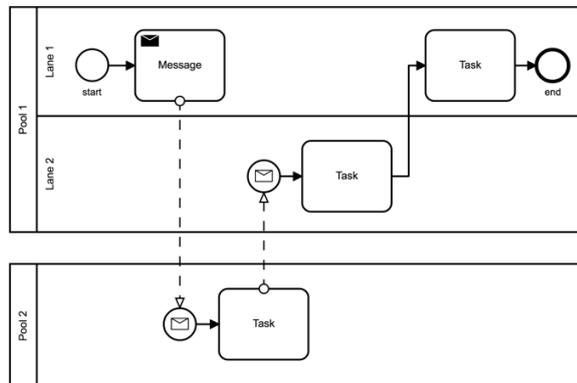


Figure 5 Pools and Lanes Example

This concludes the short introduction to definitions in BPMN 2.0. It is by no means comprehensive but allows for a quick rudimentary understanding of the offered features and principles used in the later introduced workflows. For full documentation of the standard, the current BPMN 2.0 specification [33] is available.

2.3 Limitations

Within this section the limitations of this thesis are discussed. A main limitation that comes to mind is while all generic workflows are designed to accommodate GDPR requirements, the implementation is up to the user. Therefore, it cannot be guaranteed that once the workflow is adjusted to the business needs the full compliance with requirements is still intact. Furthermore, while workflows are designed with personal data in mind, the processing of sensitive information can alter the requirements and lead to non-compliance if no necessary mitigation steps are taken.

Any provided sample forms are not peer reviewed by any legal experts, before their application it is strongly recommended to adjust them to business needs and ensure compliance by consulting a legal expert.

The market of BPMN software is subject to constant change, accuracy of the provided information can only be assumed for the exact same version of the reviewed software.

It may be necessary for any user to implement further workflows other than the ones provided within this thesis to be fully compliant with GDPR requirements, while this thesis strives to give strong support in the effort of transitioning to GDPR, not all necessary processes may be reflected. This holds especially true if information from minors or other sensitive information is processed.

This thesis is not legal advice, the first rulings to establish legal certainty lay in the future at the time this thesis is written. No legal experts have been involved during the creation of this paper.

2.4 Contributing Literature

In this chapter, the three most significant pieces of contributing literature are presented. They serve as a reference point to both the GDPR requirements and the BPMN standard. All three publications had a big influence on this master thesis.

2.4.1 Praxishandbuch BPMN 2.0 von Camunda

While the book I refer to has been written in German, camunda offers many online resources, guidelines and definitions around the topic process engineering, process automatization, and BPMN. The authors of the book are being of the FTF¹⁶ of the Object Management Group's BPMN 2.0 and thus have thorough understanding of the standard and its practical application. The book [22] offers a clear and structured introduction to BPMN.

It introduces the notation, it's syntax, and semantics and provides further information on best practices. After the introduction, a 4-step program is carried out. At step 1, the strategic level of BPMN workflows is discussed, this level is many times on par with the generic workflows presented in this thesis. Step 2 is concerned with the operational level, while some of the presented workflows may already achieve this level many users will need to adapt the model to fit the business specifications. Step 3 is concerned with the technical level and process engines. An introduction to process automation and instructions on how to achieve a model that is detailed enough to be carried out in such an engine are presented. The book also covers the establishment of BPMN within the organization.

It is recommended to first get a firm understanding on the semantics and syntax of BPMN before continuing with Part 3 of this thesis.

2.4.2 General Data Protection Regulation (EU 2016/679)

While it may seem redundant, it must be stressed that the focus point of this thesis is the Regulation (EU) 2016/679 [28] and therefore it is the single most important document. All workflows introduced are designed to comply with requirements spelled out in the standard.

2.4.3 The EU General Data Protection Regulation (GDPR) – A Practical Guide

Published by Springer, this guide provides a systematic analysis of the GDPR. Providing adept information on legal consequences, implantation and consequences of the new regulation. It serves as an important resource to the creation of generic workflows and holds true value.

A plenitude of books, articles, and online resources served as sources of information for this thesis can be found in the bibliography of the paper.

2.5 Summary

This chapter serves as a resource of information which is needed to understand the claims made in this paper. An introduction to modelling notations was given and a first example of BPMN was demonstrated. The definition section serves as a tool to create a common ground on the meaning of terms and phrases. Both topics the GDPR and BPMN have been covered. In section 2.3 the known limitations of this master thesis have been discussed. The three most significantly contributing literature pieces have been announced in section 2.4. This concludes part 1 of the paper.

¹⁶ FTF - Finalization Task Force

Part 2
Market Analysis

3 BPMN 2.0 Tool – Market Analysis

Within this chapter, a market analysis of currently available BPMN modelling tools is conducted. After the methodology is discussed, the selection process is introduced. In section 3.3, a clear rating criterion is outlined which will be used to rank the tools. Section 3.4 contains the analysis of each individual tool, a short description, and the individual scoring. Section 3.5 integrates the different results into one comparison of the tools. In section 3.6 those results are interpreted.

3.1 Research Methodology

The research is done uses quantitatively-based scores to achieve a ranking of each tool. The scoring system is described in section 3.2. After gaining the results a quantitative result is presented. Additionally, qualitative impressions of each toolkit such as UI handling are discussed in the review.

3.2 Selection Process

Before the search for fitting solutions took place a set of rules was defined. Each tool had to fulfil the following criteria:

- Free to use
- BPMN in Version 2.0 officially supported
- Available for Windows or MacOS

After online research using common tools¹⁷ the following set of software solutions has been chosen:

Table 2 BPMN Modelling Tools

Name	Platform ¹⁸
Camunda Modeller	Cross Platform
Aris Express	Windows
Bonita BPM	Cross Platform
BPMN 2 Modeller Eclipse	Cross Platform
jBPM	Cross Platform
Modelio	Cross Platform

This selection of tools serves as an insight to freely accessible BPMN 2.0 modelling tools. Aris Express is also executable on Linux and MacOS at own risk.

3.3 Rating Criteria

In addition to a qualitative rating of usability a set of criteria is introduced to allow for a comparison between the offered products. These criteria range from usability to features and functionality. This includes not only the generation of workflow models but also the available export options for such models. The following functionalities have been identified [22], if a functionality is available it is rated as a 1 of not a 0.

¹⁷ Google.com, Bing.com, Wikipedia.com

¹⁸ If Windows, MacOS and Linux are supported it is considered Cross-Platform this also applies for Cloud-based tools

- Expandable and collapsible sub-processes
- Assignment of documents to tasks
- Conformity with BPMN 2.0
- Show and hide information
- Tabs or other method to view multiple workflows
- Using self-designed artefacts
- Syntax check by the tool
- Color coding
- Attachment of key figures
- Export as BPMN
- Export as jpeg or png

This amounts to a total of 11 possible points for each tool.

3.4 Analysis

Within this section the 8 identified tools from section 3.2 are analyzed and scored.

3.4.1 Camunda Modeler

The Camunda Modeler is developed by Camunda Services GmbH and based on bpmn.io. The tool offers full offline functionality and is licensed under the MIT license¹⁹ although some parts are derived from bpmn.io and are therefore licensed under a proprietary free to use license from bpmn.io²⁰. The software was tested on an Apple iMac system running Version 10.13.5 macOS High Sierra. The tested Camunda modeller was Version 1.11.3.

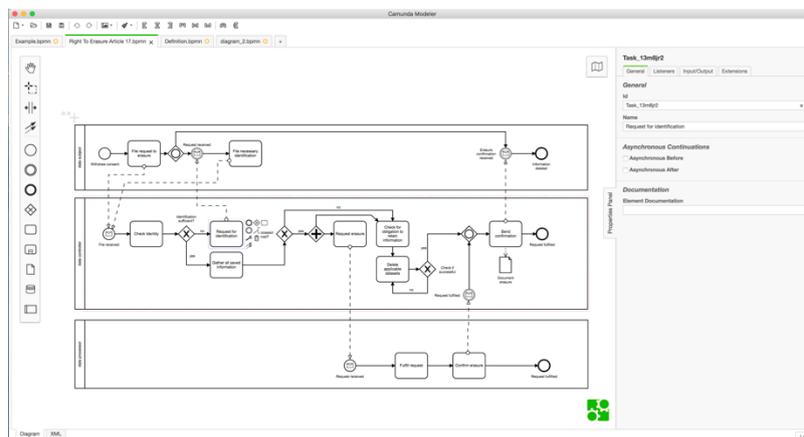


Figure 6 Camunda Modeler

The Camunda Modeler has extensive features such as using tabs to manage multiple workflows, configure tasks that can be executed in a process engine like sending a message. However, having such an extensive set of functions makes some settings appear to be hidden. A big plus is the context sensitive insert of applicable settings which helps to only see the relevant options. The tool allows to export the workflow as jpeg, png, svg, bpmn and xml. The final scores for the software are shown in table 3.

¹⁹ <https://github.com/camunda/camunda-modeler/blob/master/LICENSE>

²⁰ <https://bpmn.io/license>

Table 3 Camunda Modeler Score

Function	Score
Expandable and collapsible sub-processes	1
Assignment of documents to task	0
Conformity with BPMN 2.0	1
Show and hide information	0
Tabs or other method to view multiple workflows	1
Using self-designed artefacts	0
Syntax check by the tool	1
Color coding	1
Attachment of key figures	1
Export as BPMN	1
Export as jpeg or png	1
TOTAL	8

3.4.2 Aris Express

Aris Express is developed by Software AG is a feature reduced version of Aris [34]. The tool is fully functional in offline use but requires an online registration. However, Aris Express is freeware and can be used even for commercial applications without paid licensing. The version tested was Aris Express Version 2.4d on Windows 10 Pro 64bit Build 17134.

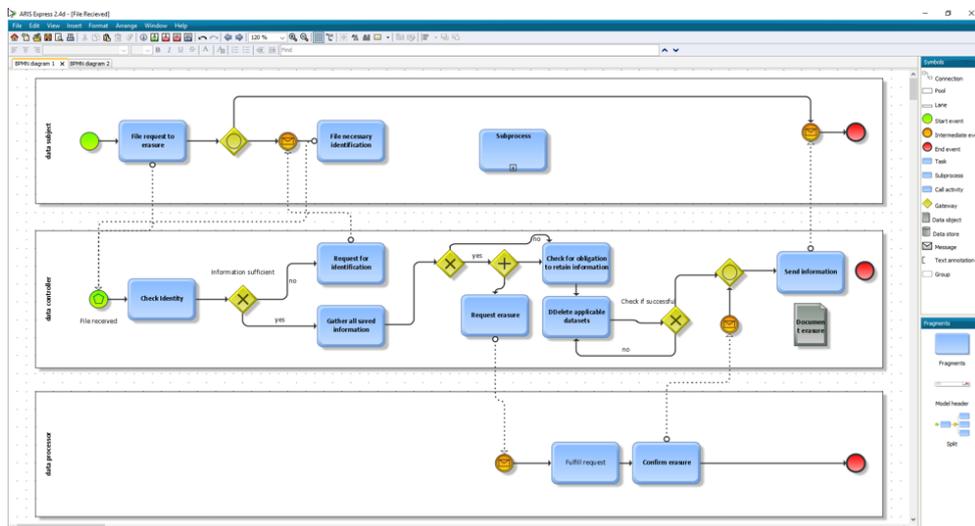


Figure 7 Aris Express

While the full Aris software offers a wide variety of functions the express version has had to cut back on advanced features. No XML import or export is available and only proprietary file formats can be used to save the workflow, it is however possible to export a PDF²¹ file with the visual representation. Unfortunately, it takes many clicks to perform simple actions like adding text and the experience feels rather slow. The software is unofficially distributed for macOS and Linux, but no guarantee of functionality is given. The diagram was colored automatically as each item has a predefined color.

²¹ PDF – Portable Document Format

Table 4 Aris Express Score

Function	Score
Expandable and collapsible sub-processes	1
Assignment of documents to task	1
Conformity with BPMN 2.0	1
Show and hide information	0
Tabs or other method to view multiple workflows	1
Using self-designed artefacts	1
Syntax check by the tool	1
Color coding	1
Attachment of key figures	0
Export as BPMN	0
Export as jpeg or png	0
TOTAL	7

2.4.3 Bonita BPM

The Bonita BPM modeler is developed by Bonitasoft. The tool has full offline functionality and doesn't require a registration. The software is released under the GNU GPL²². The software was tested on macOS 10.13.5 High Sierra the modelling software was Bonita Studio Community 7.7.2.

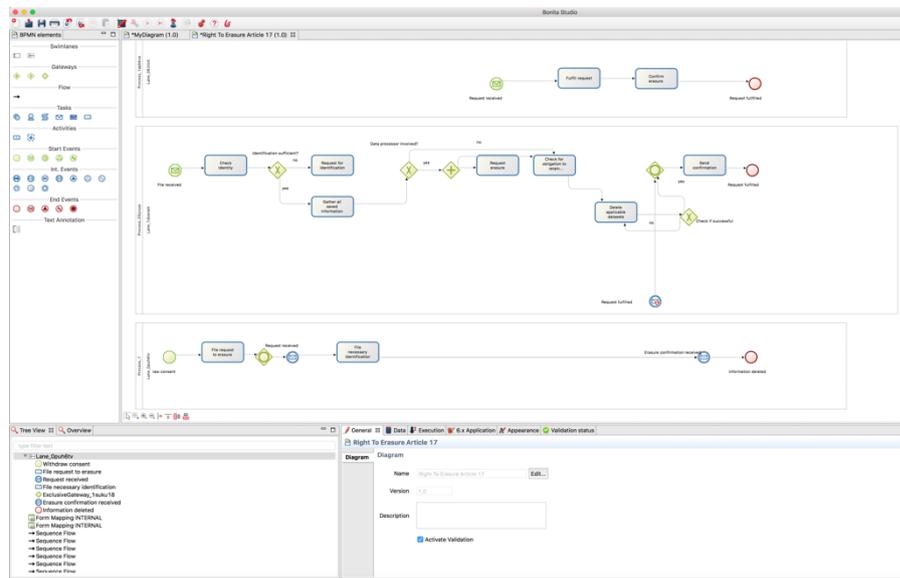


Figure 8 Bonita Studio Community

While the software did allow to import a standard bpmn file, it failed to represent the workflow correctly. Not only have the upper and lower pool switched positions, but message flows are missing. Not all symbols defined by the BPMN standard are present, only those needed to design a process flow are included. However, the software does support validation of the designed process and later integration in a business process engine.

²² GNU GPL – General Public License of GNU

Table 5 Bonita Studio Community

Function	Score
Expandable and collapsible sub-processes	1
Assignment of documents to task	0
Conformity with BPMN 2.0	0
Show and hide information	0
Tabs or other method to view multiple workflows	1
Using self-designed artefacts	0
Syntax check by the tool	1
Color coding	1
Attachment of key figures	1
Export as BPMN	1
Export as jpeg or png	1
TOTAL	7

2.4.4 BPMN 2 Modeler Eclipse

The BPMN 2 Modeler is released was developed under the SOA²³ Project as a plugin for Eclipse. The tool is fully functional offline, and no registration is required. The software is licensed under the Eclipse Public License 1.0. The plugin is version 2.14 and Eclipse is version 4.8 the operating system is macOS 10.13.5. There is no standalone version available, a current installation of Eclipse is mandatory.

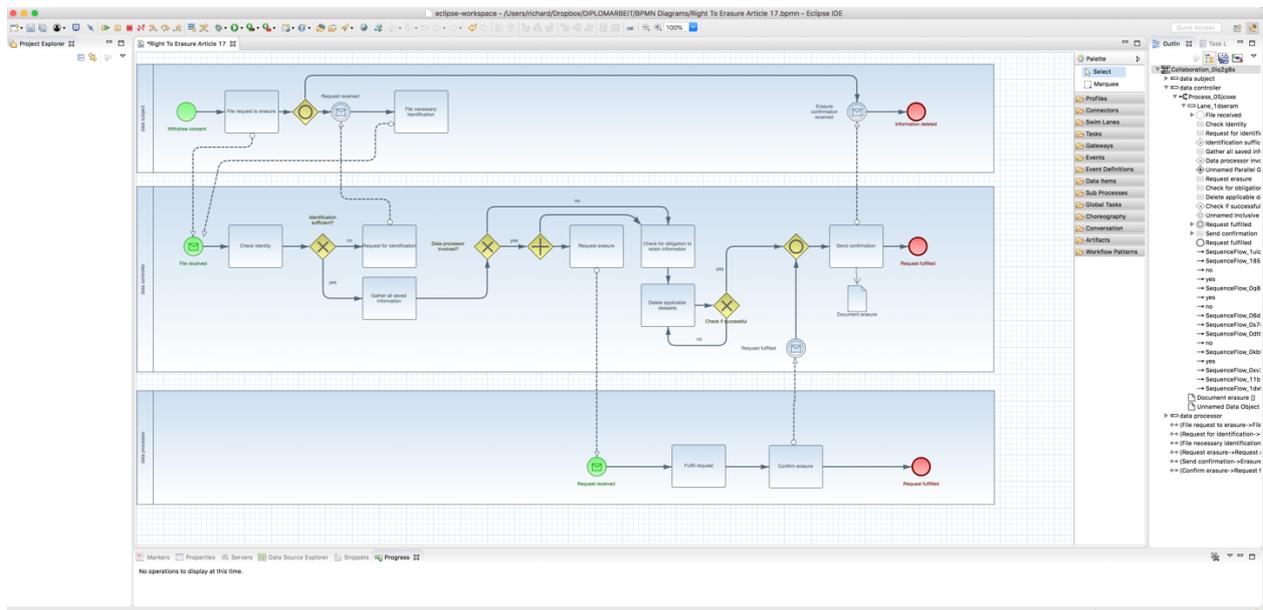


Figure 9 BPMN 2 Modeler Eclipse

The plugin can be installed through the integrated marketplace. It was able to import the bpmn file created with Camunda modeler and represent the workflow the same way. All items are colored by default, but the color can be adjusted to individual needs. Overall the tool made a very good impression. Important functionalities are easy to reach, and the visual representation is pleasing.

²³ SOA – Service Oriented Platform

Table 6 BPMN 2 Modeler Eclipse

Function	Score
Expandable and collapsible sub-processes	1
Assignment of documents to task	0
Conformity with BPMN 2.0	1
Show and hide information	1
Tabs or other method to view multiple workflows	1
Using self-designed artefacts	0
Syntax check by the tool	1
Color coding	1
Attachment of key figures	1
Export as BPMN	1
Export as jpeg or png	1
TOTAL	9

2.4.5 jBPM

jBPM is a business automatization software sponsored by Redhat. Integrated in this software is a process modeler. This modeler can be used to create BPMN workflows. While the server for this application was hosted on macOS it is entirely platform independent due to its nature as a webservice. Version 7.8.0 was used for this review, Safari²⁴ Version 11.1.1 was used to access the web application.

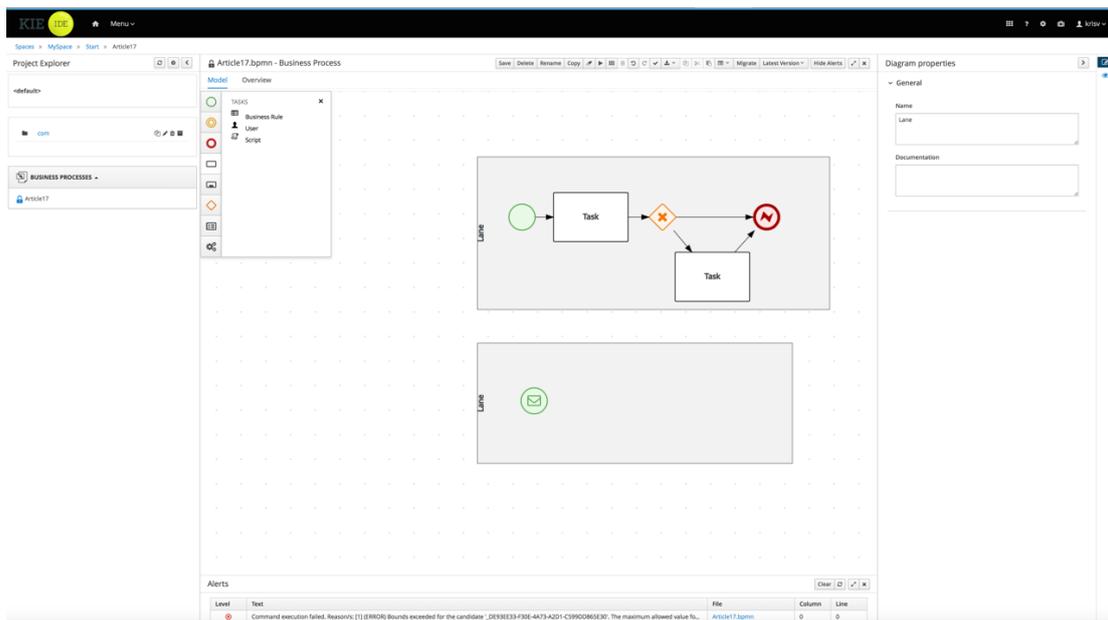


Figure 10 jBPM

Due to the implementation, no message flows between pools were possible which resulted in a rudimentary example figure. The process flow arrows could not be manipulated and some BPMN 2.0 symbols were not available. While the tool is built with process automation in focus it lacks modelling properties. Even though a bpmn file has been successfully imported only the xml portion was visible while no visual workflow was generated.

