UNIVERSITY OF TARTU
Institute of Computer Science
Cyber Security Curriculum

Awais Abbasi

# GDPR Implementation in an Airline Contact Center

Master's Thesis (30 ECTS)

Supervisor: Raimundas Matulevicius, PhD
Co-Supervisor: Jake Tom, MSc

Tartu 2018

# GDPR Implementation in an Airline Contact Center

## Abstract:

With the introduction of General Data Protection Regulation (GDPR) in upcoming May 2018, many companies that used to handle personal data of EU citizens in a more casual manner, are now at risk of facing heavy fines. Airline industry is one such example of business entity that handles and processes personal data on massive scales, which puts the airline business in the spotlight of GDPR compliance. A fair amount of such data is processed in contact centers, which makes it vital to comply with GDPR. Airlines that are not ready to adapt GDPR may face loss of reputation, loss of customer's trust and bankruptcy because of heavy fines. In today's age, most of airlines have outsourced their contact center business to third parties, which makes it even more complicated to define the roles and responsibilities of data controller and data processor and both entities have to reach an agreement to share the burden of compliance, in order to survive in today's competitive environment. The idea of this thesis is to study a running case scenario in one of the major European airline contact center, analyze the flight booking process from GDPR's perspective to find out the gaps that can cause non-compliance. The solution part of this thesis is focused on filling these gaps by means of activities introduced in the flight booking process to achieve compliance, validated by expert opinion from senior staff members of airline contact center.

**Keywords:** GDPR, data controller, data processor, consent, transparency, documentation, data security

**CERCS:** P170 – Cyber Security, Information Technology

# GDPR rakendamine lennuettevõtte kontaktkeskuses

**Lühikokkuvõte:**

Seoses GDPR kasutuselevõtmisega 2018. aasta mais, on paljudel ettevõtetel, kus kasutatakse tavapäraselt EL kodanike isikuandmeid, oht suurteks trahvideks. Lennufirmad on üks näide ärist, kus töödeldakse massiliselt isikuandmeid ja see toob teravalt esile lennuettevõtete vastavuse GDPR nõuetele. Suur osa neist andmetest töödeldakse kontaktkeskustes, mis toob vajaduse viia töötlemine vastavusse GDPR nõuetega. Lennufirmad, kus ei olda valmis kohaldama GDPR nõudeid, võivad silmitsi seista mainekahjudega, klientide usalduse kaotusega või pankrotiga suurte trahvide tõttu. Tänapäeval enamik lennufirmadest ostab kontaktkeskuse teenuseid sisse kolmandalt osapoolelt, mistõttu on keerukas andmetöötluse rolle ja vastutust jagada mõlema osapoole vahel. Pooled peavad jõudma kokkuleppele, et kanda võrdselt vastutust tänapäeva pingelises konkurentsis. Käesoleva magistritöö eesmärgiks on viia läbi Euroopa ühe suurima lennuettevõtja kontaktkeskuse juhtumianalüüs, analüüsida lendude broneerimise protsessi GDPR seisukohalt ja selgitada välja lüngad, mis võivad põhjustada nõuetele mittevastavust. Lõputöö keskendub vastavuse saavutamiseks lünkade täitmisele lennubroneerimise protsessis, tuues sisse uusi tegevusi, mida kinnitas ka lennufirma kontaktkeskuse juhtivtöötajate ekspertarvamus.

**Märksõnad:** GDPR, regulaator, andmetöötleja, nõusolek, läbipaistvus, dokumentatsioon, andmete turvalisus

**CERCS:** P170 - küberturvalisus, Infotehnoloogia

## Table of Contents

# 1 Introduction

Currently, the contact center of any airline is a place where most of customer's data is collected and processed. Sometimes, these contact centers are managed directly by the airline and sometimes these are outsourced to third parties. The data collected can be sensitive depending on nature of it and it needs careful handling. According to my own observation while working in such contact center in different roles, data is being handled in a very casual way, where the ways of conducting business do not really match the requirements set by the new upcoming regulation called the General Data Protection Regulation or "GDPR". The non-compliance to GDPR can lead to fines up to 20 million Euros [1] and also airlines would not like to be part of such scandals, which can cause loss of reputation as well as loss of customers' trust. So there is a great need to analyze the core business processes such as flight booking process and how data is being handled in a regular contact center of an airline and then propose solutions or suggestions (based on expert opinions) in order to be compliant with GDPR. Also, there is a need to clearly define roles and responsibilities of data controllers and data processors, so that both entities can work on best possible solutions to implement GDPR through mutual collaboration and agreement.

## 1.1 Goal of Thesis

The goal of this thesis is to make the business process GDPR compliant. This process of achieving GDPR compliance is divided in to following steps

I. Study the most important business process of any Airline i.e. flight booking process

II. Map the Articles of GDPR against the business activities and find out the major areas of non-compliance.

III. Present a business oriented solution to implement GDPR as a practitioner in Airline's sector

IV. Validate the solution by means of expert opinions from experienced professionals directly associated with Airline's business.

## 1.2 Research Method

The following steps briefly describe the method used for research. (The method is explained in detail in chapter 3).

1. The contact center of a well-known European Airline is taken for studying case scenario (flight booking process). In order to come up with practical solution that will meet business requirements, the data is collected from the contact center to create business models and finding out the activities that cause non-compliance. This approach can be applied by other Airlines as well working in similar fashion. Business process modelling notation (BPMN) technique is used to model the flight booking process.
2. Validation – The proposed solution is validated by means of direct feedback (interviews and discussions) from contact center's experts, thus making solution real time.
3. Qualitative research – The impact of implementing process change is studied by interviewing the experts associated with Airline's contact center.

## 1.3 Main Research Questions

The main research question (**MRQ**) is

**How to implement the EU General Data Protection Regulation (GDPR) in an airline contact center**?

This question is broken down in to different sub research questions, which we call as (SRQ)

*SRQ1. How is GDPR different from current privacy regulations and why GDPR is needed?* This question is answered in chapter 2, where literature review is conducted and current privacy regulations are discussed in details. The GDPR is then explained by highlighting the key differences introduced by GDPR in area of privacy and data protection.

*SRQ2. How much the contact center is GDPR compliant and what are the means to make the contact center GDPR compliant?* In order to answer this question, a case scenario is conducted in chapter 4 on a European Airline's contact center. The business process chosen for this purpose is flight booking process. The selected Articles of GDPR are mapped against the flight booking process and gaps causing non-compliance are highlighted and a whole new flight booking process is remodeled, along with new activities to fill the gaps of non-compliance.

*SRQ3. How the solution/means to make contact center GDPR compliant is validated?*

The solution is validated by means of interviews and discussions with most experienced employees of contact center. Feedback on proposed solution is received and the final GDPR compliant flight booking process is modeled in chapter 6.

In next chapter, the current privacy standards and GDPR are discussed in detail. The key changes brought by GDPR are highlighted by making comparison of GDPR with current privacy standards. It is followed by chapter 3, where the research method and the way of conducting research is explained. The actual flight booking process and GDPR compliant flight booking process, are modelled in chapter 4 and the overall approach to achieve GDPR compliance along with GDPR compliant flight booking process is validated in chapter 5 by means of interviews. Chapter 6 summarizes and concludes the whole research.

# 2 State Of The Art

This chapter introduces state of the art for current privacy standards and GDPR. It provides an answer to Sub Research Question **(SRQ1)** “How is GDPR different from current privacy standards and why GDPR is needed? In order to answer this SRQ, it is broken into further Sub Research Questions i.e. (1) What are the current privacy standards? (2) How are the current privacy standards implemented in aviation sector? What is GDPR and how GDPR is different from current privacy regulations? (3) How to implement privacy change in an organization and what are the implementation strategies? We will begin by first explaining the related work done and the results obtained from the previous research work in this field. The goal of this chapter is to answer the SRQ and highlight the previously conducted research related to GDPR and to do literature review in order to develop understanding about the privacy regulations and the concept of GDPR.

## 2.1 Related Work

The most closely related work to this thesis is an article “Importance of Personal Data Protection Law for Commercial Air Transport” [2]. The article presents the findings as a result of an audit conducted in LOT Polish Airlines and reveals important aspects related to “casual” personal data handling in the commercial aviation sector. Air transport is the fastest growing industry in transportation sector [3], which means that the personal data is also processed at massive scales. The degree of intricacy and complexity of the practices involved in the processing of passenger personal data makes these issues unknown and hard to understand by the average passenger, but also difficult to be wholly grasped by the carriers themselves and by other entities of the aviation sector [2]. A practical obstacle is the lack of any real dialogue between practitioners from the aviation sector, lawyers, lawmakers and privacy experts [2]. This reveals a great need for someone with a knowledge of airline business to conduct research in the field corresponding to the needs of commercial aviation and have the solution validated by means of concrete feedback from experienced professionals (which is one of the goals of this thesis). Airlines together with many other entities store, record and process the personal data of passengers on massive scales**.** Such entities are travel agents, airport baggage handling companies, vendors of flight reservation systems, ground handling staff, border control agencies, airport management companies, and even the companies that manage loyalty programs i.e. frequent flyer programs. These intermediaries and the role they play at different stages of air transport, are practically unknown to the average passenger [2]. Therefore, it gives another layer of complexity to rights of data subjects and to regulate processing of personal data. Moreover, the archaic nature of the reservation systems, resulting from the maintaining of legacy technical systems dating from the time when the first such systems were implemented [2]. This goes in line with my own personal experience of working in an airline’s contact center, where the reservation systems and other tools used for flight bookings are outdated and information security practices are somewhat neglected. So, one thing obvious from the research is that the civil aviation sector is definitely lagging behind in terms of readiness for GDPR and there is a great room for improvement, which raises questions such as, what personal data protection measures are taken in environments such as contact centers where the personal data is exposed to the human level at most. With the introduction of GDPR, it will become impossible for airlines to survive if immediate actions are not taken to ensure high standards for personal data protection.

The second most relevant work is the Master’s thesis “Compliance Challenges with the General Data Protection Regulation” [4]. This thesis explains the challenges that the business sector faces as a result of GDPR introduction. The results of thesis show that interpretation of regulation is considered problematic in both literature and by the interviewees, but not it is not a major challenge. Even though overall the GDPR is considered straightforward, still the organizations seek counselling in legal matters [4]. This implies that appointment of data protection officer can be vital for airlines. Also, the research and findings in above mentioned thesis work is limited in a sense that challenges of GDPR adjustments according to organizations from different sectors are presented in general but no specific organization or business sector is studied, neither any solution to implement GDPR in a specific business field was presented. Other part of literature review are the white papers available online, suggested that the organizations such as airlines, processing personal data of EU citizens, will face the challenge to implement GDPR in mainly four areas, i.e. 1. Consent, 2. Transparency, 3. Data Security and 4. Documentation [19]. Therefore, later in chapter 4, this thesis focuses on these four areas for GDPR compliance.

As part of literature review, the next section presents the current privacy regulations, which latter forms the basis for method of applying current privacy regulations. After that, the GDPR is compared with current privacy regulations in order to point out key differences.

## 2.2 Current Privacy Regulations

EU data protection law; Directive 95/46/EC was designed a long time ago, in order to ensure that personal data of individuals is safeguarded [5]. The Convention contains a number of basic principles for data protection to which each Party must give effect in its domestic law before it enters into force in respect of that Party [5]. These principles still form the core of any national legislation in the EU. According to the Convention, personal data are to be 'obtained and processed fairly and lawfully' and 'stored for specified and legitimate purposes and not used in a way incompatible with those purposes', as well as 'preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored' [5].

However, Directive 95/46/EC has undergone changes due to evolving technology and as other laws have been updated, the privacy laws have also undergone amendment. One of the studies conducted [6] shows how data privacy laws in Europe have evolved over the past few years. Table 2.1 shows the evolution of privacy laws and sources that contributes to privacy statues.

The Table 2.1 suggests that the continuous updates and amendments to the original EU directive has not only added complexity for law enforcement agencies but also, it made the task of transposing the directive into national law a difficult task and that suggests a great need of one central regulation that all the member states should follow and transpose to their national law. As this thesis is focused on airline’s call center, so we will narrow the scope of research to aviation business and discuss the methods used to apply current EU privacy laws and regulations in airline sector which is discussed in Section 2.3.

## 2.3 Methods of Applying Current Privacy Regulations

This section explores the methods that are currently used to regulate the personal data, collected and processed in aviation sector. The most up to date legal tool in aviation sector is called as PNR directive (the personal data airlines collect to make flight reservation for passenger is commonly called as PNR or Passenger Name Record). PNR data is information provided by passengers and collected by air carriers during reservation and check-in procedures [7].

PNR data include several different types of information, such as passenger name, date of birth, passport number, travel dates, travel itinerary, ticket information, contact details, baggage information and payment information. On 21 April 2016, the Council of Europe adopted a directive on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime. The directive is called as EU PNR directive [8]. The directive establishes that PNR data collected may only be processed for the prevention, detection, investigation and prosecution of terrorist offences and serious crime. Under the new directive, air carriers will be obliged to provide member states' authorities with the PNR data for flights entering or departing from the EU [8]. The new rules create an EU standard for the use of such data and include provisions on strong safeguards as regards protection of privacy and personal data, including the role of national supervisory authorities and the mandatory appointment of a data protection officer in each Passenger Information Unit [8].

The current state of implementation of the Directive varies greatly across Member States. A number of them already either have a functional PNR system in place or are in advanced stages of its finalization. Member States have taken different approaches towards the setup of PNR systems. Some of them started the implementation process by drafting and adopting the relevant legal basis for the collection and processing of PNR data. Others first started building the technical infrastructure needed for processing PNR data and only later engaged in the legislative process. Concerning technical IT solutions for processing PNR data, some Member States have built it in-house, while others have opted for external contractors to develop it [9].

Although the PNR directive promises air safety for passengers and ensures great protection for air travelers, the studies have shown that it has its own shortcomings [10]. The PNR directive has been greatly criticized for excessive profiling, black listing, unjustified data retention periods and excessive collection of passenger’s data [10]. Moreover, it doesn’t provide any guidelines about data collection, storage, classification and processing when data is collected at an early stage, during flight reservation. The tool used by most airline is still EU data protection directive. The current version of EU data protection directive provides protection to individuals and the airlines (as data processing entities) are liable to obliged by the EU data protection directive. However, with the evolution of internet and information technology, the meaning of personal data is beyond the basic identifiers that were defined in EU directives. At the same time, ways of collecting personal data have become increasingly elaborated and less easily detectable [9]. For example, the behavior and location of the passenger can be traced down using cookies which are collected when passenger was using airline’s website to book flight ticket(s). Or for instance, from my own observation while working in contact center, if the passenger registers for the airline’s frequent flyer program and quote the frequent flyer number while each time making the reservation, the airline can monitor basic behavior like passenger’s seat preference, meal preference (that could lead to reveal information about ethnicity of passenger as it can be predicted from certain type of meal choices), travel companion, medical information or information about health conditions (for instance, the passengers requesting the wheelchair). Airlines also have to co-operate with border control agencies and share passenger’s data in order to ensure flight safety. All this inevitably raises the question whether the existing EU data protection legislations can still fully and effectively cope with these challenges [11].

To address this question, the Commission launched a review of the current legal framework at a high-level conference in May 2009, followed by public consultations until the end of

2009. A number of studies were also launched. The findings confirmed that the core principles of the Directive are still valid and that its technologically neutral character should be preserved. However, one of the issue remains problematic, i.e. coping with the impact of modern information technology [12]. The GDPR or General Data Protection Regulation is a solution devised by the EU parliament which is introduced in Section 2.3.

**Table 2.1:** Shows the sources of data protection laws and the relationship between different European supranational bodies and their legal instruments [6].

| **Supranational body** | **Council of Europe** | **European Union** |
|---|---|---|
| Treaty-level agreements | European Convention on Human Rights, Article 8 (1950)<br>Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981) | Treaty of Lisbon, Charter of Fundamental Rights, Articles 7 and 8 (2007) |
| Existing supranational legislation | Resolution (73) 22 on the Protection of the Privacy of Individuals vis-a-vis Electronic Data Banks in the Private Sector (1973)<br>Resolution (74) 29 on the Protection of the Privacy of Individuals vis-a-vis Electronic Data Banks in the Public Sector (1974) | 1995/46/EC Data Protection Directive<br>2002/58/EC 3-Privacy Directive<br>2006/24/EC Data Retention Directive |
| Proposed supranational Law | Revised Convention 108-Data Protection | Proposed data protection packages (three parts):<br>1. COM/2012/11<br>Proposed data protection regulation.<br>2. COM/2012/11<br>Proposed directive outlining public safety outs to COM/2012/11<br>3. COM/2012/09<br>Communication from Commission proposal |
| Body interpreting | Council of Ministers | Article 29 Working Party |
| National legislations | State party data protection legislation | National implementing legislation |
| Supranational court | European Court of Human Rights | European Court of Justice |

## 2.4 Comparison of GDPR and Current Privacy Standards

This Section introduces the GDPR and by making a comparison with current privacy regulation, the need of GDPR is highlighted.

### 2.4.1 The GDPR

On May 04, 2016, the text of General data protection regulation (GDPR) was published in the Official Journal of European Union, which is the result of 4 years of efforts to make a new data protection legal frame work for Europe [12]. GDPR is the new data protection regulation applicable throughout the EU. It will be effective from 25 May 2018 when it will replace the existing EC Data Protection Directive (EC/95/46) ("Directive") [12]. The GDPR is going to replace the existing frame work of EU data directive and its patchwork across all 28 EU countries. It it will introduce more effective individual rights to consumers, increased penalties for companies not complying with GDPR and enhanced data protection rights for data subjects, thereby giving data subjects great opportunities to exercise their rights and increasing the burden of compliance for data controllers and data processors [13].

GDPR applies to all companies processing and holding personal data of data subjects e.g. passengers, employees etc. residing in the EU, regardless of the company's location. It regulates how companies, authorities and organizations that work within the EU may collect, access, store and manage personal data [29]. The purpose of the GDPR is to give the people of the EU better control over how their data is used, if at all [14]. So the users have better control over their data and the controllers such as airlines have more liability to process the data after taking clear consent (in simple language), clarifying the purpose of processing and justifying the period of data retention. Also, personal data is redefined and the data which was of little importance before or which was not considered as personal data such as the IP address has now been classified as personal data. The EU GDPR is a regulation, not a directive. A directive is a set of rules presented to the entire EU that can then be interpreted and implemented differently by each of the 28 countries within the union. The new regulation, on the other hand, creates a unified digital economy across the EU, and will be implemented uniformly by one supervisory authority across the entire union [14]. Some of the new features that will shake many organizations (operating business not only in European Union but also the companies providing services to residents of European Union) [13] as the GDPR addresses the feature likes extra-territorial reach, restricted profiling, processing sensitive data and cross border data processing. Some other issues addressed in the GDPR that will affect the businesses are consent, privacy by design, data protection officers, right to be forgotten, are such issues on which the previous directive was either completely silent or either the issues were not clearly addressed. Moreover, heavy fines (20 million euros or up to 4 % of the total worldwide annual turnover of the preceding fiscal year, whichever is higher) is something that would shake the whole organization and thus makes everyone to comply with GDPR [1].

### 2.4.2 Key Changes Brought by GDPR

The Table 2.2 summarizes the key changes introduced by GDPR [14]. In the basic definition section of GDPR, the terms like 'profiling' are described, which are not mentioned in EU directive (See appendix-1 for basic definitions of GDPR and summary of GDPR articles). The Table 2.2 gives an overview of the key areas where GDPR has brought significant changes. For example, encryption is suggested as data security technique. Whereas, the EU directive didn't suggest any technique for secure data transfer. Moreover, it makes organizations accountable by demanding demonstration of data processing purposes. Also, the EU directive is silent on the topic of penalties in case of non-compliance, i.e. it doesn't suggest the amount of it at all, however, GDPR clearly states a fine of 20 million Euros in case of non-compliance [31].

