Universiteit Leiden

ICT in Business and the Public Sector

E-mail marketing in the post-GDPR era

- A study of residual risks and recommended best practices

Name: Malik Samnani
Student-no: S1254596

Date: 23/09/2020

1st supervisor: Prof. Dr. Joost Visser
2nd supervisor: Prof. Dr. Niels van Weeren

MASTER'S THESIS

Leiden Institute of Advanced Computer Science (LIACS)
Leiden University
Niels Bohrweg 1
2333 CA Leiden
The Netherlands

Table of Contents

List of Abbreviations

Abbreviation	Full name
GDPR	General Data Protection Regulation
Art.	Article
ICO	The Information Commissioner's Office
AEPD	Agencia Española de Protección de Datos
ANSPDCP	Autoritatea Nationala de Supraveghere a Prelucrarii Datelor cu Caracter Personal
TLS	Transport Layer Security
MTA	Message Transfer Agent
CTR	Click through rate
ICT	Information Communication Technology
ROI	Return on Investment
CCPA	California Consumer Privacy Act
WPA	Washington Privacy Act
PIPEDA	Personal Information Protection and Elctronic Data Act
DPO	Data Protection Officer
EEA	European Economic Area
ESP	Email Service Provider
NCSC	National Cyber Security Center
PGP	Pretty Good Privacy
S/MIME	Secure/Multipurpose Internet Mail Extensions

List of Tables

List of Figures

Acknowledgements

This thesis is the end of the journey in obtaining my Masters in ICT in business from Leiden University. This rollercoaster ride was possible with the support and encouragement of my supervisors, family and friends. I want to thank everyone who contributed in many ways to the success of this study and being part of the journey.

Foremost, my heartiest acknowledgement to my first supervisor Prof. Dr. Joost Visser for his knowledge, advice, useful discussion, feedback and invaluable suggestions in this research. This thesis would not have been possible without his supervision, valuable guidance, support and encouragement. I am grateful to him for the time and patience that he has generously spent on our weekly skype meeting throughout the research process. I also thank him for introducing me to an expert using his network and giving me the opportunity to conduct an interview in this research study.

I would also like to thank my second supervisor Prof. Dr. Niels van Weeren for introducing to the GDPR topic to me in this research study, his review and valuable feedback to my thesis. Moreover, I highly appreciate his help in introducing me to an expert through his network that added a high value in this research study.

My sincere thanks to all the research participants who were involved in the interviews to help me gather data, give their valuable time and share their insights about my research topic.

I am incredibly grateful to my father Chhotu Samnani, brother Altaf Samnani and sister in law Anisah Naginawalla for their love, prayers, care, support and sacrifices for my master study. I must express my very profound gratitude to my girlfriend, Janneke Hommes, for always being there and supporting me through thick and thin during the process of writing this thesis.

Last but not least, I thank my best friends, Dominic Jahangier, Irfan Yuta and Rajesh Lale, for their support and encouragement during my time studying at Leiden University.

Abstract

Background. In April 2016, the GDPR privacy directive was introduced in the EU, became enforceable, embedded in EU national law in May 2018, leading to a stricter constraint on digital marketing activities, including email marketing activities.

Aim. The aim of this study is to investigate whether companies sufficiently adapted their email marketing activities to the GDPR privacy directive. In particular, our objective is to identify residual risks, exploring best-practices, and to explore if any digital marketing technologies may support GDPR compliance.

Method. In this explorative study, both academic and grey literature are used. Seven semi-structured in-depth interviews were conducted with email marketing experts and a data protection officer to validate the literature, seek for relations and obtain new information in the area of residual risks, best-practices and digital marketing technology.

Results. From the literature and interviewe, we have discovered 20 best practices for companies that run e-mail marketing campaigns and 6 third-party best practices. In addition, 18 residual risks were found in the area of insufficient compliance in email marketing. The interviews showed that companies do not fully follow the GDPR best practices, exposing them to privacy risks. We also observed a degree of over-reliance on technology for GDPR compliance. To support marketing practitioners to avoid risks and implement best practices, we have created guidance for practitioners in the form of models that connect goals, risks, and best practices, as well as process recommendations.

Conclusion. Companies have partially adapted their email marketing activities to the GDPR privacy directive. However, they are still underestimating several residual risks. Following our recommendations for the implementation of best practices may help to avoid those risks.

Chapter 1 Introduction

The world economy is impacted by vast revolutions in information and communication technology (ICT) which plays the significant role in the way businesses are operated. (Qashou & Saleh, 2018). Digital marketing is one of the critical business functions that have been impacted by such changes (Eid & El-Gohary, 2013; Tan, Chong, & Lin, 2013; Babalola & Babalola, 2015).

Digital marketing is expected to remain at the forefront of the technological revolution in the coming time (Lamberton & Stephen, 2016; Martín-Consuegra, Faraoni, Díaz, & Ranfagni, 2018). Digital marketing has become part of the daily life of billions of people around the world, often leading to the creation of customer relationships and reaching to the customer (Fujita, Harrigan, & Soutar, 2017; Han, Nguyen, & Nguyen, 2016; Woodside & Mir, 2019).

Many companies increasingly depend on the collection and use of customer information for personalized advertising, offerings and micro target specific audiences (White, Zahay, Thorbjørnsen, & Shavitt, 2008). They look out for new ways to gather more data about customers to use in digital marketing activities.

Digital marketing offers a variety of ways to reach, inform, and get engaged with customers. Digital companies use different channels such as social media marketing, content marketing, SEO and email marketing to reach their customers and promote their products and services. Additionally, it also includes online management of CRM and customer data (Janouch, 2014; Vysekalová, Juříkov, Kotyzová & Jurášková, 2011). One of the widely used channels is electronic marketing or e-marketing (Eid & El-Gohary, 2013; Tan, Chong, & Lin, 2013; Babalola & Babalola, 2015).

The marketing community explains email marketing as “a form of direct marketing which uses electronics mail as means of communicating commercial messages about products and services to an audience” (Fariborzi & Zahedifard, 2002). Email marketing helps organizations to increase site traffic and sales support via targeted sending of commercial and non-commercial messages to the users (Kirś & Harper, 2010).

Email marketing continues to highlight as a central pillar of any multi-channel marketing. Compare to any traditional marketing it remains extremely high (86%) in 2018 (DMA, 2018). E-mail marketing and email tools have become extremely useful for organizations. Email marketing technologies remain the favorite tool for customer acquisition and business promotions. More than half of the digital marketers claim that email is their biggest source of ROI (Change, 2020). From all the B2B marketers, 93% use email to spread and deliver content (Pulizzi & Handley, 2017). Almost all the online users (99%) check their email every day (Santora,2020; DMA, 2018).

The Facebook-Cambridge Analytica data breach was a data leak in early 2018 whereby Facebook users' personal data was harvested to Cambridge Analytics and used without consent for micro-targeted political ads. This scandal and new wide-sweeping data legislation have forced consumers to get to grips with their digital footprints. The Cambridge Analytica controversy raised questions about customer's privacy and how their data are being used by the company (Lamb, 2019). This controversy was a particularly striking event as millions of user's data was unknowingly pulled without user's permission, by a third-party provider, from one of the largest social media platforms in the world. Data breach incidents have not only increased fear in the public domain but have also forced governments to challenge personal data processing and develop legal reform that can protect and secure citizens from the consequences of such practices. To build customer relationships, trust has become an absolutely fundamental part of any digital company's proposition.

In April 2016, The European Union (EU) introduced the General Data Protection Regulation (GDPR) and enforcement began on May 25, 2018 and it became into full force, embedded in EU national law. Companies got two years transition period in the EU to prepare for the law from 2016 to 2018. This law defines individual privacy rights and restricts how firms can use customer personal data in business practices by increasing transparency of data collection activities. GDPR protects the collection, processing, and use of individuals' personal information of EU residents as well as all customers of EU-based companies or firms with EU offices (Goldberg, Johnson, & Shriver, 2019). Individuals receive the right to access their personal data, edit data, erase data, and port data elsewhere. Also, they have the rights to protest the data processing and object to decisions based on automated processing.

Email marketing uses digital data to get engaged with the users, and GDPR strengthens the user's privacy rights. The GDPR changed the rules of consent in email marketing. Therefore, the GDPR requirements have gained a lot of attention the way companies execute email marketing campaigns. There are security aspects like email safety and email encryption which are essential for GDPR compliance (Wolford,2019).

This research mainly focuses on e-mail marketing out of all areas of digital marketing. One of the reasons is that it is currently the most used form of direct marketing (Hudák, Kianičková, & Madleňák, 2017). It is the largest channel of marketing communication where nearly 50 % of the global population use email (Anthony, 2020). The research shows that there were 3.8 billion email users in 2018 and this number will rise to 4.4 billion users in 2023 (Clement, 2020). Secondly, it is an economical, still effective form of addressing to reach out to potential or current customers for many companies (Fabus & Fabusova, 2016). Lastly, it has stood its ground, despite the availability of faster and newer marketing channels in current time (Anthony, 2020).

1.1 Problem statement

After the introduction of GDPR in 2016, there were many companies who faced a problem with adoption of GDPR for their email marketing activities. The demanding nature of GDPR forced many companies to rethink the way they carried out their email marketing activities using customer’s digital data (Ruby, 2018). At the beginning period of GDPR, all the companies in the EU who acquired users’ personal data without consent had to review their entire mailing list. Some of the organizations were forced to delete the entire mailing database and opt for a fresh start in collecting user consent for their email marketing activities (Wolford, 2019; Ruby, 2018).

The GDPR enforcement tracker has an overview and list of all fines and penalties after the GDPR law became effective in May 2018. Many companies received fines and penalties from data protection authorities in the period from 2018 to 2020 for violating the GDPR legislation in their email marketing activities. In 2019 Vodafone ONO, S.A.U. got 36,000 euros of fine for sending a marketing email to a large number of customers without using the blind copy feature. Another two incidents related to security concern took place in March 2020. Vodafone Romania and Enel Energie got 3,000 and 4,150 euros fine respectively for sending an email to a client which contained personal data of another client. In both the incidents, companies failed to implement adequate level of information security (Enforcementtracker, 2020). These examples indicate that companies violated the GDPR law recently in their email marketing activities.

To adopt the GDPR standards, many companies started using IT solutions for GDPR compliance in their email marketing activities after the GDPR introduction in April 2016. They use manual processes and temporary controls to ensure compliance. But such a solution may not be effective for the long run. Many companies want to increase their level of automation and simultaneously maintain GDPR compliance. Although full automation is exceptional, companies can introduce such tools to make some processes automated to ease part of the burden (Mikkelsen, Rowshankish & Soller, 2017). The important question is, whether there is any digital technology that can be useful in email marketing activities in order to comply with GDPR standards.

To summarize, from the above incidents we can infer that some companies have only partially succeeded in implementing GDPR compliance and mitigating GDPR-related risks. For these companies, there are certain residual risks that exist while executing email marketing activities. Here, by we refer *residual risks* that indicate the remaining of risks associated with an undesirable event that could occur as result of insufficient privacy management, after the first iteration of measures and actions have been considered to adapt to the GDPR legislation by the companies in the EU. There is a need for digital technological solutions and best practices which can be helpful with email marketing activities considering GDPR regulations. Here, by the term *best practices* in this research, we indicate that any empirical, active and feasible course of action that is suggested by researchers or practitioners, regardless of whether there are widespread adoption and support for recommendations or evidence that following the practice guides to enhanced performance. Such companies must consider the adequate level of security for their users in email marketing activities. Based on all the problems that still exist, it is important to conduct research to find out if companies have adapted GDPR in their email marketing activities and to find ways to improve the execution of email marketing activities effectively under GDPR compliance.

1.2 Research questions

Our main research question is as follows:

Main research question:

Have companies sufficiently adapted their email marketing activities to the GDPR privacy directive?

To answer the main question of this research, we decompose it into the following sub questions:

Sub question:

SQ1: What are the residual risks companies can be exposed to email marketing activities to comply with GDPR standards?

SQ2: What are the proactive best practices that should be followed in email marketing activities to preempt any residual GDPR risks?

SQ3: Is there any digital technology that can help companies with GDPR compliance for email marketing activities?

1.3 Research objectives

This aim of this research to find out if the companies sufficiently adapted their email marketing activities to the GDPR. This study will focus on the identifying residual risks, exploring best practices and to find out digital technologies under the GDPR. We will use literature study to gather the information in these three areas. For the literature study, mostly grey literature will be used. Furthermore, in depth semi structured interviews will be taken to identify current residual risk at the organization, find out what best practices are followed, and which digital technology is used in the company to be GDPR compliant in email marketing. In the interviews with six digital marketers and one GDPR expert new information will be obtained related to research topic.

In the study the literature and findings from the interviews will be combined and analyzed together. After analyzing the literature and interviews, the link between residual risks and their associated best practices will be identified. The relation between the residual risks and best practices will be shown via a risk factor model. we will develop the best practices that also prevent risks for email marketer practitioners and companies, that can be followed under the GDPR.

Lastly, we look at digital technologies in the field of email marketing through interviews that can cover residual risks and apply best practices with regard to the GDPR legislation. The outcome of the research will be beneficial and help companies to adapt email marketing in the most effective way under the GDPR law.

1.4 Thesis structure

This thesis is divided into 9 chapters. Table 1 provides a brief overview of each chapter.

Chapter	**Description**
1.	The first chapter gives an introduction of the research, defines the problems statement along with research objectives and research questions.
2	The second chapter provides the background of the research topic and general definition of email marketing,
3	The third chapter gives explanation about GDPR, principles and its impact of GDPR in email marketing.
4	The fourth chapter outlines the research methodology used to conduct this research, research approach, research design and also explains how research data is collected and analyzed.
5	Chapter five discusses the literature review related to the research questions and finding out the information from existing research papers and using grey literature.
6	In chapter six, we conduct the interview from digital marketers and DPO to find out the missing information from the literature gap and to answer final research questions by analyzing the data.
7	In chapter seven, the result from the interviews will be analyzed
8	The chapter eight, towards guidance for practitioner via a flow chart of consent condition and factor risk models will be created linking best practices of residual risks.
9	In chapter nine the result will be discussed along with interpretation, limitations, strong side of the research, recommendations for further research and recommendation for email marketers' practitioners.
10	In the final chapter, we give final answer to the research questions along contribution of this study.

Table 1 Thesis Outline

Chapter 2 Background

This chapter explains the theoretical background of the research topic with the help of literature. This chapter will cover Introduction of email marketing, what is email marketing, process involved in email marketing, important steps in email marketing, newsletter, permission marketing, user data in email marketing and email marketing automation.

2.1 Introduction of email marketing

Email marketing continues to be recognised as an effective marketing tool (Niall, 2000). Because of its high response rate, email marketing is considered to be one of the most effective internet marketing tools. The global email marketing market is forecast to grow at 19.60% by 2025 (Anthony, 2020). The global marketing market was valued at 4.5 billion dollars in 2017 and is expected to be valued at 22.16 billion by 2025 (Transparency Market Research, 2019).

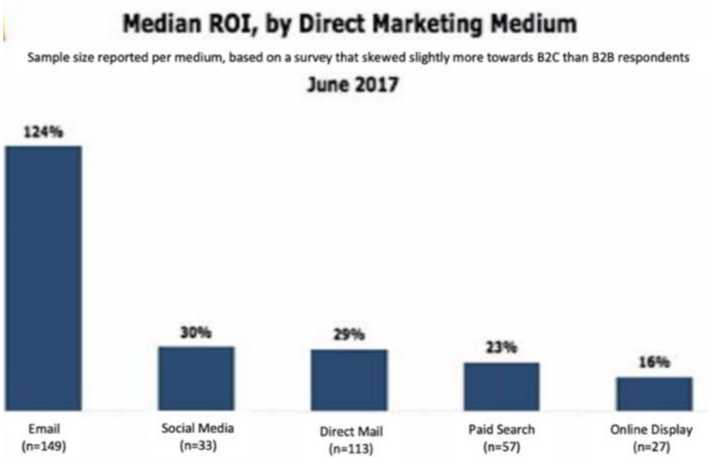


Figure 1 Different level of promotion through digital medium (Soegoto & Faherza, 2018).

The use of email marketing as an online marketing medium has a potential 124% higher in comparison with other online marketing media (Soegoto & Faherza, 2018). The business has no doubt about the power of email marketing which is used for promoting product or services. Figure 1 shows the level of promotion through online media where email stands out on top of the list.

2.2 What is email marketing

Email marketing has started to spread faster and grow with the development of ICT (Qashou & Saleh, 2018). The simple understanding of email marketing is a "unique communication platform that blends both art and science while delivering value to subscriber's inbox" (Jenkins,2008). Sterne & Priore (2000), describes email marketing "it is the most effective way to start building customer relationship and ability to provide personalization through data mining is the most effective way to ensure customer satisfaction and increase loyalty". Email marketing is considered as one of the most effective marketing activities which is involved in brand building, improving customer relationship, sales promotion and obtaining new contacts (Hudák, Kianičková, & Madleňák, 2017). The medium is push instead of pull, the customer doesn't have to initiate the interaction (Di Ianni, 2000; Rosenspan, 2000).

The benefits of email marketing have been identified by a number of authors. The benefits vary between marketing specialist as per their backgrounds and views. According to Jackson & Decormier, (1997) recognized that, "email provides communication to the digital marketers that permitted real time interaction and building relationship with consumers". Wreden, (1999) explain email marketing as the "Internet's killer application" because of the accuracy of email with which it can be tailored, tracked and targeted. Peppers and Rodgers, (2000) explain that "clear benefits, including high response rates and low cost are rapidly turning email marketing into an invaluable tool", which can be used for retention or acquisition. While Strauss & Frost (2001) describes it as "the use of electronic data and applications for planning and executing the conception, distribution and pricing of ideas, goods and services to create exchanges that satisfy individual and organizational goals".

2.3 Process of email marketing.

We have found eight different process in email marketing through literature study as shown in the Figure 2. These processes explain the eight different stages in email marketing which are useful in terms of effective email marketing communication with users.

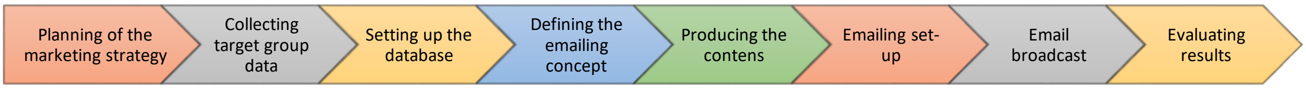


Figure 2: The eight stages process in Email marketing (Aschoff, 2011).

1. Planning of the marketing strategy: Firstly, email marketers must be defined the global goals and milestones which are supposed to be achieved via the help of email marketing. if such goals are not defined properly and only pure actionism dominates, then email marketing campaign most probably won’t be succeed. Email marketing is a marathon but not a sprint. Therefore, the path and the goal must be fined clearly, so that the provider doesn’t drift off from the track.

2. Collecting target group: After the marketing strategy have been determined, the next step is to identify which target groups should be addressed. The email addresses of the members of these target group must be collected via different methods. It can be via registration forms, using different content marketing strategies or third party. In addition, user’s consent must be obtained through user’s permission to send them emails.

3. Setting up the database: Once the information is collected of target group then it must be stored in the database. The data such as email addresses and other information like first name, last name, gender and desired email format must be stored in the database. This can be useful to personalized email according to the individual user. If marketers want to individualize the content of the email, then it can be collected via user preference. Collecting user preference helps marketers to target only relevant emails in which user will be interested and give high response rate. Therefore, it is important to collect user preference via user preference management center and store also in the database.

4. Defining the emailing concept: In this step, the concrete concept of emailing broadcasts is defined, that includes the tactical objectives and identifying email communication frequency. Additionally, the tonality, which decide the layout, design, style and language of the email. The emailing concept is useful for marketers to achieve higher clickthrough rate.

5. Producing the content: For each email marketing campaign, content must be produced for the email concept and target group. These contains advertising and/or editorial texts in the HTML, CSS format. It may also include graphics, photos and other visual elements.

6. Emailing set up: Once the concept and content are decided for respective emailing, the email must be setup. For example, the order of the texts must be identified and in the case of variable and optional text modules, it must also be specified which target groups should receive the respective text module. Lastly, the headers and footers are added, that includes the information for the email header (example: sender email address, subject line).

7. Email broadcast: When broadcasting an email to all the recipients, it should be complied as a personal email for recipients and sent accordingly to everyone. During the process of compilation, the appropriate email format as per user has to be considered such as HTML, text, PDF or Flash. The personal salutation and any variable or optional text modules must be taken into account while compiling the information. Emails which are returned back as undeliverable must be processed again depending on the reason for non-delivery. In addition, it is advisable to set up test account which can be used with the large providers to check whether emails are being delivered properly or being filtered out as spam email.

8. Evaluating results: The last stage of email marketing process is evaluating the overall result of email broadcast shown in the figure 2. Evaluation of result helps marketers to analyze the rate of undeliverable or opened email, CTR, conversation rate, bounce rate and delivery rate. Furthermore, it helps to identify the number and the revenue of orders and sales (Aschoff, 2011).

2.4 Important steps for sending a marketing email

There are 14 important points have been found through a research paper for sending marketing emails as shown in the table 2. These steps can be useful for email marketers while sending an email marketing campaign to their users. The same literature has also explained these steps via a process flow chart as shown in the figure 3.

Steps	Description of sending an email
1	Buy a suitable domain related to your product or services with dedicated IP address.
2	Use this domain to set up email account which can help to verify the email address of domain
3	Select a best Email Service Provider as per your requirement and budget, then verify your email and domain address with your ESP via verification link in your email inbox
4	Verification of domain can be done by placing SPF and DKIM records from your SMTP providers to your domain hosting website from domain has been purchased
5	In the case of using third party SMTP to send email then ensure that you configure https end point to receive the bounce emails and spam details
6	Use email cleaning service if your ESP does not provide the feature to clean the email list
7	Upload the relevant contacts in your ESP account and create proper email template for sending email along with accurate subject line.
8	Ensure that email is not too lengthy and does not contain more no. of images and too large images size
9	Ignore the uppercase letter usage in template and use standard font size. Also, color of email template and background should not be the same
10	Ignore using unethical and unsocial wording in your email and only send an email marketing campaign to the targeted audience
11	Ignore using the purchased or third-party email database instead use your own subscriber list to send email campaign. for a user who have opted in for consent.
12	Send an email for a user who have given consent and opted in to receive an email. Use double opt in process before adding into mailing list
13	Use suitable timing to send an email considering the country timing. Schedule it either early morning or late evening or also you can use your own pattern by analysis of user suitable time to send an email.
12	Don't send too many frequent emails that user get irritate and unsubscribe, instead send an email based on user preference.
13	Use website of your domain to send your email campaign so easy for user to identify.
14	In the case of shared IP address make sure the sender of your email is not the blacklisted.

Table 2: Useful steps for sending email marketing campaign (Tiwari, Ansari & Dubey, 2018).

The flow chart shown in the Figure 3 explain the process for sending an email marketing campaign to the users. There are different steps have been identified. Researcher recommend purchasing a domain at the first stage and then creating an email account. After that choosing ESP as per the requirement of your company and budget are important. Make sure that instead of choosing best ESP company more focus on following right procedure to execute email campaign. As choosing a right procedure for campaign will be more effective than choosing best ESP (Tiwari, Ansari & Dubey, 2018).

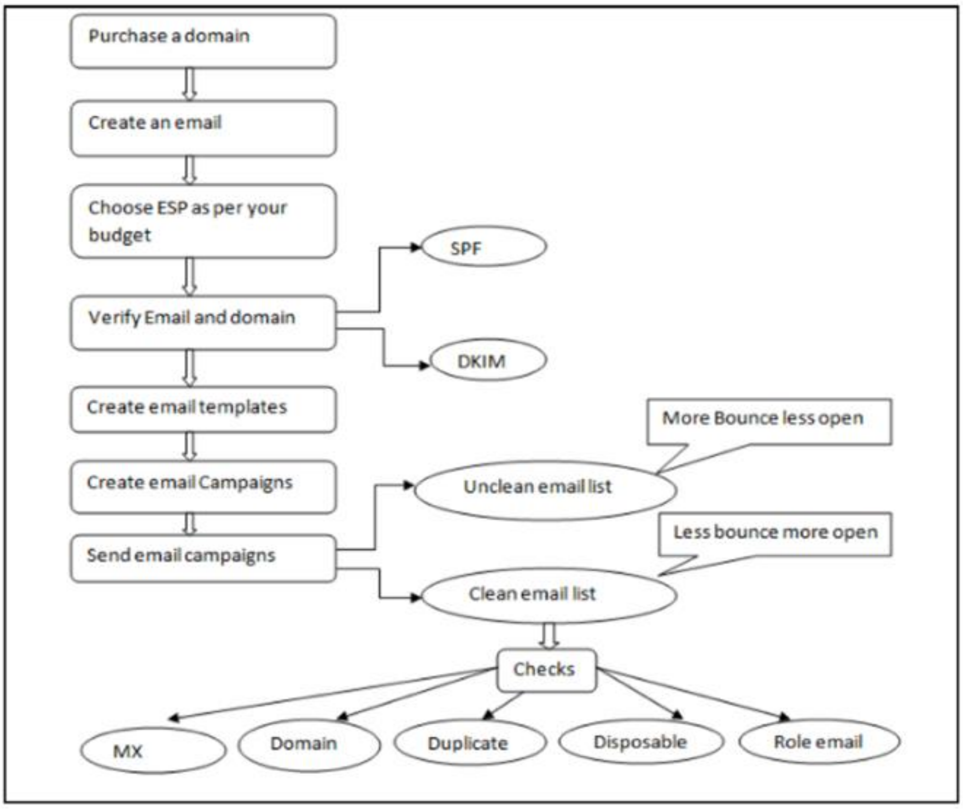


Figure 3 Flow chart process of sending email campaign (Tiwari, Ansari & Dubey, 2018).

Once you decide the ESP as per your requirement next step is to verify email and your domain. These can be done by including SPF and DKIM. SPF stands for sender policy framework. It provides s confirmation to the recipient server that server for email sending is authorized to send an email on your behalf. While DKIM stands for domain key identified mail used for checking the authenticity of your email. It includes digital signature in sending message along with public key and then decrypted at the recipient server using same public key. The purpose of this process is to confirm that whether same message came from sending server as a delivery.