²⁴ macOS internet browser

Table 7 jBPM

Function	Score
Expandable and collapsible sub-processes	0
Assignment of documents to task	0
Conformity with BPMN 2.0	0
Show and hide information	1
Tabs or other method to view multiple workflows	1
Using self-designed artefacts	0
Syntax check by the tool	1
Color coding	1
Attachment of key figures	0
Export as BPMN	1
Export as jpeg or png	1
TOTAL	6

2.4.6 Modelio

Modelio is released under the GNU GPL license and is a 2009 started open source project. The tool is usable offline and supports multiple standards such as UML, BPMN, TOGAF²⁵ and more. It can be flexibly expanded through modules available within the application. The tested version was 3.7.01 on macOS High Sierra 10.13.5.

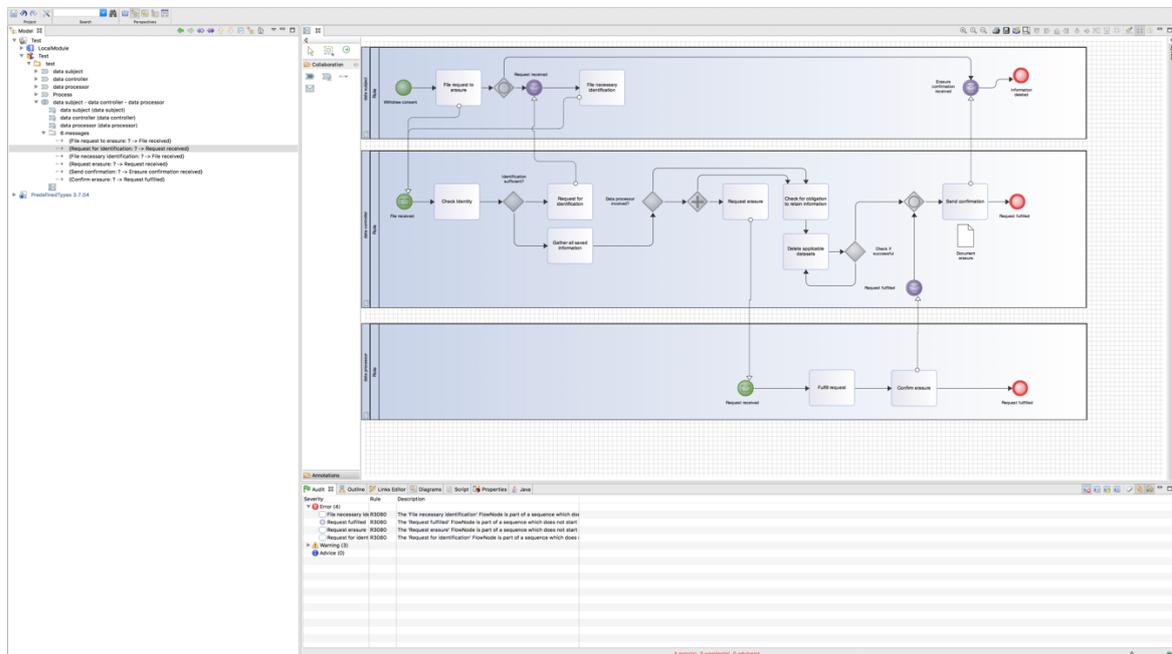


Figure 11 Modelio

Modelio offers all necessary symbols and features for prosperous workflow design. Both an import and an export of bpmn files is possible and the application excelled importing the example project. On standard setting the program automatically colors the elements used, unfortunately intermediate events are by standard purple in contrast to the more commonly used yellow color.

²⁵ The Open Group Architecture Framework

Table 8 Modelio

Function	Score
Expandable and collapsible sub-processes	0
Assignment of documents to task	1
Conformity with BPMN 2.0	1
Show and hide information	0
Tabs or other method to view multiple workflows	1
Using self-designed artefacts	0
Syntax check by the tool	1
Color coding	1
Attachment of key figures	0
Export as BPMN	1
Export as jpeg or png	1
TOTAL	7

This concludes the individual introduction of BPMN modelling software. The following section will consolidate and discuss the results.

3.5 Comparison of results

The total combined score comparison can be found in Figure 12 Comparison BPMN below. The tool “BPMN Modeler 2” was able to score 9 out of 11 points, not one product was able to score all points and not one point wasn’t scored at least once. In second place is the “camunda modeler” which offers an easy to use interface, clear documentation and easy setup. The tool scored a total of 8 points. ‘Aris Express’, ‘Bonita BPM’ and ‘Modelio’ scored all 7 points. With the set criteria ‘jBPM’ was only able to score 6 points in overall. This concludes the objective comparison, in section 3.6 further findings are discussed.

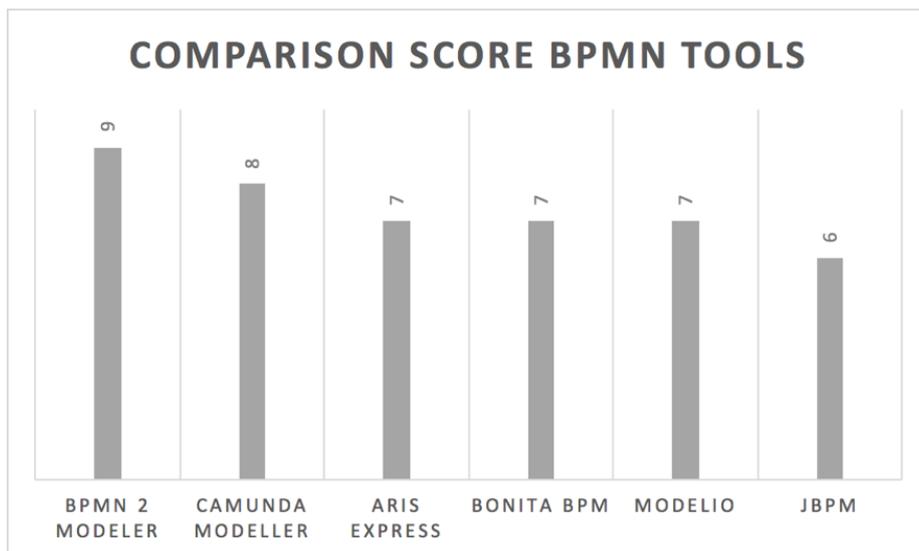


Figure 12 Comparison BPMN

3.6 Interpretation of results

While the BPMN 2 Modeler fulfilled most of the criteria, the usability was only on an average level. Two of the tools, namely Bonita BPM and jBPM were lacking BPMN 2.0 functionality as they had missing symbols or were limited on message flows. Aris Express would be a good solution if standard export functionality was given. Unfortunately, this is only a paid option with this software. Additionally, the usability was average, and the visual representation of the symbols seemed dated.

All tools were able to present one or more workflows at any given time, change the color of symbols and all tools prevented the user from making invalid connections (syntax check). However only Aris Express and Modelio allowed the user to attach Documents directly to a task.

The introduced tools stand in direct competition to commercially available software solutions which were out of scope for the analysis. Nonetheless it became clear while not every tool fits every use case there are many tools perfectly fitted for a given task. Even without taking the cost into consideration some tools performed outstanding and offer enough functionality to go beyond an introduction to BPMN.

3.7 Summary

In section 3.1 – 3.3 the research methodology, the selection process and the rating criteria are introduced. The market analysis of 6 BPMN tools has been conducted in section 3.4. The following two sections combined the results and summarized the findings.

Part 3
BPMN Workflows

4 Supporting GDPR implementation through BPMN workflows

This chapter introduces generic Workflows to support an organization during its transition to conformity with GDPR requirements through the application and adaption of here within provided sample workflows. These workflows resemble the strict requirements presented by the EU concerning personal data processing. Additionally, to the presented workflows' sample forms will be provided in some cases. These forms are to be adapted by the business to comply with the organizations' specific needs. Nevertheless, the provided forms while in accordance with the GDPR do not resemble a full set of necessary documentation.

Mandatory documentation which is not provided includes but is not limited to [28], [35]:

1. A privacy notice – the regulation calls for concise, in clear and plain language written information. The purpose of this document is to disclose how the personal data is processed. It also needs to be easily accessible for the data subject.
2. A data retention policy – the policy should contain a clear procedure to determine how long a dataset must be stored. It also describes the way the data will be destroyed once it reached its end of life. Additionally, a data retention schedule has to be maintained.
3. An employee privacy notice – this privacy notice is only concerning the staff of the corporation.
4. A personal data protection policy - this policy acts in a way as the foundation to compliance with GDPR requirements. The policy should be descriptive of the principles and purposes of the data processing, roles and responsibilities are to be defined as well as key requirements and controls. Finally the appropriate supervisory authority is to be determined [36].
5. A data protection impact assessment report
6. A data processing agreement with suppliers.
7. A record of any and all occurred data breaches within the organization.
8. Code of conduct for data processors

The following workflows can be adjusted to individual needs to do so the following shall be considered:

- Can tasks be united due to internal organization or infrastructure?
- Can existing business process be incorporated into the introduced workflow or vice versa?
- Should tasks be split into multiple tasks due to internal requirements or infrastructure?
- Do some tasks require escalation in the hierarchy under certain conditions?
- What are already internally used designations for tasks introduced (change the name)?
- Should roles be defined to fit organizational requirements (introduction of swim lanes)?

The workflows introduced are provided under the Apache 2.0 license (see Appendix).

4.1 Workflows – Data subject rights

In order to achieve conformity with the law, new processes have to be implemented in the organization. While it may be necessary for businesses to conjointly adjust old processes to comply, supporting those changes is out of scope of this paper. This paper does focus on introducing workflows providing the data subject with an option to practice the newly imposed data subject rights. By implication, that means workflows for the so called “data subject rights” will be provided. Furthermore, notification tasks shall be covered and represented by workflows within this chapter. If applicable, roles and responsibilities are mentioned in the accompanying text of the presented workflow. These may be subject to change in order to correspond with established roles within the organization.

4.1.1 Right of access by the data subject – Article 15 GDPR – Workflow

The GDPR dictates the data subject has a so called “Right of access” and specifies it as:

“A data subject should have the right of access to personal data which have been collected concerning him or her, and to exercise that right easily and at reasonable intervals, in order to be aware of, and verify, the lawfulness of the processing.” [28, p. 12]

Article 15 of the GDPR specifies the information which has to be made available to the data subject. This information consists of the purposes of the processing and which categories of personal data are involved. If the data is shared with third countries, this information needs to be disclosed. If viable, an estimate of how long the data will be stored or which criteria is used to make that determination has to be provided. The data controller has also the duty to inform the data subject about its rights to erasure or rectification and the right to file a complaint with a supervisory authority. Additionally, if data was obtained from other sources or automated decision making is deployed, the data subject has the right to receive full disclosure of this information.

If the data of the data subject is in fact possibly processed in third party countries, the data subject has to be informed about the applicable safeguards regarding the transfer. If inquiries by the data subject are made in an unreasonable manner, such as short-term repetitive requests, the controller can charge a service fee.

The workflow presented in ‘Figure 13 Right of Access’ takes the given requirements into account and renders the necessary steps in an easy to follow manner. Additionally, each step is explained, including additional information, in writing. The flow of the process will be represented by a so called “token”. The token is born at the initiating event and dies at the end event.

The process token S is born because the data subject has interest in accessing data stored referring to him. It continues to “File access request”. At this stage the data subject files a request to the data controller, this can be done in several ways including the usage of a provided form, an E-mail or a letter. The token then continues to an inclusive gateway where it sits until one of the following events happens.

Meanwhile, a token in the data controller pool is born when the access request is received. The token then flows to the identity check task. During this task, the provided identification needs to be reviewed and deemed sufficient or not. If the proof provided by the data subject is repeatedly insufficient, the request will be denied. However, before such a denial can be enforced, a request for further identification is sent to the data subject. Once the data subject has proved its identity, the token flows to a XOR gateway. If the data subject files information access requests in a repetitive manner, a fee for providing the information can be applied or the inquiry can be denied. The token then continues its path to the AND gateway if the data subject didn't refuse to pay. At this point, two tokens continue. Token A arrived at the task ‘Gather saved information’ at this task all information saved about the data subject is retrieved from the information systems used within the organization. A data map, CRM²⁶, CDM²⁷ or MDM²⁸ tool offer support, some enterprise tools are even able to automate the process. The next stop for the token is to identify what the purpose for the processing is, if the purpose is always the same, this can be a pre-defined statement or will need to be individually assessed. Moving on it is important to inform the subject about applicable rights he or she has, as mentioned in the introduction of this section. The next stop is the task of creating a statement of how long the customer's dataset will be stored. If this estimate can't be made, the data controller must give plausible reason. Once the task is completed the token flows on to the parallel gateway where it awaits token B and if applicable token C.

²⁶ Customer relationship management

²⁷ Customer data management

²⁸ Master data management

Token B flows from the parallel gateway to an XOR gateway. If data processors are involved, a request to disclose all saved information about the data subject is sent. If not, the token moves on to the next XOR gateway. If information was shared with third countries or international organizations a document about the applicable safeguards must be provided to the data subject. The token moves on to the third XOR gateway, if automated decision making is employed, a report of how this is affecting the data subject must be provided. The token flows to the fourth XOR gateway, if alternative data sources have been used to gather information about the data subject, a report must be provided. The flow of the token continues up to the parallel gateway where it potentially waits for token A and/or C.

Token C is only created if a data processor is used. In that case the token is created when the information from the processor is received. The tasks the processor must perform are out of scope and only display a very high-level perspective.

Once all expected tokens arrive at the parallel gateway one token moves on to the task “Consolidate information” where all gathered information is summarized in a report for the data subject. Before this report can be submitted a check if no legal obligations interfere with providing the data subject with the information of the report has to be conducted. After this final review the report can be sent to the data subject and the token dies at request fulfilled.

The token created by the customer continues its path either to providing more information or directly to the received response. The view of the data subject is, like the view of the data processor, out of scope and only high level to provide an impression of the tasks other parties have to perform. However, BPMN allows these pools to be collapsed and to only represent subjects who are interacted with alternatively as an empty bar.

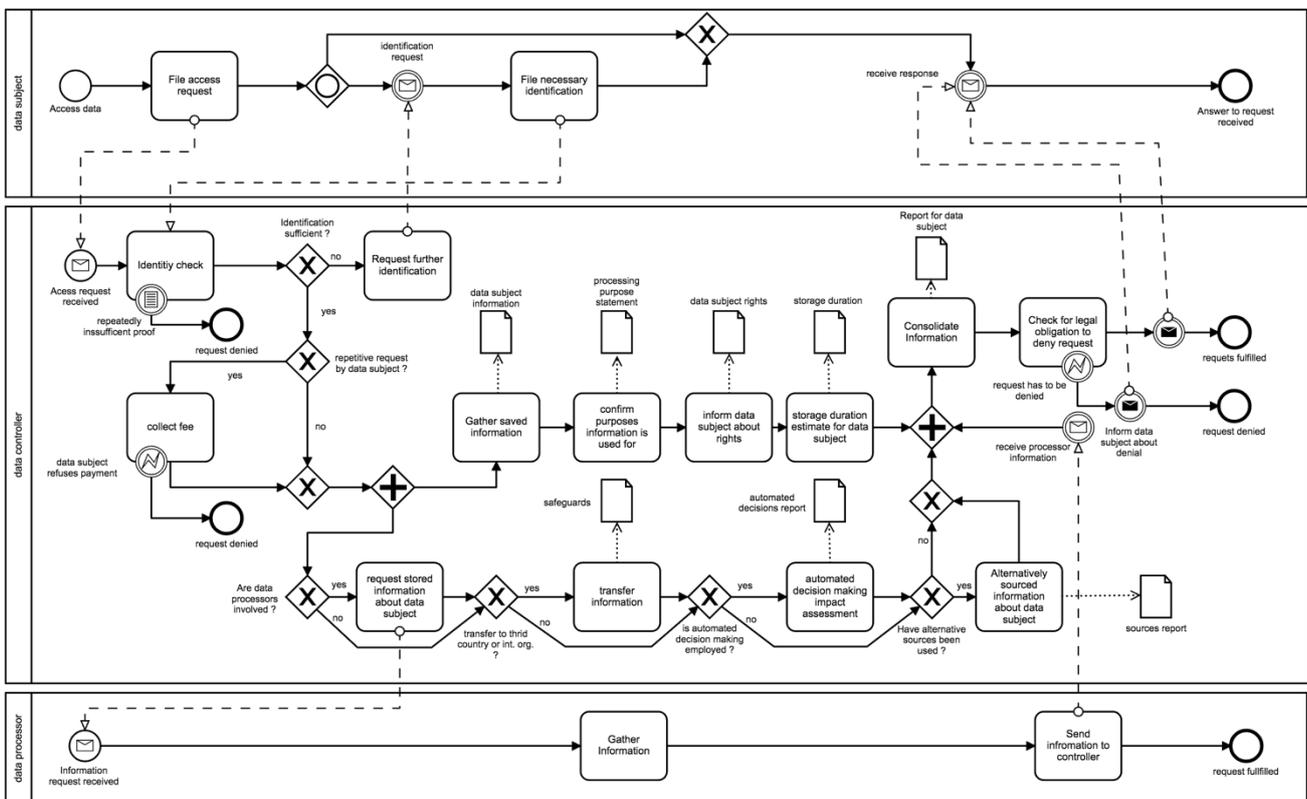


Figure 13 Right of Access

4.1.2 Right to rectification – Article 16 GDPR – Workflow

Article 16 of the GDPR dictates the “Right to rectification” a data subject has and defines it as:

“The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.” [28, p. 43]

A data subject can demand to rectify wrong information. However, it needs to prove that either the data is inaccurate and/or information is missing. This can be done without the need to provide a reason as to why the information change is requested. The right to rectification is in place to allow the data subject to intervene when the data processing is no longer lawful. [37]

To avoid confusion between the scenario where data is misrepresented and the scenario where data is missing the workflows while similar shall be represented separately

Scenario – Inaccurate Data

The personal data represented by the data processor is untrue in the sense that it doesn't reflect reality. Therefore, the data subject may suffer from inadequate decisions made regarding his or her persona. The right to rectify can only be exercised if the dataset in question is affiliated with the data subject. It is not possible to rectify the information of someone else, additionally if the data concerning the data subject is part of a bigger data sample, the right to rectification may be limited. Nonetheless, if the data is in fact inaccurate and directly relating to the data subject, the data subject has the right to immediate rectification.

The workflow for this scenario is presented in Figure 14 'Right to rectification – inaccurate data'. Both the data subject and data processor are only high-level views and can alternatively be collapsed while the focus lies on presenting a strong strategical approach to comply with Article 16 of the GDPR. The token is born when the data subject decides to have information corrected. It flows to the task of officially requesting such a change. This correction request triggers the message catch start event in the data controller pool.

The data controller token flows to the task identity check and continues its path based on if the check was successful or not. If not the token flows to further identification is required. Once the identity is confirmed the token continues its path to the verification task. At this point it needs to be verified that the claims made by the data subject are accurate. If this is not the case the request is denied. If, however, the claims hold true the token moves to the next check. The decision of if the interests of the data subject warrant the change must be made on a case-by-case basis. However, as a rule of thumb if the information concerned only represents a small part in a bigger collective it is unlikely the change is warranted, but “[i]f a value judgement leads to an incorrect impression of a person whose incorrectness can be proven, the interest of the data subject for rectification might prevail.” [38, p. 155]

If the correction is granted and no data processor is involved, the token flows to the task “Gather all saved information”. If a data processor is involved, the needs to be informed about the changes. If the request is denied, the data subject will be informed, and the token dies at request cancelled. After gathering all the information which has to be changed in various systems, a CRM, MDM or other enterprise software designed for the purpose of data management can be of help gathering said information, the token moves on to the task of actually correcting the dataset. After the corrections have been made a report of changes is created. This

report contains both the data processors and the data controllers' changes. The last task for the data controller is to inform the data subject about the changes. The token then moves on to die at "request fulfilled".