**Table 2.2:** Summary of the key changes in privacy law brought by GDPR.

| **Article from GDPR** | **Key Subject** | **Key changes in Law** |
|---|---|---|
| 3,2,37-39 | Scope | The GDPR applies not only to business entities operating within Europe but also to service providers located outside of Europe, providing services to customers within EU [19]. |
| 26,27,28 | Accountability of Data processors | GDPR requires direct compliance from data processors and appointment of data protection officers (DPOs) and data processors are liable for fines in case of non-compliance [19]. |
| 7,8 | Consent | The GDPR requires that consent should be given freely (that data subject should be able to withdraw consent) and consent should be obtained in clear, plain and simple text (separated from terms and conditions) [23]. |
| 5 | Transparency | The data subject shall be aware of the purposes for which data is collected and processed and be able to make informed decisions [20]. |
| 16,17, 20 | Individual rights | GDPR gives enhanced rights to data subjects like right to be forgotten and the portability of personal data [23]. |
| 25 | Security of data | GDPR requires the controller and processor to have appropriate security measures in place, to ensure data security (like encryption of data, secure data transfer etc.) [20]. |
| 5,6,26 | Collection and purpose | In addition to having legal basis for data collection, the GDPR requires the controller and processor to have special safeguards in place where sensitive information is processed and appoint data protection officer. Moreover, profiling based on sensitive information has been banned [30]. |
| 16 | Quality | The GDPR entitles the data subject to have incorrect personal data rectified and controller is liable to make such corrections without undue delay [23]. |
| 28,33,34 | Data breach notifications | The GDPR requires the controller (or data processor if data breach has happened at data processor's premises) to notify the supervisory authority about data breach within 72 hours' time period [20]. |
| 37,39 | Accountability | The GDPR requires the data controller and data processor to demonstrate the compliance throughout the company, to data protection authority [19]. |
| 84 | Penalties | GDPR enforces huge penalties both on data controllers and data processors in case of non-compliance (up to 20 million Euros) [20]. |

## 2.5 Strategies for Implementing Process Change

To change a process in an organization is not an easy task, especially if the organization is as large as an airline and to undergo successful change, it is important for organizations to align their strategies and do proper planning. Some of the factors that any organization should consider before addressing the process change such as implementing privacy change could be the size and nature of business, the business model, the market sector, the categories of data subjects, data being processed, the competitors, risk exposure and appetite, the level of dependency on the processing of personal data, jurisdictions, other compliance requirements, size of workforce and available resources [29]. To successfully implement a new strategy or process change, the organization should bring together all the stakeholders to address the key issues. Organizing seminars or workshops together with all the stakeholders can be a great starting point. Many inputs to the strategy, especially elements from the as-is analysis, are typically delivered as part of a pre-analysis phase of a data privacy/GDPR project or program [29]. The other useful steps (before inducting new privacy program) could be:

a) Identify challenge the organization wants to address [28]. This means that higher management should take steps to raise awareness among employees and stakeholders about what is GDPR and what kind of challenges organization will have to face with the introduction of GDPR.
b) Define the extent and nature of the challenge [28]. Together with the privacy experts and practitioners, policy makers should do GDPR assessment exercises to estimate the nature of implementing GDPR.
c) Create detailed procedures of what will be done, including strategies to involve stakeholders in planning and implementation [28]. Develop methods to implement change.
d) Develop business models of current business processes. Find out the articles of GDPR relevant to business processes and translate the articles in terms of business processes. Then highlight the gaps that cause non-compliance.
e) Point out the activities that can help to fill the gaps and work together with all stakeholders to make introduction of activities successful.
f) If the business is outsourced, then data processor and data controller should together decide the roles and responsibilities for implementing privacy change. Nowadays, most of the Airlines have outsourced their contact centers and GDPR can only be implemented in outsourced environment through mutual understanding and common agreements.
g) Remodel the business process, include the activities that can help to fill gaps and validate new business model with practitioners from industry.
h) Identify approaches to enlist support from stakeholders to overcome anticipated barriers [28]. List all the possible approaches to overcome any issues that may hinder the implementation of process change.
i) Choose goals and monitor progress, then develop a time line for the intervention [28]. It is very important because the success of any project largely depends on monitoring progress and setting milestones.
j) Evaluate whether the intervention succeeded [28]. Once all the steps to implement policy change are taken, then the next step is to perform tests in form of assessments. Make pilot projects and see how the intervention works on small scale before inducting the plan in major business environment, so that any bugs or shortcomings can be easily addressed and fixed.

Once the enterprise has established a plan to implement privacy change that meets the needs of organizational stakeholders, objectives and goals, it is time to establish the proper governance framework to execute the formal data protection program [29]. To implement a successful change, it very important to have a proper governance frame work (setup in collaboration with concerned stakeholders). The organization will need specific competencies, responsibilities and structures to support the program and maintain its compliance with applicable laws and regulations. Certain roles and reporting arrangements must be created. In addition, GDPR implementation brings its own set of new requirements. Among them is the creation of a new role in the privacy organization— the data protection officer (DPO) [29]. So, appointing DPOs to serve as leaders for implementing GDPR in an organization can be productive and organizations can seek counseling at every step of process change.

## 2.6 Summary

In this chapter, we have

I- Revealed the previous study done related to privacy laws and GDPR.

II- Developed understanding about the current privacy laws in EU.

III- Identified the methods that are being used in order to implement current privacy standards.

IV- Done the comparison of GDPR with current privacy standards in order to develop understanding about how GDPR differs from current privacy regulations.

V- Discussed the strategies for implementing process changes such as privacy change.

# 3 Research Method

Before answering the Sub Research Question **SRQ2:** How much the contact center is GDPR compliant and what are the means to make it GDPR compliant, it is important to first define the research method used and the case scenario studied for analyzing business process. In order to develop a research method, the following sub research questions were devised: 1. What is the running case scenario and what is the purpose of studying it? 2. What are the methods used to collect and gathered data for research? 3. What is the method used to validate data collection and analysis? What is the scope of the case scenario? To implement the GDPR in an airline's contact center, a case scenario is studied on one of the most common business process in a contact center called "flight booking process". Section 3.1 of this chapter explains the method used to study case scenario and its purpose. As it is beyond the scope to cover every aspect of GDPR implementation in contact center, so the second section of this chapter (Section 3.2) explains the scope of the case scenario studied in chapter 4.

## 3.1 Method Used

This section explains the method used to conduct the case scenario in an airline's contact center. In order to develop better understanding of approach used in developing the method, this section is further divided in to following sub sections:

- Purpose
- Data collection method
- Methods used to analyze and solve the problem and validate the solution
- Methods used for validation

**Purpose:** The purpose to analyze case scenario in an airline's contact center is to

1. Describe business process (flight booking process) and develop understanding about the situation when contact center's agent makes a flight booking for Customer.
2. Identify key areas where GDPR non-compliance is happening.
3. Analyze the gaps between GDPR compliant and non-compliant flight booking process.
4. Present the activities necessary to make the business process GDPR compliant.

**Data collection method:** The data is collected by combination of two techniques [15]

1. Participant observation
2. Direct observation

**Participant observation**: Participant observation is done from the following two perspectives.

- Customer
- Contact center Agent

For the sake of this case scenario, a call was made to a contact center of the airline studied in this thesis and preliminary flight booking was made on 10 January 2018. All the booking steps observed were noted.

The observation from the contact center's agent's perspective was made on 12 January 2018 (as currently, I am the employee of the same contact center), and a flight booking was made for a customer over the phone. The steps observed in previous observations were compared and they were same.

**Direct Observation:** Direct observation was made by performing side by side monitoring for the contact center's agent making the flight booking for a customer (being a Quality Specialist in an airline contact center, this is one of my routine tasks). All the booking steps were carefully noted down.

### 3.1.1 Method Used to Solve Problem and Validate Solution

Table 3.1 shows the method used to study case scenario, in order to solve problem and validate the solution. The table summarizes the steps and the sequence showing steps supporting each other by means of input and output. P.A stands for purpose achieved. Each step is endorsed for a specific purpose and the P.A row explains what purpose is achieved by executing the respective step. All steps are connected with each other and serve as input for the following step, which form the shape of the research method used.

## 3.2 Running Scenario

This section defines the scope of case scenario studied in this thesis. Following assumptions are made:

1. It is assumed that the flight booking is made only for 1 adult passenger.
2. The customer calls using a mobile phone (so, able to receive any text messages/notifications sent by the airline).
3. The data objects and data flow is analyzed only for a part of the booking, however, how the personal data is shared with third parties (i.e. border control agencies, baggage handling companies at the airport) is beyond the scope of this case scenario.
4. The technical details of the secure payment system are also beyond the scope of this case scenario.
5. Reviewing the airline's data privacy policies and defining a consent statement are beyond the scope of this case scenario.
6. It is assumed that the credit card has enough amount to pay for the flight tickets and the payment is deducted without any obstacle (such as credit card denial due to internet banking not being active, etc.)
7. Also, it is assumed that the customer accepts the consent statement and gives full acceptance to record personal information.
8. The GDPR implementation has 3 phases, (GDPR implementation from the employee's perspective within the organization, GDPR implementation from the management perspective and GDPR implementation from the client's perspective) [16]. In this thesis, the focus is on GDPR implementation from client's perspective.
9. Documentation of activities for cross border data processing and security assessment of reservation system are beyond the scope of this thesis.
10. Studying the security capabilities of flight reservation system is beyond the scope of this thesis.
11. The purpose of this thesis is to focus on four most important key areas for GDPR implementation, i.e. consent, transparency, data security and documentation.
12. It is assumed that the customer gives consent for call to be recorded.

**Table 3.1:** Detailed research method summarized in form of steps

| | | |
|---|---|---|
| **Step 1**<br>**Case description and modelling of original business process** | **Description** | 1.Describe the flight booking process (As-Is) 2. Perform business process modelling notation (BPMN) for the flight booking process to highlight the business activities, data collection, recording and the flow of data during the business process. |
| | **Input** | Data collected by method described in Section 3.1 |
| | **Output** | Section 4.3, Figure 4.2 |
| | **P.A** | Flight booking process described and the understanding about the business process of contact center developed. |
| **Step 2**<br>**Applying GDPR on original business process** | **Description** | Applying GDPR on flight booking process by: Instantiating key definitions from GDPR in terms of flight booking process and identifying and instantiating the GDPR articles relevant to flight booking process |
| | **Input** | GDPR Articles 5, 6, 7, 13, 24, 30 |
| | **Output** | Key areas Identified are Consent, Transparency, Documenting Activities, Data Security (Section 4.4, Section 4.5) |
| | **P.A** | Key areas of non-compliance identified from flight booking process |
| **Step 3**<br>**Making business process GDPR compliant** | **Description** | Finding out the activities needed to be introduced in BPMN done for flight booking process, to make flight booking process GDPR complaint. |
| | **Input** | Introduce activities in original flight booking process (Figure 4.2) |
| | **Output** | GDPR compliant flight booking process (Figure 4.3) |
| | **Purpose Achieved** | Gaps between non-compliant GDPR flight booking process and compliant GDPR flight booking process filled. Section 4.6 (Figure 4.3***)*** |
| **Step 4**<br>**Detailed analysis in terms of practical business requirements** | **Description** | Detailed analysis of means to fill gaps between GDPR compliant flight booking process and non-compliant flight booking process against key areas (output of step 2) to check validity in practical business environment. |
| | **Input** | Questionnaires to validate the activities introduced in Step 3 |
| | **Output** | Detailed analysis of means for filling gaps between GDPR complaint flight booking process and non-compliant flight booking process. Section 4.7 (Figure 4.4, Figure 4.5, Figure 4.6, Figure 4.7***)*** |
| | **P.A** | Validation of GDPR complaint flight booking process (output of Step 3) from practical business point of view. |
| **Step 5**<br>**Validation of proposed solution** | **Description** | Validation of solution proposed in step 3 and step 4 |
| | **Input** | Questionnaires designed in chapter 5 (interviews and feedback) |
| | **Output** | Results and validation |
| | **P.A** | Suggested/proposed model validated |

## 3.3 Summary

In this chapter, following research questions were answered:

1. The purpose of case scenario
2. The methods used to collect and gathered data
3. Method used to validate data collection and analysis
4. Scope of case scenario

# 4 Analysis of Airline Business

This chapter provides answer to Sub Research Question **SRQ2:** How much is the contact center GDPR compliant and what are the means to make it compliant? This question is answered by breaking down the SRQ2 in to further SRQs (1). What is the background of the case scenario? (2) What are the key systems used in a contact center? (3) What does the description of flight booking process look like? (4) Which activities in the current business process are not GDPR compliant? (5) Which terms of GDPR are relevant to flight booking process? (6) Which activities are needed to be introduced to make the business process (i.e. flight booking process) GDPR compliant? (7) How the new activities will fill the gaps between compliant and non-compliant business processes?

This chapter has my contribution in form of business process models I created using my knowledge from my 3 years of work experience in contact center of North European Airways (my current employer) where I have worked in different roles, giving me the perfect opportunity to use the data for a case scenario for flight booking process. And using my knowledge, I created business models for flight booking process (As-Is) and flight booking process (To-be).

In the previous chapter, the method used to study the case scenario was discussed. The current chapter is designed using the method described in Chapter 3. The case scenario studied is in an outsourced call center situated in the EU, handling the flight booking related business activities for a European Airline. For sake of privacy and confidentiality, the names of the business entities have been replaced by fictious names as shown in Table 4.1.

**Table 4.1:** Describes the entities used to study case scenario

| | |
|---|---|
| **Airline** | North European Airways |
| **Third party (handling contact center for airline)** | Mike Business solutions Ltd. (MBS) |
| **Actors** | MBS Agent, Customer |
| **Process** | Flight booking process |

## 4.1 Background

**Contribution:** Running case scenario is the flight booking process, for which I collected the data using the data collection method described in Section 3.1. With combined knowledge of business process modelling (BPMN), knowledge of IT and knowledge I gained over the past 3 years while working in contact center of North European Airways (outsourced to MBS), I created the models (Figure 4.2 and Figure 4.3) which forms the basis of my contribution. In order to develop the basic understanding for audience of thesis about the running case scenario, the background looks as follow:

During the flight booking process, the customer calls North European Airways' helpline to make flight booking. When customer calls, a voice recording is played, which is a welcome message and customer is presented with 3 options. as follows: (i) For booking new flights press 1, (ii) For technical support (for travel agents) press 2, (iii) for refund related inquiries press 3. It is assumed that the customer presses 1 and customer's call is received by MBS agent. The whole flight booking process consists of collaboration between customer and contact center's agent (MBS Agent). Figure 4.1a shows the broader view of flight booking process, where *seller* is the MBS agent, representing the airline and selling the product called *Ticket.* The *buyer* is the customer who calls to purchase the ticket and the MBS agent uses *Ticketing Network* to issue the flight tickets.

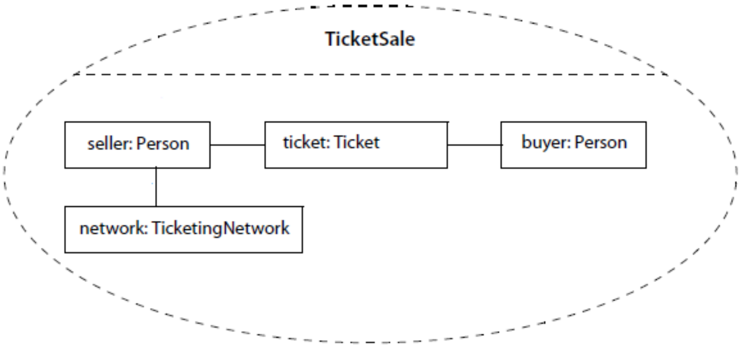


**Figure 4.1a**: The collaboration diagram for ticket sale process [18]

This collaboration may seem simple, with simple steps of airline's ticket sale, however, it has other layers. The process needs to be scrutinized deeper to gain information about the business process and to develop procedures to apply GDPR. The key systems and key components need to be described, in order to gain deeper understanding about the flight booking process. As the running case scenario is about a business process (flight booking process) of a real airline (name replaced with North European Airways), whose contact center is handled by third party (name replaced by Mike Business Solution or MBS), so the key systems used in contact center are also described in next section as observed but with real names replaced by pseudo terms.

## 4.2 Key Systems

The key systems are

1. MBS site
2. North European Airways' VDI (Virtual desktop infrastructure)
3. MBS voice recording system

Table 4.2 shows the description of each key system as well as type of information each key system stores. The customer interacts with airline by calling airline's helpline, which is connected to MBS Agent through MBS site. MBS site or MBS system is a cisco based interface, commonly used by contact centers, to receive calls [22]. This system is connected with MBS voice recording system in a way that all the incoming and outgoing calls are recorded. The MBS system also stores information like caller ID and the date and time of call. MBS agent connects with North European Airways (VDI), which is a virtual environment [18] provided by North European Airways to MBS, in order to search for flights, find flight prices, prepare flight bookings, stores customer's personal information (name, email, mobile number, date of birth, credit card information) and issue electronic tickets. The information including the personal information of customer and credit card information goes from customer to North European Airways' database by first entering the MBS system, getting recorded (in audio form) in MBS voice recording system and at the same time noted by MBS agent and then inserted in North European Airways' database (so no encryption or automated technique is used) for information that can be sensitive for example, credit card information. This makes one thing very clear, that the information security practice of contact center has very loose security policies and makes contact center non-compliant to GDPR as well as other international security standards.

### 4.2.1 Software/tool used by Airline to Book Flight Tickets

The tool or software used to setup flight booking by most Airlines and travel agencies is called as "Amadeus reservation system" [25]. This tool can be used by agents having valid IATA registration (The International Air Transport Association (IATA) supports aviation with global standards for airline safety, security, efficiency and sustainability [24]) to make flight bookings. Amadeus flight booking system can be used to display airline availability, schedules, timetables, book/cancel airline reservations, construct passenger name record (PNR), retrieve and modify PNR, and price an Itinerary [25]. Flight bookings are often referred as PNR by airlines. Although, assessing security and finding security loopholes is beyond the scope of this thesis, I have listed (from my own experience) the flaws of this reservation system which makes the software not adhering to GDPR security requirements:

1. The Amadeus system creates history for every PNR. The purpose of this feature is to document all the activities performed on PNR and keep track of actions performed by contact center agent on PNR. Figure 4.1b shows screenshot of PNR history. *AS XXXXXX* is an alpha-numeric unique code for agent who creates or modifies the booking, *DS-00000000* is the office code or location of agent (dummy values are used for this example) and *12Jan1541z* is the time stamp when the agent created or modified PNR. Amadeus tracks each and every step e.g. adding flights in PNR, adding passenger details, adding contact details etc. However, it has very poor signatures tracking capabilities. For example, it does not keep track of who access the booking. Also, the contact center's agent can search for PNR using first and last name of passenger. If the agent doesn't make any modification in PNR, then no foot prints are left, which makes it impossible to investigate if an agent from contact center has accessed the booking (for sake of stealing personal data). This makes the system quite vulnerable to certain attacks such as insider threats, social engineering etc.

2. From digital forensic investigation's point of view, it is extremely difficult to find the providence of data breaches (as details of any passenger can be retrieved just with name) because the software does not keep track of agent's foot prints (if no modifications are made in PNR).

3. The Amadeus booking system caught attention when it was "failed" due to network issue or possible hack, causing delays of thousands of flights around the world, which raised certain security concerns by IT experts [26].

As is beyond the scope of this thesis to suggest improvements for this software (due to limited information available about the specs of software used in contact center and data transfer mechanism), so it can be potential area for future research.

## 4.3 Describing and Modelling Flight Booking Process

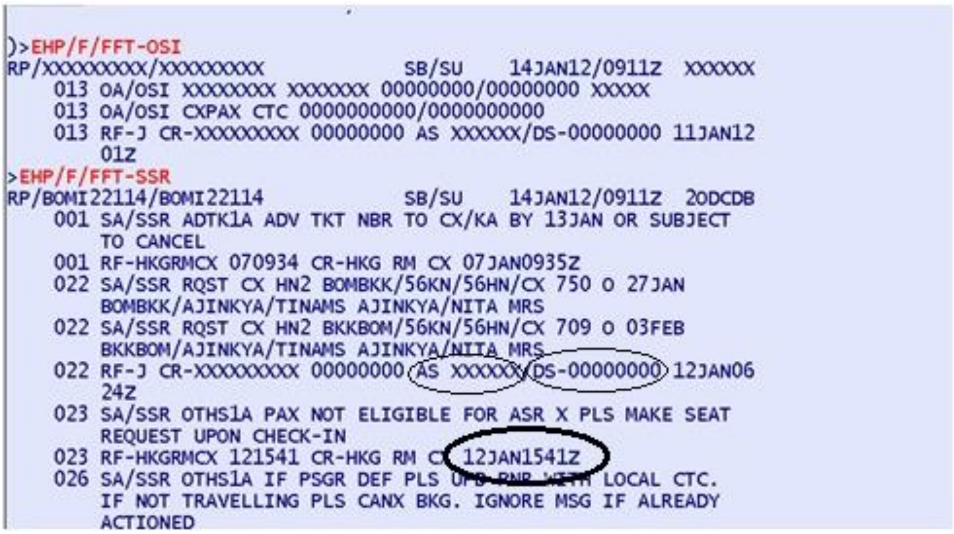
After having developed understanding about key systems and software used for booking flights, the next step is to describe flight booking process by means of business process modelling notation (BPMN).

Figure 4.2 shows the flight booking process that occurs with the collaboration of actors (the *MBS agent* and the *customer*). This Figure includes 2 main pools, presenting *customer* and

*Airline* where the *Airline's* pool is further divided in to two pools, one corresponds to *contact center's agent (MBS Agent)* and the other one is the *North European Airways' VDI System (as the CC agent* continuously interacts with this system to prepare flight booking and issue flight tickets).