The next step in process flow chat is to create email templates for email marketing campaign. Once it has created then send email campaign to only opt in users. It is important to clean email list by checking different attributes shown in the Figure 3. MX stands for mail exchange record, which is set in most of the case by domain host. Cleaning email list will give less bounce and more open rate compare to unclean email list (Tiwari, Ansari & Dubey, 2018).

2.5 Newsletter

Newsletter is a tool of email marketing which is also known as electronic newsletter. It is usually in HTML format and send on weekly, monthly or pre-decided frequency to the registered customers (Hudák, Kianičková, & Madleňák, 2017). It can be used as a B2B or B2C type of communication to perform different tasks, such as 1. Recalling existence of the company 2. Sharing the useful information to your customers. 3. Raising the brand credibility and awareness about the product or features. 4. Leads user from ordering services and products. 5 to collect feedback. Newsletter in terms of ROI is considered the one of the most effective channels along with an email marketing. The research found that up to 68 % of companies use this method and consider as an excellent channel (Viktor, 2010).

2.6 Permission marketing

Permission marketing defined as consent is giving by the consumers in order to receive marketing information (Godin, 1999). The consent concept is old, user permission had been introduced in terms of privacy issue in direct marketing in the past (Milne & Gordon, 1993). The permission marketing gives opportunity for knowing user interest and their information needs (Sterne & Priore, 2000). The consent, two-way communication and trust create the relationship between the company and the customer (Rettie & Chittenden, 2003). Permission marketing enhance relevance and the targeting of promotional message, consequently it improves response and conversion rates. The action of the internet facilitates communication of customer permission and preferences (Rettie & Chittenden, 2003; Kiran & Kishore, 2013).

2.7 User data in email marketing

According to Sposit (2018) the moment user enters on the website it starts collecting the data of the customer even before the page is not finished with loading. Individual user's data collects via search history, preference and demographics and analyzed in order to display relevant and efficient advertisement to the user. Company use user's website activity, purchase activity and activities from third party application to understand how your user are connecting with your brand. There are other ways where company targets to collect user data such as free offers, sweepstakes, contests, and point schemes can deliver detailed information on particular user like name, address, e-mail address, cell phone number, and etc. In all this process company is collecting the data constantly and storing at their online server to analyze and target users for the advertisement (Montgomery, Chester, Grier, & Dorfman, 2012).

User data is used in email marketing to give user more personalize experience in the newsletter. Data allows marketers to use advanced forms of email marketing and help to develop email marketing strategies base on automation, personalisation and segmentation. It helps marketers to improve the conversion rate. This user data is based on demographics, geography, market, user preference, transactional and behavioural. Company collects this data via different ways, such as when user signup for email newsletter, website visit and during the purchase etc. Company use this data in the email marketing automation campaign which is based on segmentation and personalisation. Data base on user preferences are important in targeting user via automation email marketing campaign. It can be collected via preference management center when user sign up for newsletter or marketing email. Company collects user preference by asking, how often user wants to receive an email or what type of content user would like to receive in the newsletter (Miranda, 2019).

2.8 Email marketing automation

Marketing automation is defined as an automating the various repetitive tasks with the help of technology that are undertaken on a regular basis in a marketing campaign. It is a software tool but also tactics that allow companies to automate marketing operations by using data and technology as a strategic initiative within companies (Mero, Tarkiainen & Tobon, 2020). Marketing automation is used in email marketing strategies, aim to fulfill its primary objectives, to build customer loyalty, trust and brand awareness (Mullen & Daniels, 2009). The marketing automation tool enables emails to be triggered on specific times (Heimbach, Kostyrs & Hinz, 2015) and allows marketers to tracking of email via tracking codes (Baggott, 2007). The use of tracking codes in email to track the behavior of user interested in a service and product. It can record which link user clicked on in email and multiple link analysis can track buyer behavior (Baggot, 2007; Mullen & Daniels, 2009).

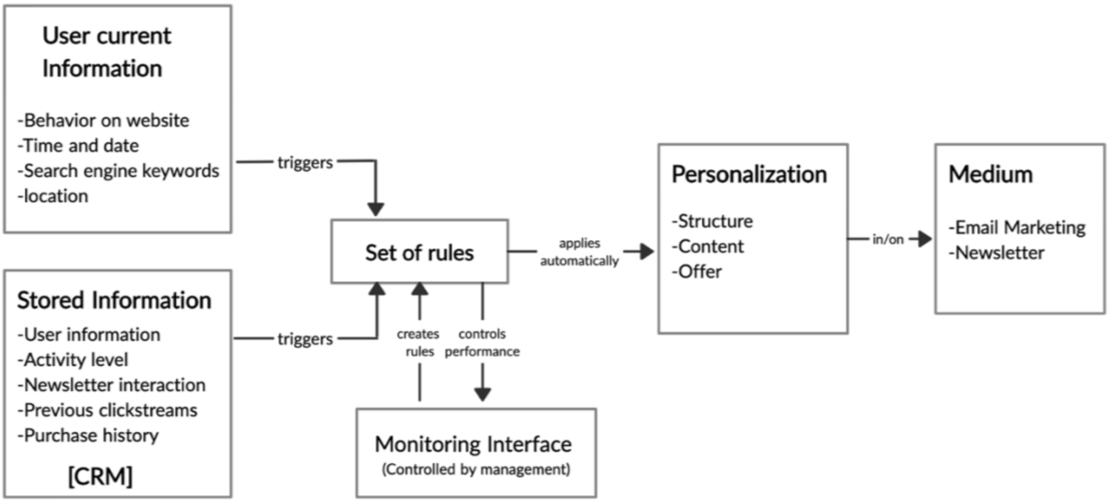


Figure 4: General framework of email marketing automation (Heimbach, Kostyra & Hinz, 2015).

The marketing automation helps to improve the efficacy and effectiveness of marketing operation via automated, analytics data driven and personalized activities with the help of CRM software (Mero, Tarkiainen & Tobon, 2020). The CRM is an application that is used for the company to organize all the data of their customers. The main purpose of CRM is to organize, track and manage all the information of customers, their activities and conversations (Todor, 2016). The effective of email marketing automation receive the data from a separate or integrated CRM to understand customer preferences and impact (Buttle & Maklan 2015; Iriana & Buttle, 2007). The CRM allow company to manage and analyze the interaction with past, current and potential customers (Todor, 2016; Bardicchia, 2020). Which helps company to improve business relationship with customer focusing customer retention and driving sales growth (Bain, 2018; Todor, 2016). The general framework for email marketing automation is shown in the Figure 4 which describe the process how automation works in email marketing.

Chapter 3 The General Data Protection Regulation

3.1 Introduction of the GDPR

The European Union (EU) regulation 2016/679, mostly known as the General Data Protection Regulation (GDPR) is the most robust privacy and security law in the world (Schweigert & Geyer-Schulz, 2019; Wolford, 2020). The GDPR was introduced by the European Parliament, in collaboration with the Council of the European Union, in May 2016 (Sposit, 2018; European Parliament, 2016). The regulation became into full force, embedded in national law from May 25, 2018, to all over the European Union. The regulation brings remarkable changes to the privacy landscape to the organizations and consumers in obtaining, processing and retaining private data (Houben, 2018). The main objectives of the GDPR are to establish data rules for the collection, analysis, storage and sharing user data (Wolford, 2020; Sposit,2018).

One of the important aspects of the GDPR is that it is applied to all the companies regardless of wherever they are located. If any company uses any personal data of EU residents, it falls under GDPR law (de Hert & Czerniawski, 2016). It is possible that the processing of user data can take place outside of the EU; still, the data controller or the data processor will fall under the authority of the GDPR (Gilbert, 2016). The GDPR secures the collection, processing and use of private data of EU residents and also customers of EU based organizations or firms with EU offices. It increases the trust in the use of 'information services by EU user at the same time protecting their fundamental rights' and user privacy (Sposit, 2018).

If the company does not comply with the GDPR law, the company can receive a heavy fine from the national security agency in the EU. This fine can be up to 20 million euros, or 4 percent of the organization’s total global turnover of the preceding fiscal year, whichever is higher (GDPR-Info, 2020; ICO, 2018; Ekman & Billgren, 2017). It is also possible for companies to receive a smaller fine of 2% of the annual global turnover. There can be different reasons such as not having the records in order or if the company does not inform authority and the affected user about a data breach. The rule is applicable for data controllers as well as data processor (Gilbert, 2016). Therefore, fines can be applied for any ESP tool or third-party company who process data on behalf of the company.

The company is recommended to have a data protection officer (DPO) for keeping track of the documentation and processes. If the company is a public authority, then the DPO is a mandatory role. DPO is responsible for supervising a data protection strategy and its implementation to ensure GDPR compliance. The DPO can help the company to understand the email marketing process and reduce the risk of fines (Tankard, 2016).

In the event of any data breaches of personal data of the user, the data controller must inform to the appropriate supervisory authority without undue delay, no later than 72 hours after the incident. Suppose the breach is likely to impact the high risk of adversely affecting individuals' rights and freedom. In that case, the company must inform the individuals without any delay (ICO, 2018). The data processor is also equally responsible for notifying the data controller without any delay after becoming aware of a personal data breach (Ekman & Billgren, 2017).

3.2 Principles of GDPR

There are seven principles defined under GDPR in order to process personal data of a user in the EU as shown in Table 3. These principles are based on Article 5 in GDPR (GDPR-Info, 2016; ICO, 2018). The data can be rereferred as user consent in email marketing activities. Therefore, these principles must be fulfilled in terms of processing of user consent in email marketing activities to comply with GDPR. The principles of the GDPR law are written down in different articles, see Appendix 2.

No	Principle name	Description of principle
1	Lawfulness, fairness and transparency	Companies must process personal data lawfully, fairly and in a transparent manner.
2	Purpose limitation	Companies should collect the data for a specified, explicit and legitimate purpose. The purpose should be clearly communicated with a user
3	Data minimization	Companies can store and process personal data. But company need to adequate, relevant and limited to what is mandatory in relation to the purpose.
4	Accuracy	User personal data must be accurate and up to date. The Company must make sure that they don’t retain old and

		outdated data. If a correction is requested by a user, action should be taken immediately in order to correct it.
5	Storage limitation	Companies must erase personal data of the user when it is no longer required to fulfil its original purpose.
6	Integrity and confidentiality (Security)	The principle of integrity and confidentiality requires the company to handle personal data with an adequate level of security. This includes “protection against unauthorized or unlawful processing and against accidental loss, damage and using appropriate technical security”. Encryption of the data should be considered the cornerstone of data security.
7	Accountability	The controller will be responsible for accountability of the data and to demonstrate GDPR compliance. The Controller can be an organization who process user data.

Table 3: Seven principles of GDPR (ICO, 2018; GDPR-Info, 2016).

3.3 Consent

Email marketing and newsletters are an essential part of online marketing. It is prohibited to process the data unless there is permission given by a user. This permission also applies to personal data, which is used for sending emails (GDPR-Info, 2016). The user's consent is required to do email marketing. Consent is an integral part of the GDPR (Gilbert, 2016). "The consent under the GDPR needs to be both informed and explicit" (Activecampaign, 2020; ICO, 2018). The GDPR emphasizes the significance of consent when transferring personal data. In terms of acquiring consent for data processing, GDPR requires an organization to proactively give a direct, compact and straightforward to understand explanation in terms of how acquired consent is being used (GDPR-Info, 2016).

The UK's independent privacy authority summaries implications for obtaining consent for data collection and processing built on GDPR articles 12, 13 and 14 (ICO, 2018). The information about handling user consent, "has to be concise, transparent, intelligible and easily accessible”; “written in clear and simple language, particularly if addressed to a child”; “free of charge" (Houben, 2018). Furthermore, two articles are allocated to this subject matter. First is Art.4(11) and second is Art.7.3 (Vollmer, 2020; GDPR-Info, 2020; Wolford, 2020). The main goal of this law in terms of obtaining consent for data processing is to allow a user to make careful decisions to what extent their private data may be used. In general, Wolford (2020), editor in chief of GDPReu defines consent conditions as shown in table 4.

No	Description
1	Consent must be freely given
2	Consent must be specific
3	Consent must be informed
4	Consent must be unambiguous
5	Consent can be revoked

Table 4: Consent condition (Wolford, 2020).

3.4 Data controller

The data controller is an essential aspect in email marketing because it involves user's name and email address. A data controller can define as "a natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data." (ICO, 2018; GDPR-Info, 2018). This entity has many responsibilities in GDPR when it comes to protecting user privacy and rights (Lynskey, 2015). Therefore, in the case of email marketing if the company decides, why and how user consent should be processed then the company is a data controller. The data controller is largely responsible for maintaining the GDPR compliance in a transparent, lawful and fair manner with their user (Ekman & Billgren, 2017).

3.5 Data processor

According to ICO, (2018), a data processor is defined as "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller" (GDPR-Info, 2018). The processor does not have any specific motive with the user data; they are asked to manage on behalf of the data controller (Eldred, Adams & Good, 2016). There must be an explicit contract agreement established between the data controller and processor in terms of processing data of the user. If the data processor hires another processor, then it must be mentioned in the contract (Koščík, 2017). In general, the data processor must be following the same rules as a data controller for GDPR compliance (Koščík, 2017). Data processor in terms of email marketing can be a third-party company or any ESP tool who processes user data on behalf of the company in email marketing activities. The privacy policy of the data controller must be reflected with the data processor's privacy policy (ICO, 2018; GDPR-Info, 2018).

3.6 Lawful bases for processing personal data

According to Article 6.1 of the GDPR defines six conditions under which companies can process personal data of the user as shown below (ICO, 2018; Irwin, 2020; GDPR-Info, 2020)**.**

1. Consent: The individual user has given clear consent for company to process their personal data for a specific purpose.
2. Contract: The processing is necessary for a contract that company have with a user, or to take specific steps before entering into a contract.
3. Legal obligation: The processing is necessary for company to comply with the law.
4. Vital interests: The processing is necessary to protect someone's life.
5. Public task: The processing is necessary for company to perform a task carried out in the public interest or in the exercise of official authority vested in the controller.
6. Legitimate interests: The processing is necessary for legitimate interests of company or third party, except where such interests are overridden by the interests, rights of freedoms of the user. (This cannot apply if you are a public authority processing data to perform your official tasks).

If company is not sure about processing user data on lawful basis, they can use 'interactive guidance tool' suggest by ICO to find out legal way of processing the data.

3.7 Legitimate interest

Legitimate interest is the most flexible of the GDPR lawful bases to process personal data of user, theoretically applying whenever a company uses personal data in a way that user would expect. This may implicit benefit inherent in processing user data for the company itself. Interests can refer to anything, including a company or third party's commercial interests (Irwin, 2020; ICO, 2018). The GDPR does not list all circumstances in which legitimate interests may apply. The legitimate interests must be thoroughly justified by the company in their documentation. Unlike the other lawful of GDPR bases, legitimate interest is not obvious how the condition applies unless company can justify reasoning to user.

The data subjects (users) can object to process their personal data if the reason is not justified by the company (Article 21). This can be done via data subject access request (DSAR), which gives users a full record of the data that company hold on them and the purpose for collecting it. If user disagree with company's justification for legitimate interest then company has to prove it legally otherwise (Irwin, 2020; ICO,2018). Company can use consent to defend themselves legally in such situations. Users have the right to withdraw the consent and right to erasure if the reason given under legitimate interest is not justified.

3.7.1 Legitimate interest for marketing purpose

Marketing under legitimate interest depends on the circumstances. According to Recital 47 "The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest". This means that direct marketing "may" be a legitimate interest, here may is the operative word and not clearly defined in the GDPR Recital 47. However, the GDPR doesn't mention that direct marketing always be a part of a legitimate interest. Hence if the company processing consent is lawful on the basis of legitimate interests that totally depends on the particular situations. (ICO, 2018; Irwin, 2020; GDPR-Info, 2020).

The GDPR does not list all the situations in which legitimate interests may apply for companies. However, company can do the three-part tests which can help in determining the legitimate interests for data collection and use in the situation where consent is not preferred or viable. These three tests are, purpose test; necessity test; balancing test (ICO, 2018; Irwin, 2020). However, if company have already obtained consent in the compliance with the GDPR, then trying to apply legitimate interests test will not be necessary (ICO, 2018).

1. Purpose: This can help company to decide whether the processing data can be considered a legitimate interest. As long as the marketing is carried out in compliance with GDPR and directly relevant to the user's needs then in most cases it is likely that direct marketing is a legitimate interest. However, company still need to show that they pass the necessity and balancing tests (ICO, 2018; Irwin, 2020; GDPR-Info, 2020; Davis, 2017).
2. Necessity: Company need to be more specific about their purposes in order to show that it is necessary and weigh the benefits in the balancing test. The marketing should be in the interest of individuals. For example, if company use profiling to target their marketing (ICO, 2018; Irwin, 2020; GDPR-Info, 2020; Davis, 2017).

3. Balancing: The final part of the test, which can help company to decide whether the user's interest override the legitimate interest. For example, if user receive money-off products or offers via marketing email that are directly relevant to user needs (ICO, 2018; Irwin, 2020; GDPR-Info, 2020; Davis, 2017).

However above example can have significant negative effect on user depending on their personal situation. If user is known to be in financial difficulties who is regularly targeting with email marketing, then in that case it is not relevant to user needs. If company intend to process personal data of user for the purpose of direct marketing via email, then legitimate interests may not always be a suitable basis for processing unless company can prove that data is correlative and fair to the user (ICO, 2018).

3.8 GDPR impact on email marketing

The GDPR has impacted all kind of marketing activities in Europe. One of the most significant marketing channels is impacted, that is email marketing under GDPR. Digital marketers need to consider the GDPR requirement in their email marketing activities to be legally compliant. It is not necessary only in terms of getting penalties but also the reputation of a company suffers. The GDPR offers the chance to companies to rethink email marketing activities and build trust with their customers.

Email marketing has been easy to implement before GDPR, but it requires proper process after the introduction of GDPR in 2016 (Uzialko, 2020; Firstcms, n.d.). The GDPR requires adjusting email marketing strategy to comply with GDPR. Marketers need to change the way for collecting consent in how they seek, acquire and store consent. According to the GDPR provisions, the user has the right to consent to the collection of data, the right to understand why and how that data is used and the right to request for the deletion of the data under certain circumstances (Uzialko, 2020).

From the literature, we have found out majorly three specific areas that have been impacted by data collection point of view, as shown in table 5. That is data permission; data access; data focus (Menon, 2019; Schweigert & Geyer-Schulz, 2019; Drokina, 2018; Lamb, 2019; Cauchi, 2019; MacDonald, 2020; Gregorio, 2019).

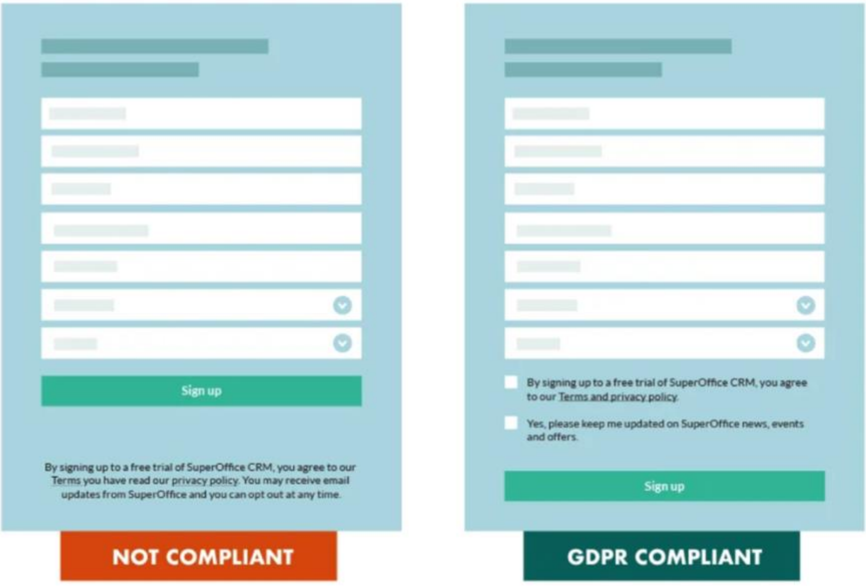
Data Permission	Data Access	Data Focus
Users need to physically confirm that they want to be connected via email opt-ins. Company requires permission from user before they send any promotional email.	Company's responsibility to ensure that your user can access their data easily and remove their consent when they wish to.	Company needs to focus on the data that they require from customer and stop asking for the "nice to have".

Table 5: Impacted areas in email marketing (Schweigert & Geyer-Schulz, 2019).

These three main areas of the GDPR allow an impetus to adopt a permission email marketing strategy to comply with GDPR standards. In the next paragraph, we discuss these three areas more in details.

First, 'Data permission' which explains that the company should request permission from the user before they send any sort of promotional material via email. The user who requests to receive any newsletter from the company that leads customers, partners need to confirm that they want to be contacted physically (Drokina, 2018; Menon, 2019; Schweigert & Geyer-Schulz, 2019). Therefore, no marketing communications are to be sent out without the user's permission to their email address (Drokina, 2018; Menon, 2019). Company should be transparent in their efforts and communicate in plain language about the details in order for them to give an "informed, unambiguous, specific and revocable" consent. User should be given control to make a choice and provide permission to be contacted or communicated via newsletter by the company (Menon, 2019; Macdonald, 2020). The research of Drokina, (2018) is in line with this; email addresses are the lifeblood of the campaigns targeting, and buying lists is strictly forbidden. Research shows that the company must ensure users opt-in for email marketing activities. Under the GDPR law, obtaining the consent became a requirement for digital marketers.

Macdonald, (2020) has given an example which shows the data permission impact before and after GDPR compliance as shown in Figure 5 and Figure 6. He has mentioned that instead of assuming that user who fills out the webform would like to receive marketing emails from the company, but now ask visitors to opt-in to newsletters by checking the box while signing up as shown in GDPR compliant Figure 5 and Figure 6. It can have a direct impact in an email marketing campaign if the user decides to opt-out from receiving any promotional contents from the company. It raises questions for the companies, how they can target those users for marketing activities who have not subscribed to checkbox of receiving a promotional email.



Sign up

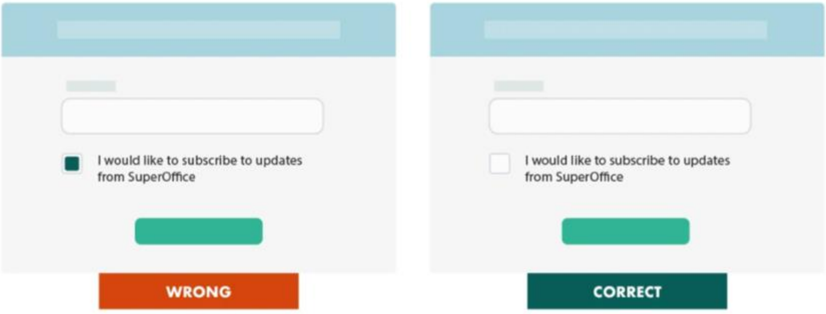
By signing up to a free trial of SuperOffice CRM, you agree to our Terms you have read our privacy policy. You may receive email updates from SuperOffice and you can opt out at any time.

□ By signing up to a free trial of SuperOffice CRM, you agree to our Terms and privacy policy.

□ Yes, please keep me updated on SuperOffice news, events and offers.

Sign up

Figure 5: Comparison of GDPR compliant and not compliant form (Macdonald, 2020).

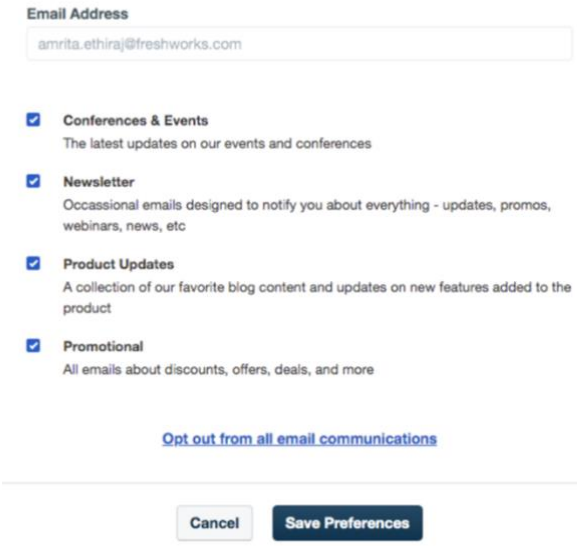


☑ I would like to subscribe to updates from SuperOffice

□ I would like to subscribe to updates from SuperOffice

Figure 6: Comparison of GDPR compliant and not compliant in newsletter (Macdonald, 2020).

The second impacted area in email marketing is data access. This area appears in “right to be forgotten” under GDPR article 17 (Wolford, 2020). An individual user has the right to have their data deleted if personal data is no longer needed for the purpose company originally collected or processed. User has full control over their personal data if the company is processing personal data for email marketing purpose (Drokina, 2018; Menon, 2019; Schweigert & Geyer-Schulz, 2019). According to Macdonald, (2020) data access offers users a method to gain more control over how their data is collected and used, including the facility to access or delete it. Digital marketers must ensure that the user can easily access their data and remove his/her consent for its use. It can be included by unsubscribe link within email marketing template and in the profile of the user. The unsubscribe link should allow users to manage their consent for email preferences, as shown in Figure 7.



Email Address

amrita.ethiraj@freshworks.com

☑ **Conferences & Events**
The latest updates on our events and conferences

☑ **Newsletter**
Occassional emails designed to notify you about everything - updates, promos, webinars, news, etc

☑ **Product Updates**
A collection of our favorite blog content and updates on new features added to the product

☑ **Promotional**
All emails about discounts, offers, deals, and more

Opt out from all email communications

Figure 7: Subscription management center.

However, data accessed is discussed positively in permission marketing by Schweigert & Geyer-Schulz, (2019), which explains that permission marketing maintains that opt-outs are an additional opportunity to show respect to the users which helps in making a good relationship with them. Email marketing campaign can be only successful if customer also asking for it, if they are not interested in receiving newsletter then it won't give any potential benefits to the company if user still receive it.