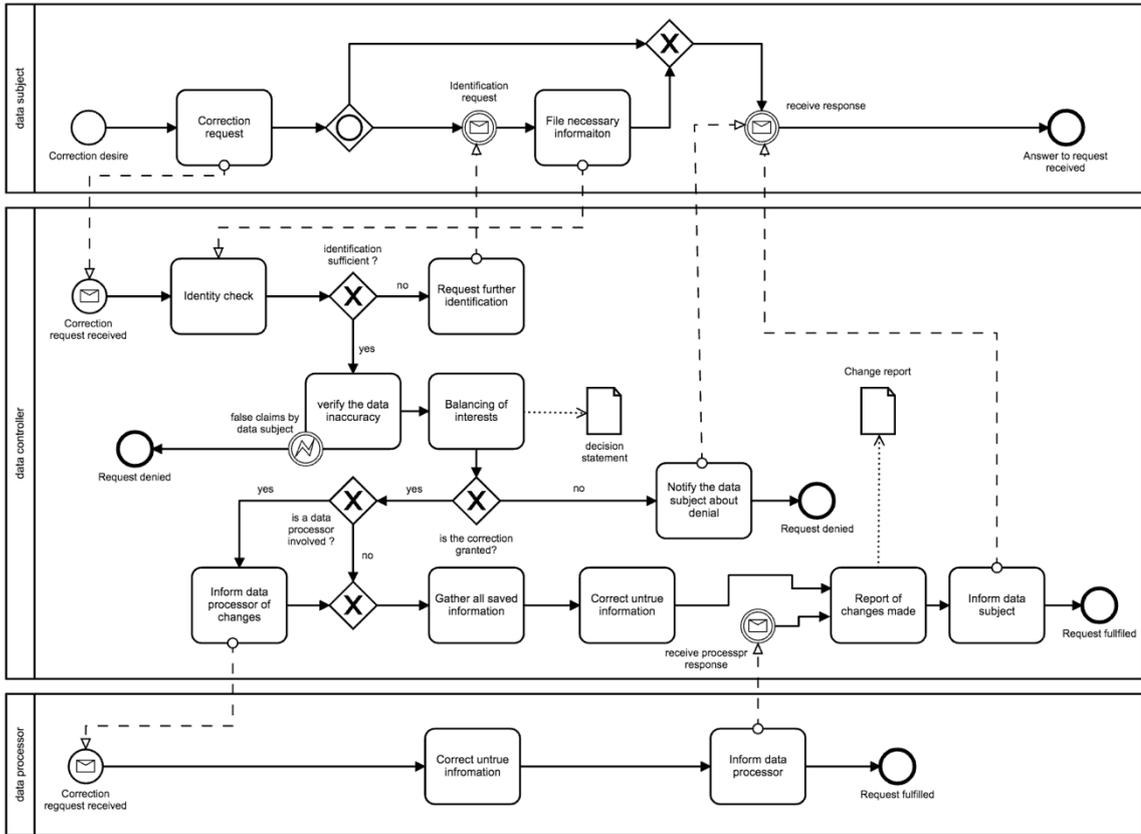


Figure 14 Right to rectification – inaccurate data

Scenario – Incomplete Data

According to Article 16 a data subject shall have the right to complete personal data records if they are incomplete and thus inaccurate. It is important to consider that added information to the data set requires increased resources for the processing of such. [38]

The GDPR calls for rectification with undue delay by the data controller. Every request made needs to be evaluated to determine if the added information serves the act of data processing, if there are risks for the data subject due to incomplete information and if the amount of work put into correcting the dataset is proportionate to the benefit it delivers. [37]

Figure 15 'Right to rectification – incomplete data' presents the corresponding workflow. While both the data subject and data processor pools are only in place to visualize on a high level the tasks performed by these parties, the data controller pool introduces a data completion approach.

The first token is born once a data subject has the want to supply further information in order to complete the personal data set. The token then flows to the first task which is a formal filing of that wish including which data is missing to the data controller.

In the data controller pool the token is born once the completion request is received. The token flows to the identity check task. If the identification provided is lacking evidence that the data subject is who they

claim to be the token is sent to the 'Request further identification' task at the identification sufficient XOR gateway.

Once the identity of the data subject has been confirmed, the token flows to the verification task. At this task the provided input needs to be checked for accuracy. If the information provided is false, the request to complete a dataset has to be denied. Once the verification task is completed the token moves on to the first of three evaluation tasks. Task one aims to evaluate if adding the information has any benefits to the processing of the dataset. Results can be kept in a 'Decision Report' but can also be documented by other means. In this example we use one report for all findings.

Once the evaluation completed, the token moves on to the second evaluation task. At this point it is evaluated if the effort undertaken in order to complete the dataset is in proportion to its benefits. At last, the token arrives at the third evaluation task. This task aims to conclude if the lack of completion of the dataset bares any risk to the data subject. After the evaluation is completed, the token moves on to the final decision task. At this point, all information from the report is taken into account and a decision of how to proceed is made.

If the data will not be completed, the token flows to the "Inform data subject about denial" task before it dies as the request is denied. If the dataset gets completed, the token either directly goes to the task of updating affected datasets or to the inform data processors task. Once all datasets are updated the event should be documented. The token flows to report changes and the data subject is informed about the fulfilment. The token then dies at "Request fulfilled".

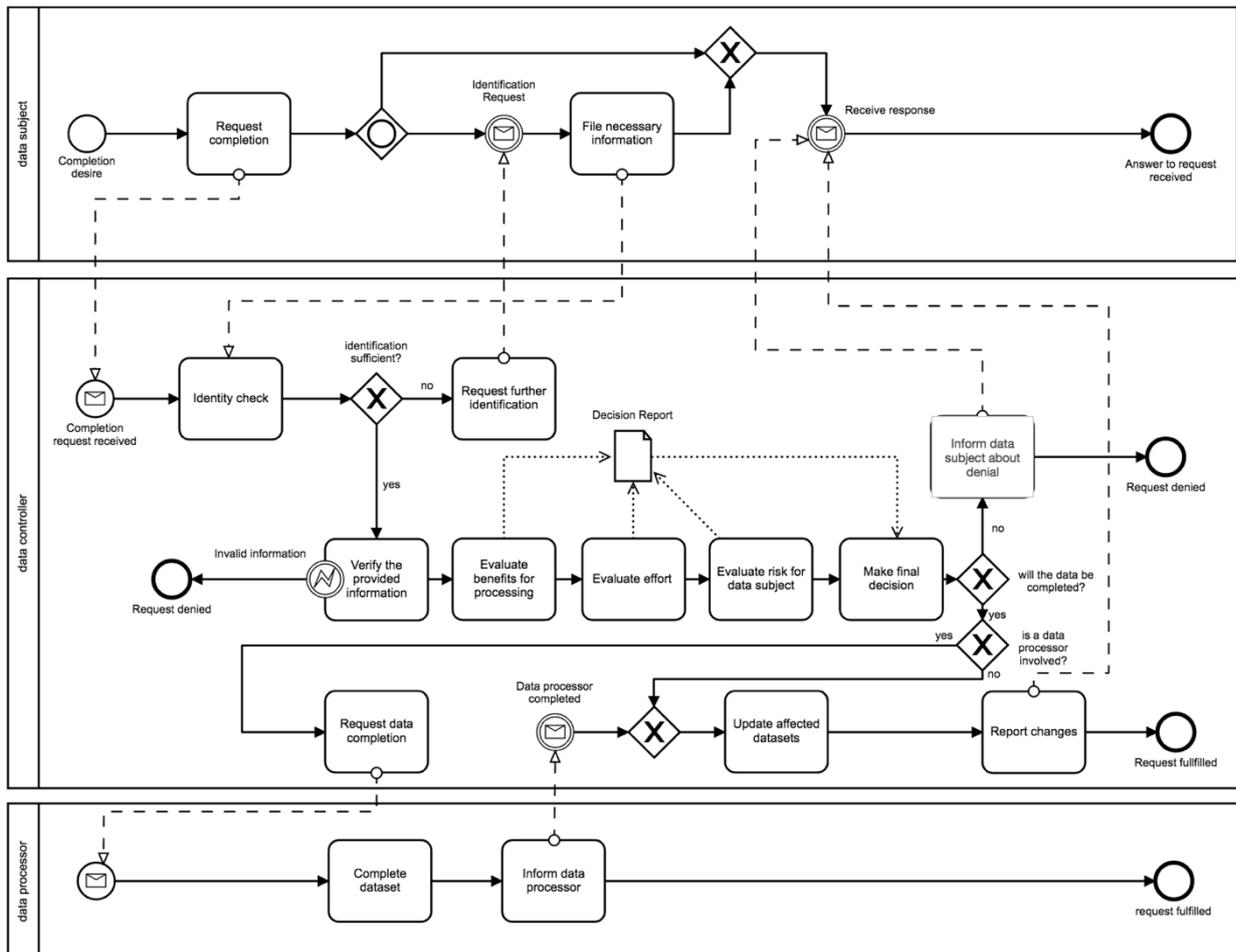


Figure 15 Right to rectification – incomplete data

4.1.3 Right to erasure – Article 17 GDPR - Workflow

Article 17 of the GDPR defines the 'Right to erasure' also known as 'right to be forgotten' as:

“The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay [...]“ [28, p. 43]

In order for the data controller to have to comply with a request to erasure, one of the following grounds needs to apply. [38]

The data that has been collected about the data subject is no longer needed for its original purpose or in another way processed. Therefore, even if the data has been sourced legally it has to be deleted if it doesn't serve any processing purpose. However, if the dataset is still used in a process relating to its original intended purpose, the erasure can be denied.

In case that the data subject withdraws the originally given consent to the processing which can be done without the data subject to give a reason as to why. Granted that there is no other reason such as legal obligations to retain the information and further process it. The personal data has to be withdrawn because Article 6 of the GDPR point “a” states that processing personal data is only lawful if the data subject has given consent to process its personal data for one or more reasons or if the data is subject to special protections due to its nature and the data subject withdraws the consent given (see Article 9 GDPR section 2 point ‘a’).

The data was processed under the application of Article 6 section “e” or “f”. If the data was processed in public interest the data subject has the right to object that processing. It is the burden of the data controller to prove that legitimate interests warrant a processing of the information and thus override the rights, freedoms, and interests of the data subject. Ongoing legal proceedings are also a reason to deny the objection. Since the evaluation and weighing of interests can be a lengthy process the data subject could restrict the processing. Another reason for the data subject to withdraw consent is if the data is used in direct marketing. If this is the case, the data controller must erase the personal data sets.

If the data was processed while the organization was not compliant with the GDPR regulation or the data was obtained through improper ways the data subject has the right to have the dataset deleted due to its unlawful processing.

If the data controller is subject to national laws from a Union or Member State which grant the data subject further rights, the data subject can exercise these only nationally applicable laws and have his personal data removed from processing.

If the services are provided to a child, the data must be removed upon request even if the data subject is at the time of the removal request no longer a child. This may lead to partial removal of personal data collected under the consent granted as a minor but allows to continue processing data which may relate to the data subject but was collected after a consent was renewed once adulthood was reached. The GDPR considers a person below the age of 16 years a child but nationally applicable law can lower the threshold to 13 years.

Therefore, it is possible that some data collected in a member state of a person 15 years of age is only legally up for processing if the holder of parental responsibility gave consent, but some persons 14 years of age can make the decision to give processing consent by itself without parental supervision.

The GDPR requests the data controller to contact other data controllers by technical means or other reasonable action to inform the other party of the request of deletion made by the data subject. This includes any links or replications of the personal data set.

The mentioned grounds do not apply if one of the following exemptions can be applied and therefore make the processing necessary.

Contingent on the exercising of the right of freedom and information an erasure can be denied. It is suggested that since not only the press but any entity can exercise this right it may become a widely used [39] practice. However, it needs to be evaluated if the currently stored personal data is necessary in its entirety and decisions have to be made on a case-to-case basis.

If an applicable legal obligation to store the data is in place by a Union or Member State, the national law and the observance of its requirements trumps the right to erasure. Additionally, if the processing is performed in public interest the data subject cannot insist on the removal of the personal data.

If the data is needed to comply with provisions introduced to support interests in the area of public health.

Personal data processed for research purposes may be exempt from the right to erasure if it is in accordance with Article 89 of the GDPR. Measures such as data minimalization and pseudoanonymization are introduced as examples for compliance with the requirements introduced.

Legal proceedings such as the exercise, defense or establishment of claims render the right to erasure null until the dispute is settled.

Figure 16 “Right to erasure” introduces a process taking the provisions made by article 16 into account and supplements these regulations with input gathered from various experts. [38], [39] However, the presented process only reflects a generic approach and should be tailored by a process analyst to applicable needs.

The token born in the data subject section flows to the task “Submit erasure request” which triggers a message being sent to the data controller. The data controllers token is born at this start event. The token then flows to the identity check task and after the task is completed continues to the XOR gateway. Based on the results of the identity check the token either:

- a. Flows to the task ‘Request further information’
- b. Flows to another XOR gateway and continues based on if the data subject included the provision in the request or not to either:
 1. The task ‘Examine the application’
 2. The task ‘Gather all information’

If the token followed the “path b 1” and the task concluded that it is not possible to conclude under which provision the data subject requests the erasure the token continues to flow to the “Inform the data subject about improper filing”. After this task is completed the token dies at deny request. However, was it possible to determine the wants of the data subject, the token flows to ‘Gather all information’

Thus, whenever the request is filled properly (particularly if a from the data controller provided form is completed to satisfaction), the token will reach the task “Gather all saved information”. This stage is critical in the process as not only the saved personal data per se is of importance but also who this information was shared with and if some of that information was gathered at a point in time where the data subject was considered a child. While the exact implementation of this task is an individual process usually MDM, CRM,

data mapping, DMP²⁹, or other enterprise systems are used to create a holistic understanding of the data, how it is processed and where it is distributed. Once this task is completed the token will based on the findings flow to one of six tasks relating to the provision the erasure was requested upon.

If the request was made based on the assumption that data was stored which is no longer necessary for the reasons it was collected, the token flows to the task “Evaluate necessity of personal data”. At this task the relevance of the gathered information stored to the originally intended purposes of processing is evaluated. Information which is in fact obsolete and no longer needed must be marked for removal.

If the data subject withdrew its consent to the processing of his or her personal information, the collected data has to be removed if there are no other legal grounds for the processing of the data. The verification of applicable reasons to retain the data will be conducted at a later point.

In order to object the processing the data subject must provide reasoning as to why the interests of him or her prevail the public or controllers’ interests. [40] An evaluation of the circumstances has to be conducted by the data controller and a removal of the data has to be decided on a case by case basis. If, however, the data was used for direct marketing, no evaluation has to be conducted since it has to be removed from the systems.

Has data been acquired and/or processed through illegal means, the data must be removed. Such unlawful processing can arise if compliance with requirements is lost. While not explicitly stated in the GDPR the workflow recommends an investigation into why and how the data was processed and as to what mitigation steps can be taken to prevent this situation in the future. For that reason, a noncompliance report is introduced. This report should contain information about shortcomings, risks and opportunities regarding data processing and GDPR compliance. It also should have a section dedicated to the initiating event and the particular circumstances which led to the unlawful processing of the data subject’s personal information.

Local Union or Member state laws may dictate a removal of personal data upon request. If the business is operating under the countries jurisdiction and a data subject requests to enforce its rights entitled to by national regulations the data controller has to comply. The evaluation of the applicability of the quoted law by the data subject has to be evaluated.

Should none of the mentioned provisions apply, it needs to be evaluated if the data stored was collected from a minor. The definition of who is a child can vary from state to state. However, if such a request is made by the data subject, and it can be verified that at the time of collection the data subject qualified as a child, the data has to be removed even if the data subject no longer is a child.

The token continues independent of the applicable provision to the evaluation of restrictions which may make it necessary to retain the data.

At first, it continues its path to the right of freedom evaluation task. If the processing of the affected information is necessary to exercise the right of freedom of expression and information, the data is not subject to deletion. The right of freedom of expression and information trumps the right to erasure if the data is needed to form an opinion.

The next stop for the token is the evaluation of other legal obligations which have to be observed as they could prohibit the erasure. A legal obligation to retain information such as tax law could prohibit the destruction of some or all data requested.

²⁹ Data Management Platform

Public interest, in regard to public health, may prohibit the erasure. “Pursuant to this provision, viable reasons are preventive or occupational medicine, the assessment of the working capacity of employees, medical diagnosis, the provision of health/social care or treatment, the management of health/social care systems and services on the basis of EU or EU Member State law or pursuant to a contract with a health professional.” [38, p. 160] Therefore, a comprehensive review needs to be conducted as to if the information is in fact of public interest.

If the data collected is necessary for conducting research, may that be historical, statistical, or scientific research. Once the data becomes unnecessary, likely once the research is done and the results are complete, the data must be deleted. However, while the research is conducted if the stored information is necessary to continue, the data subject cannot enforce an erasure.

The token continues its path to the last evaluation stop. If there are currently legal proceedings ongoing which are relying on the availability of the information the interest of the data controller and maybe applicable legal obligations halt a deletion.

After examining all factors involved such as the provision under which a deletion is requested and the obligations under which a dataset has to be retained, a final decision about the necessity of the information and its processing has to be made. The token continues to a XOR gateway at which time it either follows the path of deletion or retention. If the data is retained, the task “Inform data subject about denial” is the next step. The data subject will be informed about the denial and given a reason as to why. At this point also for internal documentation purposes, a ‘Decision Report’ is created. The token then dies at “Request denied”.

If the path of deletion is taken, the data processor is to be informed about the deletion request. The workflow of the data processor is simplified, as the data controller needs a documentation of completion and no understanding of the proceedings other than the contracted requirements within which the processor is assumed to operate.

Under the GDPR, the data controller is also obligated to contact any other data controllers about the request to erasure. The token, therefore, moves from “Request deletion from processor” to the next task “Inform other data controllers”. At this step the collected information is reviewed a matched with any corresponding data controllers. Then the data controllers are informed about the request to erasure. The token continues its path to the next critical task.

At the task “Delete applicable dataset” the dataset and copies of it are to be destroyed. If information stored in backups has to be manipulated remains unclear as no legal certainty has been established in this regard. Anyhow, all reasonable and feasible steps to ensure a full erasure should be undertaken and checks for successful erasure should be implemented.

At the next task, a final report is created for internal documentation and proof of compliance. This report contains information of what data from whom has been when deleted, and also the official response of completion to the request made to the controller. This report can serve as documentation for compliance reviews and as evidence during legal proceedings. Therefore, it is highly recommended to involve a legal consultant in the construction of the policy and template defining the report.

The token then continues its path to the task where the data subject gets informed about the successful request fulfilment. If information was only partially revoked from the systems, it should be explained what was and what wasn’t part of the erasure and what factors were critical in making the decision. The data subject has the right to file a complaint with the supervisory authority. The token then moves on to die at the event “Request fulfilled”.

The data subject token moves after the task of submitting the request to an event-based gateway. If it receives a response from the data controller requesting more information the token flows to the task “File necessary information”. If, however, a response regarding denial or approval of the request is received, the token moves directly to that event. No matter the outcome in this simplified process, the token dies at “Answer to request received”. As the data subject process only serves a visualization purpose and could also be collapsed. The data subject could take other steps such as inquiring information about how long the wait for a response is. The law does state that the data subject has the right to erasure without undue delay. How long this timeframe is, is not yet quantified and will be decided on a case-by-case basis.