Figure 4.2 shows that customer's personal data (contact number) is reached to *Airline* as soon as the call is connected when the *MBS agent* can see the caller ID (activity B1). Now as soon as the customer shows interest for booking flight tickets or inquire flight prices (activities A4 and B3), the *MBS agent* asks for further information i.e. *number of passengers, flight origin/destination, date of departure* and present the *price* (activities A7 and B7). So, we already have the data objects or data types which are being recorded in voice recording system called *MBS Voice Recording System*. The *MBS agent* then presents customer with further information such as *flights dates, times, terminals* from which the flights depart and price of flights. Figure 4.2 also shows that in case if *customer* agrees to pay the price, then *MBS agent* asks further information e.g. *customer's name, contact details (email and mobile), date of birth* and *credit card information* (activities A7 and B7). All such information, passes from *customer to MBS agent* via different channels such as cisco phone, the *MBS Voice Recording System* (which is recording all the information) and then to *North European Airways' VDI database* where all the information is stored to issue flight *ticket* (B13). The payment process clearly doesn't meet the requirements set by EU standards [20]. From GDPR point of view, this process may not be feasible or way of obtaining information have certain violations, especially the way credit card information is handled may subject to scrutiny as it depicts the insufficient technical measures adopted by contact center to protect *customer's* personal data from theft or privacy violations. Finally, once the *ticket* is generated (B15), we have the information such as *booking number* (the number that can be used to retrieve customer's booking from the *Airline's* website in order to view travel plans, to modify travel plans or to cancel the travel plans), the *price of ticket* paid, *seat number of passenger* and the *date* when the ticket was purchased.

In order to measure the compliance of this business process, the articles of GDPR need to be instantiated in terms of airline business model, which is done in next section.



```
)>EHP/F/FFT-OSI
RP/XXXXXXXXX/XXXXXXXXX            SB/SU    14JAN12/0911Z  XXXXXX
    013 OA/OSI XXXXXXXX XXXXXXX 00000000/00000000 XXXXX
    013 OA/OSI CXPAX CTC 0000000000/0000000000
    013 RF-J CR-XXXXXXXXX 00000000 AS XXXXXX/DS-00000000 11JAN12
        01Z
>EHP/F/FFT-SSR
RP/BOMI22114/BOMI22114            SB/SU    14JAN12/0911Z  2ODCDB
    001 SA/SSR ADTK1A ADV TKT NBR TO CX/KA BY 13JAN OR SUBJECT
        TO CANCEL
    001 RF-HKGRMCX 070934 CR-HKG RM CX 07JAN0935Z
    022 SA/SSR RQST CX HN2 BOMBKK/56KN/56HN/CX 750 O 27JAN
        BOMBKK/AJINKYA/TINAMS AJINKYA/NITA MRS
    022 SA/SSR RQST CX HN2 BKKBOM/56KN/56HN/CX 709 O 03FEB
        BKKBOM/AJINKYA/TINAMS AJINKYA/NITA MRS
    022 RF-J CR-XXXXXXXXX 00000000 AS XXXXXX/DS-00000000 12JAN06
        24Z
    023 SA/SSR OTHS1A PAX NOT ELIGIBLE FOR ASR X PLS MAKE SEAT
        REQUEST UPON CHECK-IN
    023 RF-HKGRMCX 121541 CR-HKG RM CX 12JAN1541Z
    026 SA/SSR OTHS1A IF PSGR DEF PLS UPD PNR WITH LOCAL CTC.
        IF NOT TRAVELLING PLS CANX BKG. IGNORE MSG IF ALREADY
        ACTIONED
```

Figure 4.1b: History created in backend by Amadeus flight booking software

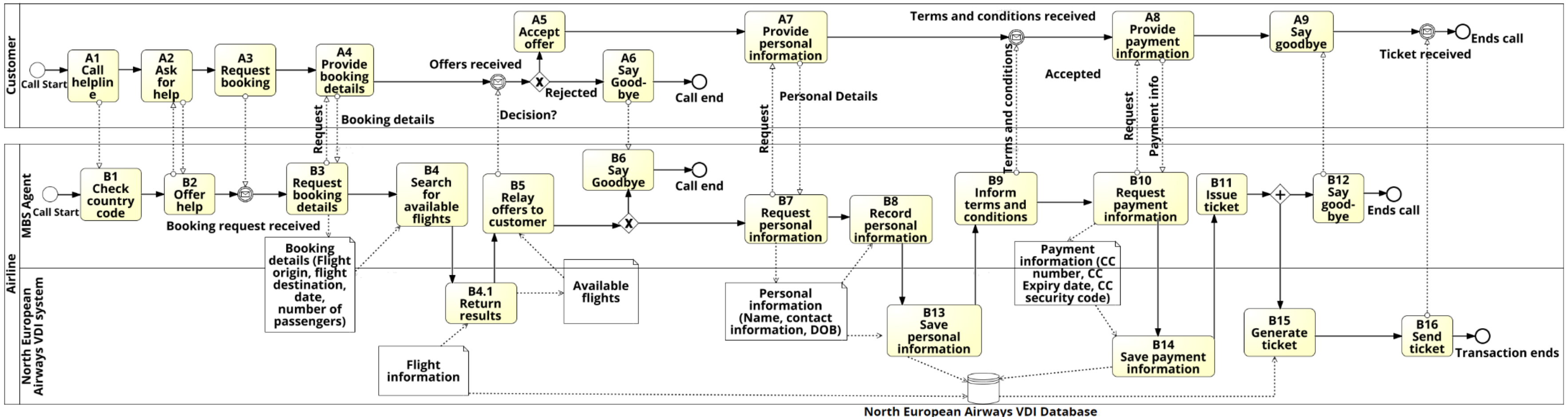

Customer
Airline
MBS Agent
North European Airways VDI system
Call Start
A1 Call helplin e
A2 Ask for help
A3 Request booking
A4 Provide booking details
Offers received
A5 Accept offer
Rejected
A6 Say Good-bye
Call end
Decision?
Request
Booking details
A7 Provide personal information
Request
Personal Details
Terms and conditions received
Terms and conditions
Accepted
A8 Provide payment information
Request
Payment info
A9 Say goodbye
Ticket received
Ends call
Call Start
B1 Check country code
B2 Offer help
Booking request received
B3 Request booking details
B4 Search for available flights
B5 Relay offers to customer
B6 Say Goodbye
Call end
B7 Request personal information
B8 Record personal information
B9 Inform terms and conditions
B10 Request payment information
B11 Issue ticket
B12 Say good-bye
Ends call
Booking details (Flight origin, flight destination, date, number of passengers)
B4.1 Return results
Available flights
Flight information
Personal information (Name, contact information, DOB)
B13 Save personal information
Payment information (CC number, CC Expiry date, CC security code)
B14 Save payment information
B15 Generate ticket
B16 Send ticket
Transaction ends
North European Airways VDI Database

**Figure 4.2**: Shows BPMN for flight booking process in an Airline's contact center

**Table 4.2:** Description of key systems used during the flight booking process.

| | | |
|---|---|---|
| **North European Airways' VDI** | **Description** | This system is known as "VDI" which is the virtual environment provided by the airline. VDI or Virtual desktop infrastructure is a virtualization technique enabling access to a virtualized desktop, which is hosted on a remote service over the Internet. It refers to the software, hardware and other resources required for the virtualization of a standard desktop system [18]. MBS Agent accesses this system by logging in to North European Airways' VDI site. This system enables the MBS agent to communicate with North European Airways' database to search for flights, find price offers as well as to setup flight bookings for customer, insert credit card details to deduct charges and to generate electronic tickets. |
| | **Type of Information recorded** | Customer details (details which are collected to setup flight booking and other information related to electronic ticket) |
| | **Access** | MBS agent having valid user name and token password (with access provided from IT department) can access the VDI site |
| **MBS Site** | **Description** | It is the system MBS agent uses to log in to MBS site to sign in to cisco system and to be able to receive calls from customers. This system is the system that handles calls interaction (i.e. answering call, ending call, putting callers on hold) etc. One such similar system is described at cisco's webpage [22]. |
| | **Type of Information recorded** | Caller ID, length of call, date and time of call |
| | **Access** | MBS agent having valid user name, password (issued by MBS' IT department) and extension number for internal cisco phone |
| **MBS Voice Recording System** | **Description** | This system records calls and runs back to back with MBS site. This system is part of MBS site because the software for this system is installed in MBS site, however, one system is handling live interaction and other system is archiving the conversation. This is also used for listening voice recordings for quality assurance purposes. |
| | **Type of Information recorded** | Voice calls recording |
| | **Access** | This system can be accessed by users (supervisors, managers) having valid username and password. It can be accessed from the company premises as well as from home. |

## 4.4 Checking Compliance of Flight booking Process With GDPR

The compliance of flight booking process with GDPR is measured by:

1. Extracting basic terms (Article 4) of GDPR in terms of flight booking process (As-Is).
2. Instantiating the articles of GDPR relevant to flight booking process (As-Is).
3. Identifying gaps between the flight booking process (As-Is), GDPR and suggesting means to fill those gaps.

### 4.4.1 Extracting Basic Terms of GDPR

In order to achieve first part of Section 4.4, Table 4.3 is made to define key terms of GDPR. The terms defined in this section will serve as basis for Table 4.4**,** which will identify the gaps between GDPR and flight booking process (As-Is), modelled in Figure 4.2. The table also refers to activities described in Section 4.3, where applicable. So, once the basic terms of GDPR have been defined in terms of flight booking process, the next step is to instantiate the articles of GDPR in terms of airline business model (As-Is) and then suggest the means to fill those gaps.

### 4.4.2 Instantiation of Relevant Articles of GDPR

Table 4.4 shows the relevant articles of GDPR instantiated in terms of flight booking process of airline. The purpose to do so is to highlight the gaps between GDPR and flight booking process modelled in Section 4.3. Each Article (Keeping the scope of thesis i.e., to achieve compliance in four key areas which are: consent, transparency, data security and documentation) is applied on activities of flight booking process (Section 4.3, Figure 4.2). The Table 4.4 shows the result of instantiation of Article 5 from GDPR and it is observed that in flight booking process (As-Is), no valid consent is obtained from customer and therefore the flight booking process described and modelled in Section 4.3 is not compliant to concept of consent from GDPR. Similarly, the instantiation of Article 6 and 7 revealed that the flight booking process (As-Is) has no legal grounds, as no valid consent is obtained from customer. So one of the key area that needs to be focused is ‘consent’. Further examination of Table 4.4 shows that GDPR requires airlines to send confirmation of data being processed, categories of data being processed, procedure to correct personal data stored by airline and process to receive copy of personal data. However, according to flight booking process (As-Is), there is no such confirmation sent to customer and therefore the process is not compliant to Article 13. Therefore, the second key area of focus for GDPR compliance is ‘transparency’. Table 4.2 shows that the airline has no proper tools to securely process the payments and therefore third key area for focus is ‘data security’. There is no documentation of activities in current flight booking process by data processor (i.e. MBS), so the fourth key area of focus for GDPR compliance is ‘documentation’. So, the Table 4.4 has revealed four key areas, where GDPR compliance is needed i.e. 1. Consent, 2. Transparency, 3. Data security and 4. Documentation.

From now onwards, we will call flight booking process described in Section 4.3 as flight booking process (As-Is) and corresponding business model (Figure 4.2) as business process model (As-Is). Similarly, flight booking process described in Section 4.6 is called as flight booking process (To-Be) and corresponding business model (Figure 4.3) as business process model (To-Be).

**Table 4.3:** Summarizes the key terms of GDPR in terms of flight booking process (As-Is)

| **Key terms from GDPR** | **Flight booking process (As-Is)** | |
|---|---|---|
| Personal data | Name, age, mobile number, email address, home address, passport number, Frequent flyer number, caller ID. | |
| Processing | Collecting | B1: Checks country code<br>B3: Requests booking details<br>B10: Requests payment information |
| | Recording | B8: Records personal information<br>B13: Saves personal information<br>B10: Saves payment information<br>Besides these activities shown in Figure 4.2, all the conversation with Customer is recorded in voice recording system. |
| | Documenting | Missing |
| Filling system | Flight Booking information (activity B15). Criteria to access: Booking reference number Accessible through: flight ticketing system (for internal use by airline's staff members). | |
| Controller | North European Airways | |
| Processor | Mike Business solutions Ltd (MBS). | |
| Recipient | • Border control agencies<br>• Baggage handling companies at airport | |
| Consent | Missing | |
| Cross border processing | Processing in multiple contact centers located in EU (so transferring data in between contact centers). | |

**Table 4.4:** Description of relevant Articles from GDPR in terms of flight booking process (As-Is)

| Relevant Articles | Instantiation of articles in terms of flight booking process (As-Is) | Gaps |
|---|---|---|
| **5** | Name, age, mobile number, email address, passport number, frequent flyer number, caller ID, be processed lawfully i.e.<br>• Consent be obtained from customer to process this data.<br>• Stored in a way that is secured and proper tools be used to safeguard such data.<br>• Provide customer with privacy notice explaining the purpose of data collecting, recording and storing (Activities B1, B3. B7, B8, B10, B13, B14) (transparency). | - No consent is taken in current business process to process personal data.<br>-The payment information is not handled securely.<br>-There is no activity in business model that would describe the transparency of data processing, i.e. privacy notice is missing. |
| **6,7** | Processing of name, age, mobile number, email address, passport number, frequent flyer number, caller ID shall have legal grounds if:<br>• The customer of airline has given consent to process personal data for the purpose of flight booking.<br>• The airline should take consent from customers using plain and simple language. | No consent is taken in current business process to process personal data (i.e. name, age, mobile number, email address, passport number, frequent flyer number, caller ID). |
| **13** | When name, age, mobile number, email address, passport number, frequent flyer number, caller ID related to customer is collected, the airline should provide the information such as:<br>• The identity and contact details of Airline<br>• The contact details of data protection officer.<br>• The recipient of personal data (baggage handling staff at airport, border control agencies). | No confirmation is sent at the moment regarding the fact that personal data is shared with ground handling staff and border control agencies. As currently there are no data protection officers appointed, so no contact details of data protection officers are given either. |
| **24** | Proper technical measures be taken to ensure personal data is processed safely i.e.<br>• Proper secure tools to process data<br>• Limited access to production floors in work spaces where such data is processed (no use of mobile phones, electronic devices, restricted access to social media websites for contact center agents) | There is no secure credit card payment system in place and the agent asks for credit card information verbally. Moreover, the network policies are also not strict and therefore making personal data vulnerable to certain cyber-attacks such as social engineering attacks. |
| **30** | MBS as representative of North European Airways should document all the activities. | Documentation of flight booking reference number is missing. |

## 4.5 Key Areas for GDPR Compliance

Figure 4.3 (flight booking process To-Be) shows the updated version of Figure 4.2 (flight booking process As-Is), after introducing the activities which are required to achieve GDPR compliance.

The key areas identified in previous section, where GDPR compliance is focused are

- Consent (Introduction of activities **G2** and **G3**)
- Transparency (Introduction of activities **G1**, **G6** and **G5**)
- Data Security (Introduction of activity **G4.1** and **G4.2**)
- Documenting activities (Introduction of activity **G5**)

So, in order to make the flight booking process (As-Is) GDPR compliant, the activities mentioned above will be introduced in it. The next section presents the detailed description of how the GDPR compliant flight booking process (i.e. flight booking process To-Be) should function.

## 4.6 Description of GDPR Complaint Flight Booking Process

As shown in Figure 4.3, the process starts when the customer calls the airline's helpline (activity A1). The contact center's agent i.e. *MBS agent* checks the caller ID to verify which country *customer* is calling from to select correct currency for ticket issuance (activity B1). The *customer* asks for help to make flight booking (activity A2). *MBS agent* offers help to make flight booking and also gives location information (activity G1), Now this is one of the GDPR activity to meet transparency requirement. Then, the *customer* requests for booking (activity A3). In order to determine specific requirements, such as number of passengers, passenger types, origin/destination of flight, departure date and flight departure/ arrival times **(**activities A4 and B3**)**. Now the information gathered (in activities A4 and B3) is input (for activity B4) for searching flights and best price. Once the agent has found the best price, the next step is to convey the *consent* that would be a statement in simple and easily understandable language (activity G2 and G3). The reason of introducing these activities at this stage is because it could be possible that the customer is making booking on behalf of someone else and thus it is important to take consent from passenger.

Once consent statement has been conveyed (activities G2 and G3), the next activity is to convey the price of flights (activity B5). This activity has two outcomes. Either the *customer* (passenger) rejects the offer (activities A6 and B6) or either the *customer* accepts offer (activity A5) and *MBS agent* requests booking details (activity B7). Then, the *customer* provides booking details (activity A7). The booking details include *name, email address, mobile number, date of birth, passport number, expiry date of passport and frequent flyer number*. The *MBS agent* records information (activity B8) and saves the information in secure database of North European Airways (activity B13). Then, the *MBS agent* advises *customer* about fare rules (i.e. ticket cancellation and change policies, etc.) as shown in Figure 4.3 (activity B9). After advising fare rules, the contact center agent (i.e. *MBS agent*) advices *customer* about the payment process. The *MBS agent* offers to send secure payment link on mobile number of *customer*. *Customer* needs to use this link within specific time frame to enter credit card details and make payment. Once the payment has been made, the payment system sends message of success to airline's system which pops up on the screen of *MBS agent*, who then issues the ticket and send it to the email of *customer* (activities B15 and B16). Also, since the previous flight booking process described in Section 4.3 did not have any documentation at the processor level, so activity G5 is introduced as shown in Figure 4.3. This activity shows that the contact center agent will document the details of booking, such as booking reference number, price paid for ticket, date and time of booking etc. The MBS agent doesn't need to document all the processing activities as the flight booking software (Amadeus) documents all the steps (as mentioned in Section 4.2.1). So, documenting flight booking reference number by MBS agent (activity G5) means documentation of all the activities involved in flight booking process. Also, as the GDPR requires the airlines to send the confirmation about the personal data and categories of personal data being processed, so activity G6 shows the email confirmation sent which will contain the data categories being processed, purposes of data processing, customer's right to be forgotten, the procedure to transport data and the right to rectify data. One example of such email is shown in Appendix 2.

## 4.7 Gap Analysis and Recommendations

In order to adapt a broader approach towards GDPR compliance and cover the topic in detail, the questionnaire based approach is used. Such questionnaires can be used by contact center to do GDPR assessment of business processes in different departments within the company. The questionnaires are designed based on my own experience of working in an airline contact center and expert opinions (Appendix 4, 5, 6).

The following section contained detailed analysis for each component identified in Section 4.5. Also, another purpose of this section is to identify the entity liable (data controller or data processor) for implementing activities suggested in Section 4.5, to achieve GDPR compliance.

### 4.7.1 Terminologies used in Following Sections

- Compliance Questions- The specific components assessed which are derived from industry standards or regulations.
- Business process model (As-Is) – Flight booking process (As-Is) modelled in Figure 4.2.
- Business process model (To-Be) – Flight booking process (To-Be) modelled in Figure 4.3.
- Degree of compliance –This represents the state of conformance/non-conformance of the contact center to the regulations.
- Recommendations –This show the suggestions to achieve compliance.
- Who is liable? – This represents whether data controller has the liability to implement solution or data processor (or mutual liability).

Note: CON means when no issues were found (conforming) and NON-CON means nonconfirming (when further action is needed to achieve compliance) and PAR means partially conforming to standards.

The purpose of next sections is to support the introduction of new activities (from Section 4.5) to achieve GDPR compliance in practical business. Each key area is analyzed separately by doing mapping against common compliance questions.

### 4.7.2 Consent

In order to map consent activities (which were suggested in Section 4.5) on broader level, to make flight booking process (As-Is) GDPR compliant and analyze how the activities fit in practical business environment, following steps are taken in Table 4.5.

- Highlight the gaps from consent perspective between business process model (As-Is) and Business Process Model (To-Be) and point out suggestions to fill the gaps.

- The means to fill the gaps are activities introduced in Section 4.5. Table 4.5 summarizes the recommendations to fill the gaps and how the activities will help to do so in practical business environment.
- In order to have broader understanding of newly suggested activities, sub processes corresponding to these activities are developed which are shown Figure 4.4 and Figure 4.5.
- The sub processes are designed to give a broader view of solving the problem and are not intended for implementation level design.

**Common mistakes:**

Some mistakes that contact center may make with respect to key area ‘consent’ are:

- Assuming that customer already knows the purpose of data processing - No matter how frequently your customer travels or how obvious is the nature of data processing, the GDPR requires the organizations to communicate the purposes of data processing and take a valid consent (over the phone), each time customer requests for new flight booking [30].
- Assuming “we will never receive consent withdrawal request; our customers never do that” – It is another example of bad practice to trust customer relationship and assume customer will never ask the airline (or contact center) to stop processing data.
- Spamming all customers with emails of consent – Another possible mistake could be that airline will simply send emails stating the new consent statement and assume that all the customers have read, understood and accepted it.
- Assuming customers have read, understood and accepted consent in the past – This is a wrong practice as the GDPR requires the airline to take fresh consent every time new flight booking is made and consent cannot be used retroactively [30].
- Not recording consent statement (for future documentation) – It is not only important to take consent but also it is very important to record that consent, so that in case of any future dispute, the airline will be able to justify the legal grounds of data processing.
- Not erasing data that belong to customer, while customer has withdrawn consent to store or process the data. Data controllers and data processors have liability to erase data from all devices if consent has been withdrawn from customer.

### 4.7.3 Transparency

Here, the compliance activities related to transparency (one of the key area identified in Section 4.4.2), are mapped against the compliance questions and analyzed how the activities will fit in practical business environment. Following steps are taken in Table 4.6 to do the mapping of activities against business process models.

- Highlight the gaps from transparency perspective between business process model (As-Is) and business process model (To-Be).
- The means to fill the gaps are new activities which are introduced in Section 4.5. Table 4.6 summarizes the recommendations to fill the gaps and how the activities will help to do so in practical business environment.
- In order to have broader understanding of activities, sub-process corresponding to these activities is developed which is shown in Figure 4.6.
- The sub process is designed to give a broader view of solving the problem and is not intended for detailed level/implementation level design.