Lastly, in terms of the data focus is discussed, digital marketers have to focus on the information they require and avoid collecting any extra data to use in email marketing activities. The company cannot ask irrelevant data which they can use for developing email marketing strategies or targeting email campaign. For example, clothing company do not need to know customer's favourite food or movie before he/she subscribe for newsletter. GDPR requires a company to legally prove the processing of the user personal data information while collecting user consent (MacDonald, 2020). Data focus can have a substantial impact on tracking and analytics. If digital marketers require to add particular parameters to track the user to target email marketing campaign, marketers have to use another way of collecting information (Schweigert & Geyer-Schulz, 2019). Company is required to have more data focus while collecting consent and make their purpose very clear with the customers; otherwise, the company might end up paying huge amounts of fines.

Chapter 4 Qualitative Research Methodology

This chapter includes the research methodology of the thesis. It explains how this research was conducted in term of collecting the required data such as the process for performing a literature review, the type of interview and participants. It also explains the detail of how we have analyzed to generate findings of this research. In this part, we outline the research design, research approach, research philosophy, literature review, data collection, sample selection and data analysis.

4.1 Research design

The design used in this research is an explorative study. The exploratory approach is carried out to study a problem which has not been researched before and to enable a researcher to answer the research questions. There is absence of relevant information about the topic from past research. Therefore, we will focus in collecting available information via different materials, as a result this research study is flexible and scattered. Explorative research is conducted to have a better understanding of the current problem, but will not provide a conclusive result (Bhat, 2018; Curtis, 2019). This research study starts with a general idea and the final outcomes of the research are used to answer to the research question. This research study can be the foundation for other researcher to identify compliance issues in email marketing under GDPR. Further, researcher can use this study to develop future research.

In order to get a detailed understanding of the research topic and answer each research question, two methods are used, following the literature review and qualitative research through in-depth interviews. In this study literature review is used as a partial base for the interview questions. Interviews are useful for filling the literature gap. It gives the opinions from digital marketers about residual risks, best practices and digital technology in email marketing. The information from the interviews and literature will give the answers to the research questions.

Below table is explaining the approach that will be taken to answer research questions.

Research Question	Data	Approach
SQ1: What are the residual risks company can be exposed to email	Research papers, articles, blogs, government website information,	Literature review, grey literature, digital marketer interviews (6), DPO(1)

marketing activities to comply with GDPR standards?	recorded audio, interviews, transcript, qualitative analysis	
SQ2: What are the proactive best practices that should be followed in email marketing activities to preempt any residual GDPR risks?	Research papers, articles, company's blogs, websites, recorded audio, interviews, transcripts, qualitative analysis	Literature review, grey literature, digital marketer interviews (6), DPO(1)
SQ3: Is there any digital technology that can help companies with GDPR compliance for email marketing activities?	Research papers, articles, blogs, website information, recorded audio interviews, transcript, qualitative analysis	Literature review, grey literature, digital marketer interviews (6) DPO(1)
RQ: Have companies sufficiently adapted their email marketing activities to the GDPR privacy directive?	Research paper, article, blogs, website information, Qualitative analysis	Conclusion based on SQ1-2-3

Table 6: Research approach.

Table 6 explains how the research carried out. The research questions are described in the first column. Column two describes how the data from various sources are analyzed to answer the (sub) research question. The last column shows which source of information are used in this study.

4.2 Research approach

The outcome of this study is developed via an inductive approach. An inductive approach is used for the analysis of qualitative evaluation data. The general inductive approach gives an easily used and systematic set of procedures for analyzing qualitative data which can produce reliable and valid findings. It gives a simple, straightforward approach for acquiring findings in the context of focused evaluation questions (Thomas, 2006). The reason for using an inductive approach is to generate raw textual data into a summary. It establishes clear links between research objectives and the summary findings obtained from the literature and interviews. The framework is built for residual risks and best practices from summary findings in Chapter 8.

4.3 Research philosophy

In this research, the research philosophy interpretivism is used. Interpretivism emphasises that reality is subjective and changing; there is no one ultimate truth. The knowledge is subjective, and there is much diverse interpretation of reality. There is not any single way or correct way of knowing (Bunniss & Kelly, 2010; Ryan, 2018). The motivation for choosing this philosophy is that small samples of in-depth investigations are used. The method derives from the experience of different people, who were involved in email marketing before GDPR and after GDPR implementation. Each participant has experienced the transformation of email marketing under GDPR. However, the range of the data collected in the interviews can be interpreted in many ways. Hence interpretivism lends itself well to studies which have a lot of grey areas in this research.

4.4 Literature review

The literature review gives information about the research topic and helps partially to answer the research question of this study. We identified that limited research has been done on the topic after the introduction of the GDPR in 2016. Because of limited information on the topic, we used mostly grey literature in this study to find information on the research topic. Following Adams et al. (2017), the gray literature is classified on the basis of different levels as shown in the Figure 8. The levels range from 1 to 3, which indicate the extent to which information is reliable.

A partially systematic literature method is used to find out current research information. The literature review is the first step to gain a thorough understanding of the topic. The objective of the literature review gives an insight into four topics: GDPR impact on email marketing, residual risk in email marketing, best practices in email marketing and digital technology in email marketing. The literature review partly answers sub-questions. The missing information from the literature review allows the development of a set of interview questions in order to discover missing information.

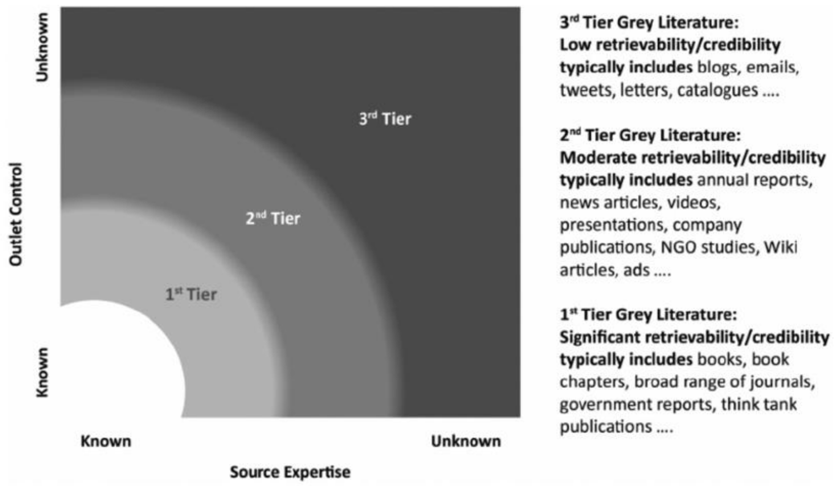

Unknown
Outlet Control
Known
3rd Tier
2nd Tier
1st Tier
Known
Unknown
Source Expertise
3rd Tier Grey Literature:
Low retrievability/credibility
typically includes blogs, emails, tweets, letters, catalogues ....
2nd Tier Grey Literature:
Moderate retrievability/credibility
typically includes annual reports, news articles, videos, presentations, company publications, NGO studies, Wiki articles, ads ....
1st Tier Grey Literature:
Significant retrievability/credibility
typically includes books, book chapters, broad range of journals, government reports, think tank publications ....

Figure 8: Shades of grey literature (Adams, Smart & Huff, 2017).

4.5 Data collection method

Data is collected via semi-structured interviews through questions in-depth. Semi-structured interviews are conducted to ensure critical questions to be answered. There is a chance to get detailed information from respondents. By making the semi-structured interview, it is important to have a few interview topics and key questions. However, it is also possible to get a detailed response by allowing the interviewee to explore other ideas. The semi-structured interview structure also gives freedom for key findings that were not thought of before the interviews. In order to draw conclusions, a sufficient number of samples will be needed, the overall length of the interview will be 30-40 mins maximum, since the experts would not like to spend a lot of time for interviews.

The semi-structured interview in this study is based on three topics: residual risks, best-practices and digital technology. These topics arose from the sub-research questions. The interview questions were determined based on the literature. Each interview has a fixed number of questions, see Table 18 for this. A number of interview questions have been created to check the information from the literature with the respondents in the interview process. Apart from that other questions have been formulated to obtain new information and insights from the respondents.

4.6 Sample selection

For this study, multiple strategies are used to obtain the sample. This study uses a non-probability sampling method. The method which is used is purposive sampling. This method is used when the sample is selected based on the judgment of the researcher. It is one of the most cost-effective and time-effective sampling methods (Etikan, Musa & Alkassim, 2016). In this study, another form of sampling that has been used is snowball sampling. Snowball sampling asks whether the interviewee can give others as suggestions for the study, which makes use of the interviewee's professional network. People from different companies were deliberately chosen for a sufficiently diverse sample.

4.7 Data analysis

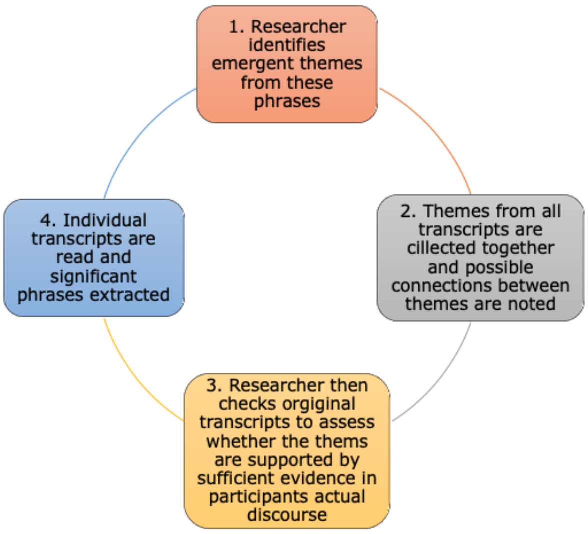

1. Researcher identifies emergent themes from these phrases
2. Themes from all transcripts are cillected together and possible connections between themes are noted
3. Researcher then checks orgiginal transcripts to assess whether the thems are supported by sufficient evidence in participants actual discourse
4. Individual transcripts are read and significant phrases extracted

Figure 9: Process of phenomenological analysis (Lewis, Lloyd & Farrell, 2013).

In this study, the phenomenological method was used for the analysis, as shown in Figure 9. It is used to generate a textual description of the experiences of the participants. It adds the structural description of their experiences and a combination of the textural and structural descriptions, which convey an overall essence of the experience (Creswell, 2007). Phenomenology is a technique to qualitative research that focuses on the commonality of a lived experience within a particular group. The essential goal of the approach is to arrive at a description of the nature of the specific phenomenon (Creswell, 2013).

The interviews of different participants are recorded. It is possible to filter relevant information from the interviews. The respondent's answers analyze the data through the interview questions. The answers to the interview questions are written out in notes for each respondent. After the analysis, information from the interviews was combined and set out in tables in Chapter 7 findings section. Via these tables, the answers to the different respondents are compared with the existing literature. This way of analyzing helps to find apparent similarities between the answers of the respondents. Given the exploratory nature of this study, the new information is discovered through analysis from the notes of each respondent. In the Chapter 7 factor model is introduced for residual risks connecting with best practices from the analysis of this study.

Chapter 5 Literature on E-mail Marketing under the GDPR

This chapter focuses on the findings from previous research and the information available on the internet in the area of email marketing with GDPR. Therefore, we have used systematic and grey literature review in order to find the information related to research questions. Three literature streams are covered in this section, which are residual risk in email marketing under GDPR, best practices in email marketing under GDPR and digital technology development in GDPR supporting email marketing activities. Residual risks in email marketing helps researcher to understand the blind spots in email marketing under GDPR and develop further the best available practices for residual risks.

5.1 Residual risk in email marketing under the GDPR

Table 7 on page number provides an overview of the literature selected in this study to cover the residual risks in email marketing under GDPR standard. Most of the literature used in this study is gray literature as GDPR became recently effective from May, 2018. There is not much research information available on the area of residual risk. The selected grey literature was published from 2018 to 2020, which shows that information is fresh and relevant to the topic.

This literature is numbered from L1 to L12 in the first column and literature L13 is a research article as shown separately in the Table 7. The source of the literature is listed in the second column. Subsequently, in the third column, the literature one to 12 are divided into a different tier for grey literature and literature 13 research article belongs to the academic category. The gray literature is divided into first and second tiers and different tiers reflect the reliability of the literature. The last column focused on the source of the grey literature. Which shows that most literature comes from national security agency handled by the government and companies' publications and articles. The gray literature has a reasonable reliability in all cases, as these are divided mainly into the first and second tiers.

Literature no.	Citation	Tiers	Tier explanation
L1	(Wolford, 2020)	1st	Government reports
L2	(Enforcementtracker, 2020)	1st	Government reports
L3	(Heckh & González, 2019)	1st	Government reports
L4	(ICO, 2018)	1st	Government reports
L5	(Robinson, 2018)	2nd	Company's publications
L6	(Uzialko, 2020)	2nd	News article

L7	(Lahav, 2018)	2nd	Company's publications
L8	(Macdonald, 2020)	2nd	Company's article
L9	(Green,2020)	2nd	Company's publications
L10	(Gourlay,2018)	2nd	News article
L11	(Tozer, 2018)	2nd	News article
L12	(BBC, 2018)	2nd	News article
L13	(GDPR Associates, 2018)	2nd	Company's article
Literature no.	**Citation**	**Category**	**Type**
L14	(Drokina,2018)	Academic	Research article

Table 7: Summary of selected literature for risks.

Table 8 shows the summary of GDPR residual risks associated with using email marketing identified after reading the various literature by different authors in Table 8. The risks are numbered in the first column from R1 to R8. Then, in the second column, a short description about residual risks of email marketing under GDPR is described. In the third column, GDPR infringed article associated with each risk is mentioned.

Risks no	Residual risk description	GDPR infringed art.
R1	To send unsolicited direct marketing email even after user has opted out for consent	Article .6.1. a GDPR, typified in art. 83.5 a) GDPR
R2	To send an email to user for asking whether he/she wants to receive a promotional email, without the right consent	Article.6.1. a GDPR, typified in art. 83.5 a) GDPR
R3	To send a marketing email to children under 13 without a consent from their parent	Article. 8 GDPR
R4	Marketing automation system sends out an email on behalf of the CRM system despite user has opted out, because CRM system is not updated	Article. 22 GDPR
R5	To send a marketing email to a large number of recipients (users) without using the blind copy feature	Article. 32 GDPR
R6	To send a personal data over email without implementing adequate level of information security	Article. 32 GDPR
R7	Hacker targets and reveal email address of the users	Article. 32 GDPR
R8	To send an email to EU resident from the company located outside EU or vice versa	Article. 3(2)

Table 8: Summary of residual risks.

Table 9 is a matrix in which per source is written about certain risks in the use of email marketing. The X-axis shows the risks as numbered earlier from Table 8. The y-axis contains the literature as numbered from table 7. The table shows that not every source describes all risks. The overview shows that the most common risks found in the literature are R1 (9), R2 (7) and R6 (8). The less frequent risks are R3 (2), R4 (3), R5 (3), and R8 (3).

Literature(y) /Risks(x)	R1	R2	R3	R4	R5	R6	R7	R8
L1			x			x	x	
L2	x				x	x	x	
L3	x	x			x	x	x	
L4	x		x			x		
L5				x		x		x
L6	x	x						x
L7				x		x		
L8	x	x		x		x		x
L9					x	x	x	
L10	x	x						
L11	x	x						
L12	x	x						
L13	x	x		x				
L14	x	x		x				

Table 9: Literature comparison with residual risks.

Between 2018 and 2020, the list of fines and penalties from data protection authorities within EU have given to the companies in EU for breaking the GDPR in email marketing activities as shown in the Appendix 3. Below, we will discuss incidents, reported in the literature, where these risks have actually occurred. These residual risks occurred in companies across Europe between 2018 to 2020. These risks are connected with R1, R2, R5, R6 & R7 shown in Table 8 which are based on real incidents occurred in the companies across the Europe. These companies have been fined by the security agency of EU for breaking the GDPR law for their email marketing activities. Residual risks R3, R4 and R8 were mentioned by authors in literature, however we have not found any real incidents based on these risks.

5.1.1 Consent risk

Under data protection act, three companies namely Flybe, Honda Motors Europe and Morrisons have been fined for sending a marketing email to their customers even though these customers had been opted out of consent (Tozer, 2018; Gourlay, 2018). There are two reasons explain this incident. First, the regulator mentioned that company should have obtained customer’s consent before sending the emails. Second, sending emails to determine whether customer want to receive marketing email, without the right user consent, is still considered marketing under the GDPR mentioned by the head of enforcement at the ICO (MacDonald, 2020; Drokina, 2018; BBC, 2018).

These three cases do not seem to be isolated. After the GDPR became effective in 2018 there have been other incidents that were reported by different data protection agency of EU, which are associated with residual risk R1 and R2. Heckh and Gonzales (2019) have mentioned various other cases reported by the AEPD (Spanish Data Protection Agency) where there is a violation of the GDPR law. There is an incident in 2018 from the company called AnimaNaturalis, which is a nonprofit animal rights organization. This company was warned by the AEPD because of company used the complainant's email address to send her newsletters even she has already opted out the consent and company already confirmed the un-subscription for the user. In all these incidents related to residual risk R1 and R2, Art.6.1.a) GDPR, typified in art. 83.5 a) GDPR were violated for breaking the law. Similarly, there have been two incidents reported by ICO in February 2019. The company name called Leave.EU group limited have been fined £45,000 for sending unsolicited direct marketing emails without the required consent and £15,000 for sending almost 300,000 unsolicited communication on a single day for all the users for which they did not have any consent (ICO, 2018).

However, we have not come across any reason for the occurrence of all these incidents, it was unknown and none of the company have officially given any statement on the incident to explain why the incident took place. Researcher clearly find the literature gap here for the occurrence of all these incidents and will try to find the information from the expert in the interviewes. It can be also seen in Table 9 that R1 and R2 risks are most common residual risks which were discussed by authors after the GDPR became effective from May, 2018 through different real incidents in the grey literature.

The GDPR states explicitly that certain protection is required where children's personal data is used for marketing purposes. So, companies require to lawful basis for processing a child's consent who is under the age of 13 years. The children have the same rights as adults for their personal data under the GDPR law. These right covers the right to access their personal data; request for correction; object to processing and rights to erase their data. The company shall make reasonable effort to verify child's consent is authorized or given by the parents or whoever holds parental responsibility for the child, taking into consideration available technology. This risk is associated to residual risk R3, where sending a marketing email to the children under 13 without a consent from their parent is violating of the GDPR law.

5.1.2 Automation risk

Marketing automation is extremely powerful tool in email marketing. But automation can give real trouble to the companies if the process is not set up correctly. Companies need to make sure that every name in the CRM database and email in the automation system must have given the permission to send marketing email. If any of user has opted out of the automated email sequence, then both the systems should be updated to ensure that no further marketing emails are sent to the user (Macdonald, 2020; Robinson, 2018). This is also applicable in the case of marketing emails which have been already scheduled by the marketing team. This residual risk is associated with R4 as shown in Table 8.

5.1.3 Security risk

According to consumer privacy study by TRUST/NCSA found that 92 % of online customers showed concern for the data privacy and security (Trustarc, 2020). Customer's security and safety should be the important priority when company send out any kind of email marketing campaign. It is about building trust and securing relationship with the customers. Creating a secure campaign customer will trust and respond to is the next step.

Cybersecurity has become a hot issue in marketing field under the GDPR because data breaches are happening more frequently. Companies take risk when sending out an email marketing campaign that is not secure is called business email compromise (Lawrence, 2020). There are residual risks (R5, R6 and R7) related to security which we have discovered through the same legal sources based on real incidents by the companies in the EU. In these reports are found that companies have been fined for breaking the GDPR law in their email activities because of lack of the security.

In November 2018, German web based online company called Knuddels had been fined 20,000 euros because the company's email address and passwords were revealed by the hacker. Approximately 330.000 user's email address were affected from this entire incident. Report shows that because of insufficient technical capability, organization failed to measure the information security (Enforcementtracker, 2020). Following with another incident of breach of security reported by AEPD (Spanish Data Protection Agency) in March 28, 2018. It had been found that because of defective configuration of an email account dedicated to internal management store, emails were visible on the devices which were sent from the account.

Although, company did not pay any fine but got an official warning to look into their security system (Heckh & Gonzales, 2019). All these incidents draw the attention to residual risks R7 to the author that some of the companies in the EU are still facing a problem to be compliant with GDPR for their email activities for residual risk R7.

Similarly, residual risks R6 concerns the insufficient level of security and lack of technical measures, where sending a personal data of the user over email can be considered one of the residual risks under GDPR law violating Article 32 and Article 5(f). According to Wolford (2020), email encryption is a technical measure. He has mentioned in his article that 91% of cyber-attacks begin with a phishing email and hackers attempt to gain access to a user device or account using malware or deception. We have found in our studies that there are examples where the companies who have sent personal data of their users or their clients via email but due to insufficient of technical security, organization have failed to protect the personal data of the users while transferring via email. Between 2019 to 2020 three Romanian companies violated GDPR law associated with residual risk R6 and were fined by Romanian ANSPDCP (the national supervisory authority for personal data processing). Three companies called Enel Energie, Vodafone Romania and Legal Company & Tax Hub Srl violated Art. 32 GDPR and fined 3000, 4150 and 3000 euros respectively. In all three incidents the companies have sent an email to a customer which contained the personal data of another customer. In this incident, companies clearly failed to implement an adequate level of information security while sending personal data over email channel (Enforcementtracker, 2020).

However, none of the incidents discussed for both R6 and R7 clarify from the literature information, that these companies got fines in their email marketing activities or one to one email sent to the company’s customer for any reason. We can see here that there is literature gap for the missing information. We will try to cover more information on security related risk in email marketing activities via interviews with digital marketers and data protection officer.

Another interesting residual risk was found in this study which is residual risk R5 mentioned in Table 8. Where sending a marketing email to large number of users without using the blind copy feature is considered to be residual risk and violating of Art.32 GDPR law. As it can be seen in table 10, R5 has been mentioned by three sources L2, L3 and L9. These three sources have discussed the real cases which violated GDPR law under email marketing. Between 2018 and 2019 four companies have been fined and warned for violating Art.32 GDPR. Vodafone

ONO and Shop Macoyn, S.L. have been fined 36.000 and 5.000 euros respectively and another two companies namely S.A.U., Quality Technology Solutions Alpe, S.L. and The Oliver Group Torrevieja, S.L. got a warning by AEPD (Heckh & González, 2019). In all four cases company sent a marketing email to a large number of users without making use of the blind copy mechanism, thereby enabling each recipient to see the email address of other recipients (Enforcementtracker, 2020; Heckh & Gonzales, 2019; Green, 2020).

5.1.4 Territory risk

Lastly, we have come across residual risk R8. GDPR is applicable to those companies who are located outside EU and dealing with EU resident. GDPR applicability follows the resident and not the business location. According to Article 3(2) of the "GDPR addresses the applicability of GDPR to businesses not located in the European Union (EU)" (Robinson, 2018). This can be also applicable for the EU companies to follow the privacy law of other countries. For example, privacy law of USA and Canada, such as CCPA, WPA, PIPEDA. Therefore, residual risks R8 can be occurred, if sending an email to EU resident from the company located outside EU or vice versa, if not following the privacy law of the country for processing user consent.

5.2 Best practices in email marketing under the GDPR

Apart from residual risks, we also scanned the literature for the best practices that may preempt those residual risks. Table 10 shows the summary of literature selected for best practices for this study. Some of these best practices come from the same literature which has also discussed the residual risks section 5.1. As a result, the literature numbering in this table is the same as the literature numbering in the Table 7 of risks. The citation is visible in the second column. The literature is divided into the different tiers from the gray literature. The table shows in the third column that most literature is classified in the second tier. We have considered the literature from different data protection agency of EU which direct reports to the government. Apart from that we have considered articles, publications and blogs published by the companies which actually works in the field of GDPR and marketing. The information from the literature is therefore reasonably reliable. Finally, the fourth column shows that most literature comes from companies and government organizations.

Literature no.	Citation	Tiers	Tier explanation
L4	(ICO, 2018)	1st	Government reports
L6	(Uzialko, 2020)	2nd	News article
L7	(Lahav, 2018)	2nd	Company's publications
L8	(MacDonald, 2020)	2nd	Company's article
L13	(GDPR Associates, 2018)	2nd	Company's article
L15	(Mailjet inc, 2020)	2nd	Company's article
L16	(SPECHT, 2018)	2nd	Company's article
L17	(Matthys, 2018)	2nd	Company's article
L18	(Eventbrite, 2016)	3rd	Company’s blog
L19	(NCSC, 2019)	1st	Government reports
Literature no.	**Citation**	**Category**	**Type**
L14	(Drokina,2018)	Academic	Research article

Table 10: Summary of selected literature for best practices.

Table 12 shown below contains the numbering of the best practices from P1 to P15 found in this study along with the description of best practices in second columns. There is not any sequence for best practices in the table. We have given best practice sequence randomly in the table 12. We will discuss all the best practices in the next paragraph in details.

Sr no	Best practices description
P1	Ensure user has opted in for email marketing and given consent to be contacted before sending an email Example: Audit your mailing list
P2	Ensure user has used ticked box explicitly in webform for email opt-ins and not via pre-ticked box assumption or any other method of default consent
P3	Use double opt-in in email marketing before user is being added to email list and receive email communication
P4	Use unsubscribe link within your email marketing template and check that it links with the user's profile which allow them to manage their email preference via subscription management center
P5	Check that every name in CRM database and every email in automation system has given you permission for email marketing and both are synchronized
P6	Check your existing email marketing automation flows and processes to ensure that no decisions are made without human interference
P7	Check how you collect personal data
P8	Use professional email service provider (ESP) like MailChimp and other similar ESP for blind copy recipients
P9	Use content marketing strategy by generating white papers, eBooks and guides that visitor can access and download in return to share their contact information
P10	Use a banner on your website for blog posts, product offers, product news and company news, where visitor can add themself to the mailing list which is linked with the privacy policy
P11	Don’t use an email instead provide mail functionality and notification system within portal for current users
P12	Ensure that communication policy for email marketing is not hidden within privacy statements
P13	Check that request for consent prominent and separate from terms and conditions

P14	Use S/MIME or PGP end-to-end encryption protocol for Secure/Multipurpose Internet Mail suggested by EU data protection authorities
P15	Use Secure email transport with STARTTLS and DANE suggested by Dutch National Cyber Security Center (NCSC)

Table 11: Summary of best practices.