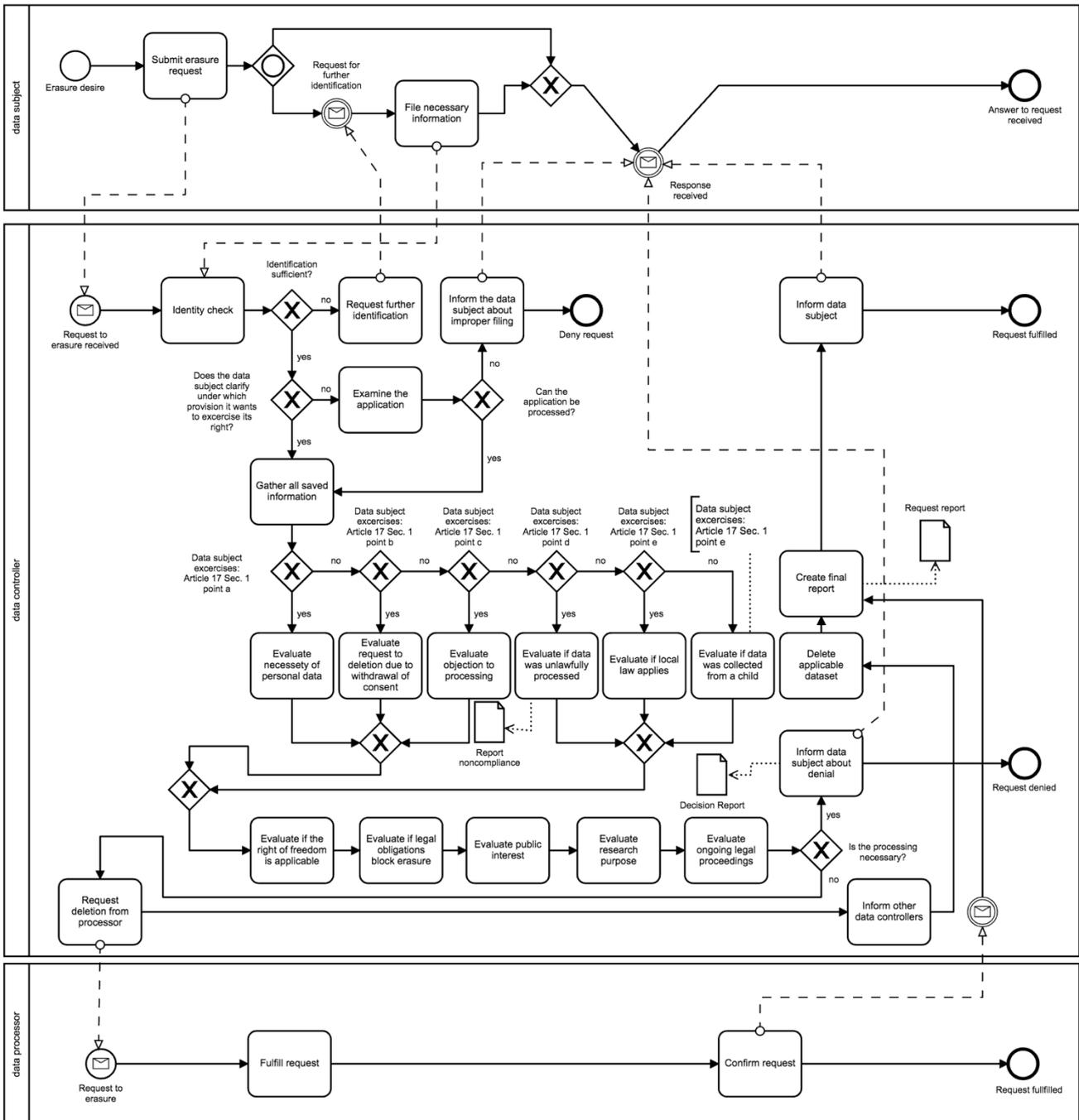


Figure 16 Right to erasure

4.1.4 Right to restriction of processing – Article 18 GDPR – Workflow

The right to restriction can be applied when the verification of the data subjects request, such as the erasure of the data, is delayed. Such a delay may arise when the interests of the data subject and the data controller collide, in which case the necessity of the deletion needs to be evaluated. Also, ongoing legal proceedings could hamper the verification process as it is necessary to determine if the data has to be retained to serve in court.

During this time the data subject has the right to restriction of processing [28], [38], [40] if one of the following applies:

1. The data subject protests and claims the data is not accurate/representing the truth. While the data subject is required to submit proof when making use of its right to rectification or erasure while basing it on the provision that the data is inaccurate it can take a considerable amount of time for the data controller to verify the claims. During this time the data subject has the right to restrict the data processing. If the data controller is unable to verify or deny the claims, the restriction has to be upheld.
2. The processing of the data has been conducted unlawfully and the data subject wants to restrict the usage instead of enforcing an erasure of the personal data. This may be of interest to the data subject if the data subject wants to use the information as evidence.
3. Similar to the previously mentioned reason, the data subject can restrict the processing of data if it will be used for the exercise, establishment, or defense regarding legal matters. However, it is mentioned specifically that this can be used to retain information that is no longer needed by the data controller for processing and thus would otherwise be erased.
4. If the data processor needs a considerable amount of time to come to a conclusion regarding the weighing of whose interests trump another's, the data subject can ask for restricted processing.

Figure 17 – “Right to restriction of processing” presents the corresponding workflow. Again, both the data subject and the data processor are only created to visualize proceedings within their respective domain. The workflow described in the data controller pool represents the conditions set by the GDPR Article 18 and can be used as a reference point.

The token is born when the data subject has a desire to have the processing of its personal information restricted. This desire can be based on one of the four aforementioned provisions. The token flows from its start event to the task “Submit restriction request”. At this point, a request including information about which data and under what provision it should be restricted is submitted.

The message flow leads to the start event in the data controller pool. From there it flows to the identity check task. This task could also be a subprocess, but in this case is displayed as a simple task. If not enough information to prove the data subject's identity was provided, a request to submit further material is sent to the data subject.

Once the identity is verified the token continues at the XOR gateway “Verification sufficient” towards the provision evaluation task. At this task, the request is processed, and it is determined if and what provision is applicable. If the data subject failed to provide the data controller with adequate reasoning as to why the

processing has to be restricted and as to what parts have to be restricted, the token follows the error event and the request gets denied.

If the evaluation was successful, the token continues its path to the parallel gateway. At this point another token is generated. One flows to inform the data processor about the restricted processing the other one flows to the information gathering task. At the “Inform data processor” task, a message is generated which triggers the start event in the data processor pool. While not displayed how the data processor fulfils its duties the processing of said data subject’s personal data is assumed to be limited from this point.

At the “Gather applicable information task”, all effected personal data should be marked for restriction additionally information about the current status of the initiating request which lead to the data subjects right of restriction such a request for erasure should be collected. If the initial request is already almost finished, it might present itself more practical to finish the first request and render the right to restriction obsolete.

Once this information has been composed, the token continues its flow and depending on which provision is applicable the token will stop at one of the following tasks:

1. During the verification of the accuracy of data concerning the data subject, the processing of such data will be restricted. If the data is, however, needed regarding legal matters, it can and shall only be used for such. Once the data has been verified regardless of the decision made the restriction will be lifted. If the data was, in fact, not accurate, the dataset needs to either be erased or the data needs to be adapted to represent reality.
2. The data subject requested to restrict the processing instead of the erasure of the data once it was determined that the processing had been unlawful. The data controller is obligated to keep the unlawful information stored for the data subject until the data subject has no further (legal) use for them, during which time the data processing is restricted. Once the restriction is lifted (the data subject gives the OK for erasure), the dataset has to be removed. If the data is needed for legal proceedings, the information can be used even while otherwise processing is restricted.
3. Similar to provision 2 the data processing has to be restricted from processing because the data subject needs the stored information for the exercise, defense, or establishment of legal claims. However, this time the data was no longer needed by the data controller regarding processing and is therefore subject to erasure. If the data processor needs to use the stored information in legal proceedings, he is allowed to do so. The data needs to be held until the data subject has no further legal claims and allows for the processing/deletion of the information. The workflow introduces an attached conditional task, if the data subject does not communicate how long the data needs to be stored for legal matters, the data controller has to contact the data subject and inquire about the current status.
4. While the verification process initiated by the data controller upon the objection to processing by the data subject is ongoing, the data subject has the right to restrict processing. Therefore, until the dispute is settled, no data can be processed by the data controller unless the data is needed regarding legal matters.

After the reason for restricting the data is obsolete, the token continues its flow from the respective task corresponding with the provision the data subject cited. All paths lead toward the task of informing the data subject about the imminent lifting of the restriction. While the GDPR clearly states that the data subject needs to be informed about the lifting of the restrictions it remains unclear if there needs to be proof that the data subject received the message. The task “Inform data subject about lifting of restriction” assumes that a

4.1.5 Right to data portability – Article 20 GDPR - Workflow

The GDPR introduces the right to data portability which is defined in Article 20 GDPR as follows:

“The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided [...]” [28, p. 45]

Easy and simple control over personal data is a key objective of the GDPR. The possibility for the data subject to retrieve and share stored information is fundamental to achieve this goal. Allowing the data subject to instruct the data controller to share the data on his behalf with other organizations is another step to minimizing barriers for the control over personal data by its owner.

On July 20th, 2018 the data transfer project was announced. Corporations such as Microsoft, Twitter, Google, and others work together to provide an open standard for data exchange. The goal is it to provide a suite of open source tools which allow the transformation of data retrieved by proprietary API's³⁰ in industry standard data formats which in turn can be easily exchanged [41].

In order for the right to be applicable several conditions have to be met. It is mandatory that the data which has been processed has been so by automated means. If, for example, the data subject only ever submitted information via a letter and the letter was filed by a manual task without it ever have been digitalized the data subject has no right for the data to be digitalized, duplicated or shared under this provision. The data must have been processed pursuant to Article 9 (2) or 6 (1), concluding that the data processed was so for the reason of the fulfilment of a contractual agreement or based on the consent of the data subject. The data is personal data if the data can be traced to the data subject even pseudonymized data is applicable to this right [38].

Figure 19 describes the process and the steps suggested for compliance with Article 20 GDPR. The workflow consists of 3 pools, the data subject pool is only representative and can only assume generic behavior. This workflow can also be collapsed like the “Third party” pool. That pool represents the receiving party of the data subject's personal data. The recipient of the exported data can also be the data subject itself.

The token is born when the data subject has the desire to retrieve personal data or to have its data transferred to another data controller. It then flows to the first task which is filing for said transfer. This task triggers a message flow which leads to the start even in the data controller pool.

The data controller needs to disclose possible communication channels via which requests can be made to data subject. These requests could be made through various channels such as letter, e-mail or in person. For this example, it is assumed that all communication with the data subject is conducted via e-mail and that standard forms for requests regarding the GDPR are made available to the respective data subject. Once the inquiry was received the token continues its path to the first task, the verification of the data subjects' identity. The identification process could be also visualized as a sub-process as it is used by various processes. This thesis offers in a later section an example workflow for an identity check.

The token continues its way to an XOR gateway at which point the token can either continue to the task “Request further identification” or to the task “Collect applicable data” depending on the results from the identity check. If the information was lacking sufficient evidence of the inquirers real identity, a request to

³⁰ API – Application Programming Interface

submit further documents has to be made. If the identification was sufficient, the collection of applicable data can be started.

During this task, all personal data will be collected this can include depending on the service which is provided to the data subject information of third parties (chat protocols, historical interactions with other users, pictures of multiple personas etc.) and thus has to be evaluated in a separate task. Additionally, some data may not be eligible to be transferred due to technical restrictions or them not being processed under provision 1 (a) of Article 20 GDPR. Once all information was collected the token continues and flows to the task 'Check for eligibility'.

At this task, it needs to be determined if the data meets the requirements to be eligible for transfer under the provisions of the right to data portability. Thus, a review of the collected data must be conducted in which the data is classified and marked if there could be legal reasons for them to not be eligible. Additionally, it needs to be verified that it is possible to export the data in a machine-readable standardized format. In case the data controller processes a particularly large data set, regarding the data subject, the data controller can ask the data subject to specify which data shall be transferred in particular if he hasn't done so. A standardized form provided by the controller to the data subject allows for faster processing of the request. If the data has been processed under the means of Article 6(1) or 9(2) of the GDPR and said data has been processed via IT systems the data renders eligible but still has to be evaluated for legal obligations which prevail the right to portability [38]. Has the affected data never been digitalized or has it been processed by other means than Article 6(1) or 9(2) the data is not eligible. In this case, an error boundary event lets the token flow to an XOR gate which unites the paths the token can take when the request is denied.

Once the data has been verified to be eligible the token continues down towards the "Check for legal obligations" task. This task is intended to ensure any action is conducted in compliance with the GDPR requirements. Thus, it needs to be evaluated if the rights/freedoms of third parties are affected or if the data was processed in public interest or if the data was processed by an official authority. In those cases, such a transfer would be unlawful. If some of the data cannot be transferred due to one of the mentioned reasons, the data controller shall provide anonymized or limited datasets [42]. If none of the can be transferred, the token continues its path to the XOR gate which unites all incoming paths leading from error events to a documentation task.

The task "Document dismissal" is intended to create a report on the dismissal of the transfer request. It shall contain information as to which legal obligation or interest has prevailed the transfer. It shall be concise and clearly state how the decision came to be. This document can serve as evidence if the data subject files a complaint with a supervising authority.

The token then continues to the task "Inform data subject about denial" at which time the data subject is provided with the circumstances and reasoning as to why the request is denied. Once the task is finished, the token flows to the event request denied, and dies.

Alternatively, after a check for legal obligations it is determined that some or all data is eligible to be transferred to another data controller or to the data subject. Therefore, the token flows to the task "Export collected data". During this task, all data which has been collected is exported from the IT systems in a machine-readable format and packaged in such a way that it can be read by another party.

Once the data has been exported the token continues its way to the XOR gateway at which time it either continues its path toward "Send data to data subject" or to "Send data to 3rd party". In order to perform either task a channel to the recipient has to be established. In case of the data subject providing a link to a secure storage from where the data can be retrieved only by the data subject through the simple download of a compressed file containing the personal information can be sufficient.

If the data is transferred to another data controller, established means shall be used. While standardized formats such as XML, PDF, or Office formats can be assumed to be state of the art, different projects are set to establish a standardized way such as the introduced data transfer project. If the intended recipient cannot be contacted, and no data can be transferred, an error occurs.

This error triggers an error boundary event “Data cannot be transmitted” and leads the token to the task “Inform data subject”. At this task, the data subject is informed that transferring the data renders impossible due to the unavailability of the recipient. The token then dies at “Request completed”.

Has the data been successfully shared, the token flows to “Inform data subject & document”. A final statement is sent to the data subject including when and what data was sent and to whom. Additionally, a final report is created on the fulfillment of the task.

The token continues its path to the end event “Request fulfilled” where it dies.

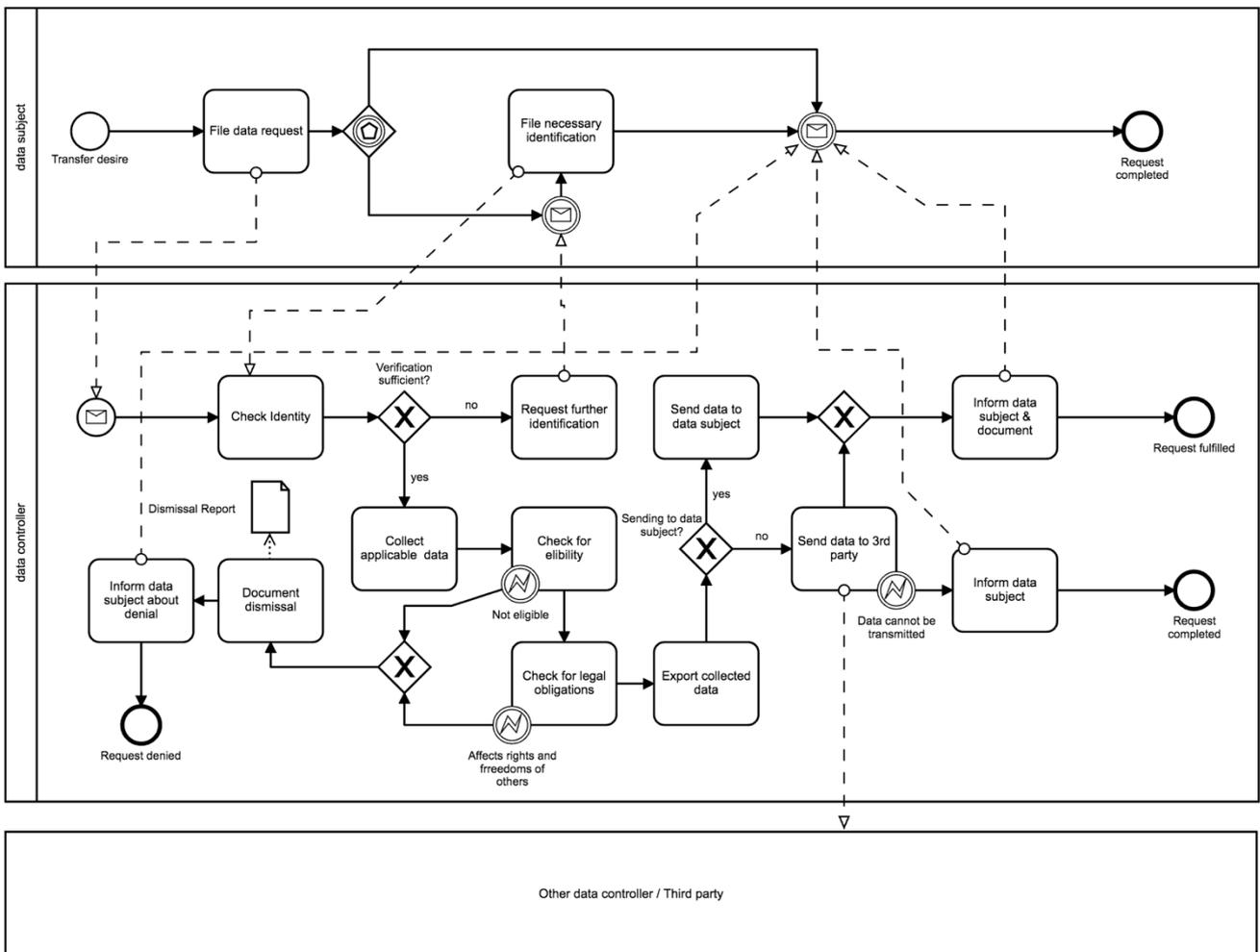


Figure 18 Right to data portability

4.1.7 Right to object – Article 21 GDPR - Workflow

The right to object only applies when certain conditions are met, therefore it is important for the data controller to verify the circumstances before carrying out a request. Every case has to be individually reviewed because the right applies only to the specific circumstances concerning the data subject [28].

The data subject can challenge and object the processing of his or her personal data which has been lawfully processed under the provision of necessity due to public interest, legitimate interest of a third party, legitimate interest of the data controller, or which has been processed by a public authority. The right to object the data processing originates from particular, distinguishing circumstances unique to the data subject. These circumstances have occurred after the processing of the personal data has started and therefore the right to objection became relevant [40]. Only if the data controller determines that his own interests still prevail the freedoms, rights, and interests of the data subject or if the data is needed for legal proceedings the data subjects' data can be further processed. The data subject may file a complaint with the supervising authority to challenge the decision. Decisions are to be made on a factual basis and well documented in order to prevent the applicable fines for non-compliance.

Is the data which is the subject of the processing is used directly for marketing the data subject has the right to object the processing. Such direct marketing can arise from individualized offers as in e-mails, banner advertisements on websites, or be done by other means. The key factor is that the data has been used to create a profile of the data subject which is used to deliver custom advertisements. No further conditions have to be met by the data subject and the processing of its personal data has to be seized without unnecessary delay by the data controller [38].

Has the data been used for scientific, statistical, or historical research purposes the data subject can object to its processing if he is particularly affected by it. However, this right is barred if the public interest trumps the interests of the data subject. The data controller has the burden to evaluate which interest prevails, and continue processing or seize processing based on the findings. This is done by the data controller demonstrating the necessity for processing [38].

The data subject can execute this right at any given time and has to be informed about it at latest during the first communication with the data subject. It is recommended to provide the data subject with a standardized request form to improve the process execution and prevent resource intensive additional steps to ensure the accuracy of the performed work.

Figure 20 has been designed to introduce an example workflow regarding the necessary steps to be taken by the data controller if a data subject submits a request to seize the processing of personal data based on the right to object. Both the data subject and data processor pool only serve illustration purposes and do not resemble accurately all steps taken by those parties.

The token is first born in the data subject pool at the start event which is to show a desire to have the processing restricted within the data subject. The token flows to the first task which is the data subject filing an objection to the current processing. If the data subject were to provide an online portal, a form, or another standardized way for the data subject, such a filing could be more efficient and easier to process. Following the message flow down from the data subject pool to the data controller pool the start event from the data controller is triggered.

The incoming request leads to the first task. An identity check has to be conducted before any of the information is reviewed. Information which can serve as proof of identity and how to conduct an identity check is discussed in the section "Identity Check – Workflow". However, if the environment within which these checks are conducted allows for it to be a single task (an assigned data protection officer verifies the digital signature),

a subprocess may not be needed. Therefore, it is illustrated as a simple task. The token continues its path to the XOR gateway at which it based on if the information was sufficient either carries on towards “Request further identification” or “Screen request”.

At “Request further identification”, an attempt is made to contact the data subject to provide further specific proof of identity. If the subject fails to do so or failed to provide any contact information, an error event within the task “Check identity” leads the token to Request denied where it dies.

Has the identity check been conducted and the result was positive, the token reaches the request screening task. This task is intended to check if all information needed for further evaluation is available. Additionally, it is determined under which provision the data subject objects any further processing. If information as to how it affects the data subject and which if not all of the information processed is affected a request is made for further information. If the data subject fails to submit such information the task has an error catch event built in. In case the request renders invalid the token takes this alternative path and dies at request denied.

Once the necessary information was gathered the token continues to the task “Collect applicable data”. At this point the data controller knows:

1. Who sent the request
2. Which data is of concern
3. Which circumstances have changed **according to the data subject**

For a full evaluation of the data subjects’ objection request all data which is applicable (personal data sourced from the data subject or third parties about the data subject) is collected. The token continues its path then to a XOR gateway. If the personal data is used for marketing, the token continues straight to the marketing task.