**Common mistakes:**

- Assuming that customers already know what will be done with their data or customers know the purposes of data collection – The airlines have liability to inform customers about purposes of data collection (each time when new flight booking is made).
- Assuming Customers would read the privacy notice on website- The airlines have liability to communicate their privacy notice and make sure customers receive it!
- Assuming having privacy notice in English is enough – It is the responsibility to translate the privacy notice in all the EU languages or at least in all the languages of countries where airline(s) operates flights (to/from) [30].
- Hiding the fact that the personal data is processed by third parties - Usually airlines are reluctant to convey that the data is processed by third parties especially when the data processor operates from non-EU countries. However, under GDPR, it is not acceptable and the airlines should clearly convey the information about any data processors processing information on behalf of airlines.

### 4.7.4 Data Security

The compliance activities related to data security (one of the key area identified in Section 4.4.2) are mapped in this section against the compliance questions and analyzed how the activities will fit in practical business environment. Following steps are taken in Table 4.7 to do the mapping.

- Highlight the gaps from data security perspective between business process model (As-Is) and business process model (To-Be) and point out suggestions to fill the gaps.
- The means to fill the gap are activities introduced in Section 4.5. Table 4.7 summarizes the recommendations to fill the gaps.
- In order to have broader understanding of activities, sub-process corresponding to these activities is developed, which is shown in Figure 4.7.
- The sub-process is designed to give a broader view of solving the problem and is not intended for detailed level/implementation level design.

Comments: The research showed some secure payment systems using similar approach, already developed. One such advanced form of secure payment system for contact center could be electronic wallet based secure system [21].

**Common mistakes:**

- Blindly trusting employees of contact center – As the flight booking system (discussed in Section 4.2.1) has very poor signatures tracking capabilities, so the airlines should use tracking software together with Amadeus flight booking tool to make sure that only the right person accesses the flight booking data and no information should be retrieved without permission of customer.
- Loose network policies – Currently, the contact center (being studied in this thesis and many other contact centers) do not pay much attention about network policies and employees working with flight reservation tool (Amadeus) may have very easy access to social media websites such as Facebook, Twitter etc. which greatly increases the chances of data breaches.

- ➢ Allowing use of electronic devices in production- This is another practice that can put the contact center on risk of different data breaches (as it is extremely easy to capture picture of client's data using mobile phone and then post it on social media for different purposes).
- ➢ Using customer's data for training purposes – Contact centers should always make sure that the data used in training does not belong to real customer.
- ➢ Improper disposal of papers on which personal information of customer was written down -To avoid data breaches, always encourage agents to use paper shredders to dispose papers containing such data.

### 4.7.5 Documentation

The Documentation activities (introduced in flight booking process (To-Be)) related to Documentation (one of the key area identified in Section 4.4.2) are mapped in this section against the compliance questions. To analyze how the activities will fit in practical business environment, following steps are taken in Table 4.8 to do the mapping.

- Highlight the gaps from documentation perspective between business process model (As-Is) and business process model (To-Be) and point out suggestions to fill the gaps.
- The means to fill the gaps is activity introduced in Section 4.5. Table 4.8 summarizes the recommendations to fill the gaps.

**Common Mistakes:**

- ➢ Assuming documentation is the task of Controller- The GDPR requires not only controllers, but also the data processors to document record of activities. It is the responsibility of data processor to identify which activities need to be documented and then devise standards for documentation.
- ➢ Documenting but not in secure data base- Both data controller and data processors should make sure that secure CRM (customer relationship management) system is used for documentation and a good back up plan exists in case of data loss. Documenting activities without any backup plan will not mitigate risk of non-compliance.

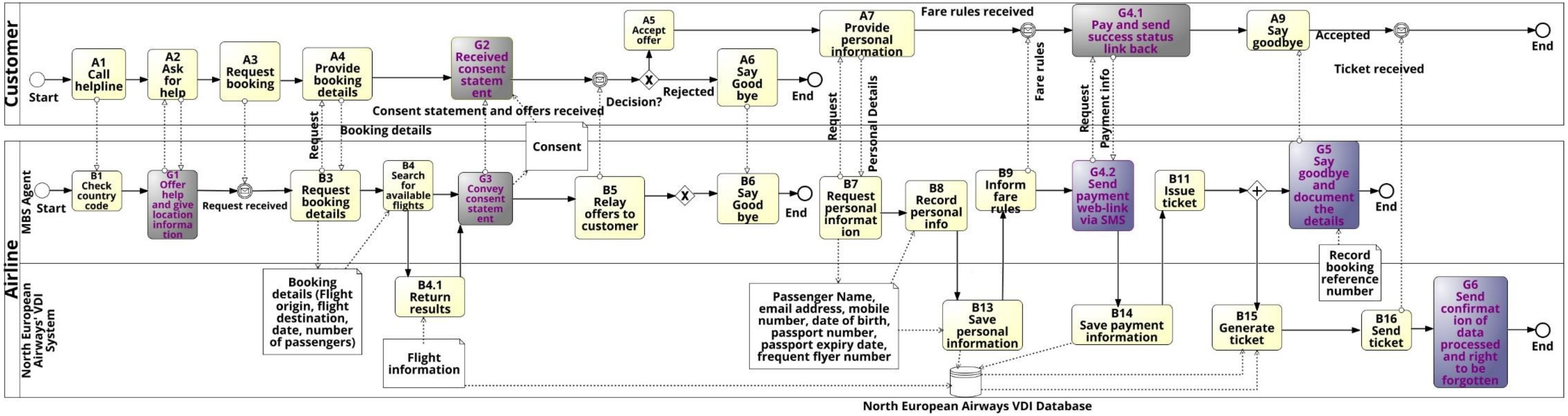

Customer
Start
A1 Call helpline
A2 Ask for help
A3 Request booking
A4 Provide booking details
G2 Received consent statem ent
Consent statement and offers received
Decision?
A5 Accept offer
Rejected
A6 Say Good bye
End
A7 Provide personal information
Fare rules received
Fare rules
G4.1 Pay and send success status link back
Request
Payment info
A9 Say goodbye
Accepted
Ticket received
End
Airline
MBS Agent
Start
B1 Check country code
G1 Offer help and give location informa tion
Request received
Request
Booking details
B3 Request booking details
B4 Search for available flights
G3 Convey consent statem ent
Consent
B5 Relay offers to customer
B6 Say Good bye
End
Request
Personal Details
B7 Request personal informat ion
B8 Record personal info
B9 Inform fare rules
G4.2 Send payment web-link via SMS
B11 Issue ticket
G5 Say goodbye and document the details
End
North European Airways' VDI System
Booking details (Flight origin, flight destination, date, number of passengers)
B4.1 Return results
Flight information
Passenger Name, email address, mobile number, date of birth, passport number, passport expiry date, frequent flyer number
B13 Save personal information
B14 Save payment information
B15 Generate ticket
Record booking reference number
B16 Send ticket
G6 Send confirmat ion of data processed and right to be forgotten
End
North European Airways VDI Database

**Figure 4.3:** Shows the GDPR compliant BPMN for flight booking process

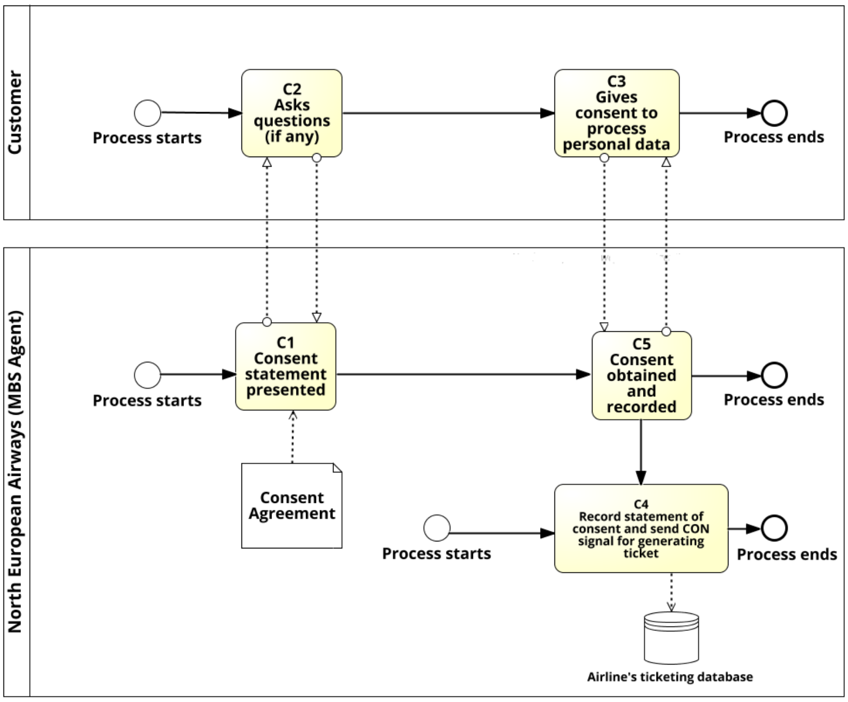

Customer
Process starts
C2 Asks questions (if any)
C3 Gives consent to process personal data
Process ends
North European Airways (MBS Agent)
Process starts
C1 Consent statement presented
C5 Consent obtained and recorded
Process ends
Consent Agreement
Process starts
C4 Record statement of consent and send CON signal for generating ticket
Process ends
Airline's ticketing database

**Figure 4.4:** Shows the sub process for consent activities introduced in Figure 4.3

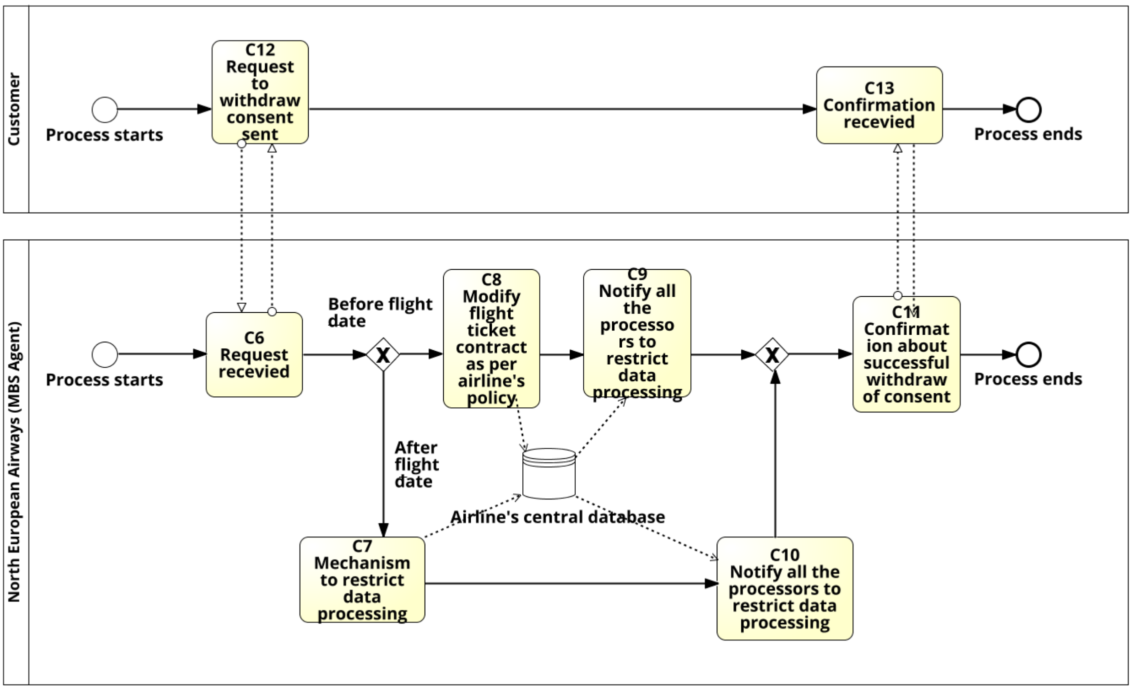

Customer
Process starts
C12 Request to withdraw consent sent
C13 Confirmation recevied
Process ends
North European Airways (MBS Agent)
Process starts
C6 Request recevied
Before flight date
C8 Modify flight ticket contract as per airline's policy
C9 Notify all the processors to restrict data processing
C11 Confirmation about successful withdraw of consent
Process ends
After flight date
Airline's central database
C7 Mechanism to restrict data processing
C10 Notify all the processors to restrict data processing

**Figure 4.5:** Shows the proposed mechanism for consent withdrawal

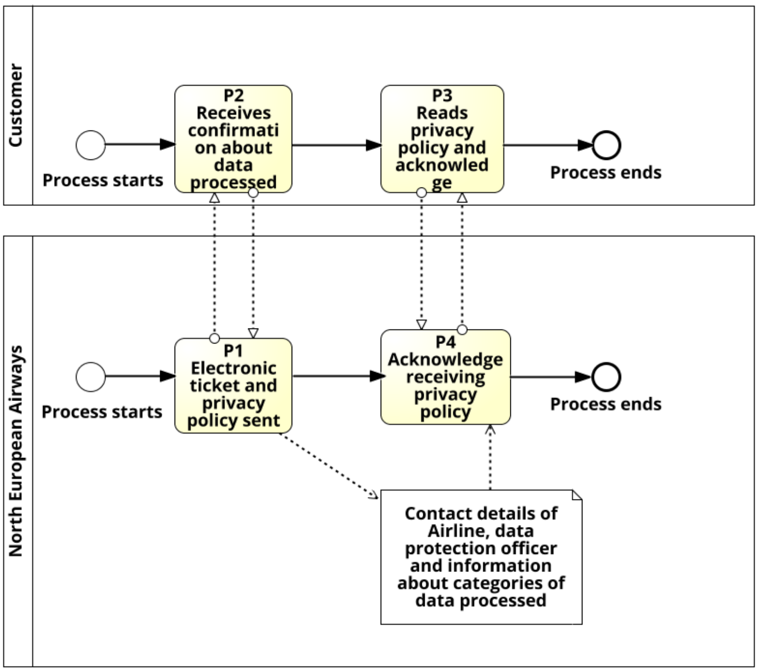

Customer
Process starts
P2 Receives confirmati on about data processed
P3 Reads privacy policy and acknowled ge
Process ends
North European Airways
Process starts
P1 Electronic ticket and privacy policy sent
P4 Acknowledge receiving privacy policy
Process ends
Contact details of Airline, data protection officer and information about categories of data processed

**Figure 4.6**: Shows the sub process for transparency activities introduced in Figure 4.3

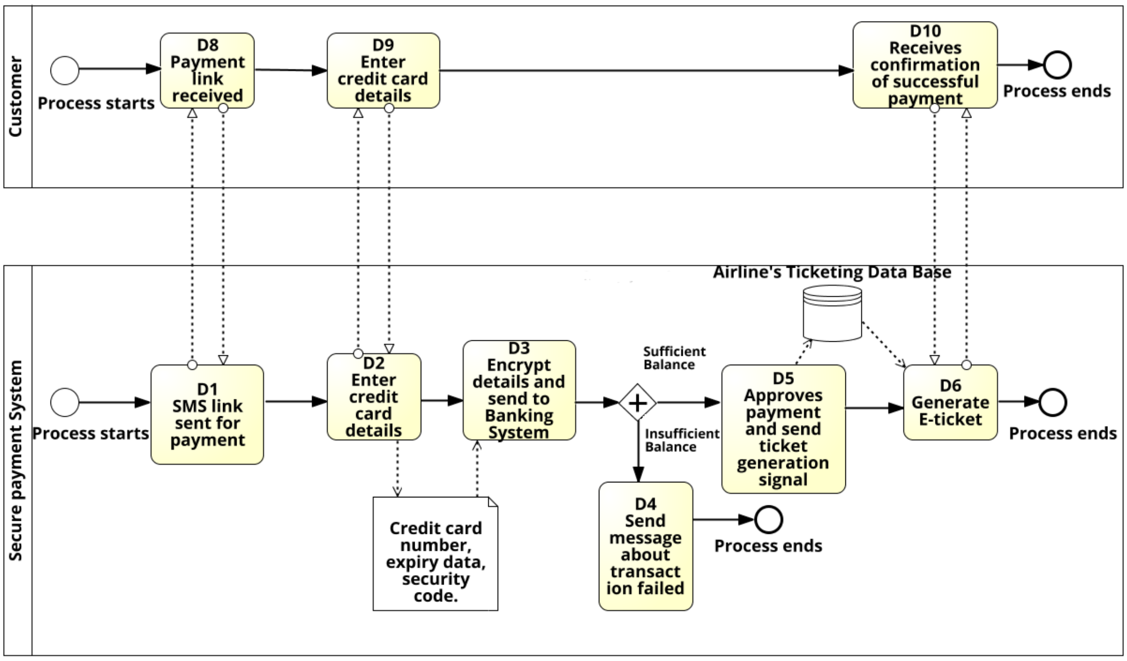

Customer
Process starts
D8 Payment link received
D9 Enter credit card details
D10 Receives confirmation of successful payment
Process ends
Secure payment System
Airline's Ticketing Data Base
Process starts
D1 SMS link sent for payment
D2 Enter credit card details
D3 Encrypt details and send to Banking System
Sufficient Balance
Insufficient Balance
D5 Approves payment and send ticket generation signal
D6 Generate E-ticket
Process ends
D4 Send message about transact ion failed
Process ends
Credit card number, expiry data, security code.

**Figure 4.7:** Shows the sub process for secure payment system

**Table 4.5:** Summarizes the suggestions to achieve consent according to GDPR criteria.

| **Item** | **Consent (Article 5,6,7)** | |
|---|---|---|
| **CON1** | *Compliance Question* | Is consent taken from individual before processing personal data? |
| | *Degree of compliance* | Non-compliant. |
| | *Reason of non-compliance* | Business process model (As-Is) shows that there is no actual consent obtained from customer to process personal data. |
| | *Recommendation* | Introduce consent activities to obtain business process model (To-Be). |
| | *New activities* | G2, G3 (C1, C2, C3, C4, C5), (Figure 4.3, Figure 4.4). |
| | *Entity Liable* | Data controller. |
| **CON2** | *Compliance Question* | Is consent obtained in clear, plain and easily understandable language? |
| | *Degree of compliance* | NON-CON |
| | *Reason of non-compliance* | Business process model (As-Is) shows that Mixing up consent with terms and conditions disqualify the consent to be easily understandable. |
| | *Recommendation* | Same as for CON1. |
| | *New activities* | G2, G3 (C1, C2, C3, C4, C5), (Figure 4.3, Figure 4.4). |
| | *Entity Liable* | Data controller and data processor. |
| **CON3** | *Compliance Question* | Are customers of airline able to withdraw consent? |
| | *Degree of compliance* | NON-CON. |
| | *Reason of non-compliance* | Business process model (As-Is) shows that as currently no consent is taken from customer to process personal data, so therefore no such mechanism exists to withdraw |
| | *Recommendation* | Figure 4.5 shows a mechanism to withdraw the consent. |
| | *New activities* | C6, C7, C8, C9, C10, C11, Figure 4.5. |
| | *Entity Liable* | Data controller and data processor. |
| **CON4** | *Compliance Question* | Is it possible to generate flight tickets only if consent is obtained? |
| | *Degree of compliance* | NON-CON |
| | Reason of non-compliance | The contact center agent can forget to take consent. |
| | *Recommendation* | Introduce mechanism that would generate a unique signal for every customer |
| | *New activities* | C4, Figure 4.4 |
| | *Entity Liable* | Data controller |

**Table 4.6:** Shows the detailed analysis for Transparency activities introduced in Figure 4.3

| **Item** | **Transparency (Article 5)** | |
|---|---|---|
| **TRN1** | *Compliance Question* | Are customers of Airline provided with privacy notice explaining the privacy policies? |
| | *Degree of compliance* | PAR |
| | *Reason of non-compliance* | In business process model (As-Is) there is no activity where the customer is provided with privacy notice explaining Airline's privacy policies. |
| | *Recommendation to fill the gap* | While sending electronic ticket for flights, also send confirmation about privacy policy and categories of data processed. |
| | *New activities and coresponding sub-process* | G6 (P1, P2, P3, P4) |
| | | Figure 4.3, Figure 4.6 |
| | *Entity Liable* | Data controller |
| **TRN2** | *Compliance Question* | Does the privacy notice include the details of data controller and data protection officer? |
| | *Degree of compliance* | PAR |
| | *Reason of non-compliance* | According to business process model (As-Is) there is no privacy notice sent to customer. Just contact details of airlines are included in flight ticket. |
| | *Recommendation to fill the gap* | Update the privacy notice with contact details of data protection officer and categories of data processed. Send privacy notice |
| | *New activities* | Same as for TRN1 |
| | *Entity Liable* | Data controller |
| **TRN3** | *Compliance Question* | Does the privacy notice explain purposes and categories of data processing? |
| | *Degree of compliance* | PAR |
| | *Reason of non-compliance* | The privacy policy, which is currently available only on website of Airline processing (but not translated in all EU languages) |
| | *Recommendation to fill the gap* | Translate the privacy policy in all European languages (countries to/from the Airline operates flights). Also, send one copy of privacy notice along with flight ticket. |
| | *New activities* | N/A |
| | *Entity Liable* | Data Controller |