Table 13 below is a matrix that lists the 15 best practices on the X axis and the literature on the Y axis. In the matrix, crosses indicate which best practices have been found in which source. The Table 13 shows that, P1, P2, P3, P4, P7, P12 and P13 are all found by many authors in the literature. It is plausible that these best practices are most useful for organizations. Best practices: P9, P10, P11, P14 and P15 have all been found less compare to other sources in the literature. This may indicate that these best practices are less useful in email marketing.

Literature(y) Best practices(x)	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14	P15
L4	x	x	x	x										x	x
L6	x		x	x			x	x				x	x		
L7					x	x	x								
L8	x	x		x	x	x	x		x	x		x	x		
L13	x	x	x		x	x	x		x	x		x	x		
L14															
L15	x		x	x		x						x	x		
L16	x	x		x									x		
L17											x	x		x	x
L18								x							
L19											x			x	x

Table 12: Literature comparison with best practices.

In next paragraph, we will discuss P1 to P15 best practices founded via literature study. After that we will connect each of the residual risks R1 to R8 that may preempt with possible practices mentioned in the Table 11.

5.2.1 Practices related to consent

According to data permission, it is important to know how your company manages their email opt-ins for a user who requests to receive promotional email. As per the GDPR protocol, company has to ensure that user has opted in and given consent for receiving email newsletter before sending an email to their users (Gourlay, 2018). Practice P1 tells the company to audit your mailing list frequently before running any email marketing campaign. Company needs to make sure they have actively sought permission for the consent and haven’t assumed about it (ICO, 2018; Uzialko, 2020; Macdonald, 2020; GDPR Associates, 2018; Mailjet inc, 2020; Sposit, 2018). Therefore, P2 is very important under the GDPR Recital 32 to ensure that user has used tick box explicitly in webform for email opt-ins and not via pre ticked box or default consent by the company itself (Macdonald, 2020; GDPR Associates, 2018; SPECHT, 2018; Gourlay, 2018).

Once a user provides consent, authors suggest that company needs to follow P3 for a stricter subscription process. Which involves a double opt-in and easy opt-out feature, and exclude required or involuntary opt-ins (Uzialko, 2020; GDPR Associates, 2018; Mailjet inc, 2020; Mendoza, 2019). Double opt-in is the way for the company to confirm the user email address from user itself and to verify that user is interested in receiving emails, weeding out any accidental requests or fraudulent before being added to the email list. This way it indicates to the company that user is happy to receive marketing communication from your company through email. It is a safety net to ensure compliance with respect to consent under GDPR (Mailjet inc, 2020).

According to Art.13 part 2, company can legally send user marketing email about the service they offer to you as long as company inform you that user can opt-out at any time and given an option to unsubscribe in every communication email (Wolford, 2020). Furthermore, Article7(3) states that unsubscribe process under GDPR should be clear and simple and the users should have the right to withdraw his or her consent at any time. It is important to ensure by the company that it doesn’t require any other information than an email address, require user to log in and ask user to visit more than one page to submit the request (Specht, 2018). Hence, company to follow P4 is good practice where each email communication contains unsubscribe link and allow user to access their email preference via subscription management center (Mailjet inc, 2020; ICO, 2018; Uzialko, 2020; Specht, 2018). Handling opt-outs and subscription management centers are particularly relevant to ‘right to be forgotten’ for email marketers (Macdonald, 2020). If a marketing email does not have the option to unsubscribe and sent to someone who never signed up for it then company will violate the GDPR protocol (Wolford, 2020).

5.2.2 Practices related to marketing automation

Most of the companies uses marketing automation tools to send out email on behalf of the CRM system. Company can face heavy penalties from the government security agency if an email is sent automatically to a user who has opted out (Macdonald, 2020; GDPR Associates, 2018). Therefore, P5 indicates that company is required to ensure that every user in their CRM database and every email in automation system has given them permission to send them an email. If user opted out of an automated email sequence, then both the systems must be updated to ensure that no further emails are sent. It is still violating the GDPR law if the next email already scheduled and system did not update. Company cannot use that as an excuse to protect their self from breaking GDPR. (Lahav, 2018; Macdonald, 2020). Therefore, P6 can be the solution along with P5. In our study we have found that author has suggested if company use algorithms to automate decision making, better to review your existing marketing automation flows and processes to ensure that no important decisions are being taken without human interference (Macdonald, 2020).

5.2.3 Practices related to keeping evidence of consent

The GDPR is applicable to all the companies which are doing business in, or with, the EU. If your company is located in one of the EU countries or in the EEA, or if any of your customer, suppliers are resident of the EU country, you are eligible to comply with the GDPR (Netherlands Enterprise Agency, 2020; Wolford, 2020).

Article 7.1 demands company to keep the evidence of the consent of the user which explain our best practices P7 in this study. It is responsibility of the company to keep the data of user’s consent where they can answer questions such as; who consented; when they consented; what they were told during the time of consent and how they consented (Specht, 2018). Company is required to review the way they are collecting user’s personal data and to know the geographical location of the user data. It is important to track the contact information from where and when it is coming from and how it is ending up in the database (Mailjet inc, 2020). Such information can help company to differentiate between EU and non-EU users. Another reason could help company gain parental consent or process personal data of children under the age of 13, as it is one of the GDPR requirement for parental consent (Wolford, 2020; Zhou, 2018).

5.2.4 Practices related to targeting user for consent

According to Macdonald (2020), Companies can focus on content marketing strategies to collect user consent under the GDPR. The author suggested P9 and P10 practices for targeting new user for consent or user who have unsubscribed from receiving marketing email. Company can focus on content marketing strategy by creating white papers, e-book and guides. User can have an access of this contents and download it, in return for them sharing their email address to subscribing for the contents. This can be good approach for the company to approach unsubscribe users to make them subscribe by providing relevant content. Another best practices we have found in the same scenario is P10. Inviting user to add themselves in company's mailing list via launching banner on the website. Such banners can be created for products and services discounts, coupons, product news, general company news and blog posts, but company must remember to link with the privacy policy to ensure GDPR compliance. (GDPR Associates, 2018; Macdonald, 2020; Bath, 2018).

5.2.5 Practices related to communication policy

We derived best practices P12 and P13 from the GDPR requirements for consent and communication policy for email marketing activities. P12 describes that company must ensure that communication policy for email marketing is not hidden within privacy statements (ICO, 2018; Supperoffice, n.d.). ICO, (2018) makes it very clear for the company about the consent requests to keep separate from other terms and condition of the website of the company(P13). Failure to include these clauses mentioned in P12 and p13 puts company in violation of GDPR law with heavy fines.

5.2.6 Practices related to security

We have earlier discussed residual risk R5, where forgetting to blind copy the recipients is the biggest sin company can make while sending a mass email. This way the company reveals potentially thousands of users' email addresses and consequently exposes them to every manner of follow up spam (Eventbrite, 2016). On other hand, we have found the best practice P8 to avoid risk R5 in our literature. Authors suggested that using email service provider (ESP) such as MailChimp or any other ESP can help company to avoid this situation. Often small companies make this mistake using normal email programme like Outlook or Gmail. It can be very easy to accidentally select the 'To' or 'Cc' field instead of 'Bcc'. But professional ESP will help companies to prevent the names and addresses from being seen by anyone else in the list.

Lastly, we have found P11, P14 and P15 best practices in our literature which is related to security risk while sending an email to the user. These practices suggested by EU data protection authority (Matthys, 2018). The Dutch data protection authority suggested that keeping user personal data in an encrypted attachment; using modern internet standards to ensure the traffic between email servers is encrypted. Further, authority suggested (P11) which states that don't use email instead create user portal with providing inbox and respond to the message combining email notification within portal for current users (Matthys, 2018; NCSC, 2019). Another practice is P14 suggested by ICO (2018) and NCSC (2019), using PGP or S/MIME for end-to-end encryption of email to provider security of the data while using email services by the company. (NCSC, 2019; Matthys, 2018; Autoriteitpersoonsgegevens, n.d.). Lastly, authority suggested P15 for using secure email transport with STARTTLS and DANE while sending personal data. However, we have not come across any literature which shows the importance and usage of these practices (P11, P14 and P15) in terms of email marketing activities. There is literature gap for the missing information, and we will try to find out in the interview with GDPR expert.

5.2.7 Residual risks preempt via best practices

Table 13 contains a link between the residual risks and best practices found through literature in this research study. These residual risks may preempt via best practices shown in the table 13. The table examines which risks can be covered through certain best practices. In the first column the risks are visible and in the second column the best practices that may cover the risk. These links between the risks and best practices are not derived from literature, but are based on the information and literature from this study.

Risks	Best Practices
R1	P1, P2, P3, P5, P6
R2	P9, P10, P11
R3	P6
R4	P5, P6
R5	P8
R6	P14
R7	P15
R8	P7

Table 13: Risks associated with best practices.

5.2.8 Best practices associated with residual risks

The best practices related residual risk is shown in below Table 14. It describes the link between the best practices and residual risk, which we could not identify the link connection in the Table 13. We have identified the residual risk associated with P4, P12 and P13 below in the Table 14. In the first column the best practices are visible and in the second column the risks that may occur if not following P4, P12 and P13. These links between best practices and the risks are not derived from literature but are based on the information and literature from this study.

Best Practices	Risks
P4	R2
P12	Violation of GDPR and fines
P13	Violation of GDPR and fines

Table 14: Best practices associated risks.

5.2.9 Third-party best practices

We will discuss third party best practices in this section. These third-party practices can be useful for the company outsourced their email marketing activities to the third-party company or company using email marketing software. Many of the companies uses email service provider software to create highly engaging email newsletter and sending promotional email campaigns for their customers. We have found third party best practices through literature study shown below in the Table 15. The third-party practices are numbered in the first column from TP1 to TP5. Then, in the second column, a description about third party best practices in email marketing under GDPR is described.

Sr no	Third party best practices description
TP1	Make a list and audit all external service providers and application use across all departments of your company to ensure your email activities are being compliant
TP2	Ensure your 3rd party providers are GDPR compliant for email marketing activities
TP3	Create 3rd party provider inventory list and map out the path your email data takes
TP4	Check for how company’s user emails are being shared, processed and stored with external providers
TP5	Check with your 3rd party providers with their security and decide how risk each provider is for your email activity

Table 15: Third-party best practices summary (Chieri, 2019; Mailjet, n.d.).

5.3 Digital technology development in the GDPR

Before we understand the digital technology in email marketing, it is important to understand that how technology plays a role of being a data processor in email marketing. The company using any ESP tool to support email marketing activities act as a data processor behalf of the company. These ESP tool process user's data behalf of the company(controller). According to Article 28 of the GDPR, "Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject." (Bouca, 2017). Therefore, any EU or non-EU company who works as a controller or processor, will have to implement required controls to make sure that they comply with the GDPR law. The GDPR fines are applicable to both controllers and processors. According to Article 4 of the EU GDPR, different roles are identified for controller and processor (Bouca, 2017; GDPR-Info, 2018). It is not necessary that all the organizations involved in the processing of personal data have the same degree of responsibility. GDPR has defined both these terms in Article 4 shown in the Chapter 3.

5.3.1 Technology support in maintaining GDPR compliance

Technology plays a role of being a data processor behalf of data controller in email marketing Companies are using different third-party tools for their email marketing activities in order to be GDPR compliant. These tools are cloud based platform which allow email marketers to create, send and analyse emails for the purpose of customer engagement and lead generation. Every email marketing tool has its own features and workflows and no two tools will provide same experience (Gaikwad, 2020). It is important for the company to maintain GDPR compliance while executing email campaigns regardless of using any ESP tool. In this research study we have identified top 5 email marketing tool based on the different factors. These factors mainly include; articles by different authors in favor of supporting these tools, google hits analysis between 2018 and 2020; security measurement; total number of users and their clients shown in Table 26 (Smith, 2020; Taylor, 2020; Enlyft, 2020; Mailchimp 2020; Sendinblue, 2020; Activecampaign, 2020; Hutchison, 2018; Aweber, 2019).

No	Email marketing tool name	Number of users	Hits on google	GDPR compliance	Security measure	Clients
T1	Mailchimp	439,894	25.200.000	Neither compliant nor non-compliant for GDPR	1. Use multiple MTAs 2. Mailchimp application is encrypted with TLS 1.2, 3. DDOS mitigation, 4. Account data is mirrored and regularly backed 5. SSL is used to protect application and transmitting sensitive data	Transferwise, Creative Mettle , Central Ohio Transit Authority (COTA)
T2	Constant Contact	78.950	639.000.000	Not fully	1 Code is subject to a strict Quality Assurance program 2 network security with HTTP and HTTPS	Integratech , The Delta Group , Allied Wire & Cable, Inc.
T3	Aweber	16,571	2.010.000	Self-certified with EU GDPR ,Not fully compliant	1 Use of encryption, Continual automated and manual monitoring 2 Routine backups, 3Regular risk assessments 4 DDoS detection and mitigation for data centers	Netsmartz LLC, ACADEMY OF MOTION PICTURE ARTS & SCIENCES , PRIMARY ARMS, LLC
T4	Sendinginblue	7,688	7.550.000	Not fully	1 Multi-level firewall 2 Encrypted data transmission using SSL/https/VPN technology 3 Tier 3 and PCI DSS certified data centres 4 Proven solutions for anti-virus protection and detection of intrusion attempts	Sungage Financial, Inc. , PRIMARY ARMS, LLC , Graymatter Limited
T5	Salesforce Marketing Cloud	5,068	102.000.000	Not fully	1 Encryption and decryption for email message 2 Email export whitelist functionality SFTP or FTP are availablity 3 Security incident	Teach First, Trivago, GlobalData PLC, Atrium Innovations Inc.

					management policies and procedures 4 Data backed up on a regular basis 5 Transport Layer Encryption	

Table 16 Comparison of ESP tool.

As we can see from the table that Mailchimp is the most popular tool for email marketing out of five tools. It is one of the leading email marketing company which claimed to send over 1 billion emails a day. Mailchimp has the highest number of users among all the tools mentioned in the Table 16. As we can see from the table that all the tools T1 to T5 are having good amount of google hits and used by many well-known companies for their email marketing.

We have found in our study that, none of these tools are neither compliant nor non- compliant for GDPR. It is the responsibility of the company that needs to be GDPR compliant in terms of processing user consent via these tools mentioned in the Table 16. Most of these tool companies have suggestions on their website for their clients advising how they can be GDPR compliant with their email marketing activities. This includes giving suggestions about setting up GDPR friendly signup form, setting up double opt- in setting GDPR marketing preferences, segmenting audience by marketing permissions, advise on collecting consent and knowledge about different GDPR fields (Mailchimp, 2020; Constantcontact, 2020; Sendinginblue, 2020).

Apart from this, Mailchimp has feature where company can manage contact profiles (Mailchimp, 2020). It can help company to show when any user opted in to receive marketing email from the company and to prove consent and modify or remove personal information of user. Mailchimp also supports GDPR principles about data request from users. These includes right of access; right to be forgotten; right to object; right to rectification; right to portability (Mailchimp, 2020).

When it comes to security measure of these tools, they claim to provide very high security to their users in terms of protection of their data in email marketing activities. As we can see from the Table 16 companies use different methods of encryption, algorithms and security protocols in terms or providing network security, application security or protection over data. They have data backed up on a regular basis and capacity to handle any kind of data breach occurs via their application. This is very serious concern of data breach for the companies. Because according to Article 33, GDPR requires notification of a personal data breach to inform the supervisory authority within 72 hours after becoming aware of it. The controller should immediately inform about data breach to the competent authority if the risk is serious and reveals the person’s personal information to the public. Similarly, this applies to the data processor also in the case of any breach from their end to inform the controller without any delay to inform the controller (ICO, 2018; GDPR-Info, 2020).

In conclusion studying all these tools mentioned in the Table 16, we can assume from our finding via literature, that companies might not have been fully dependent on these tools for email marketing activities in the organizations. But company may have been using these tool as a support to be GDPR compliant in the email marketing activities. We will try to find this literature gap to confirm the answer in our interview with marketing and GDPR expert.

Chapter 6 Expert Interviews

In this chapter, we discuss the interview process, candidate selection and interview questions for this study. First, in chapter 6.1 the interview process will be discussed. The interview process shows which information is sent to the interviewee and in which circumstances the interview is conducted. Secondly, candidate selection shows the different criteria for the respondents and the way they are approached for this study. The last section shows the interview topics and questions which are asked during the interviews.

6.1 Interview process

The interview process shows how the interviews are set-up and under which circumstances. The set-up of the interviews starts when a participant agrees to participate in this study, an appointment was made for the interview. The interview was conducted at a time that most suited the respondent. The appointment details were sent in an email together with information on the subject, see appendix 1. The information sent includes the best practices and the risks that should be read before the interview was conducted.

As a result of the corona virus, the interview was conducted through ZOOM. The advantage of this was that the interview could be scheduled more flexibly. The disadvantage of this is that certain information from body language is missed. The researcher conducted the interview in a quiet room with a good internet connection. Only the researcher was present in the room, because of the anonymity of the respondents. The interview has been recorded, when the respondents have given permission. After the interviews were conducted, a message was sent to the respondent. In this message, the respondent is thanked for participating. A few weeks after the interview was conducted, a number of questions were sent to the respondents to validate the previous interview answers.

6.2 Candidate selection

The selection of candidates was based on a number of criteria. The candidate selection includes; the geographical place where that person lives and works. This place must be within Europe. The position of that person in a company was also examined. This involves looking at a position in the field of email marketing in combination with knowledge about the GDPR law. The fourth criteria looked at the number of years of work experience, with a minimum of 3 years of work experience. Various people were viewed and screened via LinkedIn to see whether they fit the criteria. The candidates that fit the criteria were asked via LinkedIn to make a connection with the researcher. If accepted, the researcher sent a message to this person via LinkedIn. In addition, three respondents were approached via the supervisor and via a family member. Both persons participated in the interview. In total there are seven participants in this study shown in the table 17. They were approached on the basis of the information on the profile. For this study, 30 people were contacted via Linked-in via an in-mail message.

ID	Interviewe e	Company	Company profile	Marketing Channel	Position in the company	Experience
I1	Interview 1	Company A	Tech company specializing in internet related product and services in hotel industry	B2B & B2C	Global Email Marketing Specialist	4-5 years
I2	Interview 2	Company B	Global marketplace for used commercial vehicles and heavy machinery	B2B	Marketing specialist & Sales customer support	4-5 years
I3	Interview 3	Company C	Footwear manufacturing company	B2C	Email Marketing Specialist EMEA	5-6 years
I4	Interview 4	Company D	Marketing agency	B2B	Digital marketing manager	>7 years
I5	Interview 5	Company E	Marketplace for secondhand vehicles	B2C	Head of marketing	> 10 years

I6	Interview 6	Company F	Technical consulting company	B2B	Senior Marketing Strategist	>11 years
I7	Interview 7	Company G	Multinational human resource consulting firm	B2B, B2C	Global Data Protection & Information Security Officer	>22 years

Table 17: Respondent's profile.

6.3 Interview questions

For this study there are interview questions and topics prepared for digital marketers and data protection officer. First of all, three topics have been identified based on the three sub-research questions. These topics are: residual risks, best practices and digital technology. A number of interview questions have been prepared for each topic that answer these sub-research questions. Each interview contains the same topics and the same interview questions, so that the interview answers for the analysis can be compared. The interview questions are open questions, in order to generate the most information from the interviewees. Additional questions can be asked during the interview, if it is required.

Number	**Questions**
Opening questions	
1	Do you agree if I record the interview in order to have better analysis of the interview? Interview will be keeping it confidential and will be used only for analysis purpose.
2	Can you tell me who are you and your work experience in total?
3	Can you give me short description about the company you are working for and what is your role in the company and team size?
4	Can you tell me how does email marketing work in your company?
5	How do you follow the GDPR compliance for email marketing? Do you handle within the company or do you have third party GDPR experts who take care of the compliance?
6	If answer is third party: Are you fully dependent on third party solution for all the email marketing activities?
Residual risks question	
7	In my study, I have found R1 to R8 risks. Which of these risks have you recognized or encountered in your email marketing? Can you tell me how have you handled it?

8	What can be other residual risks in your company for doing email marketing under the GDPR law?
9	What is your greatest risk out of the one you have listed in your email marketing?
10	Which of these risks have actually occurred in your company? Can you explain about that situation?
11	What kind of damage have you experienced in your company from being lack of GDPR compliance in your email marketing?
Best practices questions	
12	In my study I have found some best practices P1 to P15. Can you tell me, do you apply any of these best practices in your email marketing?
13	Are there any other best practices not mentioned in my list that you are applying in your email marketing?
14	As you know that GDPR applies to the EU residents only. Can you tell me how do you handle EU and Non-EU users for your email marketing in your company?
15	How do you ask the consent to your user for email marketing? Can you tell me all the ways?
16	As many user's opt-in and opt-out on daily basis, how do you manage this process before running any email campaign or sending an email to any user?
17	When a user opted out from email marketing, how do you try to get them back so that he or she subscribes again but also being GDPR compliant same time?
18	What are the security measures do you take while doing email marketing campaign under GDPR? For example: protecting the user email address or personal data.
Digital technology	
19	Is your company using any digital technology or tool to be GDPR compliant to handle risks or best practices we have discussed earlier?
20	Can you tell me, is this technology or tool that covers all the risks and best practices we have discussed earlier? Or are there something you handle manually?
21	Can you tell me, what are you missing in the technology support software you are using for email marketing? Is there any feature would you like to see in the technology which is not available currently?
22	Are you aware of the security measure your email marketing tool is using? How do you make sure that tool you are using is GDPR compliance?
Open questions	
23	Is there something, you think I should have asked you in this interview?
24	Is there something you want me to make me aware of?
25	Did you find this interview insightful?

Table 18: Interview questions with digital marketers.

Number	Questions
Opening questions	
1	Do you agree if I record the interview in order to have better analysis of the interview? Interview will be keeping it confidential and will be used only for analysis purpose.
2	Can you tell me who are you and your work experience in total?
3	Can you give me short description about the company you are working for and what is your role in the company and team size?
4	How do you help your email marketing team for maintaining GDPR compliance process?
5	Can you tell me how do you collaborate via meeting or communicate with email marketers in your company in terms of GDPR?
6	Is there any kind of formal report or reviewing with email marketer to ensure GDPR compliance in your company?
7	In my study I found out that email marketeers and the DPO or the legal department seem less involved with each other. Is it necessary to have frequently meeting or is there a risk? What is your opinion about that?
8	Are there any changes in GDPR in terms of digital or email marketing after 2018?
9	In my study I found out that companies established their process for email marketing in 2018 during GDPR introduction and following it the same process. What do you think about that? Are there any risks?
10	Are there any grey areas in GDPR law for email marketing?
11	Which of the GDPR articles a company must consider in email marketing, shown in Table 4?
Residual risks question	
12	In my study, I have found R1 to R8 risks. Which of these risks have you recognized or encountered in your email marketing? Can you tell me how have you handled it?
13	What can be other residual risks in your company for doing email marketing under the GDPR law?
14	Which of these risks have actually occurred in your company? Can you explain about that situation?
15	What kind of damage have you experienced in your company from being lack of GDPR compliance in your email marketing?
16	How strict is GDPR law for the companies who break the law in email marketing activities?
Best practices questions	
17	In my study I have found some best practices P1 to P15. Can you tell me, do you apply any of these best practices in your email marketing?
18	In my study I have found third party best practices TP1 to TP5. Can you tell me, do you apply or recommend any of these best practices to your email marketing team?
19	Are there any other best practices not mentioned in my list that you are applying in your email marketing?
20	As you know that GDPR applies to the EU residents only. Can you tell me how do you handle EU and Non-EU users for your email marketing in your company?

21	How do you ask the consent to your user for email marketing? Can you tell me all the ways?
22	As many user’s opt-in and opt-out on daily basis, how do you manage this process before running any email campaign or sending an email to any user?
23	What are the security measures do you take while doing email marketing campaign under GDPR? For example: protecting the user email address or personal data.
Digital technology	
24	Is your company using any technology or tool to be GDPR compliant to handle risks or best practices we have discussed earlier?
25	Can you tell me, is this technology or tool that covers all the risks and best practices we have discussed earlier? Or are there something your team handles manually?
26	Do they fully rely on the tool for the data protection and security in email marketing?
	How do you make sure that the tool your team is using is GDPR compliance?
27	Can you tell me, what is missing in the technology support software you are using for email marketing? Is there any feature would you like to see in the technology which is not available currently?
Open questions	
28	Is there something, you think I should have asked you in this interview?
29	Is there something you want me to make me aware of?
30	Did you find this interview insightful?

Table 18 (a): Interview questions with DPO.

Chapter 7 Findings

This section presents the main findings of the research as derived from the interview data with six experts within the area of digital marketing roles across various companies' different departments of B2B and B2C marketing. Apart from this we include findings from an interview with a GDPR expert who works as data protection officer in a multinational company.

The findings are divided into three main categories: residual risks, best practices and digital technology. We have analyzed the information from each interview and present the findings in this chapter. During the interviews, we also validated the information found during the literature study with each participant in the interview. We provided Table 8 of residual risks and Table 11 of best practices to each of the interviewees and asked them if they have recognized or experienced these in their organizations. Findings from these interviews are shown in Table 19 and Table 22 marked with (√), if they encountered the risk or are following the best practice in their work and marked with (x) if they recognized the residual risks. The residual risks that were not recognized or best practices that interviewees did not follow are left blank.

Residual risk categories	Risk no.	Residual risk description	I1	I2	I3	I4	I5	I6	I7
Consent risk	R1	Sending of unsolicited direct marketing email even after user has opted out for consent	√	X	X	X	X	√	X
	R2	Sending an email to user for asking whether he/she wants to receive a promotional email, without the right consent	X		√	X	√	√	X
	R3	Sending an email to children under 13 without a consent from their parent			√	X			X
Automation risk	R4	Marketing automation system sends out an email on behalf of the CRM despite that user has opted out, because CRM system is not updated	√	X	X	X	√	X	X
Security risk	R5	Sending a marketing email to a large number of recipients (users) without using the blind copy feature	X			X		X	√

	R6	Sending a personal data over email without implementing adequate level of information security		X	X	X	X	X	X
	R7	Hacker targets and reveal email address of the users		X	X				X
Territory risk	R8	Sending an email to EU resident by the company located outside EU or vice versa			X	X	√	X	X

Table 19: Residual risks found in the literature (√ = Occurred X = Recognized).