At this task, it is evaluated if all data has been used for marketing purposes. The affected data cannot be processed any longer and the request to stop the processing is granted.

Has the data been processed pursuant to public interest the data subject’s situation needs to be weighed against the public interest. If the data renders necessary, the data controller needs to prove the public interest and can continue the processing. One output of the task is a decision report, which allows for the data controller to verify at a later point the compliance to a supervisory authority or it can serve as evidence during legal proceedings. Even though the processing needs to be stopped once the request is granted data can be processed for legal proceedings.

Is the continuous processing necessary based on interest originating from the data controller or the data controllers role as public authority, the newly arisen circumstance have to be evaluated. During this task the information provided by the data subject is reviewed, verified and balanced against the legitimate reasons of the data controller. Again, a decision report which serves as documentation on the decision is created and filed.

All three tasks share a common ambition; determining if the data processing can be continued lawfully or if the processing has to be halted. If the evaluation concludes that the data subjects’ request to block the processing is valid the data subject has also the right to erasure of said data. While out of scope for this workflow, the data subject can separately file for an erasure of the personal data.

The token flows towards a XOR gateway, at which time it continues its path based on the results from the evaluation. In case of a negative result, the data subject is informed about the denial. This includes

reasons as to how the decision came to be and why further processing is lawful. The token then dies at “Request completed”.

While if the evaluation concluded positive in the interest of the data subject the token splits and both the processing is halted and any data processor, processing the data subjects information contracted by the data controller is informed to halt such processing as well.

At the parallel gateway, both tokens need to arrive before one single token may flow to the “Inform data subject about approval” task. The objective of this task is it to contact the data subject and inform it of the halted processing and therefore the granted request. If the data has to be processed for legal proceedings the data subject shall be informed that processing is stopped unless it is for that specific scenario necessary to do so.

The token flows to and dies at the task “Request completed”.

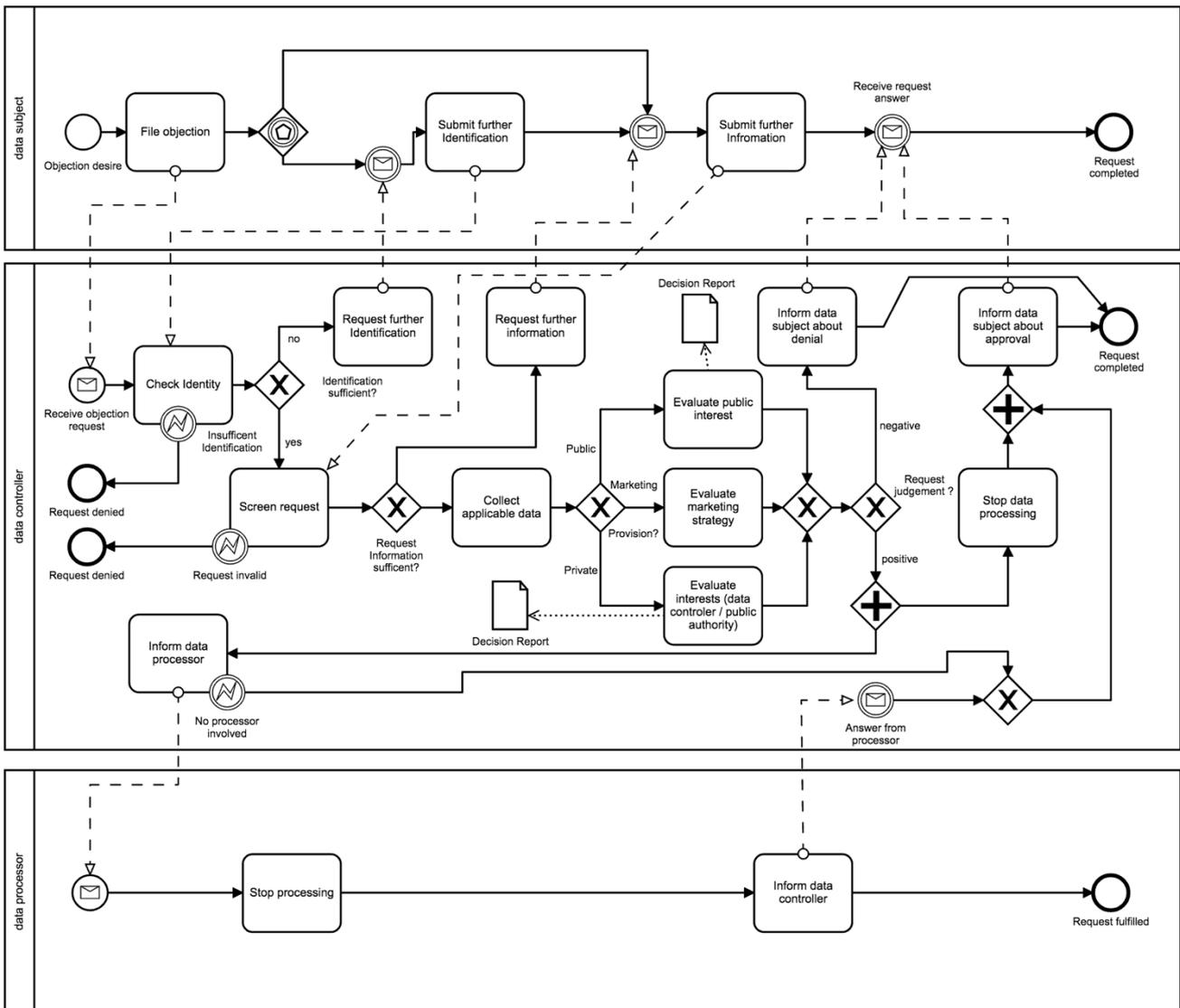


Figure 19 Right to objection

4.1.8 Automated individual decision-making – Article 22 GDPR - Workflow

Under Article 22 the GDPR, the data subject holds the right to not be subject to automated decision making, it is defined as follows:

“The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.” [28, p. 46]

Certain restrictions apply to the right, if they come into effect automated decision making may be applied. Those restrictions are as follows [38], [40]:

- A contractual agreement has been made with the data subject and in order to be able to fulfil the terms set in the contract the personal data has to be automatically processed. This may be due to technical requirements or due to legal circumstances.
- Applicable national laws may dictate the automated processing by the data controller, such as for taxation purposes or for national security interests. The data subject has no option to withdraw its information from such processing and the data controller is under the obligation to have state of the art safety measures implemented to protect the data subject's rights and freedoms.
- The data subject gave direct consent and explicitly confirmed his consent to the automated processing conducted by the data controller.

Automated decision making is employed when no human has the option to manually change the outcome in a final revision step or when no humans have decision-based tasks during the processing. Any supporting task carried out by a human such as data input does not change the fact that the decision making is conducted by automated means.

It remains unclear if the right to not be subject to automated decision making is implied, or if the data subject has to proactively exercise the right [39]. Therefore, the introduced workflow may render not applicable or necessary to be implemented. It serves the purpose as an illustration of how a request to opt out of automated decision making could be processed. Once legal certainty is established, an understanding about the necessity of such an implementation or the seizure of all automated decision making unless specifically approved may be determined.

If profiling a data subject or if data regarding attributes of the data subject is processed in order to form an opinion about the data subject which is later applied to make a decision, the profiling process is also prone to be opposed by the data subject. Hence the data subject has the right to not be subject to profiling if it affects him or her significantly [28] [43].

Figure 21 serves as an example to how the process if it renders necessary can be implemented by an organization. The process contains a data subject who objects automated decision making, the data controller, and a data processor. The data process is only illustrated as a collapsed pool due to the focus being on the implementation of the process within the data controller's environment. The data subject pool is only a simplified procedure of the steps taken by him or her.

The token is born in the data subject pool when the data subject desires to have no further decisions made by automated processes. The token then flows to the first task which is the filing of a request. The request describes that the data subject objects to any automated decisions and triggers a message flow to the start event in the data controller pool.

Once the message is received the token flows to the first task; checking the identity of the data subject. Only if the data subject is able to prove his or her identity, the request will be considered. If the proof of identity is insufficient, the token continues to the task “Request further identification”.

After passing through the XOR gateway, the token reaches the task “Request further identification”. A form is transmitted which states what information is missing and how the data subject can prove its identity and resubmit the missing information.

Has the “Check identity” task concluded that it is not possible to determine with certainty the origin of the request, the request is denied. However, has the identity been successfully confirmed, the token flows through the XOR gateway to the “Check Request” task. At this task it is evaluated under which data subject right and which provision within the right the request is made. Additionally, it is determined if the data subject submitted all necessary information to evaluate the case. Such information can be i.a.³¹ affected data, affected contract, circumstances, hardship on the data subject, or proof of hardship. Is mandatory information missing and any evaluation is impossible the request is denied due to insufficient evidence.

If the request is accepted, the applicable information is collected. Any and all information regarding the data subject which has been processed by automated means to make decisions, including profiling, has to be compiled. This includes information concerning why the processing was conducted and which processes and systems are involved. Once the information has been collected, a report of the exact circumstances regarding the data subject can be created. This report is used to determine the necessity of further automated decision making.

The token continues to the parallel gateway where it is split into three. One token continues to the evaluation of contracts task where it is evaluated if the data subject and the data controller have agreed to a service delivery which is dependent on automated processing. This process resembles a bank processing a credit score and determining the risk involved to then be used to determine an interest rate. If the processing is in fact necessary, for this reason the automated decision making is allowed to continue.

Token number 2 continues to the legal evaluation of the situation. If local laws dictate automatic processing the data subject has no right to object. If it is known that the requested automated processing is the result of regional laws, this can be simply stated, however if it is only necessary in a case to case basis. It is recommended to entrust the legal department with this obligation.

The 3rd token continues to check if explicit consent was given by the data subject. If the data subject has in fact given such explicit consent and is unable to withdraw the consent at the moment based on agreements made the processing and decision making is legitimate.

At the following parallel gateway, the three paths from the task unite. Once all tokens arrive at this point, one single token is sent to the XOR gateway. If only one of the three evaluations concluded that the automated decision making can be continued lawfully the request is denied and the token flows to “Inform data subject about denial”.

When the data subject is informed about the negative response to the received request, a report which states on what grounds the decision was made shall be included. The token then dies as the request was completed.

³¹ i.a. inter alia (among other things)

If, however, no legal reason was found, the token continues to the parallel gateway at which time it splits into two. One continues to inform any data processor about seizing the automated profiling/decision making on behalf of the data controller. If no data processor is involved, the token dies.

The other token continues to the task where a determination is made if the service provided can be provided through non-automated means. If it is possible to replace the automated decision making and employ a human based approach, the token continues upwards to “Ensure no further automated decision making is conducted”.

At this task, measures are taken to ensure the data subjects’ personal information is no longer subject to automated decision making. This can in some cases be done with as little effort as setting a flag, or it may need some more elaborate work.

Has it been determined that the services provided can no longer be conducted the data processing has to be stopped.

In either case the last task is to inform the data subject about the approval and the completion of the request.

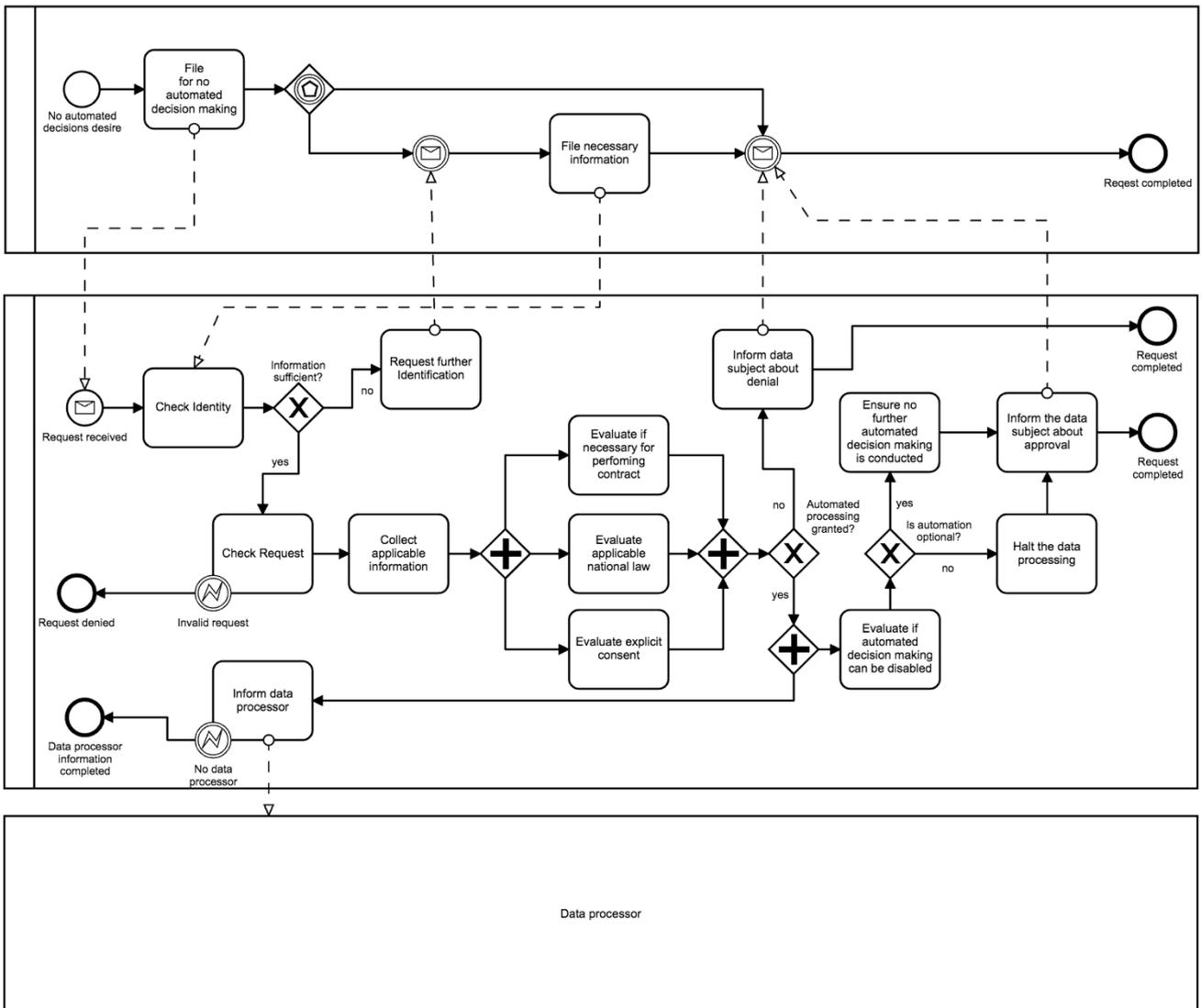


Figure 20 Right to not be subject to automated decision making

4.2 Workflows – Other

Section 4.1 was primarily concerned with the data subject rights and how compliance with these can be achieved. Introduced workflows in BPMN 2.0 notation are designed to help a transition toward the fulfillment of the requirements introduced by the GDPR.

This section is concerned with introducing workflows beyond the scope of data subject rights. The workflows introduced within this chapter are dealing with the following types of tasks:

- Notifications
- Verification
- Requests (other than from the data subject)

The GDPR introduces a set of mandatory notifications to be made by the data controller. One of them is the notification obligation. In case any information was rectified upon request of the data subject or any information was erased after the execution of the right to erasure, the data controller has to issue a notification toward the past recipients of the affected personal data. Section 4.2.1 introduces a workflow to comply with said requirement and provides further information on the subject.

If a data breach occurs, the data controller has to notify the supervising authority. Sometimes at a delayed point in time due to ongoing criminal investigations the data controller is required to inform the data subject which has been affected by the data breach about the security incident. Both of these notifications are discussed in section 4.2.2 with an BPMN process workflow describing an example procedure which can be used and adapted freely.

There are further notification obligations the data controller has to conduct. Their nature, however, is implicit, meaning that they are repetitive and not reactions to an incident or request. Among these notifications is the obligation to inform the data subject if data was collected from third party sources when profiling is conducted or the rights a data subject has.

It is a necessity to conduct a verification on both the identity and on the information provided by the data subject. Within this chapter, section 4.2.3 introduces a sample workflow for identity verification. The need to introduce an entire workflow for such an endeavor arises from the complexity and type of information which has to be verified, and the size of the organization. It is a perfectly valid solution to have one centralized verification role but through the introduction of parallelization within the organization it is recommended to introduce a well-documented workflow on how a verification of information has to be conducted. Additionally, the GDPR extends rights to minors and if information of children is processed, the identity of the person bearing the parental rights has to be confirmed before any processing can be lawfully conducted.

Incoming requests can arise from sources other than the data subject. While requests from law-enforcement in regard to criminal investigations concerning one or more data subjects' personal data is out of scope of this thesis. A look at requests from a supervising authority is taken in section 4.2.4. Those requests can arise from random compliance checks or can be triggered after a data subjects files a complaint about the handling of his or her personal information by the data controller. It is important to have a well-documented procedure and fact-based decision making in order to avoid the high fines introduced by the GDPR. Any requests from local authorities or requests arising from laws other than the GDPR are out of scope and not discussed.

4.2.1 Notification obligation – Article 19 GDPR – Workflow

Article 19 of the GDPR states:

“The controller shall communicate any rectification or erasure of personal data or restriction of processing carried out in accordance with Article 16, Article 17(1) and Article 18 to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients if the data subject requests it.” [28, p. 45]

Therefore, a procedure needs to be implemented to inform parties which have been supplied with the affected information. The information is not optional unless it would take a vast amount of resources to contact the recipients. This would arise if it is no longer known who the recipients have been or the amount of recipients proves to be extremely big [38].

Figure 18 introduces a workflow which is designed to comply with GDPR requirements while being adaptation friendly when it has to be modified to meet the particular circumstances for any business’s needs. The process only consists of one pool which represents the duties of the data controller. It is optional to introduce lanes representing the roles within the organization. Due to the wide variety of possible combinations, a single lane approach has been chosen.

The token is born once a data subject has successfully enforced its right to erasure of personal data or restriction of processing of personal data. The token then continues its path to the first task which is the evaluation if a legal obligation to inform recipients persists. A review of article 16, 17 sec.1, or 18 apply. If this is the case, the token continues to the compilation task. If not, the token continues directly to the “Inform Data subject” task.

The compilation tasks purpose is to generate a list of past recipients and the known communication channels. It outputs a document containing all the known recipients.

The token continues then and splits into two, one of them informing the data subject about the recipients, and the other one continuing to the effort evaluation. The obligation to notify all recipients does not prevail if the effort to do so is disproportionate. Therefore, a weighing of the data subject’s interests and the corporations interest must be conducted.

The token then continues its path based on the evaluation to either the task of informing all recipients or the task of informing the data subject about the denial to notify.

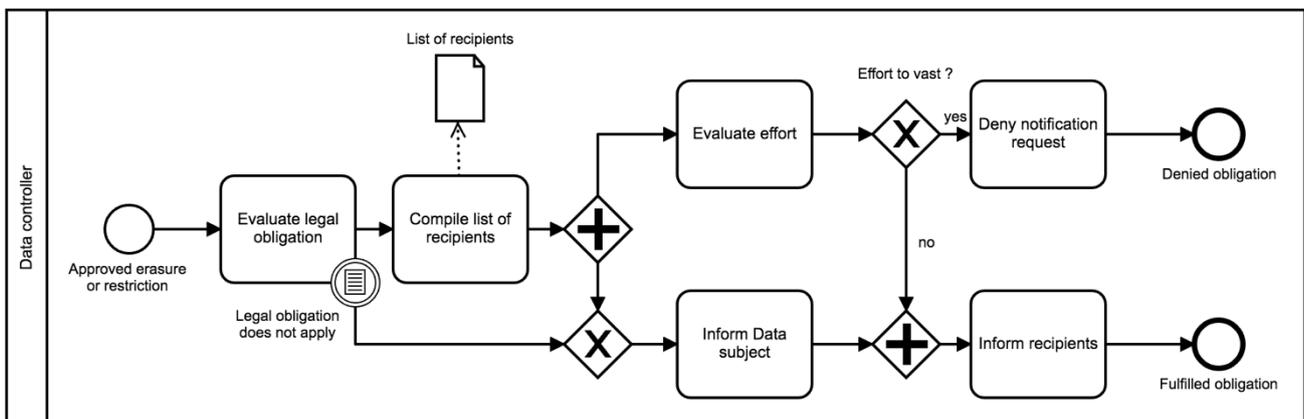


Figure 21 Notification obligation

4.2.2 Data breach notification (supervising authority)- Article 33 GDPR – Workflow

The data controller is under the obligation to file a data breach notification with the supervising authority. It is defined by the GDPR Article 33 as follows:

“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.” [28, p. 52]

This notification duty was introduced by the GDPR to ensure the protection of the rights and freedoms of the data subject. As stated above the data controller shall issue a notice to the concerned supervising authority within 72 hours, if the data controller fails to do so without sufficient proof of the necessity of the delay the data controller is subject to fines up to 2% of the annual turnover or up to EUR³² 10,000,000 [38]. While the data processor has no obligation to inform a supervising authority directly, it is under the duty to inform the data controller immediately. If it fails to do so, the same fines as mentioned apply to the data controller. Once the data controller has gained knowledge that some form of data breach has occurred the 72-hour time window to issue a notification to the supervising authority is opened. Due to the fact that no legal certainty regarding the confinements of provisions has been established, it is unclear whether the time frame which in the notification has to be made starts already once the data processor becomes aware of an occurred data breach [39].