**Table 4.7:** Shows the detailed analysis of Security activities introduced in Figure 4.3

| Item | Data Security (Article 24,25,28) | |
|---|---|---|
| **SEC1** | *Compliance Question* | Does the contact center have proper means for secure credit payments? |
| | *Degree of compliance* | NON-CON |
| | *Reason of non-compliance* | As shown in business process model (As-Is) the credit card details are asked by agent verbally and thereby exposing to various threats such as social engineering attacks, insider attacks etc. |
| | *Recommendation to fill the gap* | Induct a secure payment system e.g. a system that would generate SMS link, which is received by customer to complete payment securely, without exposing credit card details to contact center agent. |
| | *New activities and co-responding sub-process* | G4.1, G4.2 (D1, D2, D3, D4, D5, D6) |
| | | Figure 4.3, Figure 4.7 |
| | *Entity Liable* | Data Controller and data processor |
| **SEC2** | *Compliance Question* | Does the contact center have secure working environment in place? |
| | *Degree of compliance* | NON-CON |
| | *Reason of non-compliance* | The contact center agent has unrestricted access to social media websites such as Facebook, twitter etc., and the personal electronic devices such as mobile phones, tablets etc. are not forbidden to use, there by placing the personal data and credit card data at greater risk of social engineering attacks. |
| | *Recommendation to fill the gap* | Update the network access policies with restricted access to social media websites. Make usage of mobile phones forbidden in production. |
| | *New activities and co-responding sub-process* | N/A |
| | *Entity Liable* | Data processor |
| **SEC3** | *Compliance Question* | Is the security program reviewed at planned intervals? |
| | *Degree of compliance* | CON |
| | *Reason of non-compliance* | N/A |
| | *Recommendation to fill the gap* | N/A |
| | *New activities and co-responding sub-process* | N/A |
| | *Entity Liable* | N/A |

**Table 4.8:** Shows the detailed analysis of documentation activities

| **Item** | **Documentation** | |
|---|---|---|
| **DOC1** | *Compliance Question* | Does the contact center maintain documentation regarding the data collection and storage? |
| | *Degree of compliance* | NON-CON |
| | *Reason of non-compliance* | Activities are recorded but there are no standards which contact center follows to document the activities. Number of calls are documented but not the booking reference numbers or the time stamp when the booking was made. |
| | *Recommendation to fill the gap* | Setup standards to document activities. Record booking reference number, timestamp when booking was made. |
| | *New activities and co-responding sub-process* | G5 |
| | | N/A |
| | *Entity Liable* | Data processor |
| **DOC2** | *Compliance Question* | Does the company maintain documentation regarding the legal basis of cross border data transfers? |
| | *Degree of compliance* | PAR |
| | *Reason of non-compliance* | Partially details are recorded. |
| | *Recommendation to fill the gap* | Document all the activities including data transfer to third parties i.e. baggage handling company at airport, border control agencies. |
| | *New activities and co-responding sub-process* | N/A |
| | *Entity Liable* | Data controller and data processor |
| **DOC3** | *Compliance Question* | Does the company have a physical presence in the EU? |
| | *Degree of compliance* | CON |
| | *Reason of non-compliance* | N/A |
| | *Recommendation to fill the gap* | N/A |
| | *New activities and co-responding sub-process* | N/A |
| | *Entity Liable* | N/A |

## 4.8 Summary

In this chapter,

- Case scenario was analyzed related to an airline contact center business process (i.e. flight booking process).
- Current flight booking business process was modelled which highlighted the key business activities and data objects.
- GDPR articles relevant to airline flight booking process were instantiated and gaps were identified
- Gaps between GDPR compliant business model (flight booking process To-Be) and GDPR non-compliant business model (flight booking process As-Is) were identified and detailed modelling was done for each key area of compliance.
- Activities introduced to make business process compliant were mapped further at sub-process level and detailed analysis was done to show how the new activities support compliance.

The next chapter will describe how the solution to achieve compliance was validated.

# 5 Validation

One of the Sub Research Questions (**SRQ3**) is: How the solution/means to make a contact center GDPR compliant is validated? This chapter is designed to answer this question. In this chapter, the GDRP compliant flight booking process and the business process model (To-Be) are validated by receiving feedback from senior employees of an airline's contact center. The previous chapter has suggested the activities that need to be introduced in flight booking process (business process model As-Is) to achieve GDPR compliance and the recommendations were made to incorporate those activities. The current chapter is meant to validate the recommendations in practical business environment.

## 5.1 Design of Validation

This section describes how the validation for GDPR application method is designed. Interviews are conducted with some of the most professional and experienced employees of a contact center of North European Airways and the results from interviews or discussions is recorded and mapped against the GDPR compliant flight booking process (business model To-Be) (Figure 4.3). The following sections give a brief introduction about the background of employees who participated in interviews/discussions, their current position or designation in the company, the means how interviews are performed and the instruments used to perform them.

### 5.1.1 Background

In order to get expert opinion on proposed business process model (To-Be) (Figure 4.3) and have the opinion from the most experienced personal of airline contact center, criteria is designed based on a number of factors mentioned below. Each interviewee meets the following requirements.

1. Minimum experience of 7 years in airline business.
2. Currently working at a higher managerial position.
3. Have greater understanding of contact center business.
4. Have some kind of background of data privacy laws and regulations.
5. Have at least a basic understanding and familiarity with GDPR.

### 5.1.2 Interviews

This sub-section describes the positions of interviewees who participated in interviews. Some of the interviewees have worked directly for the data controller (North European Airways) some time ago but at the time when these interviews were conducted, all the interviewees were currently employed by the data processor (contact center outsourced to third party i.e. MBS) studied in this thesis. The interviewees are currently working in the following positions:

- Senior Director
- Quality Assurance Manager
- Key Account Manager

All the interview related discussions are presented in Appendix 4, 5 and 6.

### 5.1.3 Procedure to Perform Interview

Interviews are performed face to face. The time length of each interview was approximately 40-65 Minutes. First, there was a brief presentation made and then interviews were conducted. All the interviews were conducted within the same week (i.e. 3rd week of February). Table 5.1 summarizes the steps used to conduct the interviews.

**Table 5.1**: Summarizes the steps performed for interviews

| **Item Nr.** | **Material Distributed** | **Purpose** |
|---|---|---|
| 1. | Summary of GDPR articles (Appendix-1) | The interviewees still may not have strong background of GDPR. So, in order to do brain storming and bring attention of interviewees towards key areas of compliance, an introduction sheet was provided. Also, GDPR original text was distributed among them and a brief presentation about GDPR was made. |
| 2. | The flight booking process (As-Is) modelled in Figure 4.2<br>(Model and process) | In order to validate the data collected and the process described and analyzed in Section 4.3, business model (Figure 4.2) was distributed among the interviewees along with the explanation of how the process was interpreted and documented. |
| 3. | The flight booking process (To-Be) described in Section 4.6 and modelled in Figure 4.3<br>(Model and process) | In order to validate the GDPR compliant flight booking process, the model from Figure 4.3 was distributed to each interviewee. The process was explained to each of them. |
| 4. | Sub processes designed in Figure 4.4, 4.5, 4.6 and 4.7 | In order to validate each sub-process, the models were distributed, and each sub-process was explained. |

**Instruments used to perform the interview:** The instruments used to perform the interviews were

1. Laptop (all the answers/responses of interviewees were filled directly in to tables (in Appendix 4, 5, 6)
2. Mobile (for recording) – was planned earlier, however, none of the interviewee permitted voice or video recording, due to fear of being identified. Instead, all the information was filled in laptop in front of interviewee and later the answers were shown to interviewee to agree on what was documented.

**Interviews setup:** Interviews were conducted face to face. Each of the staff member was invited for a face to face interview individually and 40-65 minutes (average) was the time allocated for each interview.

**Method used to analyze interviews data:** To analyze the data collected during the interviews, I used thematic approach, similar to that used by Narantuyga to analyze the qualitative interviews in his doctoral thesis research [27]. First, I designed questions to get the most relevant information for my research and the questions that would help me to validate my models. Then, I determined the reason for asking such questions through brainstorming and keeping in mind my research requirements. As I didn't deal with a large set of interviews, so I didn't use any coding to classify the data obtained from the results. Instead, I classified the data manually according to the categories (as per needs of thesis), i.e. I divided the results in to different sections (as described in Section 5.2.1, 5.2.2, 5.2.3 and 5.2.4) and then compared the results of different interviews in each subsection.

## 5.2 Results

Altogether, there were three interviews conducted and each interview was divided in to six parts. First of all, the original flight booking process (business process model As-Is) described in Section 4.3 and modelled in Figure 4.2 was validated, to make sure initial data collected was valid. Then the GDPR compliant flight booking process (business process model To-be) (Section 4.6, Figure 4.3) was validated by receiving feedback on activities introduced (co-responding to one of the key areas i.e. consent, transparency, data security and documentation) and then the sub-process co-responding to each newly introduced activity was validated through feedback from interviewees.

The six parts of interviews were as follow:

- General questions
- Questions to validate the business process model (As-Is) for flight booking process (Figure 4.2)
- Questions to validate the business process model (To-Be) i.e. GDPR compliant flight booking process (Figure 4.3)
- Consent
- Transparency
- Data security
- Documentation

**General questions*:*** The purpose to ask general question is to give the reader an idea about the background of the interviewees. The answers to these questions were fairly simple and straightforward.

**Questions to validate the business process modelling for flight booking process (Figure 4.2):** Section 4.3 is the base of the running case scenario for this thesis and business process modelling for flight booking process in Figure 4.2. It was important to validate the data collected and the process modelled, so each interviewee was provided with the business process model (Figure 4.2) and the model was described thoroughly described in Section 4.3. All the participants of the interview confirmed the correctness of the model and the description of flight booking process in Section 4.2.

### 5.2.1 Consent

As the thesis is focused on four main key areas for GDPR compliance and one of the key areas is consent, so there were questions designed relevant to it. All the interviewees expressed their views about consent and mainly, all participants agreed that consent is agreement freely given by the customer to process personal data. Mike (P. 66, 67) showed concern about the complexity of consent in the case of contact center business. As calls are recorded, we need permission to record them not only from the customer, but also from the agent making booking and in case the employment contract is terminated, then we are not sure how to proceed with providing the customer with call recordings (if such request is made), it will be extremely difficult in case if the agent withdraws the consent. However, as it is beyond the scope of this thesis, so this might be the work for future research. All the participants have expressed their concern that there is not valid consent in the current flight booking process (Section 4.2, Figure 4.3) or as per opinion of Alexandra (P. 74, 75), consent is part of terms and conditions, however, this disqualifies the consent under GDPR definition of valid consent, so there is a need of consent to be taken separately in a clear and simple language. Moreover, Steven (P. 82, 83) and Alexandra (P. 74, 75) discussed the difficulty about obtaining the valid consent when customer calls to make a booking over the phone. Most of the time, the customer is making booking on behalf of somebody, and thereby giving the consent on behalf of someone, so the MBS agent needs to ask on the phone about the consent over the phone. Moreover, Mike, (P. 66, 67) mentioned that some of the back-office tasks relevant to flight booking are outsourced to processors located in Asia (outside of the EU), so that means consent needs to be obtained from customer and there is no backup plan in case if the customer denies his data to be processed outside the EU premises. All the participants agreed that the key area consent falls under the responsibility of both North European Airways (data controller) and MBS (data processor). The new activities introduced in Figure 4.3 (G2 and G3) and the sub processes corresponding to these activities were validated through feedback from interviewees. All the interviewees saw the solution as practical and meeting business requirements. Following were the key points from the results:

- Receiving consent from the customer from a recorded IVR message may not be suitable as the customer is not always passenger, so in order to give consent on behalf of someone, the activities G2 and G3 and the corresponding sub process (Figure 4.4) is a valid solution for the time being.
- Withdraw consent mechanism (Figure 4.5) provides a good idea at a broader level, however, the activities need to be developed further e.g. activity C8 (Modifying flight contract), activity C7 (mechanism to restrict data processing) however, such activities can only be further broken down in to more detail level only in collaboration with North European Airways (data controller).
- All the interviewees have shown the concern that the solution for obtaining consent (activities G1, G2 and Figure 4.4) and withdrawing consent (Figure 4.5) are valid processes, however, there is a cooperation needed from North European Airways in order to implement the presented solution.
- Steven (P. 82) has shown concern that such solution will have impact on business in terms of increased call duration.

- One of the possible cons for the solutions brought up by Mike (P. 66, 67) is the denial of customer to give consent to process the data (for back office tasks such as reissue of the ticket in case of schedule change) as currently, there is no backup plan to process such requests within EU premises. However, it is uncertain if obtaining consent for handling back office work falls under the GDPR and needs privacy expert's advice.

### 5.2.2 Data Security

All the interviewees i.e. Alexandra (P. 78, 79) Steven (P. 84, 85) and Mike (P. 69, 70) have identified the activities A8 and B10 as the activities causing possibilities of data breach. Exposing credit card details to MBS agents handling calls can lead to various data breaches as a result of social engineering, insider threats etc. There is a need to have a secure payment system, to ensure that credit card details are safely processed. The feedback on GDPR compliance activities (G4.1 and G4.2) and corresponding sub process (Figure 4.7) by participants were as follow:

- All the interviewees see the solution as tool to achieve GDPR compliance in terms of handling credit card information securely.
- However, Alexandra (P. 78, 79) and Mike (P. 69, 70) have stated that North European Airways has the responsibility to implement this solution and provide MBS agent with tools such as a secure payment system, so that there wouldn't be any need to ask for credit card information over the phone.
- CONS: Implementing such solutions means additional costs for North European Airways.

### 5.2.3 Transparency

All the interviewees have common understanding about the concept of transparency i.e. communicating privacy notice to the customers in a simple and plain language. For the flight booking process (Section 4.2, Figure 4.2), Alexandra (P. 76, 77) and Steven (P. 83, 84) have shown concerns that the current flight booking process (Section 4.2, Figure 4.3) is not completely transparent as the privacy notice is not communicated to the customers. Mike (P. 68, 69) showed concern that along with communicating privacy policy, customers should be aware of the fact that North European Airways (data controller) engages processors or third parties (e.g. MBS) to process data. All the participants agreed that it is the responsibility of North European Airways to communicate privacy policies and, therefore, ensure that the business process (flight booking process) is transparent.

Comments about newly introduced activities (G1 and G6). All the participants confirmed the validity of activity G6 and the privacy notice sample (Appendix-2), however, the activity G1 was irrelevant, as the contact center is not situated outside the EU premises, so it is unnecessary to have this activity (G1). The model after correction is shown latter in this chapter (Figure 5.1).

So, the main results obtained were

- Activity G6 is a valid activity and sending out privacy notice (Appendix-2) is a great idea, however, activity G1 is unnecessary.
- It is the responsibility of North European Airways to ensure that the privacy policy is communicated to customers in all of the EU languages (to where North European Airways have flights to/from).
- Major cons of solution: administrative costs.

### 5.2.4 Documentation

All the interviews Steven (P. 86), Alexandra (P. 79, 80) and Mike (P. 71, 72) identified the requirements of documentations imposed by GDPR on data processing and the need to document all the activities. Alexandra (P. 79, 80) showed concern that it is not only important to document booking reference numbers for the flight bookings made (tracking sales) but also, it is important to document all other activities in the contact center, such as when employees or agents get access to new information system. Also, Steven (P. 86) emphasized that it is not only important to document all the activities and booking reference numbers but it is also important to securely store such information in secure CRM (customer relationship manager) systems. There will be obvious costs associated for implementing such systems and MBS has to cover this cost. Mike (P. 71, 72) pointed out that it is not only important to document all the activities, but it is also important to create a backup of such information, so that in case of data loss, information can be recovered. Some of the important results from interviews discussions are as follow:

- Activity G5 is valid in terms of documenting the booking reference numbers, however, it needs secure CRM system. So, therefore, it means additional costs.
- One of the interviewees suggested the documentation of user signatures in a more detailed and formal way i.e. who was given access to the system? What was the access level? Etc. Also, it is important to keep track of system access given to users. At the moment, the contact center does not keep tracks of signatures at a more formal level.
- Currently, there are no standard procedures of documenting data breaches, so the data processor (MBS), along with collaboration of data controller (North European Airways) has to setup procedures for documenting data breaches in a more formal fashion.

**Corrections of GDPR compliant flight booking process:** After receiving feedback during interview discussions about GDPR compliant flight booking process (Section 4.3, Figure 4.3) the model was redrawn as show in Figure 5.1. The unnecessary G1 activity was eliminated while the rest of the model remained the same.

### 5.2.5 Cross validation

The flight booking process (business process model As-Is) was cross validated by Eduard Sing in his Master thesis research [33]. Eduard designed the same business process model As-Is (Figure 4.2) and performed a GDPR compliance check. Based on his meta-model driven method to check compliance, he gave out some recommendations to achieve compliance. Those recommendations were matched with my business process model (flight booking proess (To-Be)). The comparison is shown in appendix 3.

## 5.3 Threats to validity

This section sums up the possible threats to validity of the case scenario studied. The following threats could change the outcome of validation:

1. Political pressure: Each interviewee indicated some kind of political pressure to speak out. This may affect the purity of results and the interviewees may not express the same view when the interview would be conducted by someone else or the interviewees are asked to express their opinion publicly.

2. Reputation of data controller and data processor: Both data controller and data processor cannot afford to have negative publicity or attention in the media in case if it is known to the clients that the airline is not ready to comply with GDPR or for example, the payment information is not handled securely, so fear of reputation also may hold back the interviewees to freely express their opinions.
3. Mood: Stress and other emotional factors may change the output of interviews.
4. Interpretation of GDPR: At the time when interviews were conducted, most of the participants had no formal training about GDPR. So, a formal training and deeper knowledge about GDPR may change the interviewee’s opinions.
5. Interruption/Distraction: As the interviews were conducted on site in contact center, all the participants of interviews have very busy schedules. It was made sure that they were not distracted or disturbed during the interview. However, an interruption or distraction may divert the focus, resulting in different answers or lack of interest in topic.

**Highlights of Contributions Made by Thesis:** Following points summarize the main achievements as outcome of this thesis research:

1. The idea to process payments securely (suggested in Section 4.7.4) will be implemented by North European Airways (in more advanced form).
2. Questionnaire based approach used in Table 4.5, 4.6, 4.7 and 4.8 to fill the gaps, welcomed by MBS and the approach contributed to GDPR strategic priorities assessment project in contact center.
3. Business models developed in details for flight booking process. Similar models are requested for other business processes in contact center.
4. Certificate of appreciation (based on thesis work) awarded by Director of contact center.

## 5.4 Conclusion

Interviews results showed that the solution presented to achieve GDPR compliance is practical in terms of business needs as it has addressed the loopholes causing non-compliance. There is no valid consent in the original business process and therefore, there was a need to introduce activities to take valid consent. Likewise, sending privacy notices along with flight tickets and translating privacy notices in to respective European languages will prevent the threat of non-compliance to transparency. The contact center has very loose security policies due to lack of secure payment and not appropriate policies on production floors. So implementing secure payment system will definitely lower down the risk of non-compliance. GDPR requires documentation of all the activities at data processor’s side. Previously, the contact center agent was documenting information e.g. sales statistics only in North European’s Airways VDI but all the participants have agreed that it is necessary to document all the information in secure CRM systems within data processor’s systems, in order to keep the record of activities.