7.1 Findings from digital marketers about existence of residual risks

In this section, we included findings from digital marketers about residual risks. These findings are divided into four different categories of residual risks that we describe in the details: 1) consent risk, 2) automation risk, 3) security risk, and 4) territory risk.

7.1.1 Existence of consent risk

As we can see from Table 19, residual risks R1 and R2 are recognized by most interviewees, where some of these risks actually occurred in their organization. Two of the interviewees faced R1 risk during their work. In both incidents, a customer has unsubscribed by unticking the consent option but still received an email from the company. One interviewee explained that the incident took place because they did not correctly collect the user’s consent information. However, when they realized their mistake, they fixed it later on with a proper solution. The interviewee mentioned this could happen because the information about unsubscribing or the customer’s consent preference were stored at different places and not synchronized with each other, which could lead to the residual risks R4.

In a second incident, the interviewee mentioned that one of the customers forgot to unsubscribe and blamed their company for sending him an email. The customer immediately asked the company to remove all of the data which the company had stored for him from their database. Furthermore, the interviewee talked about another incident, where two of their customers got angry and put allegations on them that they violated GDPR regulation. The company clarified both the customers informing them that they received an email because of the product and services they were using and paying to the company. The interviewee mentioned that their customers forgot to unsubscribe from receiving the newsletter. However, we also found that the interviewee’s company had not developed an email preference center for their customers, which may have created confusion for a customer in this incident.

However, the company had maintained the timestamp for both the customers, so they did not get into legal problems with GDPR. This turned out to be a very important finding which can be used for the best practice in email marketing in such situation. Where a company can maintain the time stamps of a user opt-in and opt-out in their database before such incident takes place and get company into legal trouble.

When we asked other interviewees to recognized R1, they said that it never happened in their company, but they think that it can possibly occur in the company if not taking care of the GDPR compliance properly. One of the interviewees thinks that since their company is global, they run different email marketing campaigns from different regions to introduce about new features, promotional offers or discount etc. It may be possible that they are not aware of users’ consent of each other while sending an email to the customer which may probably lead to occurrence of residual risk R1.

Three of the interviewees agreed to occurrence of the risks R2 in their company. Interviewee I4 recognized this risk and mentioned that this could happen in 2018 when GDPR got introduced. Because during that time companies were struggling to obtain user consent. The rest of the interviewees just don’t send an email to the users to ask them about receiving promotional email or if they unsubscribed from their database. They strictly believe that if a user is gone, he/she is gone. They will not push them back to re-subscribe to their database. They strictly follow the policy which help them to keep their database clean and accurate.

However, other findings show that still some of the interviewees’ companies violate R2, since they send an email or approach via phone from sales team to ask the user permission for email consent or for the reason of unsubscribing. There are two reasons for doing this, one is that they don’t want to lose their customers from email marketing campaign. In second case, company wanted to know the reason why many of their customers all of sudden unsubscribe from their email marketing campaign. Whether it was their customer’s wish or were they blacklisted by their customers. Hence company approached their customers via email on mutual relationship and trust between their company and customer. Which put them in a seemingly safe place. However, in both cases, the company still violates the GDPR regulation if the customer decides to complain.

The residual risks (R3) was an eye opener for most of the interviewees, as they were not aware about this regulation of the GDPR. One of the interviewees mentioned that their company do not ask the consent to the parents for children under 13, even though they do sell products to customers of this age category. Where other interviewee replied on (R3) that it doesn't make any sense for their company to ask the consent from parents as their business is involved in B2B and deals with adults. The interviewee thinks that asking extra information such as age or birthday may end up violating GDPR regulation data focus. Risk (R3) totally depends on the situation of the company's product and services whether they will require parental consent or not.

7.1.2 Existence of automation risk

Marketing automation related to residual risk (R4) was recognized by all the participants in the interviews. We found in our interviews that some of the company's CRM systems are still not synchronized with their ESP tool. Their user preferences are stored at different places and are not aligned with their email marketing campaign. When users opt in or opt out, they manage user's consent manually and upload the list in ESP instead of making the process automated with CRM. Participants mentioned that maybe they have violated the GDPR regulation but so far, they have not received any complaints from customers.

One of the interviewees said that their global email marketing team are not aligned with their own team when they run email marketing campaigns. They are not using any centralized approach for the user consent. The interviewee also mentioned that how using two different tools by the regional team and global team makes things more complex while targeting email marketing campaign. As they have to check with the user consent manually each time and inform each other before targeting email marketing campaign. Other interviewees recognized (R4) but they believe that their CRM system are synchronized with user consent and they are doing quite good job at handling (R4).

7.1.3 Existence of security risk

None of the participants had an issue handling residual risk R5. Three of the participants recognized this risk but they think that using an ESP tool can mitigate R5. However, they also mentioned that there is always a chance of human error while using ESP.

When we asked security related residual risk R6 and R7 to all the interviewees, their knowledge was quite limited and more dependent on the legal team of the company. As their everyday task related to email marketing does not involve much security knowledge. The legal department or the third-party compliance company has to deal with these risks. The interviewees themselves are not involved in this area. However, most of the participants mentioned that they rely on technology for both of these risks. One of the participants agreed that they can do a better job in the residual risk (R7) and are currently taking this as granted. Another interviewee said that 2018, they believed that they did the right thing and connected with right people for R6 & R7. Now they are dependent on the process which had been established before. One of interviewees relies on a third-party company for security related risks since they have outsourced their email marketing for their company. In conclusion most of them are dependent on the tool and security or legal team of their company for security related risks.

7.1.4 Existence of territory risk

Most of the interviewees' companies located in the EU do not differentiate between EU users and non-EU users and treat them equally in terms of GDPR regulation in their email marketing. Hence, they don't face (R8) in their organization. However, one of the interviewees mentioned that they do differentiate between EU users and non-EU users. This company has a different email marketing strategy for EU and non-EU users. They strictly follow the GDPR compliance for EU users. But when it comes to non-EU users, they do not follow any guidelines of that country and simply send emails to build the database. This may lead them into legal trouble if not knowing the privacy regulation of that country. We did not find out how other companies located outside EU apply GDPR to EU users in their email marketing campaign, hence risk is unknown for companies located outside EU.

7.2 Findings from data protection officer about existence of residual risk

The residual risk Table 8 was presented to the DPO in the interview. The DPO recognized all the risks from the table. However, none of these risks actually occurred in the company except residual risks R3, although this risk was not found in the marketing department, but in another department of the company which used email services. The interviewee said that R3 occurred as a result of human error and later on informed the privacy authority as a part of GDPR requirement. However, company has established the proper process in place to prevent it.

7.3 Discovery of additional residual risks

Risks no.	Other Residual Risks Description
R9	Restriction on third party and company's database access and issue with GDPR compliance of the third-party email marketers
R10	User's consent preferences are stored at different places for different region of the company
R11	Don't having email preference center available to the users
R12	Lack of event logging of user consent can lead towards GDPR extortion by the customers
R13	If company is not giving opportunity to a user according to right be forgotten
R14	User's consent is not synchronized with social media platform
R15	If not updating a non-EU user's location in the database when the user shifts to the EU country from a non-EU country
R16	Differentiating between email marketing and service-oriented information sent by email under the legitimate interests
R17	Buying a database from the third-party for the purpose of email marketing activities
R18	Sending marketing email to the customer via third party behalf of original company

Table 20: Additional residual risks discovered during the interviews.

In the interviews, various of new residual risks were raised by the digital marketers and data protection officer. The interviewees experience risks in various areas that have not been identified in our literature review. These additional risks are shown in Table 20. It derives from interviewees' knowledge, experience and real occurrence in the interviewee's company. In the next paragraph we discuss these findings from digital marketers and data protection officer in detail.

7.3.1 Discovery of additional residual risks from digital marketers

As shown in Table 20, residual risk R9, which describes the restriction on third party and company's database access. There is a GDPR compliance issue with third party email marketers who are hired for marketing activities. We found out that the company and third-party databases are out of synchronization. The interviewees' company manually provides a user's consent list every month to the third-party company. Marketing managers have zero visibility for open rate, the click-through rate on those emails sent by third-party providers to the customers. This risk can occur when email marketers are not much involved with third party marketers. Other reasons can be for occurring R9, when consent lists, databases of users, or user preferences are changed. Because these changes are passed on to the third party later stage and not processed in time. As in this situation, the databases and consent lists may no longer run synchronously, because if a user unsubscribes one database, it doesn't reflect everywhere. One of the interviewees facing R9 risk currently in their company.

Another risk is R10, which is based on storing the preferences of users in various places. At large companies, certain information about users are stored in different places. This information, which is stored elsewhere, may be missed or not checked in time when a marketing campaign goes online. As a result, people receive emails they do not want, given the previously specified preferences. Sending emails that do not suit someone's previously specified preference is a violation of GDPR law. Another aspect that causes R10 is residual risk R11. We found out that the interviewee's company either has a very unclear and vague email preference center or does not have an email preference center at all to select email preference for users. They do not maintain a list of their users' email marketing preferences. As a result, the company may end up sending emails to its customers which they do not want to receive and relevant to them.

A situation arose in the interviewee's company in which a customer indicated that he had unsubscribed from the emails of a company, but still received an email. Since the company did not maintain the timestamp, they were unable to prove anything to the customer. As a result of this incident, the customer demanded a sum of money that the company had to pay, and then the case was closed. If the customer decided to go to court, the company could have suffered reputation damage or a fine. It seems easy for a customer to file a complaint when a law breaks by the company and demands money from a company. This risk is linked with (R12) because of a lack of event logging of user consent, that can lead towards GDPR extortion by misusing the GDPR law from the customer. R12 risk can occur while collecting user's consent or updating the user's consent without logging each of the events of customers. It is essential for the company to maintain the timestamp of the consent in some event log as proof that the company can prove its part in legal matters if such a situation arises with their customers.

One of the GDPR regulations is the right to be forgotten (R13); suppose any user decides to delete the account or unsubscribe from the email list. It is the company's responsibility to delete the user’s email address information from the database or any email campaign user is part of. The company must exclude users from any social media campaign target via the user’s email address. Marketers must ensure that they do not send any email after the user has opted out or decide to delete his/her account from the company’s database. One of the interviewees described the risk R14 (User’s consent is not synchronized with a social media platform) related to the social media campaign that is linked with the user’s email address. If they upload the email list on a social media platform like Facebook or LinkedIn and create a custom audience that impacts those users via ads. It is likely to happen when the user unsubscribes or changed his/her email preference but will still target via social media ads or emails if not removing the user from the social media list.

Lastly, residual risks R15(If not updating a non-EU user's location in the database when the user shifts to the EU country from a non-EU country) found in the interview. It is possible to occur R15 risk if the company does not update the non-EU user location in the database when non-EU users migrate to any EU country. GDPR will apply to that user in this situation. As in this case, he/she should be treated as an EU user. Therefore, if companies differentiate between EU and Non-EU users for their email marketing campaign, then it will be a problem when users opt-in or opt-out from email consent.

7.3.2 Discovery of new residual risks from data protection officer

In addition to the existing risks from the literature, new risks have been discovered through the interview with DPO. One of these risks is R16, which describes that the GDPR legislation does not make it clear enough for the companies in the EU to differentiate between email marketing and service-oriented information sent via email under the legitimate interests. There is no clear line drawn in GDPR law between these two types of email communication with customers. This shows a grey area among the companies who use email marketing related to their product and services. As an example of this dilemma is that information sent to the customer informing about changes on a website or upgrading with new features on the website. It is unclear whether sending this information to the customer is considered to be part of email marketing or service-oriented information via email under the legitimate interests. It is possible that in such a situation company can claim that it is relying on legitimate interests as a legal basis and not on the explicit consent of the customers.

Other findings from the interviewee mentioned about residual risk R17. The company who buys a list of customer data from a third-party for the purpose of doing email marketing. There can be a problem for the company to verify that user shared the consent with the third party to receive marketing email from the company who purchased a list. Finally, residual risk R18, it is possible to arise the problem when a third party does the email marketing and the consent is given to the original company. The third-party company may not have permission to send the marketing emails to the customers on behalf of the original company.

7.3.3 Root causes of residual risks in email marketing

Causes	**Causes Description**
C1	Lack of knowledge about the GDPR policy as an email marketer
C2	Lack involvement of sales team about the GDPR regulation while targeting customer via email
C3	By not having company’s DPO regular meeting, GDPR training and tracking with company’s email marketers to make sure the compliance with GDPR
C4	Consulted legal people to establish the process in the company when the GDPR introduced. Same process still following after 2 years of GDPR
C5	Playing a blame game with the company or customers when GDPR is involved
C6	Human error while sending an email to the users
C7	Overreliance on technology is not justified
C8	Reliance on other people with expectation that they have taken care of it

Table 21: Root causes of residual risks.

There are number of causes shown in the Table 21. We have identified these causes during the interviews with digital marketers. These causes can be reasons for the occurrence of certain residual risks found in this study. In next paragraph we discuss these causes in detail.

One of the main reasons can be C1 for the occurrence of all the residual risks found in our study. We discovered via interviews from digital marketers that as email marketers or digital marketers, many of interviewees do not have much knowledge about GDPR policy. DPO strongly believes that a marketing team has to have certain knowledge of GDPR. Email marketers can have this knowledge via training about GDPR from their company. This training will help email marketers to maintain the GDPR compliance in their email marketing activities without much involvement of the DPO. It is the responsibility of the DPO to make sure that the marketing team has the right knowledge and frequent training. The interviewee believes that it is difficult for a DPO to interact with the marketing team frequently looking at the size and the responsibility of the DPO. This can be possible if a company has dedicated budget and resources for the involvement of the legal team with the marketing team on frequent basis.

One of interviewee also mentioned about giving training to the salespeople because of their involvement with the customer on frequent basis. Since the sales team are also involved in marketing activities with customer, this interviewee thinks that the sales team should be also trained in the area of GDPR when they approach the customers via email (C2).

Marketers excessively dependent on the ESP tools to meet the legal requirement of the GDPR in their email marketing activities (C7). Interviewees' have an implicit assumption that ESP tool takes care of the GDPR compliance, which may not be completely true. Many companies got the assumption that relying on tools is the safest way to meet legal requirements. These tools are not enough and GDPR approved to maintain the GDPR compliance. In addition to relying on tools, colleagues also over-rely on each other in carrying out work (C8). If a colleague has not done certain tasks or missed, that may be important in the execution of email campaigning, which can also pose a risk because certain actions were missed from the interviewee's colleague. An example could be a colleague checking whether customers have unsubscribed or not before the new email campaign goes live. Another cause can be from data admin where the user consent information is stored in the database and is not linked with the email marketing database. When a customer unsubscribed from receiving emails, an email will still be sent to this customer because the marketer's colleague missed his/her job, which can also cause a possible risk.

Due to various causes, there may be risks for compliance under the GDPR. One of these is that employees have insufficient training in the requirements of the GDPR for doing email marketing (C3). New employees may have little knowledge of GDPR legislation. To prevent this, offering extra training can be a way of overcoming this. According to one interviewee, a legal person who has sufficient knowledge about the GDPR law can train the other departments and keep them informed of developments in the GDPR legislation. Regular consultation with the departments is important in this. When this happens, the risks of errors are minimized. From a interviewee's own experience, there were consultations with the legal team at the time of the adoption of the law 2 years ago (C4). This has not happened in recent years, as there are no changes in the law.

When we asked to all the interviewees, many of the interviewee blame the customer when GDPR got violated (C5). Company claimed that it is happened because of the customer's ignorance or their mistakes. While customers blamed on the company that they violated the GDPR law by sending them an email even after they have opted out from the newsletter. Which can cause the residual risk R12 if company is not maintaining the timestamp of user's opt-ins and opt-outs suggested by the one of the interviewees.

In addition to these causes, human error by the marketers or customers also are also possible causes for residual risks to occur (C6). An example of this is that the employee does not use BCC and puts customers in CC when sending emails. Another example could be that a marketing campaign is planned and in the meantime people unsubscribe. If the employee does not check the people who have unsubscribed again before the campaign goes live, you also speak of a human error. The people who unsubscribed in the meantime will receive an e-mail; this is also a cause of a risk under the GDPR law.

7.4 Best practices followed in the current companies

The previous section provided insight into the causes of the residual risks in email marketing under the GDPR. The current section provides insight into the best practices found earlier in the literature. Further, the current section gives the discovery of additional best practices found in interviews. The best practices found in the literature validated with each of the interviewees. The practices followed by interviewees in their company that is marked with (√) and if interviewees do not follow are left blank, as shown in Table 22.

Sr no	Best practices description	I1	I2	I3	I4	I5	I6	I7
P1	Ensure user has opted in for email marketing and given consent to be contacted before sending an email Example: Audit your mailing list	√	√	√	√	√	√	√
P2	Ensure user has used ticked box explicitly in webform for email opt-ins and not via pre-ticked box assumption or any other method of default consent	√	√	√	√	√	√	√
P3	Use double opt-in in email marketing before user is being added to email list and receive email communication	√	√	√	√	√		√

P4	Use unsubscribe link within your email marketing template and check that it links with the user's profile which allow them to manage their email preference via subscription management center	√	√		√	√		
P5	Check that every name in CRM database and every email in automation system has given you permission for email marketing and both are synchronized	√	√				√	√
P6	Check your existing email marketing automation flows and processes to ensure that no decisions are made without human interference	√	√	√	√	√	√	√
P7	Check how you collect personal data		√	√	√			√
P8	Use professional email service provider (ESP)	√	√	√	√	√	√	√
P9	Use content marketing strategy by generating white papers, eBooks and guides that visitor can access and download in return to share their contact information		√		√	√	√	√
P10	Use a banner on your website for blog posts, product offers, product news and company news where visitor can add themself to the mailing list which is linked with the privacy policy		√	√	√		√	√
P11	Don’t use an email instead provide mail functionality and notification system within portal for current users.		√	√				√
P12	Ensure that communication policy for email marketing is not hidden within privacy statements	√	√	√	√			√
P13	Check that request for consent prominent are separate from terms and conditions	√	√	√	√			√
P14	Use S/MIME or PGP end-to-end encryption protocol for Secure/Multipurpose Internet Mail suggested by EU data protection authorities		√					
P15	Use Secure email transport with STARTTLS and DANE suggested by Dutch National Cyber Security Center (NCSC)		√					

Table 22: Best practices followed by companies (√ = Following).

7.4.1 Practices followed in digital marketer’s company

The results show that various interviewees applied most of the best practices at their company, set out visually in Table 22. However, one of the interviewees mentioned that their company could do a better job of applying P1, P4, and P6. Concerning P4, one of interviewees’ company’s email subscription centers is vague and unclear, while other companies do not have email subscription centers only. Every interviewees’ company uses some kind of ESP tool in their email marketing activities (P8) as described in the section 7.7 in details.

The table also shows that only a small number of best practices is not followed by many marketers, one of these is P5 and P7. Three of the interviewees’ company do not use automated process to check user consent in CRM database with their email automation systems (P5), which means their CRM is not integrated with their ESP tool. Interviewees handles this process manually to check user consent before any email campaign send to the customers. Three of Interviewees company seem to pay less attention when it comes to collecting data from different sources and getting added in the mailing list (P7). Interviewees company use different source to collect users' personal data which includes consent for email marketing, but they don't have any verification process before user gets into mailing list. It is important for the company to know accuracy of the data and 'how', 'when' and 'from where' user data got added into the database before sending any email marketing campaign to user.

P11 also seems to be followed less by many interviewees but follow by three of interviewees' company. Many companies may use portal instead of an email for current users. A portal with mail functionality and notification system seems to be more organized and secure, which gives more overview in terms of newsletter and protecting current user data. By sending each campaign via email, there are possible chance of human errors or security issue of protection user data. The use of a portal can also serve to reduce the amount of information that needs to be stored and processed by the third-party ESP tool. However, this portal with mail functionality limits to target current customers of the company for email activities.

Finally, P14 and P15 do not seem to be followed. These best practices focus on security in the field of email encryption and the securely sending of emails. Most interviewees do not recognize this best practice. It is therefore possible that there is a lack of knowledge about the safety of the tools with which they work. There may be an encryption protocol and the emails are sent securely, but interviewees lack this knowledge. All the participants rely on their legal security team in the company.

7.4.2 Practices followed in data protection officer's company

The data protection officer describes that they follow most of the best practices in their company from list mentioned in the Table 22. However there some best practices which are not followed by the company. For example, P4, company is using unsubscribe link in their email marketing template but working on developing communication preference center which allow users to manage their email preferences. Another best practices P11, interviewee believes that it will not make sense to use web portal with providing email functionality to the users. Because it is not so useful for the marketing perspective as user conversion rate can be low. But it can be very useful for the security and privacy perspective while sending one to one email communication or sending personal data to user by the company.

Lastly, P14 and P15 do not seem feasible and unrealistic from the email marketing perspective. The interviewee thinks that P14 is impossible, as sending an email encrypted by default can only be done when all customers are using the same email security. At the moment the customers have different kinds of email security depending upon their email service provider. This makes it impossible to send the emails encrypted by default. P14 can only be implemented if the EU regulates the use sufficient encryption (S/MIME or PGP) by default to ESP and everyone follows it. Another best practice P15 which seems problematic to implement for the companies in the EU. From the perspective of the DPO, P15 is an expensive solution, which companies cannot afford. However, the interviewee believes that implementing P14 and P15 can be a good idea in email communication but from the email marketing point of view using simple email encryption is technically easy to implement and sufficient.

7.4.3 Collection of user consent

The findings from the interviews confirm that most of the interviewees follow P9 and P10 while collecting user consent in their companies. Some of the companies provide whitepaper, e-books, and guides to their customers in return to share their email address. Interviewee also thinks that using the banner for discounts, offers and other incentives are effective way to collect user consent. They also use a mobile app for this to obtain consent. But apart from this, we identified some other ways of collecting user consent. One of the interviewee’s companies uses a third-party company to collect the consent through different online platforms. Sometimes their sales and marketing team physically promote their product and services at the event and collect user consent via physical signup forms. Company also collects the consent via sponsoring some other company’s event mentioned by one of the interviewees. Some of the interviewee’s companies use paid ads on social media platforms to collect user consent.

7.4.4 Management of opt-in opt-out in marketers and DPO’s company

When it comes to managing opt in and opt out on daily basis, we analyzed that there are still companies who are managing this process manually via confirming user consent in the ESP tool and CRM. There process is not completely automated when it comes to managing user’s opt-in/opt-out. Interview with DPO recommended that this process should be automated by the company. Four of the companies CRM software is integrated with their email marketing tool therefore, the process of managing opt-in opt out is automated (P5). While one company maintains this process manually based on the country location of the user, because they have different targeting campaign for EU and non-EU users.

Email marketers target users via different email campaign based on user preferences via different team in the company. When it comes to interviewees' own team, process is automated. But when they want to target users via their email preference, they double check the user consent manually. Different team of email marketers uses different tools for email campaign in the same company. Each of the team maintains the file of the user consent on most frequency basis and pass to each other while targeting email campaign based on user's preference. They upload the file in the system to confirm the user consent before sending an email to the users.

7.4.5 Retargeting of user in marketers and DPO's company

Our findings on retargeting shows that interviewees have two different opinions. Some of the digital marketers and DPO strongly believes that once user has unsubscribed, we don't want to force them by retargeting users with different email campaign to collect their consent. The interviewees argue that this way it can be useful to keep their database clean and achieve maximum click rate outcome of their email campaign. They believe that, once user is gone, he/she's gone. Targeting them with different banner, ads or other ways to collect their consent will not help them to build strong database with consent.

While one of the interviewees believes that if your organization is small and still growing, it is better that the company uses different ways to retarget the users when they land back on your website mentioned in P9 and P10. Their company target via different banners on website and ads on social media to gain those unsubscribed user back. This way it helps them to build the database with the user consent.

7.4.6 Third party practices followed in digital marketers and DPO's company

Out of all the interviews with digital marketers and DPO, only one interviewee's company has third party company who handle their email marketing activities. We introduced the third-party practices in the interviews to digital marketers and DPO which found in our literature shown in the Table 15. All the practices from TP1 to TP4 are recognized and recommended by the data protection officer in the interview. But none of the practices are followed in the interviewees' company which has third party company handling email marketing. Their main database consent is not synchronized with their third-party consent. Every month they provide the consent list to the third party to verify the consent for the email marketing activities. However, interviewee mentioned that suggestion has been introduced to the global manager to build common platform for the consent or to use common tool between their company and third-party company.

7.5 Discovery of additional best practices from digital marketers and DPO.

Sr no	Other best practices description
P16	Data focus while collecting user preference for consent
P17	Frequent training to marketing team about GDPR
P18	Involving sales team and improve their knowledge about user consent when they reach out to the users via email
P19	Building up email nurture track
P20	Following nonrepudiation methods for collecting consent
TP6	Building or using common tool for email marketers between company and third party to keep user consent in sync

Table 23: Additional best practices discovered during the interviews.

The Table 23 shows the additional best practices discovered from the interviews. These practices are recommended or followed by digital marketers and DPO in their companies. In the next paragraph we discuss in the detail.

One of the areas in the GDPR is data focus which marketers need to be concerned. We found from our interviewees that their company strictly follow on the data focus part while collecting user preference for the consent (P16). It is very important under GDPR to ask only required consent. If consent are not relevant to the product and services, then company can violate the GDPR while sending unwanted email to the subscribers. Hence, company take care of this part carefully.

As we discussed C1 and C2 in the causes section 7.4.3, findings from digital marketers and DPO suggest that training to the marketing team is essential to maintain the GDPR compliance in email marketing activities (P17). The involvement of salespeople in connecting with the customer via email or phone call, it is useful for sales team having knowledge about user consent while connecting with the customers via phone or an email (P18). As we have seen in the residual risk section that some of the companies directly reach out to the customer even when they don’t have permission to ask for the consent. In such situation they end up violating the GDPR regulation except company don’t hold any mutual relationship with the customer.

Building an automated email nurture track can be very effective for email marketers (P19). In interview, one interviewee mentioned that they are creating an email nurture track. It will help them to target audiences based on user’s engagement and interest. The whole process can be fully automated along with GDPR compliance. With this way company can avoid sending unwanted emails to the users and saves them losing from their database maintaining with GDPR compliance.