Due to the fact that a data processor does not fall under the category of a third party [28], a controller could be held responsible for inaction taken by the data processor. However, a legal discussion is out of scope. To accommodate the situation, the data processor is illustrated in the form of a separate pool instead of being part of the external informant pool within the workflow introduced at a later point in this section.

The little amount of time between the detection of a data breach and the notification sent to the supervising authority will likely not allow for a thorough analysis of the occurred incident. However, if at any point within the investigation it renders necessary to issue a notification to reduce negative effects on the data subject the data controller has to do so with undue delay [38].

The data controller has the option to postpone a notification about the data breach if he has legitimate grounds to do so. The GDPR does however not define what legitimate reasons can be cited as reasoning for such a delay. If the supervising authority does not share the opinion of the data controller on the grounds and reasons as to why the information was transmitted after the 72-hour window the data controller is subject to be fined.

Further exceptions which may render a notification unnecessary apply. If the data breach will or will not be extremely unlikely to cause “[...] damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorized reversal of pseudonymization, damage to reputation, loss of confidentiality of personal data [...] economic or social disadvantage [...]” [28, p. 16] no notification has to be issued to the supervising authority. If, however, the data controller fails to issue a notification and the rights or freedoms of the data subject are affected by the breach, even in a minor way, the data controller is subject to fines. Therefore, it is recommended to have a very low border above which a notification is issued [38].

³² EUR - Euro

It is mandatory for the data controller to document any data breach which occurs. This documentation is used as evidence if an audit is conducted. Failure to sufficiently document a data breach or document the breach at all can lead to financial penalties. Therefore, any documentation procedure should be well documented and consist of any valuable information regarding the incident.

A notification intended to inform the supervising authority shall contain the following information:

1. What kind of data breach did occur, if available it also should contain information about the number of affected individuals, the sensibility of the data, and how many personal data records have been leaked.
2. A channel for communication needs to be established, usually the contact information of the data protection officer is exchanged to whom may be fulfilling the same position in the applicable organization.
3. If it was possible to determine what data has been leaked, information about the severity and thus the consequence of the leak shall be included. This by no means needs to be a comprehensive statement but rather an approximation as the time to conduct an investigation in the matter has been very short since the discovery of the incident.
4. A statement about the mitigation steps which are or will be taken to minimize any negative effects.

Once this information is gathered the statement is to be sent without undue delay to the supervising authority, if some of the information was unavailable at the time when the notification was due the information can be supplied at a later point, but without undue delay once it renders available.

Figure 22 introduces a workflow to create and send a notification to supervising authority which meets the requirements introduced in Article 33 of the GDPR. The workflow introduced focuses on the notification mandatory toward the supervising authority. Notifications send to the data subject are covered in Figure 23. Both external informants and the data processor are illustrated by collapsed pools. In order to provide a clean and readable strategic workflow the data supervisor was not visualized.

The token is born at one of three start events. The start events differentiate themselves from how the data controller learns about the occurred data breach. Information about the incident can either be received from a third party (External informant), the data processor, or be discovered internally.

If information is received from a third party an internal investigation is launched. Depending on the contents of the message received a data breach procedure is initiated. A data breach could also be detected by internal resources. Such a detection can happen during a security audit, through live monitoring or because of an unrelated forensic examination. At last, the data processor is under the obligation to inform the data subject if during his operation personal data was leaked. If that were the case the steps shown in the workflow still apply but would be conducted with close involvement of the data processor. Regardless of what imitated the process the token flows through a XOR gateway to the first task “Inform DPO³³”.

The GDPR requires the organization to nominate an individual responsible for the compliance with GDPR requirements. This role can be named freely, but DPO is the name used throughout the regulation. This

³³ DPO – Data protection officer

person will have oversight on the investigation and conduct the necessary steps to be compliant with requirements.

Depending on the existence of emergency plans within the organization the token continues its path beyond the XOR gateway. Assuming an emergency-plan is in place for this situation the plan is followed. After 70 hours, a conditional event triggers the task to ensure a breach notification is sent within time limits. A parallel gateway splits the token and the second token triggers a documentation process.

The documentation process runs parallel to the internally defined procedure on how to handle a security incident. All information of value regarding the incident is recorded and finalized in a data breach report. If at any point during the review of the incoming information the DPO decides that the impact on the data subject will be severe, the data subject is informed with no delay. In case the data subject is informed, the supervising authority will also be informed. In case the emergency plan came to no end before the 70-hour mark, the documentation process triggers a timing event. At this point both tokens are on their way to the parallel gateway. Once they arrive there, one token continues to a XOR gateway. If the evidence suggests that the rights and freedoms of a data subject could be endangered the authorities are informed, if however, no notification is mandatory the internal investigation is continued.

Alternatively, no emergency procedure is in place to deal with security incidents. In that case, the token flows at the “Documented Emergency Plan” XOR gateway downwards on the “no” path. The token is split at the parallel gateway and both tokens continue their path. Similar to if an emergency procedure is in place, a documentation task is started which runs parallel to other duties. The token not continuing to the documentation task continues to the “Gather information” task.

At that task, information about the incident, such as which systems and what data was affected, over which period of time, how the information was leaked (malicious attack or mistake, internal or external). While the analysis of the incident can take longer than only 72 hours this process is particularly concerned with collecting the necessary information to file a complaint with the information requested in Article 33 GDPR provision 3 a-d.

Once the necessary information has been collected, the token continues its path to the next task. At this task, the collected facts will be used to evaluate the impact on the business. How many personal data records are affected, how many data subjects are involved in the breach. What categories of information have been leaked. As soon as this information has been gathered the token moves to the next task.

At this task the consequences of the data breach are evaluated. The gained information is taken into account and the effects of the breach are weighed to make a judgement on how critical the current situation is and if authorities or the data subject need to be informed immediately. In case the DPO decides that the resulting vulnerability of the data subjects is critical the data subjects are informed immediately about the incident.

Once the evaluation phase has been concluded the token moves to the task “Implement or develop mitigations”. Measures include both mitigation against a recurring data leak and against the negative consequences data subjects may encounter after their personal data has been leaked. If possible, measures shall be taken immediately, but even measures which are in a planning stage need to be documented and included in the data breach notification sent to the supervising authority. The token then continues its path to the parallel gateway.

At the parallel gateway the token awaits the token from the completed documentation task. If the documentation task exceeds the time limit of 70 hours a catch event will ensure a notification of the supervisor authority within the limits.

Has the investigation successfully collected, all necessary information to file a proper data breach report with the supervising authority before the 72-hour time limit the token meet at the parallel gateway. The following XOR gateway marks a decision point. If the DPO concludes a threat for a data subjects' rights or freedoms the supervising authority is informed.

When officially submitting the data breach notification, it consists of contact information and the information required by the GDPR introduced in the beginning of this section. The token continues its path and dies at "Notification sent".

If the internal investigation concluded that no data subject is at risk, as could be the case if the data was strongly encrypted, the data controller is under no obligation to share information of the incident with the supervising authority at the moment, however every data breach needs to be documented and achieved and available to be reviewed by the authorities.

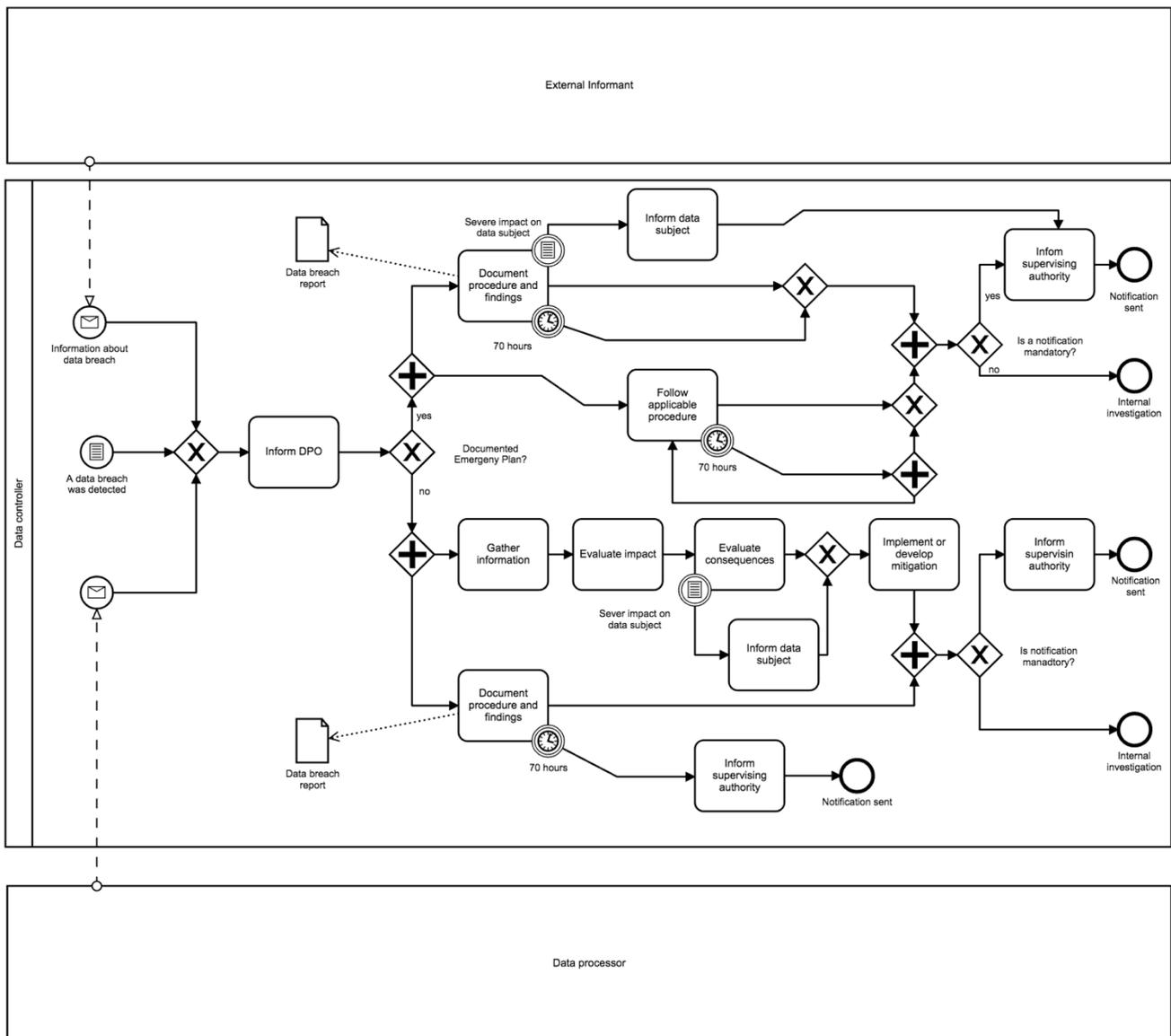


Figure 22 Data breach notification – supervisory authority

4.2.3 Data breach notification (data subject) – Article 34 GDPR – Workflow

A personal data breach occurs when personal information about the data subject is lost, altered, or if the data was accessed, transmitted, stored, or processed without permission [38]. Only if the data subjects' rights and freedoms were compromised, the data controller needs to inform the data subject. If sufficient safety measure such as state of the art encryption was employed, no notification is necessary.

It is irrelevant if the breach happened through malicious means or by accident and it is irrelevant if the breach was physical or digital. If it is determined that the data subject has to be informed about the breach the notification has to be conducted without delay, the writing of the notification has to be in simple and clear language and should contain information about the incident. Additionally, measures to mitigate the impact of the breach shall be provided [28].

In case the supervising authority determines that the data breach triggered a risk for the rights and freedoms of the data subject, the supervising authority has the power to require the data controller to issue a data breach notification toward affected data subjects. However, if one of the following applies the communication with the data subject is not required [28]:

1. The data leaked has been obfuscated through technical means by the data controller.
2. The data controller has implemented mitigation steps to reduce the risk to the data subject to a negligible level.
3. The effort to contact all individual data subjects is disproportionate, an alternative such as a public announcement can be performed.

Figure 23 shows an example workflow designed to help the compliant implementation of the requirements introduced in article 34 GDPR. It consists of a collapsed pool representing the supervising authority, a data controller pool, and a collapsed data subject pool.

The start event is either triggered by the DPO or by the supervising authority. In case of the supervising authority, a message is received which creates the token. The token then flows to the first task; the evaluation of the order received by the authorities. The documents are checked for accuracy and it is determined if any of the exceptions are applicable and thus such a request is invalid. The token continues based on the results to either reject the request or to evaluate the risks for the data subject.

If it is determined that point a, b, or c of provision 3 Article 34 apply a formal request to re-evaluate the decision is made. Including evidence supporting the reasoning behind the refusal to carry out the order received.

Was no reason to decline determined, the token flows and meets with the stream coming from the optional DPO start event at a XOR gateway.

The DPO can decide that based on the available information it is necessary to inform the data subjects about the breach. A failure to do so would lead to non-compliance and the possibility to receive high fines. The token goes through the XOR gateway which connects the two start events and unifies them into one stream.

At the first task after the gateway an evaluation about the impact on the data subject is conducted. To do so, available information about the leaked category of information is referenced with the processed and affected data of each individual. If this is impossible due to a missing implementation of automation or a

shortage of other resources and the effort renders disproportionate, the data controller can instead evaluate alternative options such as making a public announcement about the incident.

Once the evaluation is completed, the results are saved to an impact report and the token continues to the next task. At this task mitigation steps to the discovered risks are developed, evaluated, and assigned. The information gets added to the impact report and the token moves on.

At the next task the developed mitigation techniques are matched to the fitting affected data subjects based on the concerned data categories and processed information. With this information individual reports are created to comply with provision 2 of Article 34. The instructions and explanations are to be in clear and simple language.

The token continues its path to the “Inform data subject” task. At this task the data subject is informed of the data breach and is given the report containing information about the concerned data, the risks arising from the breach and how to take precaution.

At last, the token dies once the notification was sent at the end event.

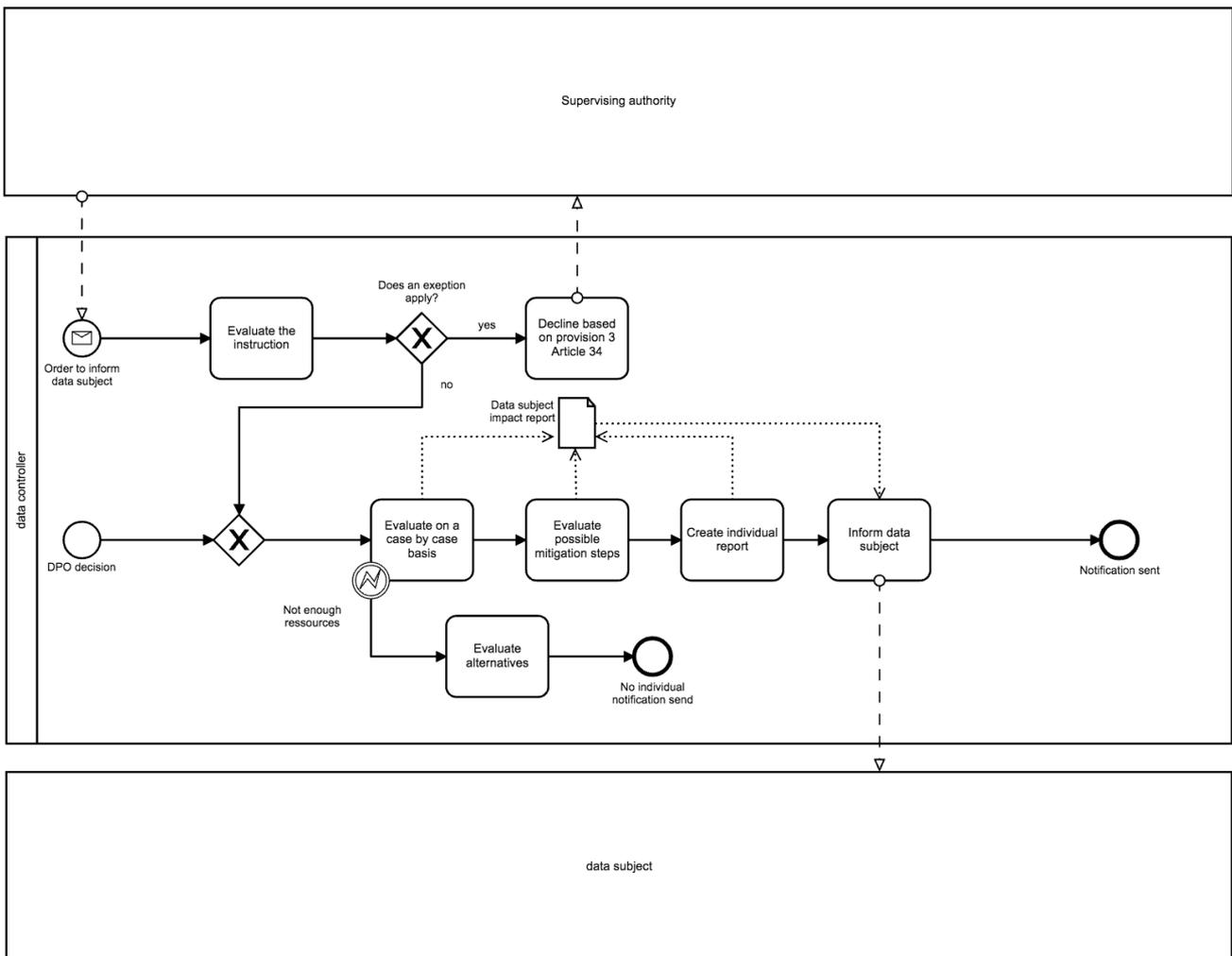


Figure 23 Data breach notification – data subject

4.2.4 Identity verification – Recital 64 GDPR – Workflow

Introduced in recital 64 of the GDPR is the duty of the data controller to verify a data subject's identity. Additionally, Article 12 provision 6 specifies the request for further identifying information if the data controller has reasonable doubt about the data subject's identity. Recital 64 defines the requirement as follows:

“The controller should use all reasonable measures to verify the identity of a data subject who requests access, in particular in the context of online services and online identifiers. A controller should not retain personal data for the sole purpose of being able to react to potential requests.” [28, p. 12]

If a service is offered to a child below the age of 16 (or below the nationally applicable age) a processing of the data is only legal if the holder of the parental responsibility agrees to the processing [28], [38]. Thus, the workflow introduced in Figure 24 accommodates this fact. As no legal certainty has been established it is unclear which documentation is sufficient to prove guardianship.

The workflow introduced contains two pools, one which is collapsed for simplification which is representative of the data subject in question, the other is the data controller pool.

The start event is triggered if for the successful verification of a data subject's identity further proof is necessary. The token is born and flows through a XOR gateway to a parallel gateway. The parallel structure was chosen to visualize different possibilities of having the identity securely verified. The path splits into 5 paths at which each ends a task regarding the evaluation of a verification option is awaiting.

Task number 1 “Evaluate user account option” revises the possibility of it being a returning customer which is known and could verify their identity through a login into their user account. The user account is known to belong to said person due to a verification in the past. Additional security steps can be taken in case the user account may be compromised including but not limited to question only the person in question could answer, automated phone calls to their phone number cited in the user account. If the verification through an existing user account is a viable option (not for new customers) it can be added to the set of verification options offered at a later point to the data subject.

A second lane leads the token to “Evaluate government issued ID option”. To prove the identity, the data subject could be asked to upload an image of a government issued ID such as a passport or a driving license. It is important that the ID requested is not outdated and the name and birth date match the data subject's personal information. If a verification by these means is impossible e.g. the data subject exercises its right to rectification and the birth date is the wrong information in question, an alternative identification possibility needs to be offered.

Centered in the workflow on a straight line with the start event is the task “Evaluate digital signature option”. At this task it is evaluated if the data subject could submit an email with a digital signature attached proving the identity. If such a verification is not feasible due to technical limitations or because the data subject doesn't have such a signature, an alternative option is to be offered.

The fourth task evaluates the option of having the data subject submit official documents issued by the government such as a birth certificate if he or she lacks any officially issued ID. Which documentation is accepted by the controller has to be determined appropriate to the content in question. It is recommended that the DPO introduces a rule set of which information categories can be accessed through which proof of identity means.