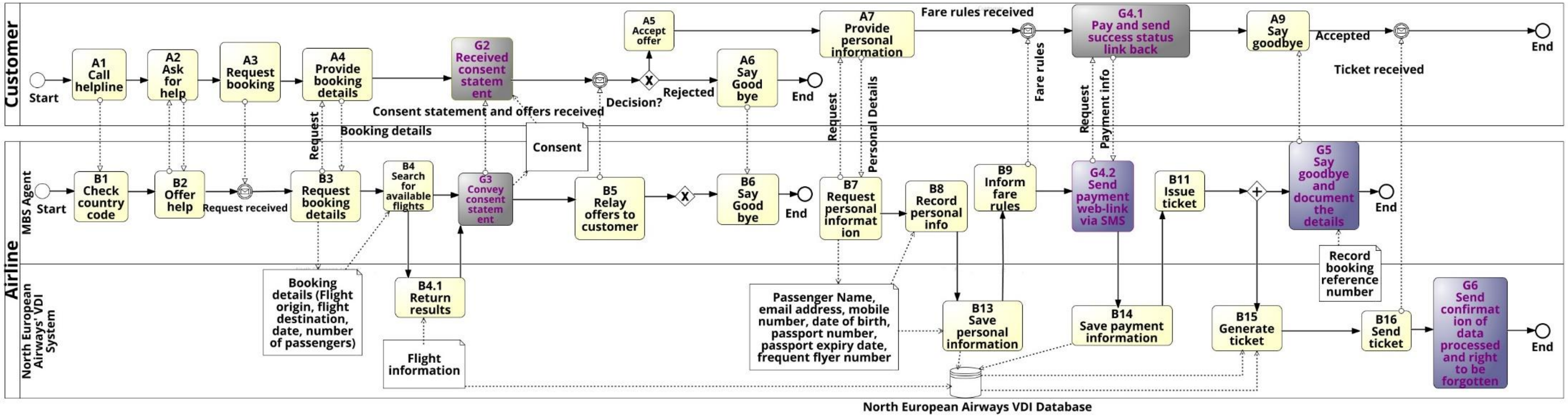

Customer
Start
A1 Call helpline
A2 Ask for help
A3 Request booking
A4 Provide booking details
G2 Received consent statem ent
Consent statement and offers received
Decision?
A5 Accept offer
Rejected
A6 Say Good bye
End
A7 Provide personal information
Fare rules received
G4.1 Pay and send success status link back
A9 Say goodbye
Accepted
Ticket received
End
Request
Booking details
Consent
Request
Personal Details
Fare rules
Request
Payment info
Airline
MBS Agent
Start
B1 Check country code
B2 Offer help
Request received
B3 Request booking details
B4 Search for available flights
G3 Convey consent statem ent
B5 Relay offers to customer
B6 Say Good bye
End
B7 Request personal informat ion
B8 Record personal info
B9 Inform fare rules
G4.2 Send payment web-link via SMS
B11 Issue ticket
G5 Say goodbye and document the details
End
North European Airways' VDI System
Booking details (Flight origin, flight destination, date, number of passengers)
B4.1 Return results
Flight information
Passenger Name, email address, mobile number, date of birth, passport number, passport expiry date, frequent flyer number
B13 Save personal information
B14 Save payment information
B15 Generate ticket
Record booking reference number
B16 Send ticket
G6 Send confirmat ion of data processed and right to be forgotten
End
North European Airways VDI Database

**Figure 5.1**: Shows the GDPR compliant fight booking process after validating from interview discussions

## 5.5 Summary

In this chapter, following were the main highlights

- The interviews were conducted and the solution presented in chapter 4 was validated.
- The results obtained from interview discussions were listed.
- The GDPR compliant model (business process model To-Be) was corrected based on interview results.
- Threats to validity were explained.
- Instruments used to conduct interviews were explained.

# 6 Concluding Remarks

This thesis presents an overview of how to make the flight booking process GDPR compliant. A European airline's contact center is used to study the case scenario on how data is collected for the flight booking process, from customer over the phone. The process is translated in terms of GDPR articles and business process modeling (BPMN) technique is used to model flight booking process. This resulted in identification of activities that contributes to non-compliance of GDPR. The work in this thesis is focused on four main areas for compliance i.e. consent, transparency, data security and documentation. So, the activities co-responding to each of these areas are introduced in flight booking process, whereas these activities are further modelled at sub process level. This approach to make flight booking process GDPR compliant, along with business models are validated by means of interviews and discussions with experienced staff members working for a contact center of an airline. The flight booking process is then remodeled after receiving feedback from airline's staff members.

## 6.1 Limitations

Some of the limitations of this thesis work are as follows:

**Key stakeholders not involved:** One of the main limitations of this thesis is that the solution was never validated from any representative of data controller (i.e. North European Airways). All the interviewees are employed by data processor (MBS) but not directly by data controller.

**Data collection from airlines:** It is complex to get permission from airlines to analyze their business processes as most airline contact centers are not willing to share the private information or to give their data for research purposes. This makes it difficult to further develop the idea presented in this thesis.

**Limited literature:** As GDPR compliance is still in implementation phase, so there is very limited literature available that directly addresses the compliance issue of GDPR in an airline contact center. Also, since flights are usually booked over the website these days, so the issue of data security in contact center is continuously neglected despite of the fact that there are still large number of customers who call the airline's helpline to make flight booking.

**Software used by airline:** This thesis discussed the software used by airlines for flight booking purposes (i.e. Amadeus) but due to limited information available, the technical aspects are not discussed in detail (for example how data is processed, what the vulnerabilities are and what data transfer mechanisms are used by software).

**Sub-processes:** The sub-processes co-responding to each key area (for instance consent), are designed to give very broad overview of how to implement GDPR. However, detailed analysis is not done about how to implement the sub processes in practical business environment.

**Validation of solution from a privacy expert:** Due to unavailability of privacy expert or data protection officer, the solution presented in this thesis was not validated from a privacy expert. However, one of the interviewee had some privacy background and previous experience with implementing privacy change process.

Due to many reasons, such as educational background, limited knowledge about privacy and technology, there are only certain aspects that the employees of contact center can cover and some aspects may need collaboration with experts from different fields such as IT, data privacy etc. For example:

- Determining storage time of data (e.g. voice calls recording) is one of the hottest issue that many contact centers are facing these days. Such issues can feasibly be addressed after consulting data privacy experts and data protection officer.
- Minimizing the amount of data to what is necessary is another issue that contact center employees can't work on alone without counselling from data protection officers and IT experts.
- The GDPR gives right to data subject, to transfer the data from one data controller to another data controller. Currently, it is not possible to transfer data from one frequent flyer program to another frequent flyer program. Resolving such issues requires mutual collaboration of contact center's employees, cyber security experts, data privacy experts, data analysts and data protection officers.
- Employees of contact center have usually very little knowledge about the technical details of software used for setting up flight bookings. This puts the data security on risk and makes extremely difficult for employees with limited IT background to determine if there can be serious vulnerabilities in software or how the software can be exploited by means of insider threat and social engineering.

On the other hand, the aspects that senior employees of contact center can cover with productive results are

- Modelling business processes and mapping the activities against the Articles of GDPR to find out gaps (after GDPR awareness trainings).
- Designing GDPR awareness trainings for the front end agents of contact centers.
- Determining the effects of GDPR implementation from business perspective i.e. impact of activities on service levels.

## 6.2 Answers to Research Questions

The primary purpose of this thesis was to answer the research questions designed in chapter 1. MRQ- ***How to implement the EU General Data Protection Regulation (GDPR) in an airline contact center***?

This MRQ was broken in to 3 sub-research questions (SRQs).

**SRQ1. How is GDPR different from current privacy regulations and why is GDPR needed?** This question is answered by reviewing the current privacy laws in the EU. Different sources contribute to the current privacy law and as there is no common privacy law that each member state has to transpose into its national law which makes it a lot more difficult to regulate privacy under common understanding among EU member states. On the other hand, GDPR is a legal instrument that every member state has to transpose in to its national law [13]. It has introduced new concept of consent, accountability of data controllers and data processors, thereby strengthening rights of data subjects. According to the literature review, the key areas which are of significant importance for any company processing data of EU citizens are, consent, data security, accountability of data controllers and processors (transparency), and documentation. Also, the heavy penalties (20 million euros or up to 4 % of the total worldwide annual turnover of the preceding fiscal year, whichever is higher) will be imposed in case of non-compliance [19].

**SRQ2. How much the contact center is GDPR compliant and what are the means to make the contact center GDPR compliant?** We used a contact center of one of the major European airline and investigated how the flight booking process is conducted. After mapping the flight booking process against the GDPR, it is revealed that the main areas where compliance is lacking are consent, data security, transparency and documentation. The activities co-responding to each of the key areas are inducted in the original flight booking and a new model called GDPR compliant flight booking process is obtained.

**SRQ3. How the solution/means to make contact center GDPR compliant is validated?** Feedback in terms of interviews with the contact center's senior staff members is obtained on the original flight booking process as well as GDPR compliant flight booking process and then a corrective process was modeled again which formed the basis for final solution.

## 6.3 Conclusion

The modelling of the original flight booking process revealed that the main areas of non-compliance to GDPR are consent, data security, transparency and documentation, which are important for any organization processing personal data of the EU residents [23]. The compliant model caters all these needs and the feedback from airline's staff members proved that it meets practical business requirements. The technique to process payment securely is accepted by airline already and it is in phase of implementation. As the contact center is physically located in the EU, it is not necessary for contact center to give location information to customer but this liability does apply in cases where the contact centers are outsourced to data processors working outside the borders of the EU.

The results of interviews also showed the complexity of any new process or activity implementation because of the outsourced environment. It is important that the data controller and the data processor should have common understanding about the liabilities and the compliance can only be achieved through mutual cooperation and common agreement. The results of interviews also showed that the responsibility of data controller exceeds than the responsibility of data processor in terms of implementing any solution or modifying any mechanism, in order to achieve compliance. As the participants of interviews have doubts about the understanding of GDPR text which goes in line with research conducted on the challenges of GDPR compliance [4], so it shows that it is necessary that special trainings should be conducted among the airline contact center staff in order to raise GDPR awareness and that there is a need of appointment of a data protection officer.

## 6.4 Future Work

As stated earlier, the tools used to setup flight bookings are not assessed in terms of privacy by design, so the future work can be to measure GDPR compliance of tools used by the airline to setup flight bookings and handle the personal data. There is a need of detailed analysis of such tools/software used to access passenger's information, such as travel itinerary, passenger's meal preference, medical needs (e.g. wheel chair) etc. Currently, the biggest threat to all such information is social engineering attacks, i.e. currently, the reservation system used by most airlines in EU have very poor signatures tracking capabilities (e.g. who has accessed the data, when the data was accessed, was the data accessed with the permission of passenger). So, there is a great need to do analysis of reservation tools, in order to determine the GDPR compliance.

Also, as there are other business processes in an airline contact center such as customer care, frequent flyer program, so the future research can be done to implement GDPR in each of these business processes. Also, there is a need to do a revenue based analysis of GDPR impact, i.e. to analyze the impact of GDPR on an airline, in terms of cost and extra effort to implement GDPR. Another great topic for future work could be about designing GDPR awareness trainings for contact center staff.

## 6.5 Summary

In this chapter,

- Concluding remarks for thesis work were presented.
- Limitations were described.
- An overview of answers to the main research questions (MRQs) was given.
- The possibility of future work relevant to thesis's work was discussed.

## References

[1] R. Boardman, A. Mole and J. Mullock, “Guide to the General Data Protection Regulation,” May 2017. [Online]. Available: http://www.twobirds.com. [Accessed 30 September 2017].

[2] D. Zadura, “Importance of Personal Data Protection Law for Commercial Air Transport,” *Transactions of the Institue of Aviation,* vol. 1, no. 246, pp. 35-44, 2017.

[3] “Challanges of Air Transport 2030 survey of experts's views,” Euro Control, Cedex, 2009.

[4] P. Billgren and L. Wipp Ekman, “Compliance Challanges with the General Data Protection Regulation,” Lund University, Lund, 2017.

[5] P. Hustinx, “European Data Protection Supervisor,” 15 September 2014. [Online]. Available: https://edps.europa.eu/data-protection/our-work/publications/speeches-articles/eu-data-protection-law-review-directive_en. [Accessed 20 January 2018].

[6] S. S McCarty-Snead and A. T. Hilby, “Research Guide to European Data Protection Law,” *Berkeley Law Scholarship Repository,* pp. 17-18, November 2013.

[7] “EU Passenger Name Record (PNR) directive: An overview,” 01 June 2016. [Online]. Available: www.europarl.europa.eu/pdfs/news/expert/20150123BKG12902_en.pdf. [Accessed 05 January 2018].

[8] R. Sadet, “Council adopts EU Passenger Name Record (PNR) directive,” 21 April 2016. [Online]. Available: http://www.consilium.europa.eu/en/press/press-releases/2016/04/21/council-adopts-eu-pnr-directive/. [Accessed 30 April 2018].

[9] D. H. DI, “European Commission Staff Working Document; Implementation Plan for Directive (EU) 2016/681,” European Commission, Brussels, 2016.

[10] “European Digital Rights,” [Online]. Available: http://www.edri.org. [Accessed 10 January 2018].

[11] I. A. T. Association, *Response by IATA to The European Commission's Communication,* Brussels: IATA Regional Office for Europe, 2016.

[12] IATA, *A comprehensive approach on personal data protection in the European Union,* Brussels: European Commission, 2010.

[13] B. Specht, “GDPR: What Europe's New Privacy Law Means for Email Marketers,” Litmus, 21 November 2016. [Online]. Available: https://litmus.com/blog/gdpr-what-europes-new-privacy-law-means-for-email-marketers. [Accessed 2018 April 30].

[14] SeeUnity, “The main differences between the DPD and the GDPR and how to address those moving forward,” [Online]. Available: https://britishlegalitforum.com/wp-content/uploads/2017/02/GDPR-Whitepaper-British-Legal-Technology-Forum-2017-Sponsor.pdf. [Accessed 30 April 2018].

[15] R. K. Yin, “Collecting Case Study Evidence,” in *Case Study Research; Design and Methods*, London, Sage, 1984, pp. 106-111.

[16] “Case Study Purpose,” Western Sydney University, Sydney, 2016.

[17] J. Raumbaugh, I. Jacobson and G. Booch, “UML Concepts,” in *The Unified Modelling Language Reference Manual*, Boston, Addison-Wesley, 2004, pp. 31-32.

[18] D. Beveridge, “VDI: A New Desktop Strategy - VMware,” 2006. [Online]. Available: https://www.vmware.com/pdf/vdi_strategy.pdf. [Accessed 30 April 2018].

[19] P. Church, “The General Data Protection Regulation - A Survival Guide,” October 2016. [Online]. Available: https://lpscdn.linklaters.com/data_protection_survival_guide. [Accessed 02 Feburary 2018].

[20] Osterman, “GDPR Compliance and Its Impacts on Security and Data Protection Programs,” Osterman Research, Washington, 2017.

[21] N. Rai, A. Ashkok, J. Chakraborty, P. Arolker and S. Gajera, “M-Wallet: An SMS Based Payment System,” *International Journal of Engineering Research and Applications,* vol. II, no. 12, pp. 258-263, 2012.

[22] G. Thorne, “Cisco Multimedia IP Contact Centre Solutions Technical Review,” [Online]. Available: https://www.cisco.com/c/dam/global/fr_ca/assets/presentations/iptelephony/ipcc_solution_for_the_mid_to_large_market.pdf. [Accessed 06 Feburary 2018].

[23] “General Data Protection Regulation Guide - DLA Piper,” November 2016. [Online]. Available: https://www.dlapiper.com/~/media/general-data-protection-regulation-broucher.pdf. [Accessed 15 December 2017].

[24] “About Us,” IATA, [Online]. Available: http://www.iata.org/Pages/default.aspx. [Accessed 15 March 2018].

[25] Amadeus, “Travel Agency Basic Functionality Course,” [Online]. Available: www.pk.amadues.com. [Accessed 10 January 2018].

[26] C. Jasper, T. Seal and B. D Katz, “Airlines Suffer Worldwide Delays After Global Booking System Fails,” Bloomberg, 28 September 2017. [Online]. Available: https://www.bloomberg.com/news/articles/2017-09-28/airlines-suffer-worldwide-delays-as-amadeus-booking-system-fails. [Accessed 29 March 2018].

[27] N. Judger, “Hillary Place Papers, University of Leeds,” January 2016. [Online]. Available: http://hpp.education.leeds.ac.uk/wp-content/uploads/sites/131/2016/02/HPP2016-3-Jugder.pdf. [Accessed 10 Feburary 2018].

[28] S. Larson and A. Hewitt, “Staff Recruitment, Retention and Training Strategies for Community Human Services Organization,” in *Selecting and implementing Strategies For Change,* Baltimore, Brookes, 2005, pp. 321-322.

[29] “Data Protection and Privacy Beyond GDPR Implementation,” 2018. [Online]. Available: https://dataethics.eu/wp-content/uploads/TimClemensWhitepaper.pdf. [Accessed 10 May 2018].

[30] V. Paul and A. von dem, The EU General Data Protection Regulation (GDPR), Cham, Switzerland: Springer, 2017.

[31] D. Gabel, “Unlocking the EU General Data Protection Regulation,” 18 July 2016. [Online]. Available: https://www.whitecase.com/publications/alert/unlocking-eu-general-data-protection-regulation. [Accessed 20 Feburary 2018].

[32] “General Data Protection Regulation,” EUR-LEX- European Union Law, 27 April 2016. [Online]. Available: https://eur-lex.europa.eu/legal-content/en/all/?uri=uriserv:oj.j_.2016.119.01.0001.01.eng. [Accessed 20 Feburary 2018].

[33] E. Sing, R. Matulevicius and T. Jake, *A Meta-Model Driven Method for Establishing Business Process Compliance to GDPR,* Tartu: University of Tartu, 2018.

## Appendix 1-Basic Definitions from GDPR and summary of Articles

**Personal data:** Personal data means any information related to an identifiable alive person

**Processing:** Processing means set of operations performed on personal data

**Restriction of processing:** Restriction of processing means marking the personal data to limit its use

**Profiling:** Profiling means using personal data of passenger to predict certain behavior or preferences

**Filing system:** Means set of structured data accessible as per specific criteria

**Controller:** Means the entity which determine the purposes of processing of personal data under union or member state's law.

**Processor:** Processor is the legal entity that processes the data on behalf of

**Recipient:** Means a natural person, or legal body to whom personal data are disclosed.

**Third party:** Is legal entity, other than controller or processor that is assigned to process data on behalf of controller.

**Consent:** Consent of data means any freely given agreement by natural person to process their personal data, while such consent is obtained using clear and plain language

**Main Establishment:** a controller or processor with one or more establishments, with central or atleast one of the establishment is situated in Union

**Cross border processing:** Cross border processing means processing on personal data is carried on in more than one establishment located in more than one member state

Articles relevant to Airline's business process are summarized with possible impact of articles in Airline's business.

**Positive impact means**: The article is in favor of our contact center.

**Negative impact means**: Our contact center needs extra work to comply with article or the article increases the burden of compliance on organization.

**Neutral impact means**: The affect is significantly the same as brought by previous directive.

**Uncertain means**: The impact is hard to predict unless the article is put in to practice [31].

**Common terminology for Articles:** For sake of simplicity and reference to latter chapter, we will name every article with its number, for instance, we will call article 1 as L1, article 2 as L2 and so on.

**Article1:** The article 1 in GDPR aims at processing of personal data on fair and legal ground grounds. The intentions are same as in the directive, however, the GDPR clarifies certain issues here, such as processing of data of deceased persons [6] as well as it introduced harmonized approach of data protection regulation across EU making the cross border legal implications easier [31].

**Impact:** Positive. The GDPR makes it easier for organization to conduct business activities across EU and the common legal framework makes the compliance less complex.

**Article2:** The GDPR makes it clear that it applies only to natural persons "alive" and it does not apply to deceased persons personal data. The EU directive for personal data was not clear in this regard [31].

**Impact:** Neutral

**Article3:** The GDPR makes it clear that the regulation applies to organization not only in EU but also those organizations that offer products or services to customer in EU and process the data of EU citizens [31].

**Impact**: Negative, as many of the business activities are outsourced by SAS to processors that are not located in EU, the airline will need to reconsider the outsourcing.

**Article 4:** The GDPR makes the definition of personal data broader, so for example, the online identifiers such as collection of cookies while using airline's websites (which is a common practice in order to predict user's behavior that is latter used for marketing purposes) will come under the definition of personal data. Moreover, the concepts of controllers and processors are largely unchanged [31].

**Impact:** Negative, the inclusion of online identifiers as "personal data" will lead to further burden of compliance for airline and it needs to reconsider its web policies of collecting cookies data etc.

**Article 5:** Article 5 makes clear that in addition to fair and lawful processing of data, the data should be processed in a transparent manner. Also, personal data should be adequate, relevant and limited to what is necessary. Also, the articles makes controller accountable by asking to demonstrate the compliance to GDPR**.** "Such information must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language". [31] Moreover, the controllers are required to demonstrate compliance with GDPR.

**Impact**: Negative, as the requirement of transparent processing means additional challenge for organization to demonstrate that processing transparent. The airline needs to reconsider the processing activities and asses which activities can be performed without collection of personal data or minimizing the personal data.

**Article 6:** The processor on order of controller can process the data only if the consent has been taken by data subject. Also, the controller can process the data for new purposes as long as the new purpose is compatible with the original purpose for which the consent was taken [31].

**Impact:** Negative, as the latter articles has made the mechanism of consent much difficult. The task to determine compatibility of new purpose with original purpose can be difficult.

**Article 7:** This article states that the data subject should give the consent "freely" and consent is not valid if the data subject has no other choice but to agree with terms and conditions set by organizations. Moreover, organizations are liable for demonstrating the purpose for which the personal data being collected is processed. Moreover, the purpose for which the processing is done should be explained using plain and clear language. Also, the consent can no longer be presented as part of terms and conditions. The controller has to show that the data subject has given valid consent. Moreover, the consent taken for initial purpose may or may not be used for latter purposes to process data again unless the latter purpose is compatible with the grounds for which the consent was taken initially [31].

**Impact:** Negative, as the GDPR does not explain what genuine consent is or how to obtain such consent. Also, the organization needs to take extra steps in order to demonstrate for what the personal data collected is processed for. Moreover, the fact that the consent is not valid in case if the data subject has no choice but to agree makes it very hard for airline business to operate as for instance. The airline needs to modify its terms and conditions for tickets for example and make consent clearly distinguished. The burden of proof to demonstrate that data subject has given valid consent will lead to additional administrative costs.

**Article 11:** If the purposes for which the controller is processing the personal data do not require the identification of the data subject, the controller is not required to maintain information identifying the data subject in order to comply with the GDPR. [31]

**Impact:** Positive, as the GDPR makes clear the retention of data that identifies the data subject for sake of compliance with GDPR.