Nonrepudiation method for collecting consent has been suggested by the one of the interviewees (P20). The interviewee believes that practicing nonrepudiation while collecting consent is important in terms of security level. Therefore, maintaining the timestamp when user opt in or opt out can be maintained. So that company can show the proof to the user if he/she blames the company for violating the GDPR law. This way company can also deal with the residual risks R12 (Lack of event logging of user consent can lead towards GDPR extortion by the customers).

Lastly, suggestion come from very experienced marketers from the interview about handling GDPR compliance with third party company to keep user consent in synchronize. Interviewee suggest that developing the tool in the company or using same tool by company and third party can solve the problem of keeping user consent in synchronize (TP6). As the process is currently handling manually while transferring user consent via file. This way it is beneficial for both the parties to be GDPR compliant and respect the customer privacy.

7.6 Digital technology use in marketers and DPO’s company

Interviewee ID	Email marketing tool name	Email marketing platform
I1	Salesforce marketing cloud	B2C
I2	SendGrid	B2B
I3	Salesforce marketing cloud, Salesforce paradot	B2C, B2B
I4	Salesforce marketing cloud	B2C
I5	E-goi	B2C
I6	Salesforce paradot	B2B
I7	MailChimp, HubSpot, Salesforce paradot, Salesforce marketing cloud	B2B, B2C

Table 24: The tools companies use in their email marketing.

The interviewees have been asked about the technology they are using for their email marketing activities. As we can see from the Table 24, most of them are using Salesforce marketing cloud and Salesforce Pardot. Salesforce marketing cloud is used in B2C marketing, where Salesforce marketing cloud is used in B2B marketing. Apart from that we also come across Mailchimp, HubSpot, Sendgrid, HubSpot and E-goi uses in the interviewees’ company. All of these tool enables marketers to execute email marketing activities with maintaining the GDPR compliance.

However, we found in our interview that none of the email marketers had deep knowledge about the security of the tool. The interview findings show that email marketers know how to use the tools. However, the interviews also show that they are not sufficiently aware of working with the GDPR law in combination with tool. Most interviewees report that they depend on the DPO and the legal department for GDPR compliance. One interviewee indicated during the interview that there are doubts about the safety and security of the tools. Despite the fact that no incident took place in their email marketing activities using these tools mentioned by interviewee. When it comes to security in email marketing, Data Protection Officer commented that, email address is impossible to protect because it is always possible that there can be security risk from the hacker to reveal email address of recipient. Additionally, DPO mentioned that email marketing should not contain any confidential information that require security protection. If it does contain confidential information then it is not email marketing, that can be one to one email communication with the customer. However, data protection officer believes that security is important in one to one email communication with company’s customer in the case of containing secure information in email.

7.6.1 Risks and best practices cover by technology

The interviews discussed technologies that overcome the risks. We also looked at whether there are technologies that are specifically used to apply best practices. The tools used by the companies do not seem to fully cover all the risks mentioned in our findings. When it comes to applying best practices, many of the practices are integrated with the tool, but there are some of the practices required to development of the best practices. To use the tool, processes must be set up by human action and manually. As per interview with data protection officer, he mentioned that company can never fully rely on any ESP tool to maintain the GDPR compliance. None of these tools can cover residual risk and best practices found in this study. Additionally, DPO mentioned that ESP tool can’t be GDPR compliant in any way, because that is not how GDPR law works for processing user data. However, tools can definitely help maintaining GDPR compliance in email marketing activities.

7.6.2 Missing feature in ESP tool

The interviewees questioned about the use of tools and the possible missing features. The interviewees mentioned that the tools used by them are most comprehensive and compatible in the market. Interviewees do not feel to require or expect any other extra features. However, two of the interviewees mentioned that they have problems with the Salesforce marketing cloud in terms of handling email subscription center. The interviewees mentioned that this may be a problem of the tool or they have not yet discovered certain tool features. In general, they seem satisfied with the functionality of the tools.

7.7 Other findings from data protection officer

The GDPR law is very strict, but it is not clearly defined. There are various gray areas within the GDPR legislation. Depending on the type of marketing B2B or B2C, that makes a difference in the strictness of following the GDPR law. The privacy authorities are more focused on breaking the law in B2C marketing than in B2B marketing. After all, consumers data are more vulnerable. Within B2B marketing a lot of information is shared that is not allowed under the GDPR. Violations in B2B marketing are, however, less reported, because companies will rarely report each other to the privacy authority. Companies protect each other, so that everyone can do their marketing activities in B2B.

Additionally, In the case of making number of small mistakes in email marketing by the company has no consequences for violating the GDPR law. But when the law is regularly violated or consumers file complaints then company will get fines from the privacy authority. Additionally, large companies are more in the sight of the privacy authority than smaller companies.

Chapter 8 Towards Guidance for Practitioners

In this chapter, we use the knowledge on residual risks, best practices and technology collected in the previous chapter from literature and interviews findings to provide towards guidance for practitioners to improve their email marketing operation with respect to GDPR compliance. To this end, we designed (1) a process flow for consent management and (2) conceptual models connecting residual risk and best practices to various GDPR- related email marketing goals. These conceptual models allow practitioners to prioritize introduction of best practices in a goal-oriented manner considering residual risks. The process flow diagram for consent management shows relationship explicit between different methods of collecting consent and consent conditions as shown in Figure 10. Other three factor risk models make the relationship explicit between residual risks and best practices, and importantly connect them to specific goals as shown in Figure 11, Figure 12 and Figure 13.

8.1 Process flow diagram for consent management

Figure 10 shows the flowchart that display the workflow for collecting user's consent in email marketing. This flow chart is created from the information gathered from literature and interviews, it is based on the best practices found in literature for collecting consent via different methods and conditions for collecting consent. We have identified sequence of the process for collecting consent from consent related best practices that is linked with conditions required before user gets added into mailing list.

The process flow chart introduced to three of the interviewees in this study. The interviewees recognized the process in the flowchart and, according to them, seems to be a good reflection of the reality in email marketing activities. The flow chart can be used for them when working in a company. Therefore, the flow chart is empirically substantiated and useful for practitioners.

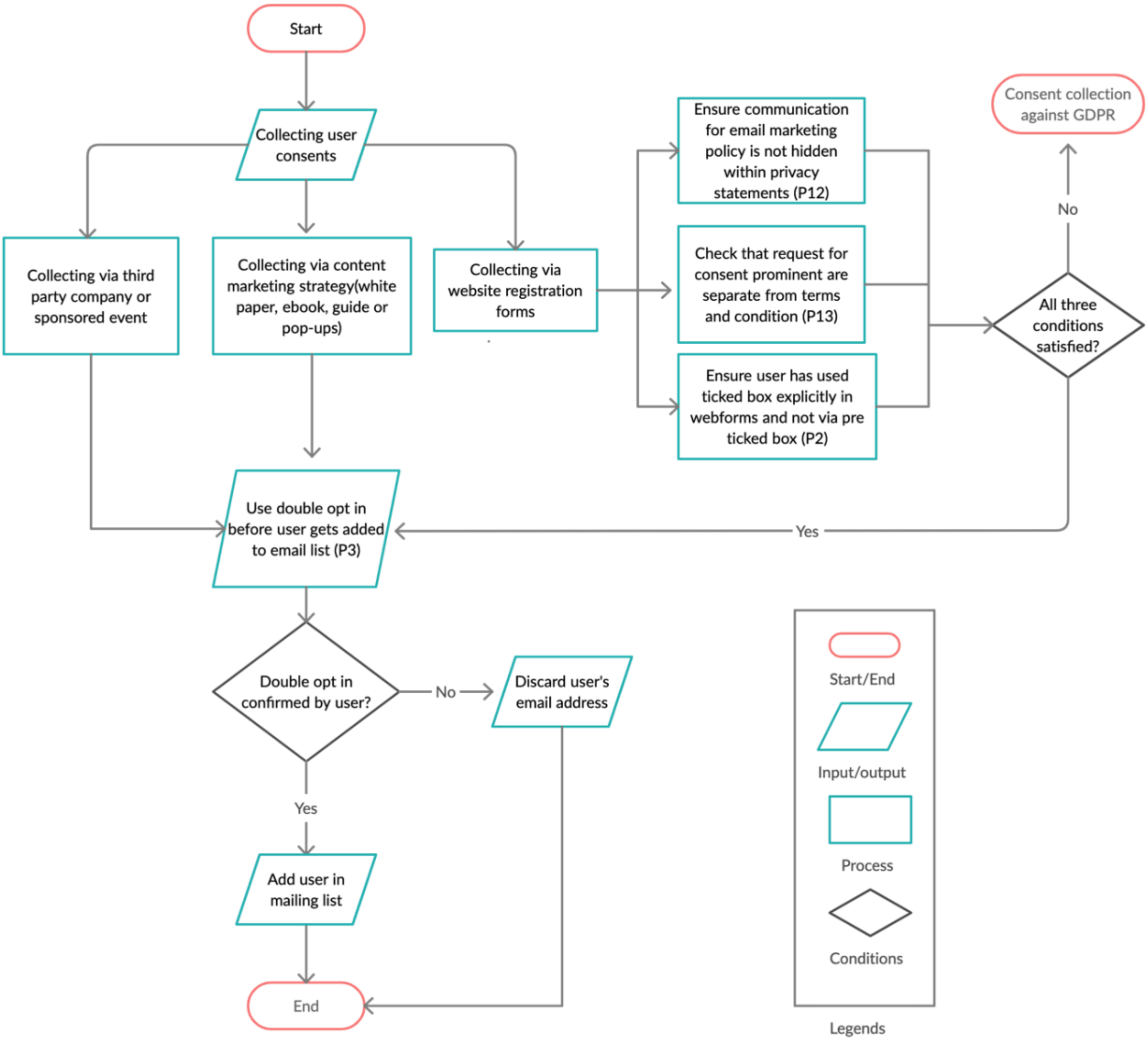

Start
Collecting user consents
Collecting via third party company or sponsored event
Collecting via content marketing strategy(white paper, ebook, guide or pop-ups)
Collecting via website registration forms
Ensure communication for email marketing policy is not hidden within privacy statements (P12)
Check that request for consent prominent are separate from terms and condition (P13)
Ensure user has used ticked box explicitly in webforms and not via pre ticked box (P2)
All three conditions satisfied?
No
Consent collection against GDPR
Yes
Use double opt in before user gets added to email list (P3)
Double opt in confirmed by user?
No
Discard user's email address
Yes
Add user in mailing list
End
Start/End
Input/output
Process
Conditions
Legends

Figure 10: Flow chart for consent management.

Figure 10 shows a graphical representation of the separate steps of a process in sequential order for collecting user consent in email marketing activities in compliance with the GDPR. Each step in the flowchart process is represented by a different symbol and explain a short description of the process step. All symbols in the process defined by the legends and contains a description of the process. The symbols are linked together with arrows, which shows the process flow direction. The process begins with collecting user consent. There are three different ways shown in the process of collecting consent. Two of the process then link with the double opt-in process, and the other process has three different processes with the conditions. If all three process conditions are satisfied, then it links with the double opt-in process. If not, then consent collection is against the GDPR and ends there. In this case, the company is not allowed to collect user's consent legally. If there are doing it, then they should immediately stop. After the company verifies double opt-in from a user, then can add the user to the mailing list. If not verified, then discard the user email's address and avoid sending any marketing email from breaking GDPR law.

8.2 Conceptual factor model

We designed three conceptual factor models shown in Figure 11, Figure 12 and Figure 13. The residual risks and best practices do not have any particular rank or importance by which risks should be treated and/or best practices should be implemented but practitioners can prioritize by looking at the models through the goals that their company wants to achieve. Practitioners can use this model to evaluate or determine which risks play a role in their company by pursuing a goal. Additionally, companies can also use this model to evaluate their current best practices against the residual risks linked to the goal in the model, then see which of these risks has highest likelihood and/or potential impact, and then prioritize the best practices associated to that risk, after prioritizing the most useful best practice can be implemented. This is applicable for all three factor models created in this study in section 8.3, 8.4 and 8.5.

8.3 Consent risk factor model

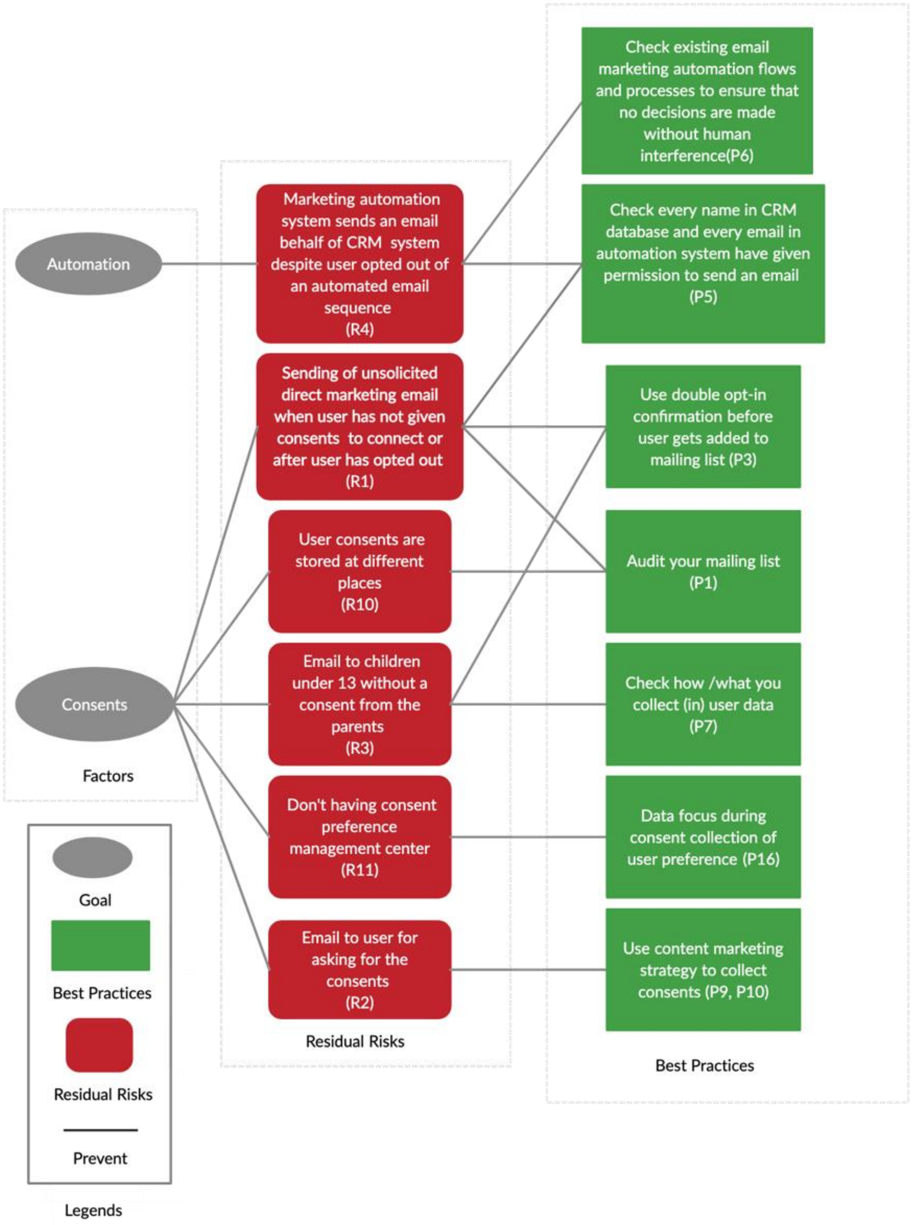

Automation
Consents
Factors
Marketing automation system sends an email behalf of CRM system despite user opted out of an automated email sequence (R4)
Sending of unsolicited direct marketing email when user has not given consents to connect or after user has opted out (R1)
User consents are stored at different places (R10)
Email to children under 13 without a consent from the parents (R3)
Don't having consent preference management center (R11)
Email to user for asking for the consents (R2)
Residual Risks
Check existing email marketing automation flows and processes to ensure that no decisions are made without human interference(P6)
Check every name in CRM database and every email in automation system have given permission to send an email (P5)
Use double opt-in confirmation before user gets added to mailing list (P3)
Audit your mailing list (P1)
Check how /what you collect (in) user data (P7)
Data focus during consent collection of user preference (P16)
Use content marketing strategy to collect consents (P9, P10)
Best Practices
Goal
Best Practices
Residual Risks
Prevent
Legends

Figure 11: Factor model of consent and automation goal connecting residual risks and best practices.

Two factors influence conceptual model, which are consent and automation shown in Figure 11. These act in this model as a separate goal within email marketing activities. Six residual risks can be distinguished in the model, linkint to automation and consent goals. Best practices have been linked to prevent these residual risks. Different symbols have been used in a factor risk model along with description of risks and best practices. The meaning of the symbol is defined by the legends in the Figure 11. The symbols are linked with the line, making a connection between residual risks and their associate best practices. Two goals, consent and automation are connected with six residual risks, which is then identified via the prevention of different best practices linking those residual risks. R1 can be prevented by P1, P3 or P5. R2 can be prevented with P9 or P10. R3 can be prevented by P3 or P7. R4 can be prevented by P5 or P6. R10 can be prevented by P1. Lastly, R11 can be prevented by P16. The aim of the above factor risk model in this research study to provide guidance for practitioners who wants to achieve consent or automation goals in their email marketing activities by considering residual risks and implementing best practices associated with consent and automation related residual risk.

8.4 Security risk factor model

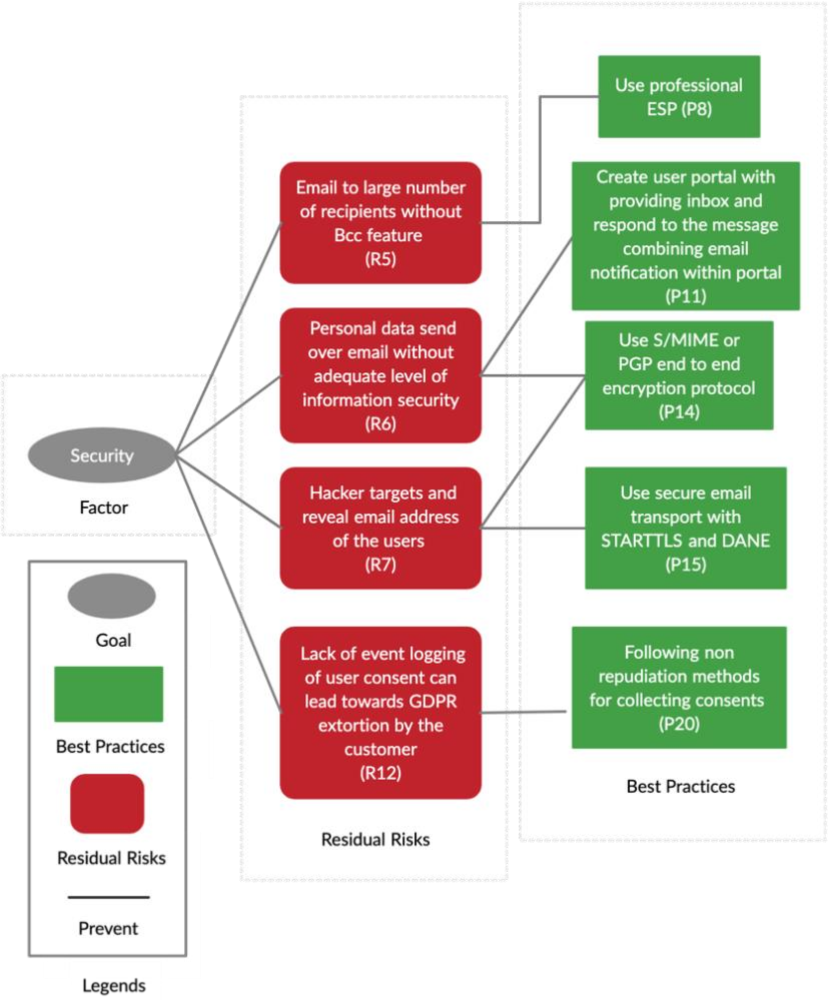

Security
Factor
Email to large number of recipients without Bcc feature (R5)
Personal data send over email without adequate level of information security (R6)
Hacker targets and reveal email address of the users (R7)
Lack of event logging of user consent can lead towards GDPR extortion by the customer (R12)
Residual Risks
Use professional ESP (P8)
Create user portal with providing inbox and respond to the message combining email notification within portal (P11)
Use S/MIME or PGP end to end encryption protocol (P14)
Use secure email transport with STARTTLS and DANE (P15)
Following non repudiation methods for collecting consents (P20)
Best Practices
Goal
Best Practices
Residual Risks
Prevent
Legends

Figure 12: Factor model of security goal connecting residual risks and best practices.

One factor influences in above conceptual model, which is security shown in Figure 12. These act in this model as a goal within email marketing activities. Practitioners can consider security related residual risk by looking at this model and apply best practices according to their security goal requirement. Four residual risks can be distinguished in the model, linking to security goal. Security related best practices have been linked to prevent these residual risks. Different symbols have been used in a factor risk model along with description of risks and best practices. The meaning of the symbol is defined by the legends in the Figure 12. The symbols are linked with the line, making a connection between residual risks and their associate best practices. Security goal is connected with four residual risks, which is then identified via prevention of five best practices. R5 can be prevented by P8. R6 can be prevented by P11 or P14. R7 can be prevented by P14 or P15. R12 can be prevented by P20. The aim of a factor risk model in this research study to provide guidance for practitioners who wants to achieve security goal in their email marketing activities by considering residual risks and implementing best practices associated with security related residual risk.

8.5 Third party risk factor model

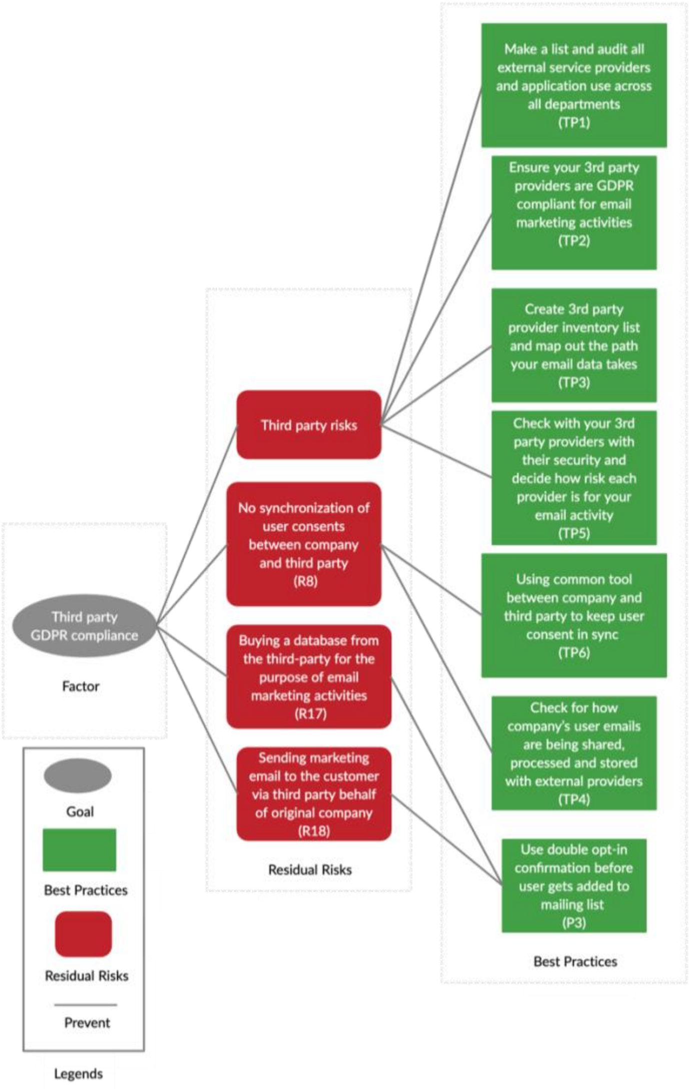

Make a list and audit all external service providers and application use across all departments (TP1)
Ensure your 3rd party providers are GDPR compliant for email marketing activities (TP2)
Create 3rd party provider inventory list and map out the path your email data takes (TP3)
Check with your 3rd party providers with their security and decide how risk each provider is for your email activity (TP5)
Using common tool between company and third party to keep user consent in sync (TP6)
Check for how company's user emails are being shared, processed and stored with external providers (TP4)
Use double opt-in confirmation before user gets added to mailing list (P3)
Best Practices
Third party risks
No synchronization of user consents between company and third party (R8)
Buying a database from the third-party for the purpose of email marketing activities (R17)
Sending marketing email to the customer via third party behalf of original company (R18)
Residual Risks
Third party GDPR compliance
Factor
Goal
Best Practices
Residual Risks
Prevent
Legends

Figure 13: Factor model of third party GDPR compliance goal connecting residual risks and best practices.

One factor influences in above conceptual model, which is third party GDPR compliance shown in Figure 13. These act in this model as a goal within email marketing activities. Company who has third party involved as a part of performing email marketing can consider this model. The aim of a factor risk model in this research study to provide guidance for practitioners who wants to achieve third party GDPR compliance goal in their email marketing activities by considering residual risks and implementing best practices associated with third party GDPR compliance related residual risk.

Practitioners can consider third party GDPR compliance related residual risk by looking at this model and apply best practices according to their third party GDPR compliance goal requirement. Four residual risks can be distinguished in the model, linking to third party GDPR compliance goal. Third party GDPR compliance related best practices have been linked to prevent these residual risks. Different symbols have been used in a factor risk model along with description of risks and best practices. The meaning of the symbol is defined by the legends in the Figure 13. The symbols are linked with the line, making a connection between residual risks and their associate best practices. We discovered three third party residual risk R8, R17 and R18 in this study from interviewes, which is connected with TP4, TP6 and P3. Other third residual risk is more general third party residual risks that is connected with a best practices TP1, TP2, TP3 and TP5 found in the literature. Practitioners can implement all these best practices which is linked with general third-party risks if their company's email marketing performing by third party company.

Chapter 9 Discussion

Chapter 9 describes interpretations of the findings, the limitations of the research, strengths of this study and recommendations for future research.

9.1 Interpretations

The study focused on examining GDPR legislation and email marketing. The interview findings and literature study show that there is a relationship between the risks and best practices. The residual risks and best practices are linked. When a best practice is absent, there is a residual risk under the GDPR law. Apart from this, certain causes found in this study can influence the occurrence of residual risks in this study.