The fifth task is tailored to the necessity of verifying the guardianship and thus the validity of the consent to process the information of children. Before such processing can take place, the guardian needs to

prove his or her identity, this can be done if the parent of the child already has an account with the corporation through adding the minors account to the parents account and request the parent to verify their identity through a credit or debit card [44]. Alternatively, official documentation such as a birth certificate or passport can be accepted as proof.

Once all options have been evaluated, the token continues to the task “Create individual request”. At this task the data controller generates a request for identification and offers the data subject methods deemed viable in the previous review. In order to reduce the effort of repeating requests, the message shall be created in simple plain text and contain exact information about which documentation and which communication channels are valid. Additionally, the data subject shall be warned that a repetitive failure to authenticate leads to a denial.

Once the identification proof is received the token flows to the task “Evaluate identification proof”. The provided information is taken into consideration and if it matches the records on hand the verification is successful. If, however, some information is missing or unreadable the verification of the identity concluded invalid and further verification options are offered to the data subject.

Has such a verification failed repeatedly, the token flows to “Inform data subject about denial and options”. At which task the data subject is informed that a verification failed. Options to successfully verify may be discussed directly with the data subject (i.e. a physical appearance of the data subject with a valid ID). The token then dies at verification failed. Has the verification been successful the token dies at the end event, “Verification successful”.

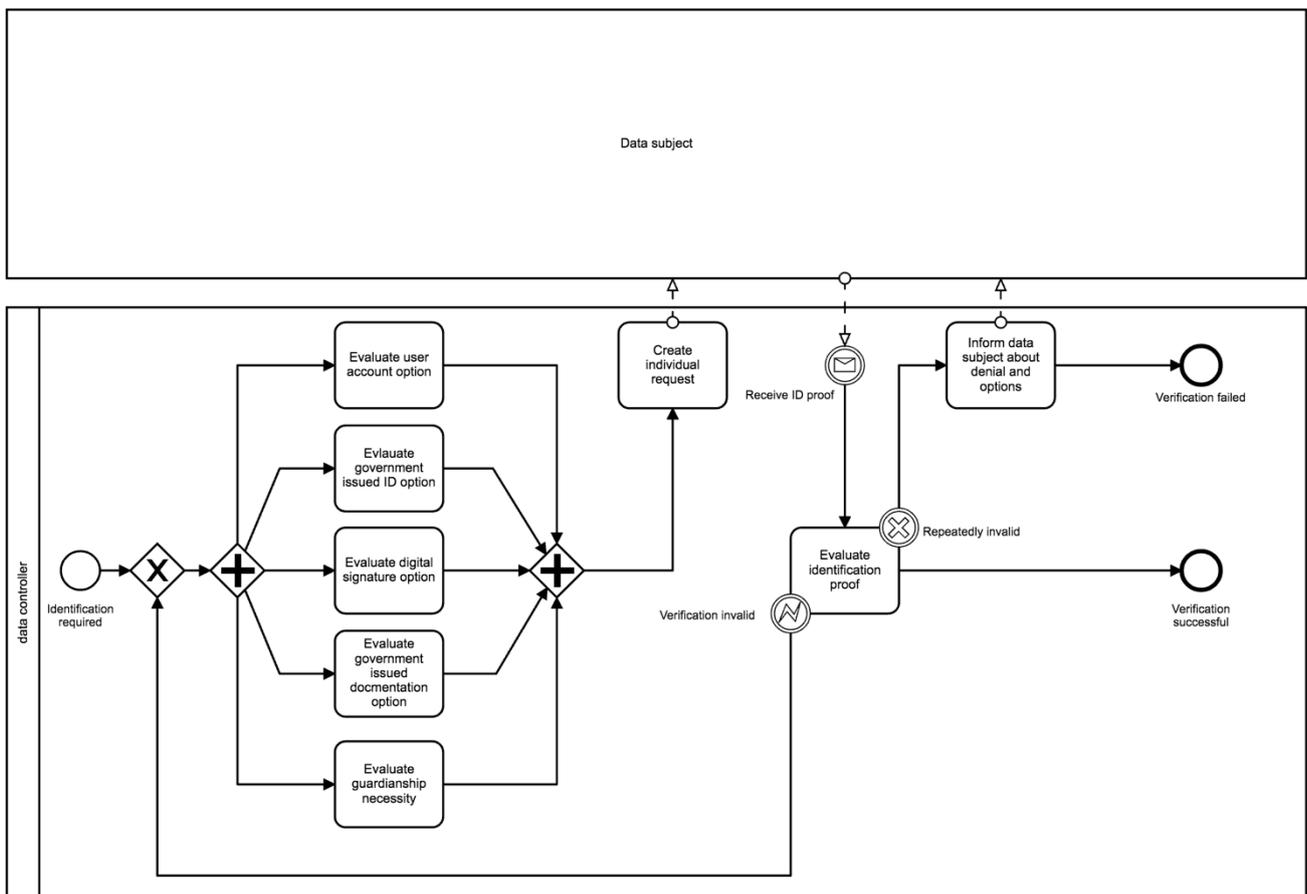


Figure 24 Data subject identity verification

4.2.5 Investigative Requests – Article 58 GDPR - Workflow

A supervising authority has the power to investigate a data controller's practices, and can therefore issue a request to provide information of particular interest in this section are Article 58 section 1 provision a and e. They are defined as, "Each supervisory authority shall have all of the following investigative powers:" [28, p.69]

- a) "to order the controller and the processor, and, where applicable, the controller's or the processor's representative to provide any information it requires for the performance of its tasks" [28, p.69]
- e) "to obtain, from the controller and the processor, access to all personal data and to all information necessary for the performance of its tasks" [28, p.69]

As Article 31 of the GDPR requests, a cooperation between the data controller and the supervising authority is mandatory [38]. The workflow introduced in Figure 25 illustrates an example of how such communication could be conducted. While not all possibilities of a corporation with the supervising authorities nor all reasons as to why a cooperation may render relevant are introduced, the example serves as an adjustable set of steps which can be applied to other requests.

The token is born once the data protection officer receives an inquiry from the supervising authority. At a first step, the token flows from the start event to the "Evaluate request" task. At this task the request is checked for validity and based on the criticality a priority level is assigned. The workflow introduced offers predetermined steps for two kinds of requests, either the supervising authority wants to review documentation of a performed task, this can occur if a data subject filed a complaint or if the data controller was selected for a check. Alternatively, the data controller needs to access personal data and/or other information necessary to fulfill its obligations as the authority.

Assuming the authority requested information about a group of records processed by the data controller the token follows the "yes" path after the XOR gateway. The first task it flows to is the "Obtain personal data – preparation" task. At which point the data controller collects the applicable data sets including information about the legal grounds on which the data has been processed. At the next point applicable BCR³⁴ regarding the handling of personal information are included with the data package. This is done to prove compliance with the requirements and is approved under Article 47 GDPR [28]. If the corporate rules are legally binding, they can serve as evidence.

Once the information is composed, a statement about retrieval options of the information is transmitted, this statement can include instructions to download the request information from a secure storage location.

Has the supervising authority launched an investigation about i.e. the proper handling of a data subject request, the token follows the "no" path at the XOR "Share personal data?" gateway. The path leads to the task "Gather evidence". As described in the introduced data subject rights workflow examples (Section 4.1.X), and as the GDPR requires, a data controller has to document proceedings as this documentation may serve as evidence of compliance.

Once the task is completed the token continues its path to the XOR gateway. If no evidence was available, the token flows to the task "Restore records". At this task applicable backup systems are used to recover lost documentation. If this operation fails, the data controller is subject to fines based on noncompliance. Therefore, if the recovery fails the token flows to "Create report on missing data".

³⁴ BCR – binding corporate rule

This report is aimed to minimize the negative effects on the corporation and should include a review on why the data is missing and which steps are taken to prevent such a loss in the future. The token dies at “Failed to perform request”.

If the recovery was successful, the token flows back to the “Gather evidence” task. Once it is completed the token flows through the XOR gateway to the “Create report” task. Ideally a report has been created during the initial fulfillment of the data subjects’ request, this report now needs to be supplemented with missing information such as BCR rules or any other information requested by the supervising authority.

Once the report has been completed the token flows to “Supply supervising authority” at which the report is transmitted to the authorities. It is crucial that such a task is completed in a timely manner and an official reception confirmation is requested.

The token continues the path and dies at “Request fulfilled”.

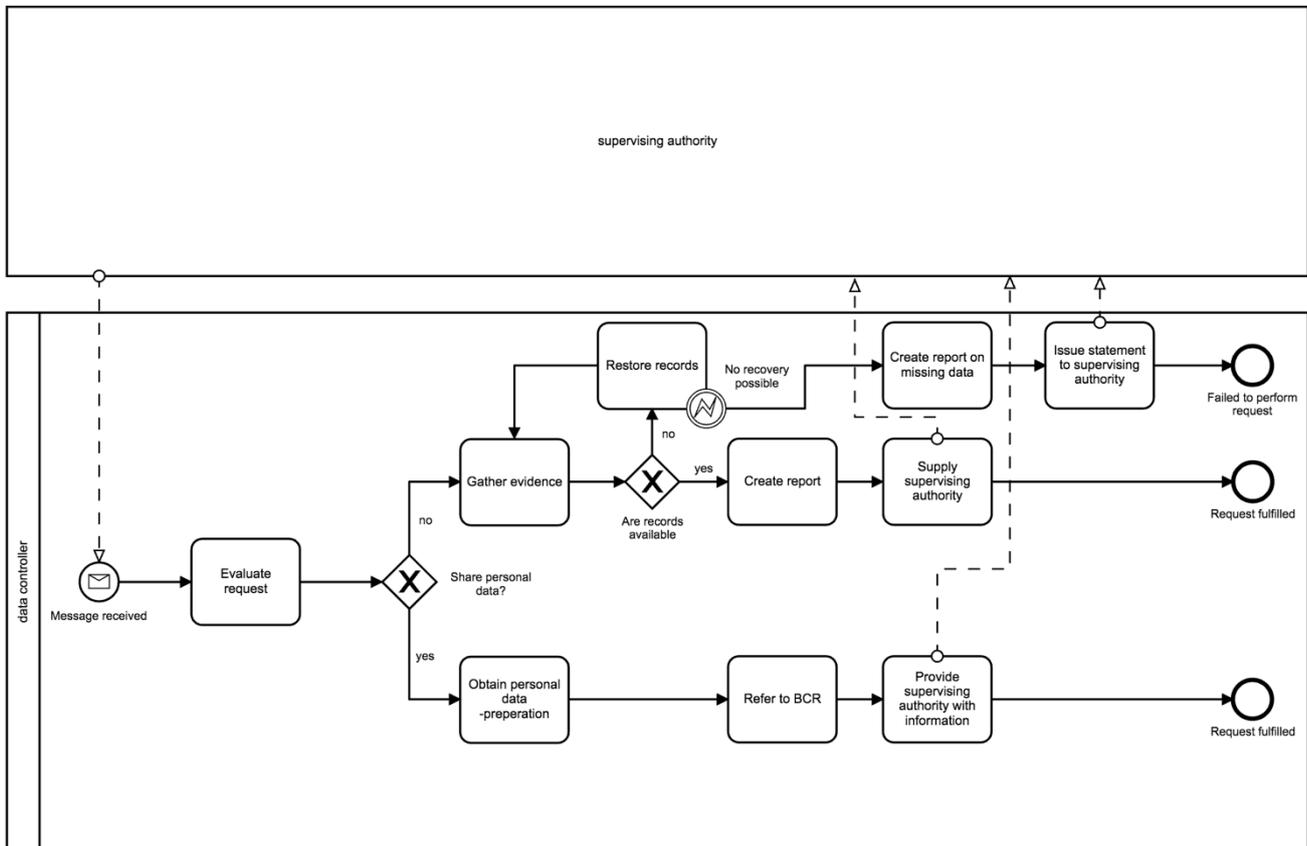


Figure 25 Investigative Request

4.3 Chapter Summary

Chapter 4 introduced generic workflows based on the BPMN 2.0 notation. The workflows illustrated are designed to support the implementation of business processes for the fulfillment of data subject rights and other types of request, notification, or verification obligations. Allowing the data controller to achieve compliance with the newly introduced requirements.

After an introduction to the chapter, including information about documentation requirements chapter section 4.1.1 introduced the first workflow. All workflows introduced under section 4.1.x are regarding data subject rights. The workflow was designed to comply with the requirements imposed by the right of access. In section 4.1.2 Article 16 of the GDPR was examined, followed by an example workflow about the right to rectification. The right to erasure was the topic of section 4.1.3 including a lengthy discussion and the introduction of a matching workflow. In section 4.1.4 the right to restriction of processing was analyzed, a step by step instruction prevailed the introduced workflow. A data subject has the right to data portability, this right was discussed in section 4.1.5 and the according workflow was presented. If the data subject disagrees with the processing of his or her personal data, he or she has the right to object. This was the subject of section 4.1.7, how to handle request was explained by the workflow within the section. 4.1.8 served a workflow to allow compliance with the right of the data subject to be exempt from automated decision making, as there is some legal uncertainty involved with this article the discussion was based on the assumption that a data subject has to exercise the right.

Once the data subject rights have been covered, other topics have been covered in section 4.2.x. regarding notification, verification and cooperation topics.

Section 4.2.1 – 4.2.3 where concerned with notification obligations. In section 4.2.1 the obligation to inform former recipients of datasets about the data subject exercising his or her rights is examined, and a short notification workflow is introduced. When a data breach occurs, the supervising authority has to be informed within 72 hours via a data breach notification. Article 33 of the GDPR dictates the requirements and the workflow introduced in section 4.2.2 reflects them. While section 4.2.2 was only directed at the supervising authority the data breach notification in section 4.2.3 is concerning the data subject.

The topic of how to verify a data subjects identity was the focus of section 4.2.4 including proposed steps to take in an introduced workflow.

The supervising authority has the power to request cooperation and the data controller has to comply with information request made. To showcase how such an interaction can look like a generic workflow was introduced in section 4.2.5. which included the possibility of failure to provide the information requested.

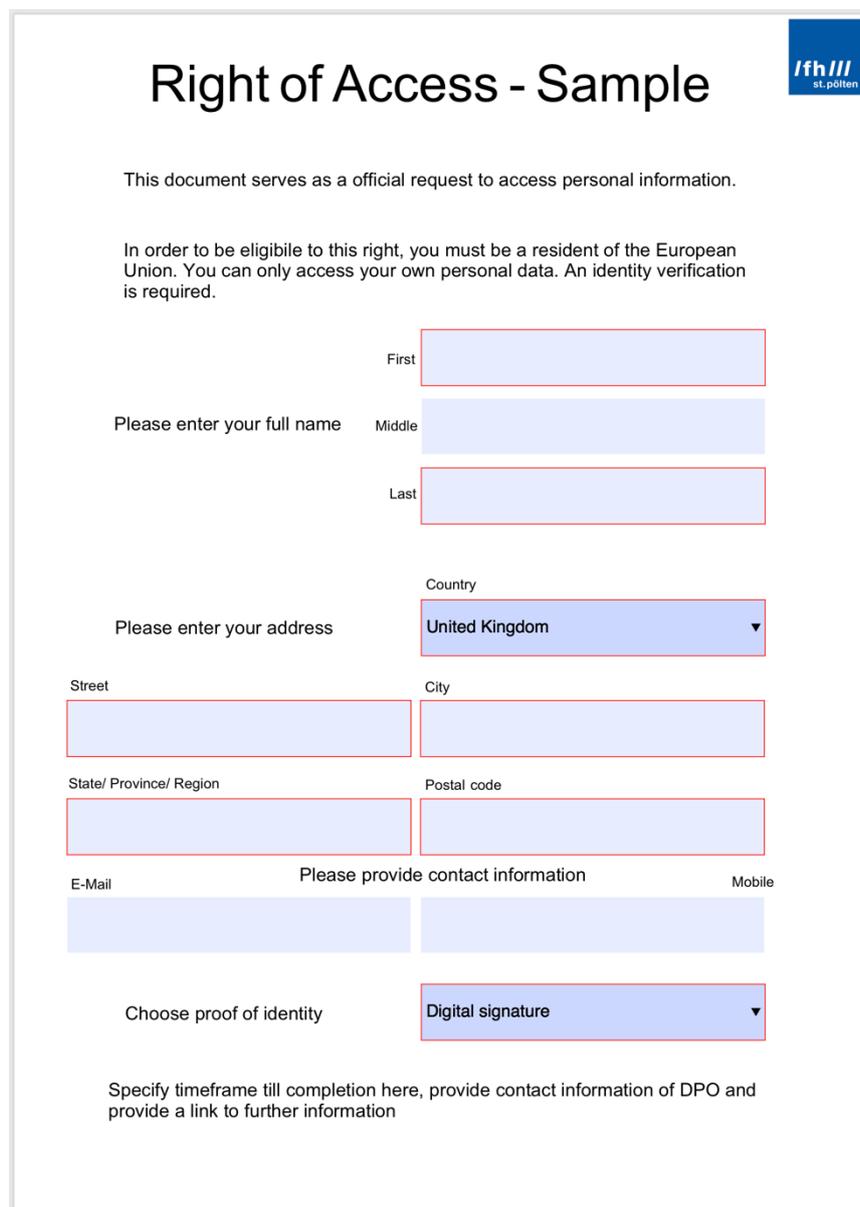
Part 4

Forms

5 Example Forms

This chapter provides the data controller with an example set of forms for access, rectification, or erasure requests made by the data subject. Providing a standardized way to communicate the exercising of a data subject right has benefits for both, the data subject, and the data controller. The data subject faces a clear, easy to complete form and can supply all the necessary information in one message. The data controller receives a request containing all the information needed to complete a request. Thus, saving resources and increasing the throughput.

5.1 Right of access by the data subject – Article 15 GDPR – Form



The form is titled "Right of Access - Sample" and includes the Ifh III st. pölten logo in the top right corner. It contains the following text and fields:

This document serves as a official request to access personal information.

In order to be eligible to this right, you must be a resident of the European Union. You can only access your own personal data. An identity verification is required.

Please enter your full name

First

Middle

Last

Please enter your address

Country

Street

City

State/ Province/ Region

Postal code

Please provide contact information

E-Mail

Mobile

Choose proof of identity

Specify timeframe till completion here, provide contact information of DPO and provide a link to further information

Figure 26 Right of Access - Form

The form introduced is a generic example of how the implementation of a request form for the data access right could be implemented. The headline states the right the data subject wants to exercise.

Below that, an explanation of which requirements the data subject must fulfill to be eligible to the right. The data subject must be able to identify himself and be an EU citizen. Additionally, it is clarified that only the individual's personal data can be accessed by the individual. Fields which are bordered in red are mandatory. Depending on the system applied contact information may be mandatory too. The data subject has to complete the form including information about his name, address, and proof of identity.

It is recommended to provide information about the expected duration until the request will be fulfilled and to provide further information as well as contact information of the DPO.

5.2 Right to rectification – Article 16 GDPR – Form



Right to Rectification - Sample

This document serves as an official request to rectify personal information. In order to be eligible to this right, you must be a resident of the European Union. You can only rectify your own personal data. An identity verification is required.

<p style="text-align: center; font-size: small;">Choose proof of identity</p> <div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 5px;">Digital signature ▼</div>	<p style="text-align: center; font-size: small;">Please enter your full name</p> <p style="font-size: x-small;">First <input style="width: 90%; border: 1px solid #ccc;" type="text"/></p> <p style="font-size: x-small;">Middle <input style="width: 90%; border: 1px solid #ccc;" type="text"/></p> <p style="font-size: x-small;">Last <input style="width: 90%; border: 1px solid #ccc;" type="text"/></p>
<p style="text-align: center; font-size: small;">Please enter your address</p> <p style="font-size: x-small;">Street <input style="width: 95%; border: 1px solid #ccc;" type="text"/></p> <p style="font-size: x-small;">State/ Province/ Region <input style="width: 95%; border: 1px solid #ccc;" type="text"/></p> <p style="font-size: x-small;">E-Mail <input style="width: 95%; border: 1px solid #ccc;" type="text"/></p>	<p style="font-size: x-small;">Country <input style="background-color: #e6f2ff;" type="text" value="United Kingdom"/></p> <p style="font-size: x-small;">City <input style="width: 95%; border: 1px solid #ccc;" type="text"/></p> <p style="font-size: x-small;">Postal code <input style="width: 95%; border: 1px solid #ccc;" type="text"/></p> <p style="text-align: center; font-size: x-small;">Please provide contact information</p> <p style="font-size: x-small;">Mobile <input style="width: 95%; border: 1px solid #ccc;" type="text"/></p>

Explain which personal data needs to be rectified
Explain how the false information is affecting you

Specify timeframe till completion here, provide contact information of DPO and provide a link to further information

Figure 27 Right to Rectification - Form

The data subject has a right to rectification, in order to support the data subject this form contains the necessary fields to successfully process such a request. The data subject can choose a form of verification such as a digital signature, a passport, or driver's license upload. Both the name and address need to be

disclosed to the data controller, it may be necessary to request contact information too. Additionally, to these fields introduced in the example form of the right for access, this form has a large text box at the bottom. In this textbox the data subject can describe which information is wrong and what risks he bears from it. At the bottom, applicable information of processing times, contact information, and further relating information shall be embedded.