**Article 12:** The GDPR makes it clear that the controller may ask additional information from data subject in order to establish the identity of data subject. This is not the requirement, however, the organization may exercise this right for verification purposes. Also, the GDPR states time limit of 1 month in order to facilitate the request of data subjects rights. Such requests must be processed by controller free of charge [31].

**Impact:** Positive, as the organization will have the right to ask further information and provide proof of identity before giving effect to their rights [31]. The negative side is the time limit puts an extra burden over organizations. Also, processing such requests free of charge means the organization will need to bear administrative costs other costs involved to handle such requests.

**Article 13:** The data subject will have right to basic information, such as identity of controller, the reasons for which their personal data is processed. The right to object to processing of personal data noted above must be communicated to the data subject no later than the time of the first communication with the data subject [31].

**Impact:** Neutral, as the article has same content as from article 10, 11 of directive. On the other hand, the negative impact is that airline will have to revise the policies communicated to customers.

**Article 15:** Article 15 makes the data subject's right of access to personal data much more comprehensive. The data subject will have right not only where their personal data is being processed but also the processors who process the personal data (recipients) and the purposes for which the data is processed, and the categories of data processed. Also, the controller will have obligation to let the data subject know about their rights to modify, update or delete their personal data (right to be forgotten), right to complaint to data protection authorities and the right to know the origin from where the data was obtained (in case of joint controllers) or where the controller has got the personal data from other sources [31].

**Impact:** negative, as this will put extra burden on organizations.

**Article 17:** Article 17 gives the "right to be forgotten" to data subject. That means that data subject can request erasure of data from controller in case the data is longer needed for the purpose for which the consent was taken to process the data. Also, the data subject can ask to disclose the identity of third parties to whom the data was disclosed [31].

**Impact:** Negative, this means the organizations will do extra work to modify the systems to erase such personal data upon receiving requests from data subject. In terms of airline business, the systems are made such that retain data for longer time periods and sometimes it is not even possible to erase all data as the feature is not built in system. This implies updating or replacing systems which will result in extra costs.

**Article 18:** Data subjects have the right to restrict the processing of personal data [31].

**Impact:** Negative, as the upon receiving such requests, the organization can no longer process the data unless the organization can demonstrate the compelling grounds for such processing.

**Article 20:** Article 20 gives data subject the right to portability of data. The data subject will have right to ask the controller to provide copy of their personal data in a structured, commonly used, machine-readable format that supports re-use and transfer their personal data from one controller to another [31].

**Impact:** Negative, as it will place extra burden over organization to build a system to exchange data in between them.

On the other hand, the positive impact will be that it will provide opportunity to attract customers from competitors. For example, currently, it is impossible to port data for frequent flyer program of one airline to another, however, with the formation of new systems resulting from this article will allows customers to port their data from one airline to another.

**Article 21:** The GDPR allows the data subject to ask the controller to restrict the data processing and the controller cannot continue data processing unless it can show compelling ground for which the data processing is necessary [31].

**Impact:** Negative, the organizations will now need to show the compelling grounds for which the data is processed.

**Article 24:** The controller is responsible for implementing appropriate technical and organizational measures to ensure and to demonstrate that its processing activities are compliant with the requirements of the GDPR [31]. Therefore, the controllers are required to show the evidence of compliance.

**Impact:** Negative, as the organization will need to do extra work and design programs that would demonstrate the compliance with GDPR.

**Article 25:** Controllers must ensure that, both in the planning phase of processing activities and the implementation phase of any new product or service, Data Protection Principles, and appropriate safeguards, are addressed and implemented [31].

**Impact:** Negative, as the organizations are now needed to ensure that privacy by design is the core of their business processes. This means not only updating current systems but in some cases replacing entire systems, thereby leading to additional costs.

**Article 26:** The GDPR puts the liability on controller (joint controllers) in the event when the damage is done to data subject and it is proved unless the controller can provide evidence that it is not responsible for such damage [31].

**Impact:** the GDPR does not exempt the liability or provide any kind of remedy to controller the event when the damage to data subject happens in case of “extra ordinary” circumstances or “unavoidable situations”.

**Article 28:** The appointment of processors by controllers has to meet certain conditions including the condition of ability to demonstrate the compliance with GDPR [31].

**Impact:** Negative, as some of the processors appointed by airline are not even based in EU/EEA so making them comply with GDPR will be a challenging task.

**Article 30:** Instead, each controller (and its representative, if any) must keep records of the controller's processing activities. Upon request, these records must be disclosed to DPAs [31].

**Impact:** Neutral, The obligation to record and document the activities is essentially same as mentioned in directive. On positive side, this obligation does not apply to organizations that has less than 250 employees.

**Article 31:** The controllers are required to cooperate with DPA [31].

**Impact:** Neutral

**Article 32:** The controller must implement appropriate technical and organizational security measures to protect personal data against accidental or unlawful destruction or loss, alteration, unauthorized disclosure or access [31]. Depending on the nature of the processing, these measures may include:

- Encryption of the personal data;
- On-going reviews of security measures;
- Redundancy and back-up facilities; and
- Regular security testing.

**Impact:** Neutral, as the concept is same as in directive, that the organizations must be able to ensure the safety- measures to protect the personal data.

**Article 33:** In the event of data breach, the controllers are required to notify DPA within 72 hours of time period. The exemption is only in case where there is no harm to data subject happens [31].

**Impact:** Negative, the 72 hours deadline puts a lot of pressure and burden over organization to prepare, document and report the breach to DPA.

**Article 34:** In case where the data subject is harmed due to data breach, the controller is required to notify data subject. The only exemption exists where the harm is remote for example, the controller has employed strong encryption techniques to protect data [31].

**Impact:** Negative, as notifying data subject may damage the reputation of organization and loss of trust from customers. On the other hand, the GDPR welcomes the organization to employ strong encryption techniques for data protection in order to not become the easy prey for modern age cyber-attacks.

**Article 44:** Under the GDPR, the obligations regarding Cross-Border Data Transfers apply directly to processors [31].

Impact: Negative, as it means extra burden of compliance for processors.

**Article 82:** Data subjects can bring claims directly against processors, in case the processor has not complied with GDPR [31].

**Impact:** Negative. This will significantly increase the liability on processors and the processors can face penalties if such claim has been proved by data subject.

**Article 40:** Associations and other industry bodies may prepare Codes of Conduct covering compliance with the GDPR, in respect of general or specific aspects of the GDPR [31].

**Impact:** Neutral, as the concept is same as conveyed in directive with the aim to enhance the compliance with data protection regulations.

**Article 44:** The cross-border data transfer is only permitted in case where the country outside the EU has appropriate data protection safeguard and have proper data security measures [31].

**Impact:** Negative, the airlines outsourced their business processes to third countries such as India, Philippines, It is questionable whether the data protection laws of such member states will satisfy GDPR's concept of "appropriate data security measures"

**Article 46:** A Cross-Border Data Transfer may take place on the basis of certifications together with binding and enforceable commitments of the data importer to apply the certification to the transferred data [31].

**Impact:** Uncertain

**Article 48:** A judgment from a third country, requiring a Cross-Border Data Transfer, only provides a lawful basis for such a transfer if the transfer is based on an appropriate international agreement, such as a Mutual Legal Assistance Treaty [31].

**Impact:** Negative, the transfer to third countries without international agreement will become a challenge and it will not be possible to comply with order from courts from third countries such as US, India etc, without the presence of such international agreement.

**Article 49:** A Cross-Border Data Transfer may be made on the basis that the data subject, having been informed of the possible risks of such transfer, explicitly consents [31].

**Impact:** Negative, this will place extra burden over organization to prove the consent taken from data subject for the purpose of cross border data protection and the fact that the data subject was made aware of it in plain and simple language.

**Article 77:** Data Subjects have the right to lodge complaints concerning the processing of his or her personal data with a DPA in the Member State in which they live or work, or the Member State in which the alleged infringement occurred [31].

**Impact:** Uncertain, as it is unclear what will happen in case the data subject complains to DPA against a controller for which the DPA is not responsible to regulate. Or what will be the cooperation mechanisms between DPAs.

**Article 82:** A data subject who has suffered harm as a result of the unlawful processing of his or her personal data has the right to receive compensation from the controller or processor for the harm suffered. A controller or processor is exempted from liability in case if they can prove such damage has not happened on their part [31].

**Impact:** Negative, as the GDPR extends the concept of liability on controllers and processors. It puts burden of proof on controllers to open an investigation in order to gather evidence that such damage has not happened due to organization's mistake.

**Article 83:** The maximum fine that can be imposed for serious infringements of the GDPR is the greater of €20 million or four percent of an undertaking's worldwide turnover for the preceding financial year [31].

**Impact:** Negative, the fines can shake the whole organization or may result in bankruptcy.

# Appendix 2- Example of privacy notice for Customers from Airline

Dear Passengers,

We would like you to take a moment and go through below form in order to get familiar with our data policies and find our contact details in case of any questions.

***North European Airlines System***

Helpline: 1-000-000-000

Email: contactus@Europeanairways.com

Contact number of data protection officer: 1-234-567-89

| | |
|---|---|
| **Personal data collected** | We collect your personal information such as your name, age, email address, mobile number, passport number |
| **Purpose of collecting** | To setup flight booking, to issue boarding pass, to ensure flight safety.<br>Contact details can be used to contact passengers in order to inform about possible changes in flight schedules or flight delays/cancellations. Also, we use your email address to send you notifications about your flights schedule changes. |
| **Recipients of data** | We share your data with **Ground handling partners**: to ensure your luggage gets to right destination. **Border control agencies:** To ensure security and safety of you and other passengers. Also, we engage processors to process data on behalf of us. We always make sure that the processors have appropriate technical safeguard to guarantee safety of your personal data. |
| **To correct your data** | If you believe that the data we hold about you is not correct or it needs to be rectified, please notify us by sending us an email on fly@northeuropeanairways.com and we will fulfill your request. |
| **To request copy of your data** | If you would like to receive copy of your personal data we hold, please send us your request by email on fly@northeuropeanairways.com. |
| **Categories of data we collect** | - Name and contact details(email address, mobile number)<br>- Information about booking and travel itinerary<br>- Information about transactions (e.g. credit card details)<br>- Passport number<br>- Advance passenger information (data of birth, passport number)<br>- Frequent flyer number<br>- Communications done over the call (in form of voice recordings). |
| **Control of data** | You have more control over your personal data. You can review details and let us know if any data needs to be rectified, or if you want the data to be deleted from our system or if you want us to stop processing your data. |
| **More secure data transfers** | Whenever we exchange with our partners at airport or with border control agencies, we make sure that proper encryption is used and your personal data is transferred securely using modern security techniques. |

# Appendix 3- Cross validation of Business Process Model As-Is with Eduard's model

| **Eduards's comments to make business process model As-Is GDPR compliant** | **Awais's comments to make business process model As-Is GDPR compliant** | **Validation remarks** |
|---|---|---|
| There is no consent asked from Customer. Add sub-process or introduce consent activities in As-Is Model. | There is no consent in As-Is model, so activities G2 and G3 activities are introduced (business process model To-Be) | Successful match. |
| Each processing activities should be logged according to Article 30. | As all the information is logged in history of PNR, so documenting booking reference number means keep log of all the activities. | Partially successful match. |
| There is no rectification process in As-Is model. | There is no rectification process, so I introduced activity G6 that will send privacy notice to Customer and inform about right to data rectification. | Successful match |
| There is no process for data subject to access information about personal data or process to export personal data. | There is currently no such process in business process model As-Is, so I introduced activity G6, which will send privacy notice to Customer and informing about the procedure to export personal data. | Successful match. |

# Appendix 4- Interview with Senior Director of Contact Center - Mike

| General Questions | | |
|---|---|---|
| Item Nr. | Questions | Answers |
| 1 | What position do you have in company? | Senior Director |
| 2 | What are your responsibilities? | I am responsible for business development and overall site maintenance. I make sure that all the service standards are up to date, the company has appropriate staffing level and any appropriate trainings can be arranged for teams when requested by team managers. |
| 3 | How long have you been working in company? | 13 Years. |
| 4 | On a scale of 0-10, how much are you familiar with GDPR? (In case of no-familiarity, a 4 page brief summary of GDPR along with link to GDPR detailed text is handled) | 6 or 7 is realistic. |

| Questions to validate business process modelling (Figure 4.2) | | | |
|---|---|---|---|
| **Item Nr.** | **Questions asked by interviewer** | **Purpose of Question** | **Answers of Interviewee** |
| 1. | I have done modelling of flight booking process in figure 4.2. Could you look at the model carefully and confirm if this is how the | *To validate Business Process Modelled in Figure 4.2* | Yes. |

| | | | |
|---|---|---|---|
| | currently the flight booking process works? | | |
| 2. | What are the actors in flight booking process? | *To validate data collected for flight booking process* | Customer and MBS agent. |
| 3. | What is the virtual environment called, and what is the purpose of using this tool? | *By looking at figure 4.2, which are the activities where the personal data is captured/recorded?* | It is called VDI, and it is a virtual machine provided by North European Airways, to access the reservation system and issue tickets. |

| **Questions related to key area Consent** | | | |
|---|---|---|---|
| Item Nr. | Questions asked by interviewer | Purpose of Question | Answers of Interviewee |
| 1. | How do you interpret the concept of consent from GDPR? | *To establish understanding about the concept of Consent of interviewee* | Every single Customer touch points has to have a consent attached to it. Especially if we collect their Personal data. That’s one part, second part is you have a lot of employee data, so right of consent also applies to personal data of employees. Having said that, from GDPR point of view, such consent should be taken in very simple text, explaining each and every purpose of personal data collection. |
| 2. | Is there a valid consent in flight booking process modelled in figure 4.2? | *To validate GDPR non-compliance of flight booking process (Figure 4.2)* | Perhaps not. But we do let our callers know that interaction is being recorded and will be stored. However, the purposes of data collection and third parties with whom data is shared is not communicated clearly to Customers. |
| 3. | What are the difficulties to obtain valid consent? | *To grasp interviewee’s knowledge of consent.* | Making booking on behalf of someone else. If the customer is making on behalf of someone else, then the customer making the booking could give consent on behalf of the person for whom the booking is being made or not, it is uncertain. Also, all of our back office tasks such as |

| | | | |
|---|---|---|---|
| | | | rebooking in case of irregularities, are done in India, so under GDPR, we may have to take Customer's consent before transferring personal data to third country, and we don't have any backup plan yet if Customer refuses to give permission for data transfer to third country. |
| 4. | In your opinion, who is responsible for obtaining valid consent? Data controllers or Data processors? | *To determine the entity responsible for implementing solution* | Controller (North European Airways) and Processor (MBS) |
| 5. | By looking at figure 4.3, is it a valid way to take consent? Can you please comment on new activities introduced G2 and G3 to obtain valid consent? | *To validate GDPR compliant flight booking process (Figure 4.3)* | The solution looks very feasible to me and something which can be completely achievable. The challenges might be at implementation level. If North European Airways would be ready to modify their system to modify their system and have the valid consent mechanism in place. We need to have collaboration and cooperation in order to have such mechanism implemented. |
| 6. | Can you please briefly give feedback about sub process | *To validate sub processes for consent mechanism (figure 4.3 and Figure 4.4)* | While looking at both models, It looks practical to me to further break down such mechanism at implementation level and embed it in our business process but the questionable activities are modifying flight ticket contract. The North European Airways need to refine policies and documentation about what will be course of action in case of consent withdrawal. However, I do see both models as valid solutions. |
| 7. | Will it affect your Business? Is this solution practical? | *To determine the feasibility/practicality of proposed solution.* | Honestly, I think the impact will be huge because we engage so many sub-processors to process data on our behalf, for example for rebooking of tickets, we have one sub-processor, for refunds we have another sub-processor and so data is stored in so many layers, that we need to work hard to develop processes to have this request fulfilled. The solution is fea- |

| | | | |
|---|---|---|---|
| | | | sible at broader level but we need to further break in to more detail level. Also, we need collaboration with North European Airways in order to have these sub processes implemented. |

| **Questions related to key area Transparency** | | | |
|---|---|---|---|
| **Item Nr.** | **Questions asked by interviewer** | **Purpose of Question** | **Answers of Interviewee** |
| 1. | How do you interpret concept of transparency? What does transparent business mean? | *To establish understanding about the concept of Consent of interviewee* | Communicating information to customers in as simple manner as possible. |
| 2. | Is the flight booking process modelled in figure 4.2 transparent from GDPR perspective? | *To validate flight booking process in figure 4.2 from transparency perspective* | Partially. As we are not communicating customer our privacy policy, neither we are informing the Customer that the Airline has engaged processors in different locations to process the data, so that makes our business partially transparent. Although North European Airways do have its privacy policy on its website. |
| 3. | What changes need to be done to make business process transparent? | *To establish interviewee's level of understanding about transparency* | We need to communicate our privacy polices not only in English, but in all EU languages (to which Airline has flight operations). Also, we need to communicate the Customer regarding engagement of processors by controller to process the data. |
| 4. | In your opinion, who is responsible for transparency? Data controllers or Data processors? | *To determine the entity responsible for implementing solution* | Data Controller (North European Airways) |
| 5. | By looking at figure 4.3, the new activities | *To validate GDPR complaint flight* | I agree with new activity G6 but I think the activity G1 is unnecessary as we are not the contact center situated outside of |

|  |  |  |  |
|---|---|---|---|
|  | introduced are G1 and G6 to make flight booking process transparent. Do you agree? | *booking process (figure 4.3)* | EU premises. I think it will be important if our contact center would be located in a country outside of EU. |
| 6. | Please provide your feedback on sub process for transparency activities in figure 4.6 | *To validate transparency sub process modelled in figure 4.6* | I believe the activity G6 and privacy notice appendix-2 both are very valid propositions to make the flight booking process GDPR compliant. |
| 7. | Will it affect your Business? Is this solution practical? | *To determine the practicality of solution* | As a processor, it will not have any impact on business as such, as the controller has the responsibility to prepare such privacy notices and then make a built-in mechanism, so that such privacy notices will be sent every time when the customer receives electronic ticket in email. As currently, the sales control tasks are outsourced to third countries, what if the customer denies to give permission for the data to be processed outside of EU premises? We don't have any back up plan for that. I am not sure if communicating information about back office tasks to customers, falls under GDPR. |

<table>
<tr><th colspan="4">Questions related to key area Data Security</th></tr>
<tr><th>Item Nr.</th><th>Questions asked by interviewer</th><th>Purpose of Question</th><th>Answers of Interviewee</th></tr>
<tr><td>1.</td><td>How do you classify the information security assets or what the key assets? Any examples?</td><td><i>To establish understanding about the concept of data security of interviewee</i></td><td>The key assets are Employees, our computer sys-tems and any piece of paper on which we write Customer's information.</td></tr>
</table>

| | | | |
|---|---|---|---|
| 2. | By looking at figure 4.2, do you see any data breaches or non-compliance with GDPR? Please highlight the activities that cause non-compliance. | *To validate GDPR non-compliance of flight booking process (figure 4.2)* | Certainly, activity A8 and B10 are something that exposes credit card information to certain threats e.g. social engineering threats, so there is non-compliance to GDPR as well as international secure payment standards. However, this is something I would say "work in progress". First of all, handling data securely has two aspects. First aspect is to make the environment i.e. our work place secure. Currently, all kind of electronic devices are allowed in production floors. This shouldn't be the case, as it puts us at risk of data breach possibilities.<br>Secondly, there is a responsibility that rests with controller, i.e. providing us with proper tools to process the information securely. For instance, we ask the credit card information over the phone, which makes the credit card information extremely vulnerable to threats such as social engineering, insider threats etc. |
| 4. | In your opinion, who is responsible for data security? Data controllers or Data processors? | *To determine the entity responsible for implementing solution* | Both (North European Airways and SBS) |
| 5. | By looking at figure 4.3, the new activities introduced to make flight booking process GDPR compliant are activities G4.1 and G4.2. Will these activities help to make flight booking process GDPR complaint? | *To validate GDPR complaint flight booking process modelled in figure 4.3* | As data processor, we are also trying to be ISO 27001 and PCI compliant, so we have got strong focus on information security and data security. However, we are trying to seek collaboration from North European Airways, which is our data controller to provide us tools to process the credit card information securely. I see it as a very good approach to make us PCI complaint. As per latest communication with one of the key account manager from North European Airways (data controller), they are seeking a similar solution. I will forward your input to make the solution realistic, as I see it as a very good approach. |

|  |  |  |  |
|---|---|---|---|
| 6. | The activities introduced are further explained at sub process level in figure 4.7. Please provide your feedback. | *To validate the sub processes.* | As I said earlier, it is a valid and very feasible approach which will minimize problem of credit card security risks. But it needs collaboration and communication from North European Airways. |
| 7. | Will it affect your Business? If yes, the how? | *To validate the practicality of solution.* | North European Airways will need to modify our systems, so there will be extra cost for it. Also, we will have to restrict electronic devices usage in production floor, which will make our agents unhappy, so we will have to think some incentive about them as well. |

| **Questions related to key area Documentation** | | | |
|---|---|---|---|
| **Item Nr.** | **Questions asked by interviewer** | **Purpose of Question** | **Answers of Interviewee** |
| 1. | How do you interpret the concept of documentation from GDPR? | *To establish understanding about the concept of documentation of interviewee* | Documentation of processes, policies, typically if data processor has their own processes, and then those policies should apply. However, if the data controller has policies and those need to be implemented, then data controller policies take precedence. |
| 2. | By looking at flight booking process modelled in figure 4.3, do you see any lack of compliance in terms of documentation? | *To validate GDPR non-compliance of flight booking process (figure 4.2)* | We are not using and CLM or CRM systems to document the details such as the booking reference numbers, the price of tickets, the date when tickets were sold through our contact center as all such details are currently being saved in North European Airways VDI system, but perhaps it is a good idea that we should start documenting these details as well in our secure CRM systems, after having permission from North European Airways. |
| 3. | The activity introduced in figure 4.3 is G5, to make flight booking process | *To validate GDPR compliant flight booking process* | Yes. I see it as a valid approach. |

| | | | |
|---|---|---|---|
| | GDPR compliant from documentation perspective. Is it a valid solution? | *modelled in figure 4.3* | |
| 5. | In your opinion, who is responsible for data security? Data controllers or Data processors? | *To determine the entity responsible for implementing solution* | Both (MBS and North European Airways). |
| 6. | Is the solution practical or implementable in your point of view? | *To determine the practicality of solution.* | It will full fill the needs from data processor perspective. However, Extra/additional administrative work will occur. |