In addition to the relationships found, there are various outcomes that do not match expectations based on the literature of this study. The literature study lists a number of residual risks and best practices, on the basis of which it was expected that companies have a good understanding of these residual risks and applying the best practices in their email marketing. The study shows that this is not the case. Companies set up the processes in 2018 and have not reviewed them afterwards. Best practices are not applied entirely, and companies face various risks for violating the GDPR law.

Firstly, it is clear from interviews that there is one or more existence of residual risk in most of the companies in this study. Certain residual risks are still present in the companies and getting overlooked. None of the companies that are involved in the interviews are following all best practices found in this study. The interviews findings shows that companies are still in progress of adopting the GDPR compliance even after two years of GDPR introduction.

Secondly, there is an unexpected result about GDPR extortion in B2C companies. Businesses have to deal with customers who claim that the GDPR law is being violated and threaten to go to court or demand sums of money. However, this is not the case when it comes to B2B companies.

Thirdly, companies are still contacting customers via email or by phone about the consent and the reason for opting out from receiving marketing mails. These actions may violate the GDPR law. Company can only contact their customers or business clients for collecting consent under Article 6.4.b if company holds mutual relationship with their customers or business clients which is allowed under the GDPR.

Fourth interpretation of the study is that the marketers seem to overly depend on ESP tools. The marketeers themselves seem to have insufficient knowledge of the GDPR legislation and for this they stick to the compliance of the tool. There are certain features of the tool are not fully used yet. It is possible that they are not aware of the features of the tool or they have not discovered them yet. Some of the features are missing by these tools where email marketers are more relying on manual process than automation process for checking up consent. Another interpretation of the study is that marketers have insufficient knowledge of security and protocols about the tool. Most marketers stick to the tools or the legal department when it comes to security.

Lastly, depending on the company, there are either annual meetings or no meetings or tracking between the DPO and marketers for checking up on the compliance. Training on GDPR legislation also seems to be missing for marketers. The email marketing process was set up under the GDPR law in 2018. After setting it up, this has not been revised.

Apart from above discussion of the result, we saw in our study that, residual risks R8(Sending an email to EU resident by the company located outside EU or vice versa), R13(If company is not giving opportunity to a user according to right be forgotten), R14 (User’s consent is not synchronized with social media platform) and R15 (If not updating a non-EU user's location in the database when the user shifts to the EU country from a non-EU country), could not match with any best practices in our findings. It is also because these residual risks are obvious and can be managed by following proper precautions Considering the R8 risk, all the interviewees’ companies belong to EU countries. Therefore, we can not determine how the company located outside the EU deals with EU users in email marketing activities. From our interviewees’ answer we interpret that they don’t send an email to EU resident without consent, as company located outside EU have to strictly follow the GDPR for EU resident. However, when it comes to sending a marketing email to a non-EU residents from EU company, we interpret that companies target email marketing campaigns without user consent to non-EU countries, even privacy rules and regulations implemented by these countries such as the USA, Canada, Australia, Brazil and others. In reality, the company must follow the regulation law defined by those countries located outside the EU.

We also interpret in our study for residual risks R15, that company do update the location of non-EU resident when they migrate from non-EU countries to EU countries. As in that case the user falls under GDPR regulation and the company has to strictly follow the law without missing user's location update.

We believe that, according to right to be forgotten (R13), companies are deleting user's email address and not approaching anymore for via email marketing campaign. As per the GDPR, company is supposed to delete all the data of user under right to be forgotten.

Finally, we understand that the GDPR law specifies how company may use and process user data. However, there are grey areas within the law which don't make a clear distinction between email marketing and service-oriented information send by email (R16). As it is not allowed to send marketing emails based on explicit consent without permission from the client. However, it is permitted to send service-oriented information via email without consent. Which create the confusion for the company to make a difference regarding type of communication via email with their customers.

9.2 Limitations

In this chapter, the limitations and recommendations for further studies will be discussed. The weaknesses are visible in the area of interviewees, research model and implementation of the research.

Only a few research papers have been published on this subject. As a result, mainly gray literature was used for this study. This means that the information used may be less reliable than if it came from research papers. Another weak side of this study was that interviewees were sometimes unwilling to share information. It was noticeable in this study that interviewees sometimes had doubts about sharing information. During the interview and while connecting with the interviewees, the researcher repeatedly stated both in writing and orally that the information will be made anonymous. Despite that, a number of interviewees asked whether the information is anonymous or seemed to have doubts when answering questions. It is possible that not every interviewees dared to share all information or may have deliberately not shared important information. It is also possible that the interviewees gave socially desirable answers. In one case, a interviewees' responses seemed to be in conflict or little information was shared on the subject. One cause could be that the employee has problems with his employer if he or she shares sensitive information and this information will become public. As a result, important information for this study may have been missed.

A further limitation of this study is the small sample. As a result, essential information may have been missed. The small sample means that the results of this research can be generalized to a limited extent. In addition to the small sample, only one research method was used in this research. As a result, interviewees' opinions could not be further investigated.

Another weakness of this study is that it only spoke to digital marketing experts and DPO. Hence, information related to digital technology are not discovered in the detail. As a result, information from IT staff is missing. The reason is that for the digital technology first choice was digital marketers since they are directly involved with email marketing activities in the company. Therefore, IT staff was not among the interviewees. However, it does make sense to also include IT staff to serving more best practices more in detail, as they have good knowledge and hands on experience with technologies. Therefore, if this research is carried further it will be important to include IT staff in this research. Considering IT staff into this research may have helped in research findings to discover more details about the root cause of residual risks, implementation of best practice and information related to digital technology. These findings could give a different conclusion about digital technology support respective of its usage to maintain GDPR compliance in email marketing activities.

Finally, the study took place at the time of the Corona outbreak. As a result of this, companies did not allow an external research and also employees from the companies worked at home. Therefore, it was not possible to do a case study in an organization, which was plan at first stage.

9.3 Strong sides

This research has a few strong sides. A strong side of this research is that relatively little research seems to have been done on this topic. As a result, this research is innovative and offers starting points for follow-up research. Besides, the findings show that in many cases, people are less aware of the risks of working with marketing in combination with the GDPR legislation. It also appears that the results of the research do not fully correspond with the literature, which makes the research valuable in closing the gap between literature and the professional field. The research may have contributed to raising awareness among the spoken interviewees and the companies in which they work. This research can be used for any company in Europe to maintain GDPR compliance in email marketing activities or email communication with the customers.

9.4 Recommendations for further research

There are various recommendations for follow-up research are set out in this section. Follow-up research will be able to focus on conducting this research with a larger regional test. Greater diversity of the sample will also contribute to greater diversity of opinions and experiences. It can be valuable when a diversity of national and international companies in Europe participate, can contribute to generating new insights. It is possible that countries in Europe and the size of companies may provide new insights. Another recommendation is to involve more people in the interview from the legal and technical departments of companies. Involving these people in this study may provide more information and new insights on this topic.

In addition to a larger and more diverse sample, further research methods can be used in follow-up research. Using an additional research method, such as a questionnaire, could potentially validate or support interviewees' answers. In subsequent research, face to face interviews can be more interactive and can be used to generate more information.

Lastly, we realized that this thesis can focus on user personal data on a broader level with GDPR law that can cover personal data such as names, phone number, health data, fingerprints, IP address, cookies, browser history, CCTV cameras footage etc.

9.5 Recommendations for email marketer practitioners

In this section, we write the recommendations to improve email marketing for the company under GDPR. Email marketers can follow these steps under GDPR according to the situation in their company. It depends on two different scenarios, whether company is handling email marketing within themselves or via third party company. In any case, first of all, the company must consider all the GDPR articles found in this study, as shown in Appendix 2 for their email marketing activities. These GDPR articles help the company to understand the rules clearly and implement them into their email marketing process to compliant with the GDPR. Secondly, company can also use 'interactive guidance tool' to find out legal way of processing the consent in their email marketing activities, if they cannot determine from the Article 6.

Lastly, practitioners can look into residual risk Table 25 to identify the existence of any residual risks in their company for email marketing activities by looking at different residual risk's categories shown in Table 25.

9.5.1 Different categories of residual risks

In the below Table 25 we recommend practitioners to avoid residual risk in their company as per different risk's categories. Practitioners can identify residual risk base on their company's current process in email marketing activities by looking into these different residual risk's categories and can decide which residual risk to avoid. These residual risks divided into six categories. 1. Consent risk 2. Automation risk 3. Security risk 4. Territory risk 5. Third-party risk 5. Other risk.

Risk no.	**Residual Risk Description**
Consent risk	
R1	Sending of unsolicited direct marketing email even after user has opted out for consent
R2	Sending an email to user for asking whether he/she wants to receive a promotional email, without the right consent
R3	Sending an email to children under 13 without a consent from their parent
R9	Restriction on third party and company's database access and issue with GDPR compliance of the third-party email marketers.
R10	User's consent preferences are stored at different places for different region of the company
R11	Don't having email preference center available to the users

R14	User email consent of the company are not synchronized with social media platform
Automation risk	
R4	Marketing automation system sends out an email on behalf of the CRM despite that user has opted out, because CRM system is not updated
R12	Lack of event logging of user consent can lead towards GDPR extortion by the customers
Security risk	
R5	Sending a marketing email to a large number of recipients (users) without using the blind copy feature
R6	Sending a personal data over email without implementing adequate level of information security
R7	Hacker targets and reveal email address of the users
Territory risk	
R8	Sending an email to EU resident by the company located outside EU or vice versa
R15	Don't updating the location of non-EU user in database when user shifts to EU country from non-EU country
Third party risk	
R9	Restriction on third party and company's database access and issue with GDPR compliance of the third-party email marketers.
R17	Buying a database from the third-party for the purpose of email marketing activities
R18	Sending marketing email to the customer via third party behalf of original company
Other risk	
R13	If not giving opportunity to user according to right be forgotten
R16	Differentiating between email marketing and service-oriented information sent by email under the legitimate interests

Table 25: Recommendation list to avoid residual risk in the company.

9.5.2 Different scenarios to follow best practices

In this section we write two different scenarios for practitioners to follow best practices in their company for email marketing activities.

First scenario: E-mail marketing via company (Controller).

There are three ways in this case to follow the best practices for e-mail marketing under GDPR.

1. Suppose the practitioner's company is not yet compliant with GDPR or starting fresh in email marketing. In this case, the practitioner can follow all the best practices discovered in this study, shown in Table 25. However, practices related to security may

not be useful in email marketing activities but can be useful in email communication. The company can use a simple encryption technique in email marketing activities for security purposes or rely on reliable ESP tools such as Salesforce Marketing Cloud for the B2C platform and Salesforce Pardot for the B2B platform.

2. Another way is that practitioner's company can check out the different categories of best practices under GDPR mentioned below in Table 25. Such as consent, collecting new consent, email marketing automation and security. The practitioner can decide which one is implemented in their company and which one is not. After that, based on the given answer, they can follow best practices accordingly.

Sr no	Best practices description
Consent	
P1	Ensure user has opted in for email marketing and given consent to be contacted before sending an email Example: Audit your mailing list
P2	Ensure user has used ticked box explicitly in webform for email opt-ins and not via pre-ticked box assumption or any other method of default consent
P3	Use double opt-in in email marketing before user is being added to email list and receive email communication
P4	Use unsubscribe link within your email marketing template and check that it links with the user's profile which allow them to manage their email preference via subscription management center
P12	Ensure that communication policy for email marketing is not hidden within privacy statements
P13	Check that request for consent prominent are separate from terms and conditions
P16	Data focus while collecting user preference for consent
P17	Involving sales team and improve their knowledge about user consent when they reach out to the users via email
P20	Following nonrepudiation methods for collecting consent
Collecting consent from new user or retargeting user	
P9	Use content marketing strategy by generating white papers, eBooks and guides that visitor can access and download in return to share their contact information
P10	Use a banner on your website for blog posts, product offers, product news and company news, where visitor can add themself to the mailing list which is linked with the privacy policy
Email marketing automation	
P5	Check that every name in CRM database and every email in automation system has given you permission for email marketing and both are synchronized
P6	Check your existing email marketing automation flows and processes to ensure that no decisions are made without human interference
P18	Building up email nurture track

Security	
P7	Check how you collect personal data use in email marketing
P8	Use professional email service provider (ESP)
P11	Don’t use an email instead provide mail functionality and notification system within portal for current users.
P14	Use S/MIME or PGP end-to-end encryption protocol for Secure/Multipurpose Internet Mail suggested by EU data protection authorities
P15	Use Secure email transport with STARTTLS and DANE suggested by Dutch National Cyber Security Centre (NCSC)

Table 26: Recommendation list to follow best practices in the company.

3. Lastly, it depends on the existence of the residual risk in email marketing in the practitioner's company. As shown in Figures 11 and 12 in chapter 8, these factor models of residual risks about consent, automation and security can guide practitioners to follow best practices linked with their existing residual risks. The Company also should avoid the residual risks mentioned in Table 19 and Table 20 in their email marketing.

Second scenario: E-marketing via third party company (Processor).

There are two ways in this case to follow the procedure for e-mail marketing under GDPR.

1. The practitioner’s company can check out all the third-party best practices mentioned in Table 26 and follow which one is not implemented accordingly.

Sr no	Third party best practices description
TP1	Make a list and audit all external service providers and application use across all departments of your company to ensure your email activities are being compliant
TP2	Ensure your 3rd party providers are GDPR compliant for email marketing activities
TP3	Create 3rd party provider inventory list and map out the path your email data takes
TP4	Check for how company’s user emails are being shared, processed and stored with external providers
TP5	Check with your 3rd party providers with their security and decide how risk each provider is for your email activity
TP6	Building new platform or using common ESP for email marketers between company and third party to keep user consent in synchronization

Table 27: Recommendation list to follow of third-party best practices.

2. If the practitioner’s company has a consent synchronization issue with the third-party company, then practitioners can look into TP4. Their company can use the same platform to maintain user consent or use a standard ESP tool with third-party companies that can help maintain the consent in synchronization.

Chapter 10 Conclusion

This study investigated the factors that influence the execution of marketing under the GDPR law. To investigate this topic, there are three sub-research questions made. The first question focusses on residual risk companies can be exposed to email marketing under the GDPR. The second question investigates the proactive best practices that can be applied in email marketing to preempt any residual risk under the GDPR. The last sub-question looked at whether there are certain technologies that facilitate email marketing under the GDPR law. After answering the three sub research questions, an answer will be given to the main question of this research. The main question is: **Have companies sufficiently adapted their email marketing activities to the GDPR privacy directive?**

10.1 Answers to research question

Chapter 9.1 will answer the research questions, first of all the sub-research questions will be answered. The main research question is then answered.

SQ1: What are the residual risks companies can be exposed to email marketing activities to comply with GDPR standards?

This sub-research question can be answered by means of the information found in the literature review and the interviews. A total of 18 residual risks were found in this study shown in Table 19 and Table 20. The 18 risks are in the areas of consent, automation, security, territory and third-party residual risk. From these 18 risks, eight risks are taken from the literature and validated through the interviews. In addition, ten risks have been described by the interviewees, which were not known from the literature. This study also looked at the possible causes of risks shown in the Table 21. There are certain possible causes that can be linked for the occurrence of residual risks. It is important that companies consider these causes for the emergence of risks. As a result, it is important that all 18 risks can be avoided by companies under GDPR in their email marketing activities.

SQ2: **What are the proactive best practices that should be followed in email marketing activities to preempt any residual GDPR risks?**

Literature review and interviews help answering this sub-question. Many best practices emerged from this research study. In total, 19 best practices were found for the companies that do email marketing themselves. These best practices focus on four different areas of email marketing shown in the Table 25. These practices are related to consent, collecting consent from new user or retargeting user, e-mail marketing automation, security. There are six best third party practices have been found shown in the Table 26. Procedure for following these practices under GDPR are described in the section 9.5 which can help email marketers to be compliant with GDPR. It depends on whether the company follows the best practices when they do the email marketing themselves or whether they have this done by a third party. In both cases, the best practices can be followed.

SQ3**: Is there any digital technology that can help company with GDPR compliance for email marketing activities?**

The study showed that companies often use compliance` tools for the GDPR. The interviews reveal two popular tools. One of these is Salesforce Pardot for B2B email marketing and other is Salesforce Marketing Cloud which is mainly used for B2C email marketing. The information from the interviews shows that these tools help to be compliant with the GDPR. However, it is important that it is not possible to be completely dependent on the tool. Not all risks and best practices are covered by using the tool. Procedures must be done manually before using the tool. As a result, human errors can arise. It is important that the procedures should be in the order and that companies are not completely dependent on the tool.

When the above information from the sub-research questions is bundled, an answer can be given to the research question from this study. This research main question is**: Have companies sufficiently adapted their email marketing activities to the GDPR privacy directive?**

The answers from three sub-questions can form the final answer to this research study. SQ1 indicate that what are the residual risks company can be exposed. RQ2 indicate that what are the proactive best practices can be followed. Finally, RQ3 answers about the technology which can help in a way to be GDPR compliant. The combination of these factors provides an answer to the main question.

The companies have partially adapted their email marketing activities to the GDPR privacy directive. There are grey areas within the GDPR law which do not make it the clear difference between email marketing and service-oriented information send via email from the company under the legitimate interests. Therefore, the companies can do a better job of implementing its user preference management center to make email communication clear with their customers by collecting their consent. As currently some companies are missing this functionality or have not adequately implemented. It is necessary for companies to clearly define their email communication policy for the legitimate interest.

Apart from this, companies are still underestimating residual risks such as R1, R2, R3, R4, R5, R9, R10, R11, R12, R13 and R17. There are certain causes that may be playing a role in the occurrence of residual risks in this study. These causes are C1, C3, C4, C6. C7 and C8. There are some best practices which are not followed by a few of the companies; these are P5, P7, P12, P13, P14, P15, P17. Apart from this, some companies need to follow third party best practices TP1, TP3, TP4 and TP6.

One of our findings related to security practices P14 and P15 are not recommended to be original cases in this study but only to very specific cases. These practices can be more useful when any sensitive information or personal data is shared with a user in one to one email communication rather than using in email marketing. All of the companies are relying on their ESP tool for security compliance in their email marketing activities. ESP tool can support maintaining the GDPR compliance in email marketing activities, but the company cannot be entirely relied on the ESP tool, as none of these ESP tools is GDPR approved. To summarize, the companies have not fully adapted GDPR in their email marketing activities. Some of the companies still lack the GDPR privacy directive in this study and still require certain areas found in this study to improve in email marketing.

10.2 Contribution

We have contributed to the several areas in this study, see the bullet points below:

- This study contributed to validate the grey literature used in this study. This means that the literature has gained greater value and further can be classified into research literature or grey literature tier 1.

- This study has identified relevant literature from multiple sources such as government website, news articles, research articles, company's publication and information from data privacy organization. Apart from that, we have identified incidents in email marketing activities occurred in the different companies of the Europe between 2016 to 2020.
- We have identified the gaps in the literature about the current state of the companies in their email marketing activities under the GDPR legislation.
- We have filled those gaps through interviews with digital marketers and data protection officer in this study.
- There is a total of 18 residual risks have been pulled off from multiple resources through literature and interviews. All these eighteen risks are compiled in the list and presented in the table. There is now a reference list for the risks in the email marketing under the GDPR.
- We have delivered a total of 20 best practices and six third party best practices through literature and interviews in this study. All these best practices are composed together in the table. We have created a reference list for the best practices in email marketing under the GDPR.
- We have connected residual risks with their relevant best practices and put them into a factor model.
- This study can provide more knowledge and insights for email marketers and companies.
- Lastly, this study provides a recommendation to the email marketer practitioner and company to follow email marketing activities under the GDPR law.

Reference

Activecampaign. (n.d.). Email Marketing - Marketing Automation - Small Business CRM. Retrieved August 8, 2020, from https://www.activecampaign.com/legal/gdpr-updates/gdpr-overview

Adams, R. J., Smart, P., & Huff, A. S. (2017). Shades of grey: guidelines for working with the grey literature in systematic reviews for management and organizational studies. *International Journal of Management Reviews*, *19*(4), 432-454.

Anthony, J. (2020). 141 Compelling Email Marketing Statistics: 2020 Market Share Analysis & Data. Retrieved from https://financesonline.com/email-marketing-statistics/#link1

Aschoff, M. (2011, April 5). E-Mail-Marketing im Marketing-Mix. Retrieved August 6, 2020, from https://www.email-marketing-forum.de/fachartikel/details/e-mail-marketing-im-marketing-mix/28838

Autoriteitpersoonsgegevens. (n.d.). Beveiliging van persoonsgegevens. Retrieved March 7, 2020, from https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/beveiliging-van-persoonsgegevens#hoe-kan-ik-veilig-persoonsgegevens-via-e-mail-versturen-6172

Aweber. (2020). GDPR Data Processing and Security Terms. Retrieved May 13, 2020, from https://www.aweber.com/dpst.htm

Babalola, O. O., &Babalola, G. O. (2015). E-marketing tools and small & medium enterprises in Nigeria. International Journal of Banking, Finance, Management & Development Studies, 2(23), 386–406

Baggot, C. (2007). Email marketing by the numbers. John Wiley & Sons, Inc. Hoboken, New Jersey.

Bain. (2018, April 2). Customer Relationship Management. Retrieved August 10, 2020, from https://www.bain.com/insights/management-tools-customer-relationship-management

Bardicchia, M. (2020). *Digital CRM: Strategies and Emerging Trends: Building Customer Relationship in the Digital Era*. p. 12.

Bath, M. (2018, June 24). GDPR – content marketing strategies to win and retain customers. Retrieved August 3, 2020, from https://submergemedia.co.uk/marketing/gdpr-transformation-content-marketing-2018-guide/

BBC. (2018, March 29). Flybe sent 3.3 million unwanted emails. Retrieved August 4, 2020, from https://www.bbc.com/news/technology-39430349

Bhat, A. (2018). Exploratory research: Definition, methods, types and examples.

Bothma, C. H., & Burgess, S. M. (2007). International marketing. Cape Town: Oxford University Press Southern Africa512.

Bouca, C. (2017, September 18). EU GDPR controller vs. processor – The differences. Retrieved May 13, 2020, from https://advisera.com/eugdpracademy/knowledgebase/eu-gdpr-controller-vs-processor-what-are-the-differences/

Bunniss, S., & Kelly, D. R. (2010). Research paradigms in medical education research. *Medical education*, *44*(4), 358-366.

Buttle, F., Maklan, S. (2015). Customer Relationship Management (3rd ed.). New York: Routledge.

Cauchi, D. “GDPR & Digital Marketing: How Regulation Affects the Industry.” EUGDPRAcademy, 20 Feb. 2019, advisera.com/eugdpracademy/blog/2019/02/20/how-does-gdpr-affect-digital marketing/.

Chieri, L. (2019, December 2). Is Your ESP GDPR compliant? Here’s How To Find Out. Retrieved March 11, 2020, from https://www.emailvendorselection.com/is-your-esp-gdpr-ready-heres-how-to-find-out/

Clement, J. (2020, March 25). Number of e-mail users worldwide 2024. Retrieved from https://www.statista.com/statistics/255080/number-of-e-mail-users-worldwide/

Creswell, J. W., Hanson, W. E., Clark Plano, V. L., & Morales, A. (2007). Qualitative research designs: Selection and implementation. The counseling psychologist, 35(2), 236-264.

Creswell, J. W. (2013). Qualitative inquiry: Choosing among five approaches. Los Angeles, CA, 244.

Curtis, M. (2019). An Exploratory Thematic Analysis of Mindfulness Definitions, Test Instruments, and Methods Used in Current Research.

Davis, B. (2017, August 1). GDPR for marketers: Five examples of 'Legitimate Interests.' Retrieved August 25, 2020, from https://econsultancy.com/gdpr-for-marketers-five-examples-of-legitimate-interests/

De Hert, P., & Czerniawski, M. (2016). Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context. International Data Privacy Law, 6(3), 230-243.

DMA. (2018). DMA insight: Consumer email tracker 2017. Retrieved from https://dma.org.uk/uploads/misc/marketers-email-tracker-2019.pdf

Di Ianni, A. (2000) "The E-business Enterprise and the 'Web-first' Principle of E-marketing", Journal of Interactive Marketing, Vol 2, Issue 2, pp158-170.

Drokina, N. I. (2018). Influence of EU general data protection regulation for marketing in Ukraine. 316–324.

Eid, R., & El-Gohary, H. (2013). The impact of E-marketing use on small business enterprises' marketing success. *The Service Industries Journal, 33*(1), 31–50.

Ekman, W, L., & Billgren, P. (2017). Compliance Challenges with the General Data Protection Regulation.

Eldred, M., Adams, C., & Good, A. (2015). Impact of EU data protection laws on cloud computing: capturing cloud-computing challenges and fault lines. In *Delivery and adoption of cloud computing services in contemporary organizations* (pp. 56-79). IGI Global.

Enforcementtracker. (2020). GDPR Enforcement Tracker - list of GDPR fines. Retrieved April 3, 2020, from https://www.enforcementtracker.com/

Enlyft. (2020). Top 5 products in the Email & Social Media Marketing market. Retrieved May 13, 2020, from https://enlyft.com/tech/email-social-media-marketing

European Parliament, (2016, April 27). REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL OF 27 APRIL [PDF].

Eventbrite. (2016). How to Avoid These 7 Common Email Marketing Mistakes. Retrieved May 13, 2020, from https://www.eventbrite.co.uk/blog/email-marketing-mistakes-ds00/

Etikan, I., Musa, S. A., & Alkassim, R. S. (2016). Comparison of convenience sampling and purposive sampling. *American journal of theoretical and applied statistics*, *5*(1), 1-4

Fabus, J., & Fabusova, V. (2016). Customer satisfaction with presentation of the Department of Communication of Zilinska univerzita v Ziline. Procedia-Social and Behavioral Sciences, 230, 49-57.

Firstcms. (n.d.). GDPR and Email Marketing - FirstCMS. Retrieved August 12, 2020, from https://www.firstcms.co.uk/email-marketing/gdpr-and-email-marketing

Fujita, M., Harrigan, P., & Soutar, G. (2017). A netnography of a university's social media brand community: Exploring collaborative co-creation tactics. Journal of Global Scholars of Marketing Science, 27(2), 148–164.