5.3 Right to erasure – Article 17 GDPR - Form

Right to Erasure - Sample



This document serves as a official request to erase personal data. In order to be eligible to this right, you must be a resident of the European Union . You can only request erasure of your own personal data. An identity verification is required.

Choose proof of identity

Digital signature ▼

Disclaimer:
Data which has been removed cannot be recovered!

Please enter your full name

First

Middle

Last

Please enter your address

Street

Country

Austria ▼

City

State/ Province/ Region

Postal code

E-Mail

Please provide contact information

Mobile

Under what circumstances do you request the erasure of your personal data? Please explain:

Specify timeframe till completion here, provide contact information of DPO and provide a link to further information

Figure 28 Right to Erasure – Form

The information requested from the data subject hardly differs from the information required by the “Right to Rectification” form. However, a disclaimer is introduced warning of the consequences of an erasure of the data.

Functional examples (working drop down lists) of these forms are supplied in a PDF format on the digital appendix (CD within the physical copy of this thesis).

Part 5
Conclusion

Solution to the Research Problem

This chapter presents the solutions to the two research questions introduced in Part 1 of this thesis and concludes the paper as well as introduces ideas for future work on the matter. Additionally, predictions on future developments are presented.

6.1 Solution to research problem 1

The first research problem was defined as follows:

“Which cost free specialized tools are available on the market to create BPMN 2.0 diagrams and how do they differ in their functionality?”

After conducting a market analysis, six modelling tools have been chosen. All six tools claimed to be compliant with the BPMN 2.0 standard and where available at no cost. An exact comparison between the features and usability is available in Chapter 3 of this thesis. A ranking was conducted based on point system introduced in section 3.3. The following list of tools is ordered to range between those that received the most to the least points:

1. BPMN 2 Modeller
2. Camunda Modeller
3. Aris Express
4. Bonita BPM
5. Modelio
6. JBPM

Therefore, it can be concluded that while a wide variety of cost-free business process modelling software solutions is available, only some serve the intended purpose in a satisfying manner.

6.2 Solution to research problem 2

The second research problem was defined as follows:

“How can generic workflows support the implementation process of GDPR requirements?”

Chapter 4 introduced workflows which are compliant to GDPR requirements. These workflows are illustrative solutions to the requirements set by data subject rights and additionally covers topics of the areas notification, verification, and cooperation with the supervising authority. The implementation of the requirements can be supported by the workflows due to their flexible and generic nature, at the same time they present key tasks to ensure compliance with the GDPR.

Even in the case that a data controller is not willing to automate processes in the organization to accommodate the new challenges, the workflows can serve as a reference when needed. To ensure a broad understanding of the workflows, a short introduction to the topic of BPMN was given in addition to the presentation of key symbolics within the notation.

Concluding that the implementation process can be supported through providing flexible processes which are compliant with the requirements of the GDPR to data controllers at no cost.

As to further help data controllers to achieve compliance, a set of forms to provide any data subject for requests was also provided.

6.3 Limitations (Solution)

The introduced workflows are generic and need to be modified by the individual data controller in accordance with applicable GDPR requirements to the needs of the organization. A successful modification (i.e. a GDPR compliant modification) cannot be guaranteed as the author has no influence on the implementation.

In favor of readability and simplicity of a general workflow, not all communication paths are visualized. To conquer this fact a description was provided with each introduced workflow.

Due to legal uncertainties in some areas of the application of the GDPR, some changes may become necessary to workflows after legal certainty has been established.

The conducted market analysis was conducted at a majority on MacOS. Results may not reflect on other operating systems such as Windows or Linux.

None of the work conducted has been reviewed by legal experts.

6.4 Conclusion

The paper was set to provide organizations struggling with the implementation of the diverse requirements introduced by the GDPR. To create a paper beneficial to the data controller a lengthy introduction to the topic GDPR, the struggling of organization with meeting the requirements and the general motivation behind this work was given.

After the reason was established and the research question was clearly defined, background information was introduced. The modelling notation used to create workflows was BPMN in version 2.0. Therefore, a short introduction into why this notation was chosen and how to use it was given. This included the establishment of rules and definitions used. After all the essential information was conveyed, the paper moved on to determining the best tool to modify and create workflows with BPMN 2.0 notation.

A set of rules to determine which software will be reviewed was established. Then a market analysis was conducted. After the final tools for evaluation were chosen each one was individually reviewed. Based on the set rules points have been assigned for having certain key functionalities. Once all points have been assigned a comparison between the tools was conducted. This analysis allows an individual to make an educated decision on which available software to choose for the intended use case. Thus, allowing a corporation to save resources on trial and error when determining which modelling tool will be used.

After learning which tool is the most suitable for this use-case the paper moved on to chapter 4. In chapter 4 the individual requirements set by the GDPR, in particular concerning data subject rights have been reviewed. After learning about the duties and restrictions a workflow has been carefully designed to comply with the regulation. The workflow was then described step by step as if a request would actually pass through it. In addition to data subject rights workflows to comply with notification obligations have been introduced. Also, a workflow each to verify a data subject's identity and a workflow about working with the supervising authority have been illustrated. The data controller can use the developed workflows to implement a new process within the organization which is in compliance with the GDPR or use the information to make

adjustments to existing processes. The developed platform allows any user to crosscheck their implementation with the examples made within this paper to confirm compliance. Additionally, due to the nature of BPMN the processes can be made executable, meaning after an adjustment to the existing infrastructure an organization can introduce automated processes. The BPMN file can be executed in a business process engine which in turn ensures not only high efficiency as tasks can be handled by automated means but also compliance through steps where human verification is required.

To further help the data controller with implementing measures to achieve compliance with the GDPR a set of sample forms was provided in Chapter 5. These forms covered request of the data subject about the right of access, the right to rectification, and the right to erasure. Such standardized forms allow for easy and efficient communication with the data subject and at the same time guarantee compliance with the regulation.

After completing the chapter, the research question could be answered in Part 5 of this thesis. In fact, both questions could be positively concluded. However, some restrictions do apply to the solution introduced in Chapter 6. A final conclusion of the thesis is conducted and an outlook on both future work and the impact of the GDPR is expressed.

Below the key achievements of this work are highlighted.

- A market analysis of BPMN modelling tools
 - Data controllers can easily choose a tool fitting their use case
 - Data controllers save resources on skipping trial and error when choosing a modelling tool
 - Data controllers are introduced to the differences between the available tools
- Illustration of 12 GDPR compliant workflows designed in BPMN 2.0
 - Data controllers can check their own implementations for missing tasks
 - Data controllers can use the introduced models to build their own processes
 - Data controllers can adjust the introduced models to their business needs
 - Data controllers are presented all workflows to achieve a full implementation of data subject rights
 - Data controllers can save significant resources when transitioning towards GDPR compliance
 - The introduced models can be adjusted to run automated in a business process engine depending on the data controller's infrastructure
 - All files including XML code are supplied on the media (see Appendix)
 - Since all introduced workflows discuss the requirements only little prior knowledge of the data controller is required
 - The introduced processes can serve as educational material
- Introduction to sample request forms (data subject – data controller)
 - The sample forms work in conjunction with the introduced processes
 - The sample forms are used to standardize communication of data subject requests
 - The sample forms are compliant with GDPR requirements.
 - The sample forms are interactive and supplied on the media (see Appendix)
 - The sample forms can serve as template for the creation of other forms in compliance with the GDPR

6.5 Outlook

Using information technology is increasingly difficult to avoid. Data processing is the core of our modern information-based society, however false or unlawfully processed information can have critical impacts on the life of individuals. Regulations such as the GDPR are an approach to preserve the human right to privacy and mitigate the negative effects of widely spread data processing.

Though such a protection comes with complications for data controllers. To continue helping organizations to cope with the changing legal environment, the steps to achieve compliance must be simplified. Therefore, future work such as the following should be conducted:

- Creating generic workflows for specific industries
- Creating an example implementation of an operational workflows derived from strategic workflows
- Creating an example of using automated processes by implementing technical workflows derived from operational workflows
- Update the workflows introduced in this paper once legal certainty regarding the GDPR has been established.
- Provide example contractual agreements for data processing
- Provide example reports, policies, and forms

All information is to be provided free of charge, considering small and medium sized data controllers struggle significantly, many due to the lack of resources as mentioned in the motivation of this paper.

The USA has announced to be working on a “Consumer Data Privacy Policy” which could have the GDPR as its template [45]. Underlining the important role of individual privacy even in a seemingly transparent modern world.

We stand at a transitional point in time where data controllers face big changes as to how data can and should be processed. In addition to regulations it is of importance to raise awareness and create a common understanding of the significant role privacy has in our society.

Table of Figures

Figure 1 Thesis Outline.....	11
Figure 2 BPMN Symbols Example	13
Figure 3 BPMN Activity Types.....	15
Figure 4 BPMN Gateways	16
Figure 5 Pools and Lanes Exampel.....	17
Figure 6 Camunda Modeler	21
Figure 7 Aris Express	22
Figure 8 Bonita Studio Community.....	23
Figure 9 BPMN 2 Modeler Eclipse	24
Figure 10 jBPM.....	25
Figure 11 Modelio	26
Figure 12 Comparison BPMN	27
Figure 13 Right of Access.....	32
Figure 14 Right to rectification – inaccurate data.....	34
Figure 15 Right to rectification – incomplete data	35
Figure 16 Right to erasure	40
Figure 17 Right to restriction of processing	43
Figure 18 Right to data portability	46
Figure 19 Right to objection	49
Figure 20 Right to not be subject to automated decision making	52
Figure 21 Notification obligation	54
Figure 22 Data breach notification – supervisory authority.....	58
Figure 23 Data breach notification – data subject.....	60
Figure 24 Data subject identity verification	62
Figure 25 Investigative Request.....	64
Figure 26 Right of Access - Form.....	67
Figure 27 Right to Rectification - Form.....	68
Figure 28 Right to Erasue – Form	69

Table of Tables

Table 1 UML Diagram types	12
Table 2 BPMN Modelling Tools.....	20
Table 3 Camunda Modeler Score	22
Table 4 Aris Express Score.....	23
Table 5 Bonita Studio Community	23
Table 6 BPMN 2 Modeler Eclipse	25
Table 7 jBPM.....	26
Table 8 Modelio.....	26

Bibliography

- [1] Deloitte, "The time is now The Deloitte General Data Protection Regulation Benchmarking Survey," 2017.
- [2] European Data Protection Supervisor, "The History of the General Data Protection Regulation - European Data Protection Supervisor." [Online]. Available: https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en. [Accessed: 09-Jun-2018].
- [3] European Commission, "IP/12/46," Eur. Comm. Press Release Database, no. January, 2012.
- [4] Bitkom, "DS-GVO: Jedes dritte Unternehmen hat sich noch nicht mit der Datenschutzgrundverordnung beschäftigt," 2017. [Online]. Available: <https://www.bitkom.org/Presse/Presseinformation/Jedes-dritte-Unternehmen-hat-sich-noch-nicht-mit-der-Datenschutzgrundverordnung-beschaeftigt.html>. [Accessed: 10-Jun-2018].
- [5] Peter Tsai, "Most will miss GDPR deadline: UK most prepared, US and rest of EU lag behind - Spiceworks." [Online]. Available: <https://community.spiceworks.com/blog/3023-most-will-miss-gdpr-deadline-uk-most-prepared-us-and-rest-of-eu-lag-behind>. [Accessed: 10-Jun-2018].
- [6] Mathias Brandt, "Statistik der Woche: Die Deutschen und die DSGVO | Technology Review," Technology Review, 2018. [Online]. Available: <https://www.heise.de/tr/artikel/Statistik-der-Woche-Die-Deutschen-und-die-DSGVO-4075880.html>. [Accessed: 10-Jun-2018].
- [7] Oliver Smith, "The GDPR Racket: Who's Making Money From This \$9bn Business Shakedown," Forbes. [Online]. Available: <https://www.forbes.com/sites/oliversmith/2018/05/02/the-gdpr-racket-whos-making-money-from-this-9bn-business-shakedown/#73b0433534a2>. [Accessed: 11-May-2018].
- [8] Nadine Oberhuber, "DSGVO: "Man reimt sich das alles irgendwie zusammen" | ZEIT ONLINE," Zeit. [Online]. Available: <https://www.zeit.de/wirtschaft/2018-05/dsgvo-datenschutz-mittelstand-kleinunternehmer>. [Accessed: 11-Jun-2018].
- [9] European Commission, "Data protection in the EU | European Commission." [Online]. Available: https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en. [Accessed: 09-Jun-2018].
- [10] "WhatsApp raises minimum age to 16 in Europe ahead of GDPR | TechCrunch." [Online]. Available: <https://techcrunch.com/2018/04/25/whatsapp-raises-minimum-age-to-16-in-europe-ahead-of-gdpr/?guccounter=1>. [Accessed: 11-Jun-2018].
- [11] Jake Madders, "Data protection: why businesses should be motivated to make a security change." [Online]. Available: <https://www.continuitycentral.com/index.php/news/technology/1693-data-protection-why-businesses-should-be-motivated-to-make-a-security-change>. [Accessed: 11-Jun-2018].
- [12] Kalliopi Spyridaki, "general-data-protection-regulation-from-burden-to-opportunity." [Online]. Available: https://www.sas.com/en_us/insights/articles/data-management/general-data-protection-regulation-from-burden-to-opportunity.html.
- [13] "The Cambridge Analytica Files | The Guardian." [Online]. Available: <https://www.theguardian.com/news/series/cambridge-analytica-files>. [Accessed: 11-Jun-2018].
- [14] Information Commissioner's Office, "Guide to the General Data Protection Regulation (GDPR)," 2017.
- [15] "GDPR fines: how GDPR administrative fines and sanctions are applied." [Online]. Available: <https://www.i-scoop.eu/gdpr/gdpr-fines-guidelines-application-penalties/>. [Accessed: 11-Jun-2018].
- [16] M. Goddard, "The EU General Data Protection Regulation (GDPR): European regulation that has a global impact," *Int. J. Mark. Res.*, vol. 59, no. 6, pp. 703–705, 2017.
- [17] "Fines and Penalties – GDPR EU.org." [Online]. Available: <https://www.gdpreu.org/compliance/fines-and-penalties/>. [Accessed: 11-Jun-2018].
- [18] Michale Baxter, "GDPR is a journey not a destination - GDPR.Report." [Online]. Available: <https://gdpr.report/news/2018/02/02/gdpr-journey-not-destination-2/>. [Accessed: 11-Jun-2018].
- [19] B. Silver, *BPMN Method and Style, with BPMN Implementer's Guide: A structured approach for business process modeling and implementation using BPMN 2.0*. Cody-Cassidy Press Aptos, 2011.
- [20] G. Booch, J. Rumbaugh, and I. Jacobson, *The unified modeling language user guide*. Addison-Wesley, 2005.
- [21] "UML Diagram - Everything You Need to Know About UML Diagrams." [Online]. Available: <https://www.smartdraw.com/uml-diagram/>. [Accessed: 12-Jun-2018].
- [22] J. Freund and B. Rücker, *Praxishandbuch BPMN 2.0*. Carl Hanser Verlag GmbH Co KG, 2014.
- [23] S. Morris, "Ernestine Gilbreth Carey Interview," pp. 1–30, 2006.
- [24] Kenia Sousa, "What is the difference between flow charts and BPMN?" [Online]. Available: <https://keniasousa.github.io/2014/10/flowchart-bpmn.html>. [Accessed: 12-Jun-2018].

- [25] A. Tsai, J. Wang, W. Tepfenhart, and D. Rosca, "EPC workflow model to WIFA model conversion," in *Systems, Man and Cybernetics*, 2006. SMC'06. IEEE International Conference on, 2006, vol. 4, pp. 2758–2763.
- [26] W. Tscheschner, "Transformation from EPC to BPMN," 2006.
- [27] "About OMG | Object Management Group." [Online]. Available: <https://www.omg.org/about/index.htm>. [Accessed: 12-Jun-2018].
- [28] European Union, Regulation 2016/679 of the European parliament and the Council of the European Union. 2016.
- [29] T. H. Dr. Detlev Gabel, "Chapter 5: Key definitions – Unlocking the EU General Data Protection Regulation | White & Case LLP International Law Firm, Global Law Practice," 2017. [Online]. Available: <https://www.whitecase.com/publications/article/chapter-5-key-definitions-unlocking-eu-general-data-protection-regulation>. [Accessed: 13-Jun-2018].
- [30] "GDPR Personal Data and Sensitive Personal Data," 2016. [Online]. Available: <https://www.burges-salmon.com/news-and-insight/legal-updates/gdpr-personal-data-and-sensitive-personal-data/>. [Accessed: 13-Jun-2018].
- [31] Gregor Polančič, "Common BPMN Modeling Mistakes - Activities," 2013. [Online]. Available: <http://blog.goodelearning.com/subject-areas/bpmn/common-bpmn-modeling-mistakes-activities/>. [Accessed: 13-Jun-2018].
- [32] "Event Subprocess | docs.camunda.org." [Online]. Available: <https://docs.camunda.org/manual/7.5/reference/bpmn20/subprocesses/event-subprocess/>. [Accessed: 13-Jul-2018].
- [33] Object Management Group (OMG), "Business Process Model and Notation (BPMN) Version 2.0," Business. 2011.
- [34] "ARIS Express details | ARIS BPM Community." [Online]. Available: <https://www.ariscommunity.com/aris-express/details>. [Accessed: 14-Jun-2018].
- [35] Dejan Kosutic, "GDPR documents – Which policies and procedures are required?" [Online]. Available: <https://advisera.com/eugdpracademy/knowledgebase/list-of-mandatory-documents-required-by-eu-gdpr/>. [Accessed: 24-Jun-2018].
- [36] Punit Bhatia, "What are the contents of the GDPR Data Protection Policy?" [Online]. Available: <https://advisera.com/eugdpracademy/knowledgebase/contents-of-the-data-protection-policy-according-to-gdpr/>. [Accessed: 16-Jul-2018].
- [37] Stefan Brink, "BeckOK DatenschutzR - beck-online," 2018. [Online]. Available: https://beck-online.beck.de/?vpath=bibdata%2Fkomm%2FBeckOKDatenS_23%2Fcont%2FBECKOKDATENS.htm. [Accessed: 29-Jun-2018].
- [38] P. Voigt and A. von dem Bussche, *The EU General Data Protection Regulation (GDPR) – A Practical Guide*, no. June. Springer, 2012.
- [39] K.-U. Plath, T. Becker, P. von Braunmühl, A. von dem Bussche, A.-M. Frey, and J.-M. Grages, *BDSG/DSGVO: Kommentar zum BDSG und zur DSGVO sowie den Datenschutzbestimmungen von TMG und TKG*. Otto Schmidt, 2018.
- [40] B. P. 1974- Paal, D. A. Pauly, and S. 1966- Ernst, *Datenschutz-Grundverordnung Bundesdatenschutzgesetz*.
- [41] "Introducing Data Transfer Project: an open source platform promoting universal data portability | Google Open Source Blog." [Online]. Available: <https://opensource.googleblog.com/2018/07/introducing-data-transfer-project.html>. [Accessed: 28-Jul-2018].
- [42] Bitkom, "Stellungnahme," 2017.
- [43] P. Laue, J. Nink, and S. Kremer, *Das neue Datenschutzrecht in der betrieblichen Praxis*. Nomos, 2016.
- [44] "TrustArc," 2014. [Online]. Available: <https://www.trustarc.com/blog/2014/07/25/ftc-revises-faq-guidance-on-coppa-and-verifiable-parental-consent/>. [Accessed: 14-Jul-2018].
- [45] Reuters, "Consumer Data Privacy Policy." [Online]. Available: <https://www.nytimes.com/reuters/2018/07/27/technology/27reuters-usa-internet-privacy.html>. [Accessed: 27-Jul-2018].

Appendix

All workflows introduced can be found on the CD in the folder "Workflows" which is supplied with the print version of this paper. The workflow format is ".bpmn" the XML code can be exported. The workflows are published under the Apache 2.0 license:

Copyright 2018 FH St. Pölten / Richard Lechner

Licensed under the Apache License, Version 2.0 (the "License");
you may not use this file except in compliance with the License.

You may obtain a copy of the License at

<http://www.apache.org/licenses/LICENSE-2.0>

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

The sample forms can be found also found on CD in the folder "Forms".