## Appendix 5- Interview with Manager Quality Assurance of Contact Center -Alexandra

| General Questions | | |
|---|---|---|
| **Item Nr.** | **Questions** | **Answers** |
| 1 | What position do you have in company? | Manager Quality Assurance |
| 2 | What are your responsibilities? | My responsibilities are to to look after the quality parameters, design trainings and brush ups, update the knowledge portal with latest information updates and manage the quality team. Other tasks include arranging weekly meetings, managing customer satisfaction survey reports and keep the voice recording system up to date when needed. |
| 3 | How long have you been working in company? | I have worked 14 years for the airline. In 2014, the contact center was outsourced to third party, since then, (from 4 years) I am working for third party. (All together, 18 years of work experience in Airline business). |
| 4 | On a scale of 0-10, how much are you familiar with GDPR? (In case of no-familiarity, a 4 page brief summary of GDPR along with link to GDPR detailed text is handled) | It is difficult to answer this question. I have read the GDPR text briefly and read couple of articles, however, no deep knowledge. |

| Questions to validate business process modelling (Figure 4.2) | | | |
|---|---|---|---|
| **Item Nr.** | **Questions asked by interviewer** | **Purpose of Question** | **Answers of Interviewee** |

| | | | |
|---|---|---|---|
| 1. | I have done modelling of flight booking process in figure 4.2. Could you look at the model carefully and confirm if this is how the currently the flight booking process works? | *To validate Business Process Modelled in figure 4.2* | Yes. This model has captured the business process at detail level. |
| 2. | What are the actors in flight booking process? | *To validate data collected for flight booking process* | Customer and MBS agent. There are other actors for example IT staff, but perhaps that's beyond the scope at this moment. |
| 3. | What is the virtual environment called, and what is the purpose of using this tool? | *By looking at figure 4.2, which are the activities where the personal data is captured/recorded?* | A virtual machine provided by North European Airways which is used by our agents to setup flight bookings. |

| **Questions related to key area Consent** | | | |
|---|---|---|---|
| Item Nr. | Questions asked by interviewer | Purpose of Question | Answers of Interviewee |
| 1. | How do you interpret the concept of consent from GDPR? | *To establish understanding about the concept of Consent of interviewee* | I think consent is a freely given agreement by customer to use his or her personal data, while the text of consent should be simple and clear. |
| 2. | Is there a valid consent in flight booking process modelled in figure 4.2? | *To validate GDPR non-compliance of flight booking process (figure 4.2)* | I would say yes and no. Currently, we take consent in form of terms and conditions (activity B9) but GDPR disqualifies such consent, so no, we are not taking consent to use customer's personal data. However, we do take consent of Customer to record phone call (IVR message) but the issue is that customer has no option but to accept the consent statement, so it is not a freely given consent. |

|  |  |  |  |
|---|---|---|---|
| 3. | What are the difficulties to obtain valid consent? | *To grasp interviewee's knowledge* | It depends what you call as valid consent. In my opinion, it is matter of common sense and should be understood by Customer that we need personal details to setup flight booking and the calls are recorded in case to overcome any dispute related to product that may come, for example, one of the common problem we have is that Customers often argue about miscommunication about ticket price quoted by agent. The only way for us to verify what price of ticket was quoted by agent, is to listen to call recordings, so in case if customer choose his call not to be recorded, or if Customer decides to withdraw consent at any later stage, then it would become extremely difficult for us to tackle such dispute cases. |
| 4. | In your opinion, who is responsible for obtaining valid consent? Data controllers or Data processors? | *To determine the entity responsible for implementing solution* | I think both are responsible for making sure that a valid consent is obtained from customer and after that personal details including voice recording is processed/stored. |
| 5. | By looking at figure 4.3, is it a valid way to take consent? Can you please comment on new activities introduced G2 and G3 to obtain valid consent? | *To validate GDPR compliant flight booking process (figure 4.3)* | The solution does seem to meet the requirements of obtaining valid consent, however there are few challenges associated. First of all, both North European Airways and MBS need to reach an agreement and discuss how the solution will be implemented because without cooperation of both entities, it is not only difficult to comply with GDPR but also there is a risk of dispute in case of non-compliance as there might be a blame game between data controller and data processor if the liabilities are not clearly set and defined beforehand. Secondly, it would be easier if the agent will just transfer the customer to IVR. As the consent needs to be obtained if Cus- |

| | | | |
|---|---|---|---|
| | | | tomer's data is shared with third parties e.g. border control agencies in US, Russia or Asia (depending on destination), so design different IVRs and the agent should ask about origin and destination from Customer and then transfer the call to suitable IVR. |
| 6. | Can you please briefly give feedback about sub process | *To validate sub processes for consent mechanism (figure 4.3 and figure 4.4)* | I would approve the models as meeting our business process requirements, however, I am not sure how the modifying contract before the flight date will work. |
| 7. | Will it affect your Business? Is this solution practical? | *To determine the feasibility/practicality of proposed solution.* | Yes, first of all, it means extra work. Secondly, as I mentioned earlier, we have to reach agreement with North European Airways and such solution can only be realistic in case of cooperation between SBS (data processor) and North European Airways (data controller). |

| **Questions related to key area Transparency** | | | |
|---|---|---|---|
| **Item Nr.** | **Questions asked by interviewer** | **Purpose of Question** | **Answers of Interviewee** |
| 1. | How do you interpret concept of transparency? What does transparent business mean? | *To establish understanding about the concept of Consent of interviewee* | Information communicated to Customer in as simple and plan text as possible, so that there are no confusions. Also, making clear what categories of data we are processing and what is the purpose of data processing. |
| 2. | Is the flight booking process modelled in figure 4.2 transparent from GDPR perspective? | *To validate flight booking process in figure 4.2 from transparency perspective* | I think we are partially transparent, in a way that we try to communicate our policies in simple manner, however, most of the time, we refer our Customers to visit the website of Airline to read about privacy policies and the information may not always be easy to find. May be it's a |

| | | | |
|---|---|---|---|
| | | | good idea to send privacy notice along with electronic ticket. |
| 3. | What changes need to be done to make business process transparent? | *To establish interviewee's level of understanding about transparency* | At this point, I am not sure but I think it will be a good idea if the privacy notices are sent in more clear and plan language to Customers. Privacy policies are missing in certain EU languages (countries to which we do operate flights), so the Airline has to translate the privacy policies in respective EU languages. |
| 4. | In your opinion, who is responsible for transparency? Data controllers or Data processors? | *To determine the entity responsible for implementing solution* | Airline ( North European Airways) |
| 5. | By looking at figure 4.3, the new activities introduced are G1 and G6 to make flight booking process transparent. Do you agree? | *To validate GDPR complaint flight booking process (figure 4.3)* | Yes I agree. Activity G6 is a valid activity but I think activity G1 is unnecessary as we are not operating from a country outside of EU. |
| 6. | Please provide your feedback on sub process for transparency activities in figure 4.6 and also on privacy notice example (appendix-2) | *To validate transparency sub process modelled in figure 4.6* | The Appendix-2 solution looks feasible. However, we have to consider that some of our Customers who make booking over the phone are not computer literate or there are blind Customers as well, so it is questionable how the privacy notices will be communicated to such Customers. |
| 7. | Will it affect your Business? Is this solution practical? | *To determine the practicality of solution* | As data processor (MBS), it will have no affects but for North European Airways, there might be some additional costs for implementing this solution. |

**Questions related to key area Data Security**

| Item Nr. | Questions asked by interviewer | Purpose of Question | Answers of Interviewee |
|---|---|---|---|
| 1. | How do you classify the information security assets or what the key assets? Any examples? | *To establish understanding about the concept of data security of interviewee* | 1. Paper and pen.<br>2. Few people who have access to recording. Who has access, take signature, I am not going to use this data for any other purposes than work.<br>3. Employee id should be there who has played call. |
| 2. | By looking at figure 4.2, do you see any data breaches or non-compliance with GDPR? Please highlight the activities that cause non-compliance. | *To validate GDPR non-compliance of flight booking process (figure 4.2)* | Yes. It is obvious that credit card information is handled very casually. The information asked by agent is written on pen and paper which is a direct violation of secure credit card handling standards. So, activities A8 and B10 should be replaced with some kind of secure mechanism. |
| 4. | In your opinion, who is responsible for data security? Data controllers or Data processors? | *To determine the entity responsible for implementing solution* | Both, Controller (North European Airways) and data processor (MBS). |
| 5. | By looking at figure 4.3, the new activities introduced to make flight booking process GDPR compliant are activities G4.1 and G4.2. Will these activities help to make flight booking process GDPR complaint? | *To validate GDPR complaint flight booking process modelled in figure 4.3* | It will definitely solve the problems to certain ex-tent, however, implementing such solution means that the North European Airways (data controller) has to modify the system.<br>As a data processor, we need to make sure that the agents would no longer ask for credit card information (insider threat) and we update our policies such as stricter rules in production with respect to usage of electronic devices, access to social media websites etc. etc. |

|  |  |  |  |
|---|---|---|---|
| 6. | The activities introduced are further explained at sub process level in figure 4.7. Please provide your feedback. | *To validate the sub processes.* | The solutions looks optimistic and our needs will be full filed. |
| 7. | Will it affect your Business? If yes, the how? | *To validate the practicality of solution.* | Yes, it will create overhead for North European Airways. Implementing new system means additional costs. |

| **Questions related to key area Documentation** |  |  |  |
|---|---|---|---|
| **Item Nr.** | **Questions asked by interviewer** | **Purpose of Question** | **Answers of Interviewee** |
| 1. | How do you interpret the concept of documentation from GDPR? | *To establish understanding about the concept of documentation of interviewee* | As a data processor, it means that we should document all the activities such as keep track of sale activities, recording sales statistics etc. |
| 2. | By looking at flight booking process modelled in figure 4.3, do you see any lack of compliance in terms of documentation? | *To validate GDPR non-compliance of flight booking process (figure 4.2)* | I think there should be additional activities where we should keep track of sales activities such as recording booking reference numbers. |
| 3. | The activity introduced in figure 4.3 is G5, to make flight booking process GDPR compliant from documentation perspective. Is it a valid solution? | *To validate GDPR compliant flight booking process modelled in figure 4.3* | Yes. I see it as a very good solution. But we need to have secure CRM systems as well, in order to securely save such information. |

| | | | |
|---|---|---|---|
| 5. | In your opinion, who is responsible for data security? Data controllers or Data processors? | *To determine the entity responsible for implementing solution* | Both, North European Airways and MBS. |
| 6. | Is the solution practical or implementable in your point of view? | *To determine the practicality of solution.* | Well, I think it puts some administrative burden, but in long run, it gives incentive of being GDPR compliant. |

## Appendix 6- Interview with Key Account Manager of Contact Center – Steven

| General Questions | | |
|---|---|---|
| Item Nr. | Questions | Answers |
| 1 | What position do you have in company? | Key account manager |
| 2 | What are your responsibilities? | To manage accounts of MBS and manage team of team managers. |
| 3 | How long have you been working in company? | 13 year. |
| 4 | On a scale of 0-10, how much are you familiar with GDPR? (In case of no-familiarity, a 4 page brief summary of GDPR along with link to GDPR detailed text is handled) | 5-6 |

| Questions to validate business process modelling (Figure 4.2) | | | |
|---|---|---|---|
| **Item Nr.** | **Questions asked by interviewer** | **Purpose of Question** | **Answers of Interviewee** |
| 1. | I have done modelling of flight booking process in figure 4.2. Could you look at the model carefully and confirm if this is how the currently the | *To validate Business Process Modelled in figure 4.2* | Yes, I think pretty much all the details are covered and shown in details in this model. |

| | | | |
|---|---|---|---|
| | flight booking process works? | | |
| 2. | What are the actors in flight booking process? | *To validate data collected for flight booking process* | MBS Agent, customer and someone listening to the call live (for quality assurance purposes) |
| 3. | What is the virtual environment called, and what is the purpose of using this tool? | *By looking at figure 4.2, which are the activities where the personal data is captured/recorded?* | It is called VDI and it is provided by North European Airways to access the reservation system. Each agent has unique ID to access this virtual environment system. |

| **Questions related to key area Consent** | | | |
|---|---|---|---|
| Item Nr. | Questions asked by interviewer | Purpose of Question | Answers of Interviewee |
| 1. | How do you interpret the concept of consent from GDPR? | *To establish understanding about the concept of Consent of interviewee* | The permission to process the data. Such permission be taken in a manner that it is clear and understandable. The owner of data has to clearly state that he or she is willing to let us use his or her personal data |
| 2. | Is there a valid consent in flight booking process modelled in figure 4.2? | *To validate GDPR non-compliance of flight booking process (figure 4.2)* | Well, before the arrival of GDPR, yes. In activity B9, we used to take consent in form of terms and conditions but as the GDPR doesn't allow the consent to be part of terms and conditions, then that makes our current consent in flight booking invalid. |
| 3. | What are the difficulties to obtain valid consent? | *To grasp interviewee's knowledge* | Well, I think it depends. I am not sure if the customer calling is making the booking for someone else, then who has the right to give consent and who has the right to withdraw consent, also if the customer wishes the call not be recorded, then we are uncertain how we will go with that. |
| 4. | In your opinion, who is responsible for obtaining valid consent? Data controllers or Data processors? | *To determine the entity responsible for implementing solution* | Both, North European Airways and MBS. |

|  |  |  |  |
|---|---|---|---|
| 5. | By looking at figure 4.3, is it a valid way to take consent? Can you please comment on new activities introduced G2 and G3 to obtain valid consent? | *To validate GDPR compliant flight booking process (figure 4.3)* | Yes, on a broader level, the solution looks valid, however, we need to dig in to more detail level, i.e. what mechanism can be developed in case of consent withdraw before the commencement of flight. |
| 6. | Can you please briefly give feedback about sub process in figure 4.3 and figure 4.4 | *To validate sub processes for consent mechanism (figure 4.3 and figure 4.4)* | The solution looks valid but as I said earlier, at implementation level, we need to dig in to more detail, which is the task for North European Airways. |
| 7. | Will it affect your Business? Is this solution practical? | *To determine the feasibility/practicality of proposed solution.* | Well, I think the call handling times will be increased, which means our service levels will have negative impact. |

| **Questions related to key area Transparency** | | | |
|---|---|---|---|
| **Item Nr.** | **Questions asked by interviewer** | **Purpose of Question** | **Answers of Interviewee** |
| 1. | How do you interpret concept of transparency? What does transparent business mean? | *To establish understanding about the concept of Consent of interviewee* | I think we need to communicate to our customers not only the purpose of data processing but also the fact that North European Airways engages processors (MBS) to process the data. |
| 2. | Is the flight booking process modelled in figure 4.2 transparent from GDPR perspective? | *To validate flight booking process in figure 4.2 from transparency perspective* | Partially, as there is a link to website mentioned in electronic ticket, that customers can visit to read the privacy notice. But there is no separate privacy notice sent along with E-ticket. |
| 3. | What changes need to be done | *To establish interviewee's level of understanding about transparency* | Sending out privacy notice is a good idea. |

|  |  |  |  |
|---|---|---|---|
|  | to make business process transparent? |  |  |
| 4. | In your opinion, who is responsible for transparency? Data controllers or Data processors? | *To determine the entity responsible for implementing solution* | North European Airways (Data controller) |
| 5. | By looking at figure 4.3, the new activities introduced are G1 and G6 to make flight booking process transparent. Do you agree? | *To validate GDPR complaint flight booking process (figure 4.3)* | Activity G1 is unnecessary. With activity G6, I agree, sending privacy notice will not harm anyone, infact it will make our business process more transparent from GDPR perspective and we will client's trust. |
| 6. | Please provide your feedback on sub process for transparency activities in figure 4.6 and also on privacy notice example (appendix-2) | *To validate transparency sub process modelled in figure 4.6* | The solution looks valid and doable to me. |
| 7. | Will it affect your Business? Is this solution practical? | *To determine the practicality of solution* | Yes, I think the solution is very much practical and I don't think there would be big costs attached with such solution. |

| **Questions related to key area Data Security** | | | |
|---|---|---|---|
| **Item Nr.** | **Questions asked by interviewer** | **Purpose of Question** | **Answers of Interviewee** |
| 1. | How do you classify the information security assets or | *To establish understanding about the concept of data security of interviewee* | Employees, computer systems. |

| | | | |
|---|---|---|---|
| | what the key assets? Any examples? | | |
| 2. | By looking at figure 4.2, do you see any data breaches or non-compliance with GDPR? Please highlight the activities that cause non-compliance. | *To validate GDPR non-compliance of flight booking process (figure 4.2)* | Activity A8 and B10 where the agent asks for credit card details. This is something we have been trying to convince North European Airways to implement some kind of secure payment system but unfortunately, there has not been any solution came from them yet. |
| 4. | In your opinion, who is responsible for data security? Data controllers or Data processors? | *To determine the entity responsible for implementing solution* | Both. (North European Airways and MBS) |
| 5. | By looking at figure 4.3, the new activities introduced to make flight booking process GDPR compliant are activities G4.1 and G4.2. Will these activities help to make flight booking process GDPR complaint? | *To validate GDPR complaint flight booking process modelled in figure 4.3* | I see it as an excellent solution. This is the suggestion we have made to North European Airways already and we are expecting activities similar to G4.1 and G4.2 to be part of current flight booking process. |
| 6. | The activities introduced are further explained at sub process level in figure 4.7. Please provide your feedback. | *To validate the sub processes.* | As I said earlier, I like the solution and we are expecting it to be available soon. |

|  |  |  |  |
|---|---|---|---|
| 7. | Will it affect your Business? If yes, the how? | *To validate the practicality of solution.* | For North European Airways, there will be cost wise affects. |

| **Questions related to key area Documentation** | | | |
|---|---|---|---|
| **Item Nr.** | **Questions asked by interviewer** | **Purpose of Question** | **Answers of Interviewee** |
| 1. | How do you interpret the concept of documentation from GDPR? | *To establish understanding about the concept of documentation of interviewee* | Documenting each and every details such as who made the flight booking, when the flight booking was made, storing such information in CLM systems. |
| 2. | By looking at flight booking process modelled in figure 4.3, do you see any lack of compliance in terms of documentation? | *To validate GDPR non-compliance of flight booking process (figure 4.2)* | The booking reference numbers we don't document as we don't have secure CRM systems but we have demanded the secure CRM systems from our head office, which will be available soon and we will start documenting booking details. |
| 3. | The activity introduced in figure 4.3 is G5, to make flight booking process GDPR compliant from documentation perspective. Is it a valid solution? | *To validate GDPR compliant flight booking process modelled in figure 4.3* | Yes, as I mentioned before, we are waiting for secure CRM systems to be available soon and then we will start documenting the details such as booking reference, price of ticket, data of ticket issuance, agent who has issued the ticket etc. etc. |
| 5. | In your opinion, who is responsible for data security? Data controllers or Data processors? | *To determine the entity responsible for implementing solution* | Both (North European Airways and MBS) |
| 6. | Is the solution practical (activity G5 in figure | *To determine the practicality of solution.* | Yes, the solution looks very much doable and meeting our business requirements. |

| | | | |
|---|---|---|---|
| | 4.3) or implementable in your point of view? | | |

**Non-exclusive license to reproduce thesis and make thesis public**

I, Awais Abbasi (date of birth: 25th of Feburary 1990),

herewith grant the University of Tartu a free permit (non-exclusive license) to:

1.1. reproduce, for the purpose of preservation and making available to the public, including for addition to the DSpace digital archives until expiry of the term of validity of the copyright, and

1.2. make available to the public via the web environment of the University of Tartu, including via the DSpace digital archives until expiry of the term of validity of the copyright,

GDPR Implementation in an Airline's Contact Center

supervised by Raimundas Matulevicius and Jake Tom.

2. I am aware of the fact that the author retains these rights.

3. I certify that granting the non-exclusive license does not infringe the intellectual property rights or rights arising from the Personal Data Protection Act.

Tartu, 21.05.2018