Gaikwad, M. (2020, June 9). Top 10 Best Email Marketing Services Software Platforms for 2020. Retrieved May 13, 2020, from https://www.toolbox.com/marketing/marketing-automation/articles/top-10-best-email-marketing-services-software-platforms-for-2020/

GDPR Associates. (2018, April 27). The GDPR: How Will New EU Data Privacy Regulations Affect Marketing? Retrieved April 4, 2020, from https://www.gdpr.associates/gdpr-will-affect-marketing/

GDPR-Info. (2020, September 2). General Data Protection Regulation (GDPR) – Official Legal Text. Retrieved May 12, 2020, from https://gdpr-info.eu/

GDPR-Info. (2016, August 30). Art. 5 GDPR – Principles relating to processing of personal data. Retrieved August 11, 2020, from https://gdpr-info.eu/art-5-gdpr/

GDPR-Info. (2020, July 13). Fines / Penalties. Retrieved April 5, 2020, from https://gdpr-info.eu/issues/fines-penalties/#:%7E:text=For%20especially%20severe%20violations%2C%20listed,less%20severe%20violations%20in%20Art.

GDPR-Info. (2018, March 29). Art. 4 GDPR – Definitions. Retrieved August 1, 2020, from https://gdpr-info.eu/art-4-gdpr/

Gilbert, F. (2016). EU GENERAL DATA PROTECTION REGULATION: WHAT IM-PACT FOR BUSINESSES ESTABLISHED OUTSIDE THE EUROPEAN UN-ION. Journal of Internet Law, vol. 19, no. 11, pp.3-8

Godin, S. (1999). Permission Marketing: Turning Strangers Into Friends And Friends Into Customers. New York: Simon & Schuster.

Goldberg, S., Johnson, G., & Shriver, S. (2019). Regulating Privacy Online: The Early Impact of the GDPR on European Web Traffic &amp; E-Commerce Outcomes. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3421731

Gourlay, D. (2018). Direct Marketing and The Rules on Privacy. Mondaq Business Briefing, p. Mondaq Business Briefing, April 6, 2017.

Green, A. (2020, June 19). GDPR Data Breach Guidelines. Retrieved March 5, 2020, from https://www.varonis.com/blog/guide-eu-gdpr-breach-notification-rule/

Gregorio, Jomer. “Ways GDPR Will Transform the Digital Marketing Industry (Infographic).” Digital Marketing Philippines, 25 July 2018, Retrieved from digitalmarketingphilippines.com/ways-gdpr-will-transform-the-digital-marketing-industry-infographic/

Han, S.-L., Nguyen, T. P. T., & Nguyen, V. A. (2016). Antecedents of intention and usage toward customers’ mobile commerce: Evidence in Vietnam. Journal of Global Scholars of Marketing Science, 26(2), 129–151.

Heckh, N., & González, M. L. (2019, November 5). Fines imposed since the entry in force of the GDPR. Retrieved May 4, 2020, from https://www.ramonycajalabogados.com/es/node/1873

Heimbach, I., Kostyra, D. S., & Hinz, O. (2015). Marketing automation. Business & Information Systems Engineering, 57(2), 129-133.

Houben, L. (2018). Assessing the impact of the 2018 General Data Protection Regulation on the willingness to disclose information. UvA.

Hudák, M., Kianičková, E., & Madleňák, R. (2017). The Importance of E-mail Marketing in E-commerce. Procedia Engineering, 192, 342–347. https://doi.org/10.1016/j.proeng.2017.06.059

Hutchison, A. (2018, April 27). GDPR: What You Need to Know and How Helps You Comply. Retrieved May 13, 2020, from https://blogs.constantcontact.com/gdpr-how-to-comply/

ICO. (2018). The principles. Retrieved August 11, 2020, from https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/

ICO. (2018). What are 'controllers' and 'processors'? Retrieved August 11, 2020, from https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/controllers-and-processors/what-are-controllers-and-processors/#:%7E:text=The%20GDPR%20defines%20a%20controller,make%20decisions%20about%20processing%20activities.

ICO. (2018, March 22). Children and the GDPR. Retrieved August 4, 2020, from https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-gdpr-1-0.pdf

ICO. (2018). Data protection officers. Retrieved August 11, 2020, from https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-officers/

ICO. (2018). Encryption scenarios. Retrieved March 3, 2020, from https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/encryption/encryption-scenarios/#4

ICO. (2018). Direct-marketing-guidance. Retrieved March 12, 2020, from https://ico.org.uk/media/1555/direct-marketing-guidance.pdf

ICO. (2018). Consent. Retrieved March 4, 2020, from https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/

ICO. (2018). When can we rely on legitimate interests? Retrieved August 2, 2020, from https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/when-can-we-rely-on-legitimate interests/#:%7E:text=The%20processing%20of%20personal%20data,may%20be%20a%20legitimate%20interest.&text=However%20this%20does%20not%20automatically,is%20lawful%20on%20this%20basis.

Iriana, R., Buttle, F. (2007). Strategic, operational, and analytical customer relationship management. *Journal of Relationship Marketing*, Vol 7, pp. 23-42.

Irwin, L. (2020, February 26). The GDPR: Legitimate interest – what is it and when does it apply? Retrieved August 24, 2020, from https://www.itgovernance.eu/blog/en/the-gdpr-legitimate-interest-what-is-it-and-when-does-it-apply

Jackson, A. and DeCormier, R. (1999) "E-mail Survey Response Rates: Targeting Increases Response", *Journal of Marketing Intelligence and Planning*, Vol 17, Issue 3, pp135-139.

Janouch, V. (2014). Internetový marketing. Albatros Media as.

Jenkins, S. (2008). *The truth about email marketing*. FT Press.

Kiran, V., & Kishore, K. (2013). TOWARDS SUSTAINABLE EMAIL MARKETING THROUGH PERMISSION MARKETING. International Journal of Engineering, Business and Enterprise Applications, 113-120.

Kirś, D., & Harper, M. E-mail marketing. Brno, 2010.

Koščík, M. (2017). The Impact of General Data Protection Regulation on the grey literature. Grey Journal (TGJ), 13, 42-45.

Lamb, D. (2019). The Post-GDPR Digital Advertising Industry. 1–70.

Lahav, S. S. (2018, February 3). 3 GDPR blind spots to avoid. Retrieved April 6, 2020, from

https://venturebeat.com/2018/02/03/3-gdpr-blind-spots-to-avoid/

Lamberton, C., & Stephen, A. T. (2016). A Thematic exploration of digital, social media, and mobile marketing: Research evolution from 2000 to 2015 and an agenda for future inquiry. *Journal of Marketing,* 80(November), 146–172.

Lawrence, A. (2020, April 19). The Importance of Security in Email Marketing. Retrieved August 4, 2020, from https://smaily.com/the-importance-of-security-in-email-marketing/

Lewis, E., Lloyd, D. M., & Farrell, M. J. (2013). The role of the environment in eliciting phantom-like sensations in non-amputees. *Frontiers in psychology*, *3*, 600.

Lynskey, O. (2015). *The foundations of EU data protection law*. Oxford University Press.

MacDonald, S. (2020, June 15). GDPR for Marketing: The Definitive Guide for 2020. Retrieved April 19, 2020, from https://www.superoffice.com/blog/gdpr-marketing/

Mailchimp. (2020). General Data Protection Regulation (GDPR) Compliance: Get GDPR Consent for Marketing |. Retrieved May 13, 2020, from https://mailchimp.com/gdpr/

Mailchimp. (2020). Collect Consent with GDPR Forms. Retrieved May 13, 2020, from https://mailchimp.com/help/collect-consent-with-gdpr-forms/

Mailjet. (2020). GDPR Email Marketing Checklist. Retrieved April 11, 2020, from https://www.mailjet.com/gdpr/email-marketing-checklist/

Mailjet. (2020). GDPR Third Party - Requirements For Your Solution Providers. Retrieved April 5, 2020, from https://www.mailjet.com/gdpr/third-party-solutions/

Mailjet. (2020a). GDPR Compliant Email Marketing Solution - Mailing lists and Newsletters. Retrieved April 5, 2020, from https://www.mailjet.com/gdpr/email-marketing/

Martin-Consuegra, D., Faraoni, M., Díaz, E., & Ranfagni, S. (2018). Exploring relationships among brand credibility, purchase intention and social media for fashion brands: A conditional mediation model. *Journal of Global Fashion Marketing, 9*(3), 237–251.

Matthys, B. (2018, August 11). The GDPR: Sending personal data by email. Retrieved March 3, 2020, from https://www.vulnscan.org/the-gdpr-sending-personal-data-by-email/

Mero, J., Tarkiainen, A., Tobon, J. (2020). Effectual and causal reasoning in the adoption of marketing automation. Industrial Marketing Management. Vol. 86, pp. 212-222.

Mikkelsen, D., Rowshankish, K., & Soller, H. (2017). Tackling GDPR Compliance Before Time Runs Out. McKinsey Global Institute.

Milne, G. R., & Gordon, M. E. (1993). Direct mail privacy-efficiency trade-offs within an implied social contract framework. Journal of Public Policy & Marketing, 206-215.

Miranda, L. (2019, December 17). How to use data to enhance the effectiveness of your email marketing. Retrieved August 10, 2020, from https://www.itproportal.com/features/how-to-use-data-to-enhance-the-effectiveness-of-your-email-marketing/

Montgomery, K. C., Chester, J., Grier, S. A., & Dorfman, L. (2012). The New Threat of Digital Marketing. *Pediatric Clinics of North America, 59*(3), 659–675. https://doi.org/10.1016/j.pcl.2012.03.022

Mullen, J., Daniels, D. (2009) Email Marketing - An Hour a Day. Wiley Publishing. Indiapolis, Indiana.

Menon, M. (2019). GDPR and Data Powered Marketing: The Beginning of a New Paradigm. *Journal of Marketing Development and Competitiveness, 13*(2), 73–84. https://doi.org/10.33423/jmdc.v13i2.2010

Niall, Jim (2000), The Email Marketing Dialogue, Cambridge, M.A., Forrester. Pastore, NCSC. (2019, June 25). Factsheet Secure the connections of mail servers. Retrieved March 4, 2020, from https://english.ncsc.nl/publications/factsheets/2019/juni/01/factsheet-secure-the-connections-of-mail-servers

Nicole, O. (2020, April 23). A Privacy Policy for Email Marketing23. Retrieved May 1, 2020, from https://www.privacypolicies.com/blog/email-marketing-privacy-policy/#Why_You_Must_Mention_Email_Marketing_In_Your_Privacy_Policy

Pulizzi, J., & Handley, A. (2017). B2B CONTENT MARKETING. Retrieved from https://contentmarketinginstitute.com/wp-content/uploads/2016/09/2017_B2B_Research_FINAL.pdf

Peppers, D. and Rogers, M. (2001) Email Marketing Maximized, Peppers: Stamford, CA.

Qashou, A., & Saleh, Y. (2018). E-marketing implementation in small and medium-sized restaurants in Palestine. A*rab Economic and Business Journal, 13*(2), 93–110. https://doi.org/10.1016/j.aebj.2018.07.001

Ryan, G. (2018). Introduction to positivism, interpretivism and critical theory. Nurse researcher, 25(4), 41-49.

Ryan, J. (2018, October 6). Email Marketing StatPack 2018. Retrieved August 5, 2020, from https://thesmallbusinessexpo.com/media/email-marketing-statpack-2018-1.pdf

Rettie, R., & Chittenden, L. (2003). Email Marketing: Success Factors. The Eighth Australian World Wide Web Conference, (50), 1–11. Retrieved from http://eprints.kingston.ac.uk/2108/1/paper.html

Ruby, J. (2018, June 20). Use the New GDPR Legislation to Rethink the Way You Market. Retrieved August 3, 2020, from https://www.logisticsmarketing.com/blog/use-gdpr-legislation-rethink-the-way-you-market

Rosenspan, A. (2000) “Permission is Not Enough”, Journal of Interactive Marketing, Vol 2, Issue 3, pp215-218.

Robinson, B. N. (2018, July 12). Complying with GDPR: Where Are Your Blind Spots? Retrieved April 5, 2020, from https://businessalabama.com/complying-with-gdpr-where-are-your-blind-spots/

Santora, J. (2020, April 23). Is Email Marketing Dead? Statistics Say: Not a Chance. Retrieved August 3, 2020, from https://optinmonster.com/is-email-marketing-dead-heres-what-the-statistics-show/

Sendingblue. (2020, April 10). GDPR: All Your Questions Answered. Retrieved May 13, 2020, from https://www.sendinblue.com/gdpr/

Schweigert, V.A., & Geyer-Schulz, A. (2019). The Impact of the General Data Protection Regulation on the Design and Measurement of Marketing Activities: Introducing Permission Marketing and Tracking for Improved Marketing & CRM Compliance with Legal Requirements. *Journal of Marketing Development and Competitiveness*, *13*(4), 63–71. Retrieved from http://search.proquest.com/docview/2336296753/

Smith, B. (2020, August 17). 10 Best Email Marketing Services for Small Business. Retrieved May 14, 2020, from https://hostingfacts.com/best-email-marketing-services/

Specht, B. (2018, January 22). 5 Things You Must Know about Email Consent under GDPR. Retrieved April 9, 2020, from https://litmus.com/blog/5-things-you-must-know-about-email-consent-under-gdpr

Soegoto, E S, & Fahreza, T H. (2018). Email Marketing as a Business Promotional Media. IOP Conference Series. Materials Science and Engineering, 407, 12182.

Sposit, A. N. (2018). Adapting to Digital Marketing Regulations: An Exploratory Analysis of the GDPR and its Effects on Individualized, Behavior-Based Marketing Techniques. 1–9.

Sterne, J and Priore, A. (2000), Email Marketing: Using Email to Reach Your Target Audience and Build Customer Relationships, John Wiley & Sons, Inc. New York, NY, USA.

Strauss, J., & Frost, R. (2008). E-marketing. Prentice hall press.

Superoffice. (n.d.). GDPR and email marketing: A practical guide for B2B marketers. Retrieved March 15, 2020, from https://www.superoffice.co.uk/resources/articles/gdpr-email-marketing/

Tan, K. S., Chong, S. C., & Lin, B. (2013). Intention to use internet marketing: A comparative study between Malaysians and South Koreans.Kybernetes, 42(6), 888–905.

Tankard, C. (2016). What the GDPR means for businesses. Network Security, 2016(6), 5-8.

Taylor, M. (2020, August 11). 10 Best Email Marketing Software & Email Automation Tools of 2020. Retrieved April 14, 2020, from https://www.ventureharbour.com/email-marketing-software-tools-one-best/

Thomas, D. R. (2006). A general inductive approach for analyzing qualitative evaluation data. American journal of evaluation, 27(2), 237-246.

Tiwari, A., Ansari, M. A., & Dubey, R. (2018). An Effective Email Marketing using Optimized Email Cleaning Process.

Todor, R. D. (2016). Marketing automation. Bulletin of the Transilvania University of Brasov. Economic Sciences. Series V, 9(2), 87.

Tozer, D. (2018). GDPR Guidelines Released, How Not To Update Marketing Databases, And A Record ICO Fine. Mondaq Business Briefing, p. Mondaq Business Briefing, May 22, 2017.

Transparency Market Research. (2019, June 21). Email Marketing Market: Digital Marketing Era to Provide Impetus to Email Marketing Industry. Retrieved August 5, 2020, from https://www.transparencymarketresearch.com/pressrelease/email-marketing-industry.htm

Trustarc. (2020, June 29). TrustArc Privacy Research Resources. Retrieved August 17, 2020, from https://trustarc.com/resources/privacy-research/

Uzialko, A. (2020, February 19). How GDPR Is Affecting Email Marketing. Retrieved March 2, 2020, from https://www.businessnewsdaily.com/10959-gdpr-email-marketing.html

Viktor, J. (2010). Internetový marketing. Brno: Computer Press, a. s., ISBN 978-80-251-2795-7

Vysekalová, J., Juříková, M., Kotyzová, P., & Jurášková, O. (2011). Chování zákazníka: Jak odkrýt tajemství černé skříňky. Grada Publishing

Vollmer, N. (2020, May 22). Article 4 EU General Data Protection Regulation (EU-GDPR). Privacy/Privazy according to plan. Retrieved August 8, 2020, from https://www.privacy-regulation.eu/en/article-4-definitions-GDPR.htm

White, T. B., Zahay, D. L., Thorbjørnsen, H., & Shavitt, S. (2008). Getting too personal: Reactance to highly personalized email solicitations. Marketing Letters, 19(1), 39-50.

Wolford, B. (2019). How does the GDPR affect email? Retrieved March 4, 2020, from https://gdpr.eu/email-encryption/

Wolford, B. (2019, February 13). How does the GDPR affect email? Retrieved May 3, 2020, from https://gdpr.eu/email-encryption/

Wolford, B. (2020, February 13). What are the GDPR consent requirements? Retrieved March 4, 2020, from https://gdpr.eu/gdpr-consent-requirements/

Woodside, A. G., & Mir, P. M. (2019). Clicks and purchase effects of an embedded, social media, platform endorsement in internet advertising. *Journal of Global Scholars of Marketing Science, 29*(3), 343–357.

Wreden, N. (1999). Mapping the Frontiers of E-mail Marketing. Harvard Business Review.

Appendix 1: Interview Invitation Details

Email invitation:

Dear XYZ,

Hope you are doing well and safe.

My name is Malik Samnani, I am a master student in ICT in business at Leiden University. I am currently doing a research study on **"Have companies sufficiently adapted their email marketing activities to the GDPR privacy directive?"**

I would like to invite you to participate in an interview for my research. Please find below more information about the research study:

The research will cover three main topics:

1. Residual risks the company can be exposed to email marketing activities under the GDPR standards.
2. Proactive best practices to follow under the GDPR for email marketing activities.
3. Digital technology that can help to be compliant with GDPR standards for email marketing activities.

This interview will take about 30-40 minutes and your response will be treated anonymously. If you are willing to participate please reply to this email.
Looking forward to hearing from you.
Thank you in advance.

Regards,
Malik Samnani
+31-XXXXXX

LinkedIn invitation:

HI XYZ,
My name is Malik Samnani. I am a master student from Leiden University doing research on "the execution of email marketing under GDPR". I come across your profile on LinkedIn and it looks very interesting. I am looking for participants in my research study and I see you are the best fit. Please respond if you are willing to participate in my research. Thank you.

Appendix 2: Useful GDPR Articles in E-mail Marketing

Table A below shows all the important articles company must consider in email marketing activities under the GDPR.

No.	Art./Recital GDPR	Name
1	Art. 3	Territorial scope
2	Art.4	Definition
3	Art.5	Principles relating to processing of personal data
4	Art. 6	Lawfulness of processing
5	Art. 7	Conditions for consent
6	Art. 8	Conditions applicable to child's consent in relation to information society services
7	Art. 9	Processing of special categories of personal data
8	Art. 12	Transparent information, communication and modalities for the exercise of the rights of the data subject
9	Art.13	Information to be provided where personal data are collected from the data subject
10	Art 14	Information to be provided where personal data have not been obtained from the data subject
11	Art 15	Right of access by the data subject
12	Art 16	Right to rectification
13	Art 17	Right to erasure (‘right to be forgotten’)
14	Art 18	Right to restriction of processing
15	Art 19	Notification obligation regarding rectification or erasure of personal data or restriction of processing
16	Art 20	Right to data portability
17	Art 21	Right to object
18	Art 22	Automated individual decision-making, including profiling
19	Art. 24	Responsibility of the controller
20	Art. 28	Processor
21	Art 29	Processing under the authority of the controller or processor
22	Art. 32	Security of processing
23	Recital 32	Silence, pre-ticked boxes or inactivity should not constitute consent.
24	Art 37	Designation of the data protection officer
25	Art 39	Tasks of the data protection officer
26	Recital 47	*“The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest”*
27	Art. 83.5 a)	*the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9*
28	Art.4.11	*“Consent’ of the data subject means any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her”*
29	Art.7.3	*“The data subject shall have the right to withdraw his or her consent at any time”. The withdrawal of consent shall not affect the lawfulness of processing based on consent before withdrawal”. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent”*
30	Art.6.1. a	*“The data subject has given consent to the processing of his or her personal data for one or more specific purposes”*

Table A: The list of the GDPR articles (GDPR-Info, 2020).

Appendix 3: The List of Fines and Penalties under the GDPR

Table B shows the list of the fines and penalties between 2018 to 2020 in the Europe for email marketing activities under the GDPR.

Sr no.	Date	Company name	Country	Authority	Fine	Description	Quoted Article
1	Nov 2018	Leave.EU	UK	ICO	£15,000 £ 45,000	For sending unsolicited direct marketing emails without the required consent and sending almost 300,000 unsolicited communication email messages on a single day for which users did not unsubscribe.	Art. 6 GDPR, Art. 21 GDPR
2	2018	AnimaNaturalis	Spain	AEPD	Warning	The company used the complainant's email address to send her newsletters when she had already withdrawn her consent and the company confirmed that the unsubscription had been completed.	Art.6.1.a) GDPR, Art. 83.5 a) GDPR
3	2019	VODAFONE ONO, S.A.U.	Spain	AEPD	€36,000	The company sent a marketing email to a large number of recipients (clients) without using the blind copy feature.	Art. 5 (1) f) GDPR
4	23-07-2020	El Real Sporting de Gijón S.A.D.	Spain	AEPD	€5,000	Sending direct marketing communications without sufficient consent, Company did not comply with the GDPR (opt-out instead of opt-in).	Art. 6 GDPR, Art. 7 GDPR
5	13-07-2020	Wind Tre S.p.A	Italy	Garante	€16,700,000	Data processing activities relating to direct marketing. Hundreds of data subjects claimed to have received unsolicited communications sent without their prior consent by email The data subjects were not able to exercise their right to withdraw their consent and object to processing for direct marketing purposes. because the information contained in the Data Protection Policy was incomplete in relation to the contact details	Art. 5 GDPR, Art. 6 GDPR, Art. 12 GDPR, Art. 24 GDPR, Art. 25 GDPR
5	09-06-2020	Consulting de Seguridad e Investigacion Mira Dp Madrid S.L.	Spain	AEPD	€5,000	A data subject has received marketing messages without having consented.	Art. 5 GDPR, Art. 6 GDPR
6	29-05-2020	Non-profit organisation	Belgium	APD	€1,000	For sending out direct email marketing messages, despite the fact that data subjects had exercised their right to erasure and objection. The organisation claimed that it was relying on legitimate interests as a legal basis and not on the explicit consent of the data subjects. The data protection authority, however, denied the existence of any outweighing of legitimate interests.	Art. 6 GDPR, Art. 21 GDPR

7	22-05-2020	Posti Group Oyj	Finland	Deputy Data Protection Ombudsman	€ 100,000	Data subjects received direct marketing email from the company although they had requested that their postal data be deleted.	Art. 12 GDPR, Art. 13 GDPR, Art. 14 GDPR, Art. 15 GDPR
8	03-03-2020	Royal Dutch Tennis Association ("KNLTB")	The Netherlands	Dutch Supervisory Authority for Data Protection (AP)	€ 525,000	Selling the personal data of more than 350,000 of its members to sponsors who had contacted some of the members by mail and telephone for direct marketing purposes. It was found that the KNLTB sold personal data such as name, gender and email address to third parties without obtaining the consent of the data subjects.	Art. 5 GDPR, Art. 6 GDPR
9	25-03-2020	Enel Energie	Romania	ANSPDCP	€ 3,000	The company has sent an email to a client which contained personal data of another client since the company failed to implement adequate technical and organisational measures to ensure an adequate level of information security.	Art. 32 GDPR
10	25-03-2020	Vodafone Romania	Romania	ANSPDCP	€ 4,150	The company has sent an email to a customer which contained personal data of another customer due to inadequate technical and organisational measures to ensure information security.	Art. 32 GDPR
11	21-11-2018	Knuddels.de	Germany	Data Protection Authority of Baden-Wuerttemberg	€ 20,000	After a hacker attack in July personal data of approx. 330.000 users, including passwords and email addresses had been revealed.	Art. 32 GDPR
12	19-06-2020	Unknown	Belgium	APD	€ 10,000	The company sent an e-mail to the person concerned without his consent.	Art. 5 GDPR, Art. 6 GDPR, Art. 15 GDPR
13	16-06-2020	Unknown	Belgium	APD	€ 1,000	The data subject repeatedly received e-mails with advertising content from a company, although the data subject had objected to the processing of his personal data and requested the deletion of his data	Art. 17 GDPR, Art. 21 GDPR, Art. 31 GDPR
14	25-03-2020	Dante International	Romania	ANSPDCP	€ 3,000	The company has sent a commercial e-mail to a client though the client had previously unsubscribed from commercial communications	Art. 6 GDPR, Art. 21 GDPR
15	03-02-2020	Iberia Lineas Aereas de Espana, S.A.	Spain	AEPD	€ 20,000	Beria continued to send e-mails to the data subject, despite the data subject had requested the	Art. 5 GDPR,

		Operadora Unipersonal				withdrawal of his consent and the erasure of his personal data and that the execution of these measures had already been confirmed to him.	Art. 6 GDPR, Art. 21 GDPR
16	10-12-2019	Shop Macoyn, S.L.	Spain	AEPD	€ 5,000	The company has sent advertising e-mails to several recipients where the e-mail addresses of all other recipients were visible to all recipients, because the recipient addresses were inserted as CC and not as BCC.	Art. 32 GDPR
17	03-12-2019	Linea Directa Aseguradora	Spain	AEPD	€ 5,000	The insurance company has sent advertising e-mails for the "Reto Nuez" platform without the required consent.	Art. 6 GDPR
18	28-11-2019	Mayor	Belgium	APD	€ 5,000	Fine for sending election mailings without a sufficient legal basis. The e-mail addresses used have not been collected for this purpose	Art. 6 GDPR
19	28-11-2019	Municipal alderman	Belgium	APD	€ 5,000	Fine for sending election mailings without a sufficient legal basis. The e-mail addresses used have not been collected for this purpose	Art. 6 GDPR
20	2019	Hamburger Volksbank eG	Germany	Data Protection Authority of Hamburg	Unknown	The company had sent a customer a newsletter with advertising content by e-mail, although this customer had previously expressly objected to the sending of further advertising letters.	Art. 21 GDPR

Table B: Overview of fines and penalties (Enforcementtracker, 2020; Heckh & González, 2019).